Securing Payments: Payments Tokenization in Primetime

Federal Reserve Bank of Boston
Payments Symposium
January 20, 2016

Susan Pandy, Ph.D., Director, Payment Strategies
Federal Reserve Bank of Boston

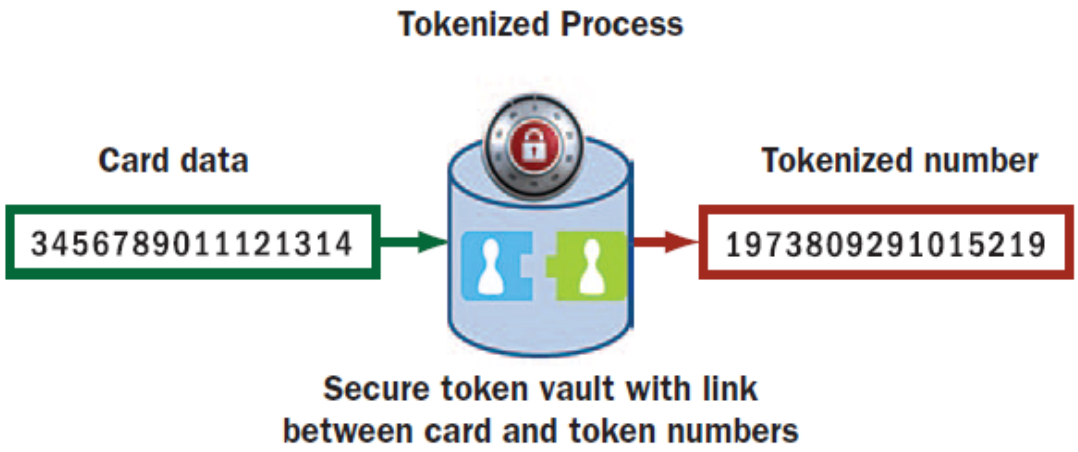
FEDERAL RESERVE BANK OF BOSTON™

Agenda

- Introduction to Tokenization
- Tokenization Models: Security v. Payments
- Tokenization and Mobile/Digital Wallets
- Tokenization Challenges
- Industry Perspectives on Tokenization
- Conclusions

Introduction to Tokenization

- Replaces underlying sensitive value (e.g., PAN) with non-sensitive token value after payment authorization process has begun or post-authorization for data-at-rest in merchant or processor database



First Data and Bank of America. (2011, April). *How security can help grow your business: the marketing side of tokenization*.

- Tokenization is not the same thing as encryption
- Encryption uses a mathematical process to make the data unintelligible or unusable and it can be repeatable and/or reversible

