FEDERAL RESERVE BANK OF BOSTON™

B R I E F

Creating a National Standard for Mobile Financial Services[1] in the U.S.

January 23, 2019

By Susan Pandy, Ph.D., Director, Payment Strategies

The use of smartphones for mobile banking and payments at the point of sale (POS) or remotely (e.g., mobile app, in-app, browser) continues to grow. Statista estimates that mobile commerce sales in 2018 will represent 39.6 percent of U.S. e-commerce retail sales.[2] A 2017 Forrester study predicts that the volume of mobile payments will triple by 2021, growing at a 20 percent annual compound rate.[3] In spite of this predicted growth trend, the market remains highly fragmented, with many different solutions available to consumers and financial institutions (FIs). No open industry standards have emerged to guide this development, which would greatly benefit the ecosystem.[4] For this reason, the Accredited Standards Committee (ASC) X9[5] has undertaken the X9.134 initiative to develop a domestic mobile financial services (MFS) standard modeled after the *ISO 12812: Core Banking – Mobile Financial Services* standard and technical specifications published in 2017.[6] This brief describes the purpose and scope of the X9.134 standard work effort and future expectations for U.S. industry adoption of a mobile banking and payments standard.

The Need for Standardization of Mobile Financial Services (MFSs)

Standardization is essential for sound development of MFS features to allow: 1) interoperability[7] between the different MFS components and functions; 2) ease of consumer experience and choice among mobile devices or products;[8] and 3) a secure environment to ensure trust in the mobile financial service provider (MFSP)[9] and enable FIs to manage risks. Success for mobile retail payments depends on the availability

[1] X9.134 defines mobile financial services (MFS) as mobile payments (including retail) and other mobile banking services.
[2] Statista (2018) *U.S. mobile retail commerce sales as percentage of retail e-commerce sales from 2017 to 2021*. Retrieved from https://www.statista.com/statistics/249863/us-mobile-retail-commerce-sales-as-percentage-of-e-commerce-sales/.
[3] Forrester Research (2017, Feb. 6). *Mobile payments forecast, 2016 to 2021 (US)*. Available at https://www.forrester.com/report/Forrester+Data+Mobile+Payments+Forecast+2016+To+2021+US+Q4+2016+Update/-/E-RES137043.
[4] No public voluntary standards have emerged from groups such as ASC X9 that promote an open consensus development process, where members directly influence the development of technical standards by participating in its formulating groups. EMVCo is a consortium, jointly owned by American Express, Discover, Visa, Mastercard, JCB, and Union Pay, that manages the security specifications for chip-based payment cards (EMV), including payments tokenization and the 3DS authentication protocol. The Payment Card Industry Security Standards Council is a global forum for the card payment industry that is owned by the card brands and develops security requirements for payment account data. Non-card entities may participate in these discussions but have no voting authority.
[5] For more information, see https://x9.org.
[6] ISO 12812 is a five-part standard that includes: Part 1 - general framework, adopted as an international standard, and Parts 2-5 adopted as technical specifications. Part 2 addresses security requirements, Part 3 mobile financial application management, Part 4 payments to persons, and Part 5 payments to businesses. The X9 work proposals for Parts 1 and 2 are available on the X9 Members website. It should be noted that ISO 12812 ultimately decided to include banking functions and app requirements within the overall language, rather than develop a separate part. Accordingly, X9.134 will include an evaluation of the use of mobile devices to enable a bank customer to initiate performance of specific banking functions. For more information, see https://www.iso.org/news/2016/05/Ref2083.html and https://www.iso.org/standard/59844.html.
[7] Interoperability is the ability for systems and organizations to work together, or to inter-operate.
[8] Including the ability to transfer MFSs from one device to another (i.e., portability).
[9] The term "mobile financial service provider" (MFSP) is used in this standard to designate an institution that has created an MFS offering accessed by its customers via a mobile device. For example, Apple, Google, Samsung, PayPal, financial institutions, and other third-party mobile wallet providers can be considered MFSPs. An institution that is part of an MFS value chain but does not provide a service via a mobile device is not considered an MFSP.

of a standardized interface between devices and individual payment systems (i.e., mobile apps), including how those apps interface between MFSP and FI payment systems. To strive for a ubiquitous mobile payments environment, transparency and interoperability between users across systems should exist.

