white paper

MOBILE PAYMENT SOLUTIONS:
BEST PRACTICES AND GUIDELINES

PRESENTED BY THE
MOBILE PAYMENTS COMMITTEE
OF THE ELECTRONIC
TRANSACTIONS ASSOCIATION

ETA
ELECTRONIC TRANSACTIONS ASSOCIATION

ETA's Best Practices and Guidelines for Mobile Payment Solutions
Table of Contents

Section 1: Purpose

Develop and deliver best practices that ensure merchants and consumers have access to the most innovative and effective mobile payment solutions. Establish industry best practices to ensure that regardless of company, technology or platform, mobile payment products and services enhance and improve merchant sales while providing consumers a secure and reliable experience.

Section 2: Definition of Mobile Payments

A payment transaction conducted through a mobile device such as a smartphone or tablet. For consumers, the mobile device can function to make payment transactions or accept payment transactions, and to make payment transactions at the Point of Sale or online within an eCommerce site. A Point of Sale (POS) or Point of Interaction (POI) device is usually part of the mobile payments solution.

Section 3: Key Stakeholders

a. **Merchant** – A person or company engaged in the sale of goods and services to consumers and other businesses.
b. **Consumer** - An individual who buys products or services for personal use and not for manufacture or resale.
c. **Federal/State Legislators –** Organizations such as the US House of Representative's Financial Services Committee and the US Senate Banking Committee.
d. **Federal Agencies –** Agencies that include the Federal Trade Commission, the Consumer Financial Protection Bureau and the Federal Reserve Board.
e. **Merchant Acquirers –** Companies that sell merchant accounts and associated services (i.e. gateways, wallets, processing) to merchants to enable them to process various forms of payment including mobile payments.
f. **Credit Card Issuers** - Financial institutions that provide products and services that enable their consumer customers to participate in and conduct mobile payments.
g. **Infrastructure Providers (Hardware, Device Manufacturers, Software and Services) –** Includes companies who develop and/or manufacture payment acceptance and consumer mobile devices, payment solutions software, or offer services such as gateway and transaction processing.

Section 4: Key Stakeholder Interest

a. Merchants – Interested in the use of technology solutions that drive higher revenue, increased staff efficiency and lower costs, as well as a secure payment process.
b. Consumers – Interested in utilizing technology solutions on a mobile device to make payments for goods and services. They are also interested in ensuring that their use of technology solutions create at least as secure a payment transaction, or greater than the use of plastic credit cards.
c. Federal/State Legislators (House Committee on Financial Services and The Senate Banking Committee) – Interested in better understanding the mobile payment benefits and risks to consumers, specifically for the purpose of purchasing goods or services, and to businesses, specifically for the purpose of receiving payment for such goods or services, related to the use of mobile devices conducting payment processes for the purpose of purchasing goods or services.
d. Federal Agencies (Federal Trade Commission, Consumer Financial Protection Bureau, etc.) – Interested in better understanding the benefits and risks to consumers related to the use of mobile devices conducting payment processes, to make markets for consumer financial products and services work for Americans. As it relates to the CFPB within the context of The Dodd-Frank

Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), interested in ensuring accurate and sufficient privacy and security protections are in place regarding the consumer's financial data.

e. **Merchant Acquirers –** Interested in providing their merchant clients with a set of tools and services that facilitate the secure processing of mobile payment transactions while managing fraud and other losses as efficiently as possible.
f. **Credit Card Issuers –** Interested in the most effective, efficient and secure ways to implement mobile payments for consumers.
g. **Infrastructure Providers (Hardware, Software & Services) –** Interested in promoting the sale of products and services for merchants to use in the effective, efficient and secure acceptance of mobile payment transactions, while working to prevent fraud and protect merchant and consumer information.

Section 5: Best Practices and Guidelines

A. Security - Protection of Credit Card Data

In 2006, American Express, Discover, JCB International, MasterCard and Visa formed the Payment Card Industry Security Standards Council (PCI SSC), which is now comprised of over 600 participating organizations representing merchants, banks, acquirers, processors and other vendors worldwide. The PCI SSC develops and maintains the PCI Data Security Standard (PCI DSS) as well as other standards aimed to increase payment data security.