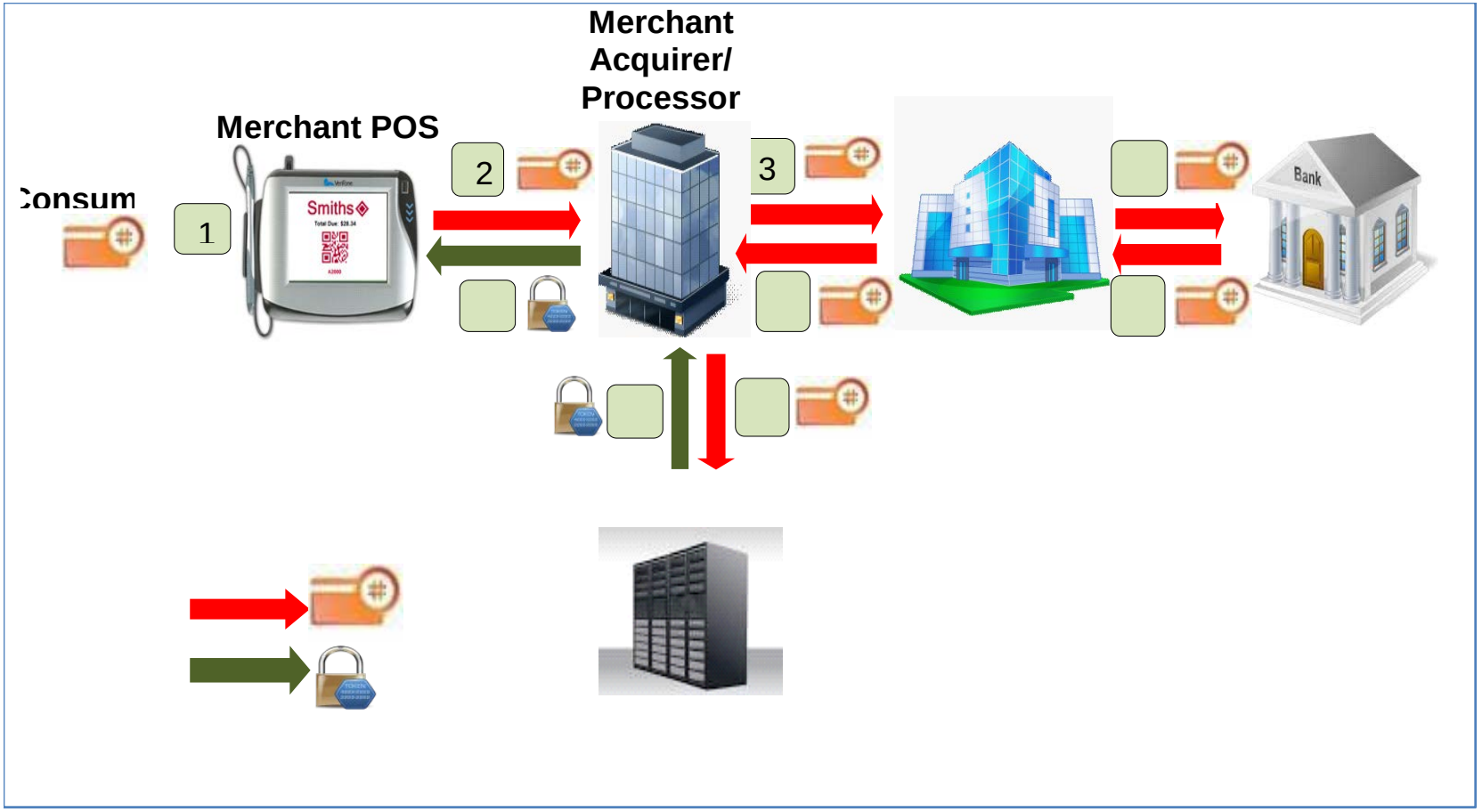
Different Tokenization Models

- Many different models and definitions
- ***Security (or Merchant/Acquirer) Tokenization*** protects sensitive data ***post-authorization*** (i.e., data-at-rest)
- ***Payment (or Issuer) Tokenization***: creates substitute value for real payment credentials to use in a mobile or digital financial transaction

Security (Merchant/Acquirer) Tokenization

- Introduced a decade ago to better protect payment data from compromise as breaches increased
- Many merchants developed proprietary systems or used services offered by their acquirer/processor
- Helped merchants reduce PCI compliance costs
  - 2004 *PCI SSC Data Security Standard* (PCI-DSS) defined merchant requirements for protecting cardholder data and drove use of security tokenization
  - PCI SSC *2011 Tokenization Guidelines*
- ANSI X9.119-2 requirements being developed to support use of tokens to secure and protect sensitive information –but not to replace PAN during a financial transaction processed over a payment network

Security Tokenization Process



Examples Tokenization & Digital Wallets

Cloud

Security Tokenization

QR Code

2D barcode downloaded from m-App, contains payment info to scan at POS QR code reader