Interoperability is a central tenet of the X9.134 standard because multiple entities comprised of technical components or systems are often involved in the payments value chain. For example, FIs in a payment network are bound by the rules of that network, which allows payments to flow from an end-user customer of one FI to an end-user customer of another FI (i.e., both FIs use the same "network"). Check, Automated Clearing House (ACH), and Electronic Funds Transfer (EFT) are examples of such banking networks. The X9.134 standard reviews the introduction of the mobile device into the payments chain and its impact on newly created components and/or interfaces.

Mobile payments can occur at the POS or remotely via the online channel. Mobile payments can be made by a consumer to a business or to another person (e.g., person-to-person payments). The underlying technology can range from near field communications (NFC) to cloud-based mobile payment solutions that leverage mobile apps installed on a consumer's mobile device and may even use QR codes or other codes to facilitate transactions. The funding sources for mobile payments may include credit, debit, and prepaid accounts, ACH/DDA accounts, or other alternative payment sources. As the mobile payments marketplace evolves and new technologies are introduced, current technologies will coexist, and no single technology is likely to dominate. This emerging payments ecosystem creates a complex supply chain, emphasizing the need for standards that support the technology and process components and help to minimize risk.

Purpose and Scope of X9.134

A critical aspect of building a U.S. standard is developing common terminology and basic principles for the design and operation of MFSs. Accordingly, X9.134 will: 1) define the components and related interfaces as well as the roles necessary to operate MFS according to recognized use cases; 2) identify existing standards that address MFS; and 3) ascertain possible gaps. X9.134 consists of five parts. X9 members will focus on one part at a time with new proposals for Parts 2-5 of the standard to be submitted separately throughout 2019. This staggered approach will ensure that all stakeholders have an opportunity to provide input on the mobile payment functionalities that most directly affect them.

Part 1 of X9.134 provides a general framework for mobile banking and payments, including a comprehensive list of terms and definitions that apply throughout the entire standard. The framework provides an overview that applies to any type of mobile app or other mobile features developed or used operationally. Part 1 does not include any requirements, but it does present general principles for how the other four parts of the standard interact with one another, and it provides guidance on how MFSs should operate.[10] While X9.134 Part 1 does not include technical requirements, Parts 2-5 will include requirements. For example, *X9.134 Part 2 – Security and Data Protection for Mobile Financial Services* will include requirements for MFSPs that detail what a mobile financial application must do to protect personal data and secure transactions, such as using mutual authentication,[11] protecting sensitive data from

[10] This X9 work effort will not reinvent existing X9 or other national/international standards (e.g., ISO 8583, ISO 20022). Relevant existing X9 standards will be leveraged. X9.134 will not address specific communications protocols or mobile devices, where several existing standards by different standards bodies have already been developed and are being utilized in the marketplace. This standard will not drive technology to any specific mobile application.

[11] Mutual authentication is a security feature in which a client process must prove its identity to a service, and the service must prove its identity to the client, before any application traffic is transmitted over the client/service connection.

unauthorized disclosure, modification, or substitution, and authenticating credentials (e.g., mobile passwords, PINs) and account numbers.

Multiple U.S. providers are developing solutions for the evolving MFS market. X9.134 Part 1 seeks to facilitate and promote the interoperability, security, and quality of these MFS solutions. It also aims to contribute to the efficient development of MFS products and solutions by leveraging various mobile environment features and supporting resolution of identified standardization challenges. These challenges include navigating complex ecosystems and regulatory systems, adapting MFSs to a fast-evolving technology, meeting consumer expectations for access to MFSs, and managing risk in the mobile environment.