The PCI SSC has recently introduced programs with direct applicability to payments accepted in or on mobile devices and MasterCard and other card brands have reiterated these best practices and programs. The PCI SSC maintains programs for merchants (PCI DSS), payment application providers (PA DSS), hardware vendors (SRED and P2PE), and service providers (P2PE service provider validation).

For non-mobile payment applications, merchants are required to use 3rd party payment applications that comply with the PA-DSS standards and that are listed on the PCI Security Standards Council website. At this time the PCI SSC has not released formal programs aimed at certifying mobile POS (mPOS) payment applications residing on multi-purpose consumer mobile devices.

The Council has released the "PCI Mobile Payment Acceptance Security Guidelines for Developers" (September 2012), which provides guidance on how to:

- Prevent account data from being intercepted when entered into a mobile device
- Prevent account data from compromise while processed or stored within the mobile device
- Prevent account data from interception upon transmission out of a mobile device

Security Best Practices for Merchants

The PCI SSC, Visa, and MasterCard Worldwide recommended best practices for mobile payment acceptance by merchants include:

- General Security Goals

- ✓ Ensure the secure use of mobile payment acceptance solutions, by using the device and applications only as intended by the solution provider.
- ✓ Limit the exposure of the consumer's credit card data. This can be accomplished by ensuring that only authorized persons have access to the payment functionality of the solution and having polices to manage and remediate lost or stolen devices.
- ✓ Prevent software attacks on consumer mobile devices, by only downloading software from trusted sources and providing sufficient security controls to protect devices from malware.

- Point to Point Encryption (P2PE)
  - ✓ Merchants should utilize mobile card input devices that employ point-to-point encryption (P2PE) and are optionally validated with the PCI Secure Reading and Exchange of Data (SRED) program. The PCI SSC will maintain a list of validated SRED compliant devices.
  - ✓ Merchants should optionally utilize service providers (hosts, gateways, processors and acquirers) that have optionally certified and validated P2PE compliant solutions. The PCI SSC will maintain a list of certified P2PE compliant solutions and service providers. Merchants are strongly encouraged to use mPOS solutions with P2PE in accordance with the PCI P2PE solution requirements.

  - ✓ P2PE capable devices and service providers will allow the cardholder data to be encrypted within the card reader accessory and enciphered data will travel all the way to the mPOS solution provider or acquiring host

- Merchants should have policies in place that deal with the loss and/or theft of a mobile device that has a mobile payment application installed on it, and have the ability to remediate or disable any payment applications that reside on the lost/stolen device.

- Any cardholder data entered into the mobile application, outside of an external SRED or P2PE validated point of input device (for example key entered account data), should be immediately encrypted for transmission.

- If the mobile application is enabled for EMV transactions, EMV should be configured for on-line only authorizations and should not be accepted in an off-line state.

- If the merchant accepts EMV transactions on a mobile device, the merchants should only use mPOS applications that have been certified by EMVCo and the MasterCard Terminal Integration Process (M-TIP).

- If merchants wish to accept PIN debit transactions on mobile devices, they should only be capturing the cardholder PIN on mobile devices that comply and are registered with the PCI PTS program.

  Sources:
  - MASTERCARD BEST PRACTICES FOR MOBILE POINT OF SALE ACCEPTANCE, MAY 2012
  - PCI MOBILE PAYMENT ACCEPTANCE SECURITY, AT A GLANCE, MAY 2012

- PCI MOBILE PAYMENT ACCEPTANCE SECURITY GUIDELINES, SEPTEMBER 2012
- PCI SSC GUIDANCE TO MERCHANTS ON MOBILE PAYMENT ACCEPTANCE SECURITY, MAY 2012
- VISA BEST PRACTICES FOR MOBILE PAYMENT ACCEPTANCE SOLUTIONS VERSION 1.0, APRIL 2011

Resources:

- PCI SSC Document Library:
  https://www.pcisecuritystandards.org/security_standards/documents.php
  Merchant PCI DSS Standards
  Payment Application PA-DSS Standards
  Point to Point Encryption Standards
  PIN Transaction Security (PTS) Standards
- PCI Approved Companies and providers:
  https://www.pcisecuritystandards.org/approved_companies_providers/index.php
  Approved PIN Devices
  Approved SRED Devices
  Validated P2PE Solution Providers
  Validated P2PE Applications
- EMVCo Mobile Payments: http://www.emvco.com/mobile.aspx

B. Privacy - Privacy Guidelines: Protection of Personally Identifiable Information

Definitions:

- ✓ Personally Identifiable Information (PII) is information collected or used by the Mobile Payment Solutions (MPS) provider and directly identifies or can reasonably be used to identify an individual. MPS PII does not include anonymous or aggregated information, which does not directly identify or cannot reasonably be used to identify, an individual customer or user.