Mobile Number + PIN

Enter at POS to access payment credentials stored in cloud

Starbucks

LevelUp

MCX CurrentC

PayPal

Acquired Paydiant

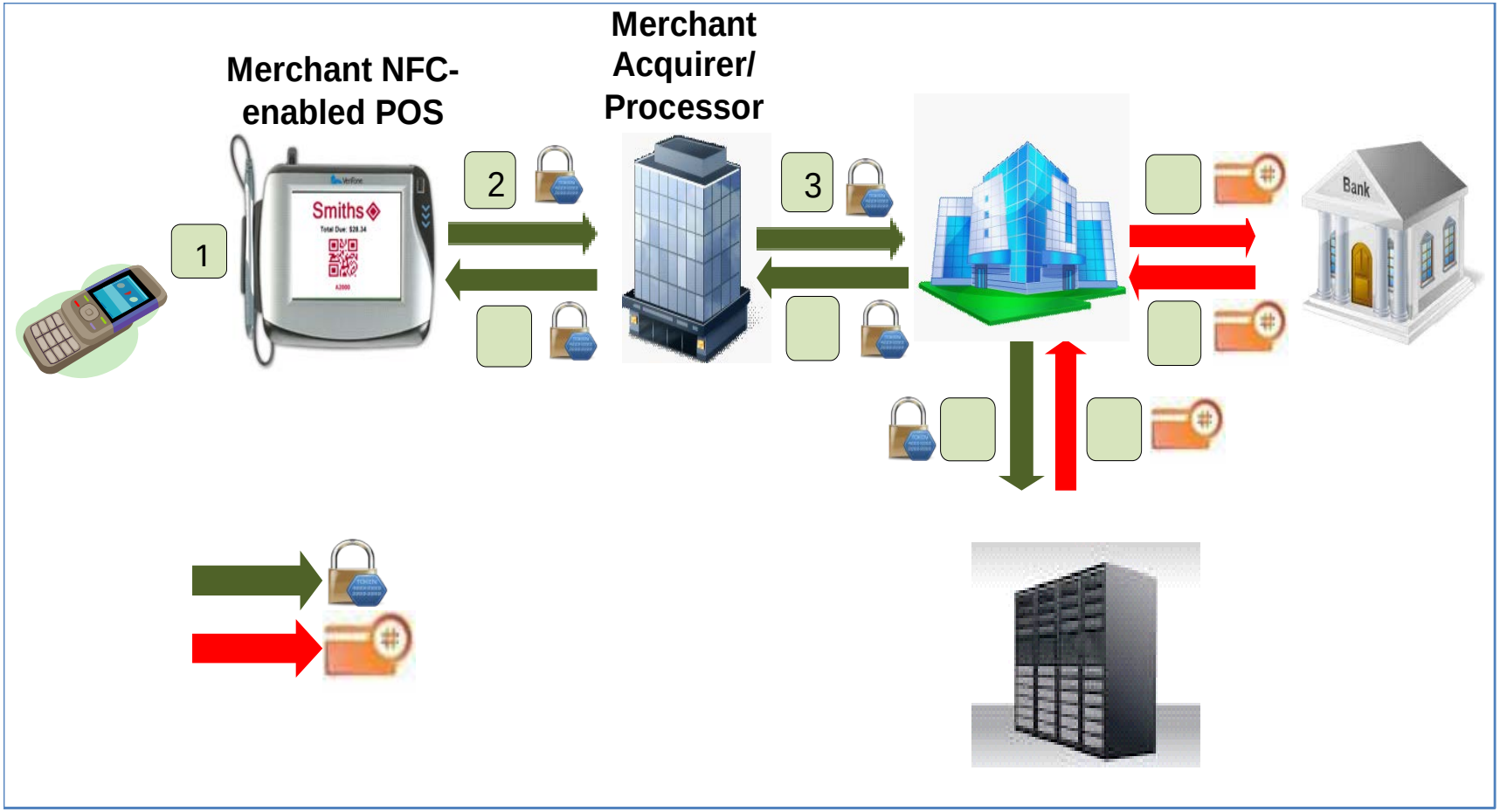
Payment Tokenization

- ***Payment tokenization*** models are newer and driven by the card networks
  - Supported by *EMV Payment Tokenization Specification – Technical Framework v. 1.0* in March 2014
- Combines Token and Dynamic Cryptogram
- **Token Service Provider** (TSP) issues payment tokens on behalf of an FI to a **Token Requestor** (TR) to load into customer's mobile wallet before initiating a mobile/digital payment transaction
- Token value is present throughout the transaction process, except when PAN is transmitted over secure network from TSP to the issuer for authorization

Why Payment Tokenization?

- Payment card data was under increasing attack and mobile created more concerns about increase in payment card fraud and current threat environment
- Key challenges around proliferation and obfuscation of data
- Need for solution to remove sensitive payment card data from transaction end-to-end and reduce payment risk, *before* large scale adoption of mobile/digital payments
- Card networks wanted global standards to secure digital payments and worked with EMVCo to develop specification

Payment Tokenization Process



Examples of Payment Tokenization in Mobile Wallets