A national standard will give MFSPs clear requirements for implementing mobile banking and payments. First, for an MFSP to offer an MFS to a wide range of customers and host their service on different consumer mobile devices, an MFSP must support multiple implementations and manage frequent new releases or updates. Second, an MFSP must accommodate the needs of the different service providers operating MFSs on the same device. To meet this requirement, an MFSP should offer customers a convenient user interface for accessing the different mobile services. Finally, security is critical to building trust in MFSs, to ensure continued merchant acceptance and consumer adoption and use. An MFSP has little control over mobile devices or the vulnerabilities presented by access to the Internet or use of WiFi networks, leaving devices susceptible to malware and data breach attacks. For these reasons, an MFSP needs to conduct an assessment to identify risks and define proper countermeasures relevant to any MFS. MFSPs should then implement specific security mechanisms (e.g., secure environment) to prevent the identified risks and minimize fraud. Such mechanisms have to be cost-efficient, yet sufficiently robust to prevent or mitigate possible attacks, with minimal impact on the transaction time.

Addressing Market and Technology Changes Since ISO 12812 Release

Some of the challenges adapting an international standard to the U.S. are that industry models have evolved since the international standard was released and some context or terminology is based on international perspectives that may not apply to the U.S. market. The ISO 12812 standard was released in 2017, six years after development began in 2011, and by then market factors such as the technology, stakeholder roles, and terminology had changed. For example, the implementation of NFC-enabled wallets in the U.S. was nascent when the international standard was being developed. The adoption of "Pay" wallets (e.g., Apple Pay, Samsung Pay, Google Pay) and EMV payment tokenization,[12] coupled with increasing merchant implementations of NFC-enabled terminals, led to some important changes in stakeholder roles. Wallet providers and token service providers (TSPs) were introduced,[13] while mobile network operator roles diminished, compared to their prevalence in Europe when ISO 12812 was under development. In the U.S.,

[12] For more information on EMV payment tokenization, see Pandy, S. and Crowe, M. (2018). *Industry perspectives on the evolution of EMV payment tokenization.* Available at https://www.bostonfed.org/publications/mobile-payments-industry-workgroup/industry-perspectives-on-the-evolution-of-emv-payment-tokenization.aspx and Crowe, M. and Pandy, S., et al. (2015). *Is Payment Tokenization Ready for Primetime? Perspectives from Industry Stakeholders on the Tokenization Landscape.*

[13] The *EMV Payment Tokenisation Specification* defines a token service provider as a role within the payment tokenization ecosystem that is authorized by a token program to provide payment tokens to registered token requestors (e.g., merchants, wallet providers). EMVCo (2017, Sept). *EMV Payment Tokenisation Specification – Technical Framework Version 2.0*. Available at https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/EMVCo-Payment-Tokenisation-Specification-Technical-Framework-v2.0-1.pdf.

TSPs replaced the trusted service manager (TSM)[14] in faciliating the provision of tokenized payment credentials to a mobile device, although TSMs may still perform this role in other countries. Acceptance of QR codes at the POS has also expanded in the U.S. market, along with new proprietary (Venmo) and FI-led (Zelle) person-to-person (P2P) mobile payment apps.[15]

One section in X9.134 Part 1 was modified to address MFS supporting technology components, such as the mobile device, mobile applications, the user interface, mobile wallet, etc. Supporting technologies also need a secure environment, which can be achieved using a trusted execution environment,[16] secured server, secure element,[17] or supplemental software security controls. Securing the underlying MFS environment is needed because mobile devices are subject to the some of the same vulnerabilities as the desktop PC when used to communicate information over a wireless network to the online environment. A secure environment includes controls such as the separation of applications (e.g., identity, banking, retail payments) and MFSP supervision of application management and control of application access rules. A secure environment for an MFS application should provide the following basic trusted services: strong customer authentication, integrity, end-to-end confidentiality and non-repudiation of transactions, and protection of consumer privacy.