Scope of Coverage:

- ✓ These privacy guidelines govern the collection, use, storage and sharing of Personally Identifiable Information in MPS and are applicable to all entities in the MPS ecosystem including device manufacturers, application developers, platform providers, merchants, acquiring processors, online payment services (online bill pay, charges to wireless bills), providers of payment products, and payment networks that operate on a mobile device.

The privacy guidelines are not applicable to mobile-based payment information used or shared:

- ✓ As mandated to comply with court orders, subpoenas, lawful discovery requests and other legal or regulatory requirements (e.g. Bank Secrecy Act ("BSA"), FinCEN's anti-money laundering ("AML") regulation); or to enforce the MPS provider's legal rights or defend against legal claims;
- ✓ For testing, product fulfillment, or maintenance in the standard operation of any payment -based service; or
- ✓ When data is made in aggregate or anonymously.

Guidelines:

- ✓ Mobile Payment Privacy Guidelines focus on consumers who use their phones to initiate payment transactions. Consumers should have the confidence that their payment-based PII will be protected by companies that sign on to these guidelines and that their PII will not be shared with third parties without their knowledge or consent.

Notice:

- ✓ MPS must provide notice consistent with the context of the payment-based service or transaction. The notice should be easy to understand, concise and include descriptions of the data types that will be used, associated data practices, and any options consumers have for controlling such use. Furthermore, these notices should be clearly readable on small screens.
- ✓ MPS providers should adopt industry-standard self-regulatory symbols, short notices and other forms of enhanced transparency to communicate data practices in the mobile payments arena and support greater consumer awareness.

Choice:

- ✓ Providers must provide choice mechanisms consistent with the context of a particular transaction or the business relationship with the consumer before initiating an MPS service.
  - Purpose specification/usage—MPS providers must clearly and plainly articulate to consumers the purposes for which they collect and use payment-based PII.
    - Use of aggregate and anonymous information - If an MPS provider plans to use anonymous or aggregate information, they should apply industry best practices and state-of-the-art techniques applicable to the intended use and sensitivity of the data. Anonymization practices should be designed to reasonably de-identify the data by using a "hashed" or otherwise permanently obscured data field (for instance with regard to name, address or telephone number).

C. Competition

In economics, competition is the rivalry among sellers trying to achieve goals such as increasing profits, market share, and sales volume by varying the elements of the marketing mix: price, product, distribution, and promotion. Merriam-Webster defines competition in business as "the effort of two or more parties acting independently to secure the business of a third party by offering the most favorable terms." In other words, competition is essential when new markets are developing.

Literally every week there's a new company, startup, or financial institution launching a new way to pay, issue rewards, or process transactions from a mobile device. All with a very similar end goal – making offline payments easier. While the various entities vying for consumer and merchant attention for their mobile payment solution all have good intentions – making offline payments easier – there is also an opportunity to generate revenue and gain market share that is creating a large number of entrants. Consumers and merchants must do their own due diligence to determine the security, product/market viability and the applicability of the chosen solution to match their operational flow.

Generally speaking, as long as the companies entering the mobile payment solution market follow the guidelines and best practices outlined in this document, consumers and merchants will benefit from competition. While there is currently no one clear-cut winner in the mobile payments/digital wallet race, we will begin to see consolidation occurring in the coming 12-24 months, primarily due to competition. Ultimately, the companies that survive and become the dominant providers of mobile payment solutions will be the companies that deliver secure, convenient, reasonably priced, valued added solutions to consumers and merchants.