NFC
Standards-based wireless communication exchanges data between devices a few centimeters apart

HCE
Host card emulation software replaces SE. Routes NFC communication via mobile host processor

Secure Element
Tamper-resistant, encrypted smart chip in mobile phone. Stores customer account credentials for NFC / contactless payments

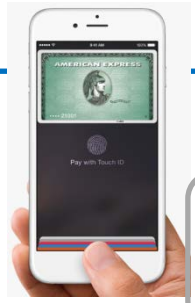
Cloud
Payment credentials stored in remote server

Payment Tokenization
Substitution of card PAN with unique, random number to reference sensitive data being protected

Apple Pay

Google Android Pay

SAMSUNG pay



TEE in Phone

FEDERAL RESERVE BANK OF BOSTON™

Token Use Case
Apple Pay Customer View

Customer SET-UP to add card(s) to Passbook

- Upload from existing iTunes account or scan credit/debit card with phone camera (card information is not stored on the phone or Apple Pay)
- Apple verifies user information with issuing bank and links card to Passbook with token
- PAN is tokenized and stored in token vault

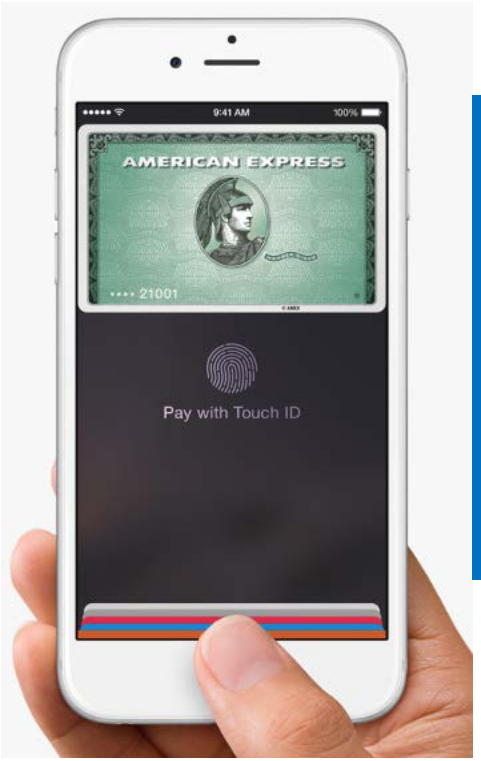
Look for this icon at checkout.

Cashier rings up purchase

Customer selects payment card from Passbook

Consumer waves/taps iPhone near terminal with finger on Touch ID

No need to open app or wake display



Vibration and beep to confirm payment info successfully sent.
On screen "payment accepted" notification. Paper or email receipt.