Addressing Industry Expectations and 2019 Next Steps

Adoption of X9.134 Part 1 is expected in early 2019. Work will then proceed on Part 2. Interested parties should consider X9 membership so they can participate in this effort. The development process for Part 2 – Security and Data Protection for MFSs, Part 4 – Payments to Persons, and Part 5 – Payments to Businesses, will be time-consuming. There have been many changes to the MFS environment over the last several years that will require some extensive consideration for Part 2. For example, ISO 12812 – Part 2 does not cover in detail EMV payment tokenization, which was introduced by EMVCo in 2014 with the launch of Apple Pay.[18] EMV payment tokenization is a new method for tokenizing payment credentials from end-to-end in a transaction, versus the use of acquirer or security tokenization to secure payment data at rest or post-authorization. Part 2 also needs to address the new stakeholder roles introduced with payment tokenization, such as the TSP and token requestor,[19] as well as new security processes using domain

[14] The TSM enables service providers to distribute and manage their contactless applications remotely by allowing access to the secure element in NFC-enabled handsets. The term is a standardized name used by the GSMA.
[15] ISO 12812 Part 4 refers to payments-to-persons, rather than P2P.
[16] A trusted execution environment comprises hardware and/or software in the mobile device and provides security services to the mobile device computing environment, protects data against general software attacks and isolates hardware and software security resources from the operating system.
[17] A secure element is a tamper-resistant platform in the mobile device capable of securely hosting and executing applications and associated confidential and cryptographic data (e.g., key management).
[18] EMVCo (2014, March). *EMV Payment Tokenisation Specification – Technical Framework Version 1.0.* Available at https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/EMVCo_Payment_Tokenisation_Specification_Technical_Framework_v1.0.pdf. The specification was updated in 2017, EMVCo (2017, Sept). *EMV Payment Tokenisation Specification – Technical Framework Version 2.0.* Available at https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/EMVCo-Payment-Tokenisation-Specification-Technical-Framework-v2.0-1.pdf.
[19] A token requestor (TR) is an entity that procures payment tokens from a token service provider (TSP) to use to complete a purchase (e.g., mobile wallet providers, shopping applications, web browsers, card issuers, merchants, acquirers, acquirer processors, and payment gateways). TRs must register and comply with a TSP's proprietary requirements, receive a token requestor ID, and implement the specified Token API. The TR can then request tokens from the TSP to provision to customer NFC-enabled mobile devices containing secure elements or other storage (e.g., host card emulation).

restriction controls,[20] identification and verification, and token assurance methods.[21] The use of payment tokens and related matters is equally relevant to ISO 12812 Part 5 – Payments to Businesses, along with issues related to mobile wallets.

The U.S. has also experienced significant growth and expansion of mobile P2P solutions (e.g., Zelle and Venmo) in recent years that will need to be described in Part 4 – Payments to Persons. While the ISO-12812 – Part 4 specification describes similar FI-centric or proprietary-based P2P models, it was developed based on the Single European Payments Area card-based payment models. Therefore, the standard requires modifications to reflect the U.S. market and changes in user experience. For example, Venmo includes a social-based personal messaging feature with payments.

The work on Parts 2 and 4 of X9.134 is expected to extend into 2020. X9.134 Part 3 – Financial Application Management and Part 5 – Payments to Businesses should require fewer changes to be more readily adaptable to a national standard. Completing Parts 2 and 5 of X9.134 in 2019 will depend on the level of participation by industry experts who can help the group to accurately develop the U.S. requirements. This underscores the importance of generating industry awareness of this effort and encouraging broader participation, which requires interested parties to become members of X9.

A national standard for MFSs in the U.S. will address some of the fragmentation in the current market, create safeguards to address potential fraud, and hopefully drive greater adoption of mobile banking and payments. While X9's primary focus is writing standards for the U.S., other countries often tend to adopt these standards. A U.S. mobile banking and payments standard will mark an important step forward in supporting future innovation and establishing the U.S. as a leader in this market, especially as the ISO community considers the next steps in evaluating ISO 12812 – Parts 2 through 5 to move from Technical Specifications to International Standards.

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

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