D. Technology

There is a tendency during early stages of paradigm shifts (such as mobile payments), for various players to focus on proprietary solutions that can create defensible differentiation. The adoption of mobile payments and the creation of enough value for both the consumer and merchant, which can lead to a large enough market for a diverse group of service providers to build value added features that will produce revenue and profit opportunities, requires that a baseline of standards and interoperability prevail. A rising tide will lift all boats. There are endless examples in payments where great ideas have ended up in the trash bin because of the challenges of solving the proverbial chicken and egg problem - getting enough consumers and merchants ready to transact in a compact enough period of time, so that investment levels are tolerable and momentum can be built. It is also often not the best technology or the most secure solution that wins, but one that balances convenience, security, cost, etc. Mobile is having a profound impact on every facet of our lives. Overcoming the pervasiveness of the magnetic stripe card and the deeply ingrained habits of consumer payments is a challenge that can only be overcome with a sound foundation of guidelines and best practices. (Context = US market and use of mobile payments at the retail POS.)

There is extensive debate about which technologies are ideal for this contactless connection. Possibilities include; NFC, QR Codes, Barcode, Bluetooth, Sound, 3-4G/Wifi, cloud based solutions, etc.

One possible best practice approach would be for multiple methods to be supported by each mobile wallet provider. As with magnetic stripe cards today, the numbers can be read off the stripe, manually entered into a POS or captured on an imprinter.

While we can debate the reliability and security of these various methods, the key is that the basic transaction can be completed with minimal chance of fraud or of a sale being lost, thereby protecting consumer data.

- **Reliability –** Regardless of the technology used to complete any given transaction, the results for the consumer and the other parties to the transaction should be consistent from transaction to transaction. There is likely to be a lengthy transition period from magnetic stripe to mobile initiated transactions, so a heightened sensitivity to the training required and potential turnover at the POS is essential.

- **Security –** It is critical that there be a balance between security and convenience for any payment mechanism to thrive in the US market. When surveyed, consumers will often cite

security features as highly desirable, but in practice will often bypass or undermine enhanced security. A classic example of this is the use of a PIN. If optional, consumers will often not activate it and if mandatory will often choose the absolute minimum # of digits required and something like 2,5,8,0 or 1,1,1,1. Therefore, it is imperative that security not be dependent on the end consumer but be embedded in the underlying infrastructure as much as possible and available as a backstop when needed. A great example is the ability for the consumer or service provider to disable a mobile wallet remotely, when needed, to prevent fraudulent use. Another example is what is known as "risk based" fraud prevention, which can be implemented in a wide variety of ways but essentially involves the screening of transactions based on risk factors like excessive activity. When a high-risk situation is identified, the consumer can be prompted for additional authentication during a transaction, or the dollar amount of the transaction can be limited or denied.

E. Contracts

Historically, a common practice for merchant acquirers and infrastructure providers has been to set contract terms with merchants, when the merchant was purchasing services from these companies. These contracts presumably allowed the providers of these services the ability to offer their services over a term (months or years) as opposed to requesting that the services be paid for up front. As competition related to enhanced products improved service levels and caused prices to lower, merchants have grown increasingly wary of providers that attempt to lock them into a long term contract. As the service and support from these providers continues to improve and the products and services they offer grow, it is important that the merchant has the option of choosing the services that provide them with the highest quality of service and support at the most competitive prices. Mobile payment solutions in general have had a significant impact on the velocity of change in both products and pricing for merchants. It is important that merchants fully understand both the terms and conditions of these contracts as they relate to cancellation and product/service switching, as well as their ability to terminate the contracts should the service providers not deliver.

Section 6: About the Electronic Transactions Association and the ETA Mobile Payment Committee

The Electronic Transactions Association is an international trade association representing companies who offer electronic transaction processing products and services. The purpose of ETA is to influence, monitor and help shape the merchant acquiring industry by providing leadership through education, advocacy and the exchange of information.

ETA is the international trade association serving the needs of organizations offering transaction-processing products/services.

ETA's stated mission is to fully serve its members and advance their profession by providing leadership through education, advocacy and the exchange of information.
The Mobile Payments Committee will address several issues facing the future of mobile payments, including:

- The business relationships needed to foster innovation and achieve network interoperability among merchants, credit card companies, mobile networks, equipment operators, equipment manufacturers and financial institutions;
- Exploring the necessity of “best practices” that ensure merchants and consumers have access to the most innovative and effective mobile payments solutions;
- The education of legislators and regulators developing public policy around mobile payments; and
- The education of merchants and consumers about the potential of mobile payments to provide a more efficient, reliable and secure experience at the point of purchase.

Section 7: Education Sub-Committee
www.electran.org/mobile

Section 8: Mobile Payments Glossary
www.electran.org/mobile