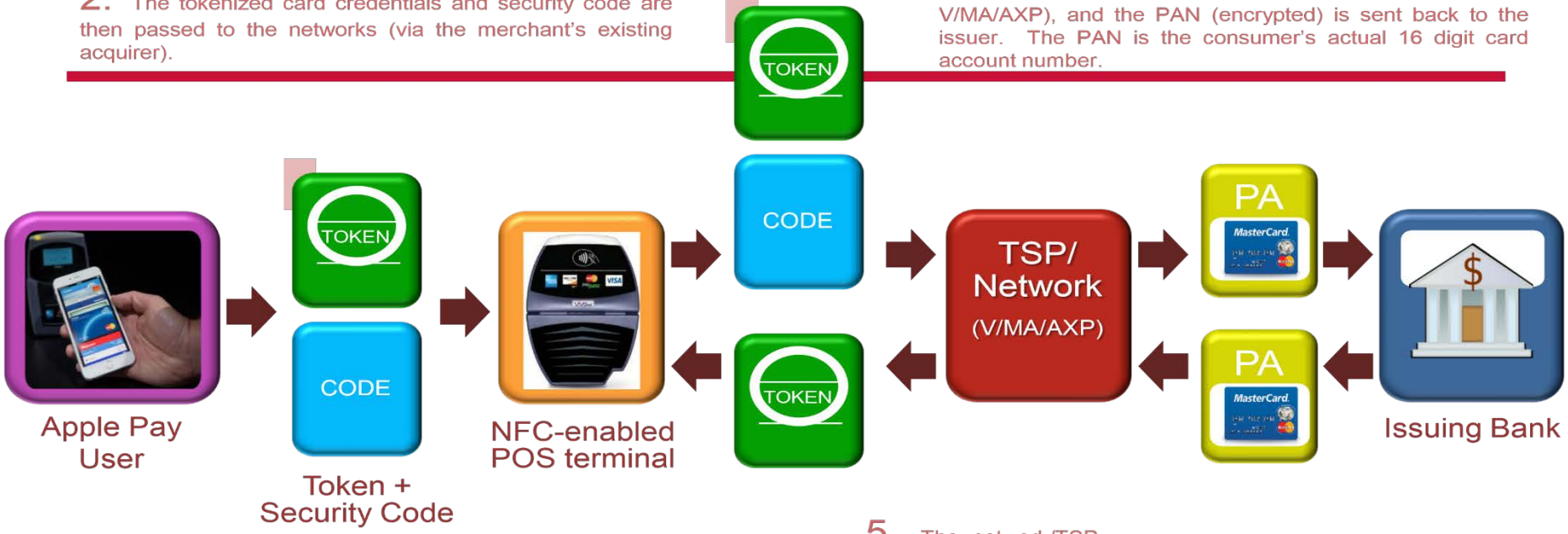
FEDERAL RESERVE BANK OF BOSTON™

Payment Tokenization Use Case

Apple Pay In-Store Transaction

2. The tokenized card credentials and security code are then passed to the networks (via the merchant's existing acquirer).

3. The credentials are "de-tokenized" by the TSP (ie, V/MA/AXP), and the PAN (encrypted) is sent back to the issuer. The PAN is the consumer's actual 16 digit card account number.



1. A user taps an iPhone on an NFC-enabled terminal (default card credentials from Passbook jump to top of lock screen). After the transaction is authenticated with a thumb print, the phone transmits the Device Account Number (ie, the token), and also pushes a randomly generated dynamic security code (ie, the token cryptogram) to the POS terminal.

5. The network/TSP (V/MA/AXP) then "re-tokenizes" the PAN, returning the token to the merchant terminal (via the merchant acquirer) to complete the transaction.

4. The issuer's authorization response (triggered by validating the PAN's sufficient funds) is returned to the network.

Source: Jefferies West Coast payments Summit, Half Moon Bay, CA, September 22-23, 2014, Jason Kupferberg, Senior Analyst, and Ramsey El-Assal, Equity Analyst, Computer Services & IT Consulting, Jefferies.

Payment Tokenization Challenges

- Token vault security is paramount
  - Need to guarantee vault is secure at all times to prevent it from becoming an easy target for criminals
- Merchant reconciliation for chargebacks, customer service, loyalty, look-ups
- Application to ecommerce

Industry Perspectives: Financial Institutions

- FIs included large, regional, and small banks and credit unions
  - General support for EMVCo spec and Apple Pay
  - Payment token enhances FI's ability to manage risk
  - General consensus among FIs that mobile phone based transactions have greater degree of security than other types of payment
  - Initial challenges/concerns around token provisioning process (e.g., Yellow Path authentication)
  - Card network rules for setting up Apple Pay ID&V vary
    - Creates a challenge for FIs to build separate applications for each network they support
  - Some FIs prefer to have customers use their mobile banking app for provisioning

Processors

- Processors interviewed represented acquirers, merchants, vendors, and gateways
  - Have long supported merchant-centric/security tokenization schemes
  - Many interviewed participate in EMVCo as associate members
  - Strongly believe they can help develop functionality and features that would be useful to the market and address some merchant challenges
  - Some are interested in becoming TSPs

Merchants

- Merchants believe in potential of mobile to be secure and affordable, but are also aware of risks inherent in mobile channel
- Merchants want to leverage mobile beyond payments (for shopping, rewards, loyalty, etc.)
- Concern about some challenges around payment tokens with returns and ability to perform customer lookup with token instead of card
- Merchants want an open and inclusive tokenization standards process

Conclusions

- Apple Pay has made payment tokenization for retail payments an implementable reality and scalable solution
  - This has triggered a transformation in the mobile/digital payment landscape
- Tokenization is a key component for improving the security of retail mobile payments and protecting payment credentials by removing them from the transaction process
- EMVCo framework has introduced new concepts to enhance security (e.g., domain restriction controls, token assurance levels) and an updated spec is expected in 2016
- Tokenization alone will not address potential shift in fraud to e-commerce

Payment Strategies Publications 2010-2015

Date	Activity
June 2015	Published *Is Payments Tokenization Ready for Primetime? Perspectives from Industry Stakeholders on the Tokenization Landscape*
April 2015 & Dec 2014	Published *Current Perspectives on the Mobile Wallet Evolution* (July 2015) Published *Industry Perspectives on Mobile/Digital Wallets and Channel Convergence* (March 2015)
June 2014	Published *Summary of Mobile Payments Industry Workgroup (MPIW) Meeting Discussion on the U.S. Tokenization Landscape – June 2-3, 2014* (Sept 2014)
March 2014 – May 2014	Published s*Update on the U.S. Regulatory Landscape for Mobile Payments* and *MPIW Security Workgroup Initiative Progress to Date and Current Status*
November 2013	Published *Meeting the Needs of Non-Traditional Consumers and Achieving Scale with Mobile Contactless Payments in the U.S.* (Jan. 2014)
June 2013	Published s*Technology and Security Considerations for Mobile Contactless Payments at the Point-of-Sale in the U.S.* (Nov. 2013)
January 2013	Updated *Mobile Payments in the U.S.* and *Future of Mobile Security: Understanding the Risk Environment for Mobile Payments* (Oct. 2013)
September 2012	Published *Summary of Mobile Payments Industry Workgroup (MPIW) Meeting with Merchants and Mobile Payment Start-ups* (June 2013)
April 2012	Published *U.S. Regulatory Landscape for Mobile Payments* (July 2012)
March 2011	Published *Mobile Payments in the U.S. – Mapping Out the Road Ahead*

Questions?

Susan Pandy, Ph.D.
Director, Payment Strategies
Federal Reserve Bank of Boston
susan.pandy@bos.frb.org

http://www.bostonfed.org/bankinfo/payment-strategies/index.htm