Fostering Next Generation Security

Chicago Payments Symposium 2016
October 12, 2016
Marianne Crowe
Federal Reserve Bank of Boston

The views expressed in this presentation are those of the presenter and do not necessarily represent those of the Federal Reserve Bank of Boston or the Federal Reserve System. Mention or display of a trademark, proprietary product or firm in this presentation does not constitute an endorsement or criticism by the FR Bank of Boston or the FR System and does not imply approval to the exclusion of other suitable products or firms.
Channel convergence poses more complex payment security risks

- Mobile payments environment changing rapidly - new technology platforms, solutions, channels and participants
- New payment models: card on file services, digital and QR code cloud-based mobile payments and POS NFC wallets
  - Payment card data breaches highlight risks of storing sensitive payment data at POS
  - Mobile creating more concerns about increase in payment card fraud as EMV chip migration shifts fraud from card-present to CNP
- Need to remove sensitive payment card data from transaction end-to-end and reduce payment risk
- No framework to secure payment credentials and associated end-to-end mobile payment transactions
Wallets developing around key platforms
Building Blocks for Payment Security & Authentication require Multi-layered approach

- **EMV chip card**: Protects against cards, adds PIN security.
- **Tokenization**: Makes PAN less valuable.
- **Encryption**: Makes it difficult to extract cardholder data.
Fed role in driving payments security

• Mobile Payments Industry Workgroup (MPIW)
  – Collaboration of 40+ mobile payment industry experts
  – Share perspectives and assessments of mobile/digital topics of common concern, e.g. security, EMV migration, HCE, tokenization, wallets, CNP, regulation

• Tokenization Landscape Stakeholder Assessment (2014-15)
  – Benefits, challenges, opportunities of payment & security tokenization models

• Mobile CNP Payments Fraud Risk Assessment (2015-16)
  – Compare different mobile CNP payment models, associated risks and security gaps
  – WP: November 2016
Conducted Tokenization Landscape Assessment

- Provisioning and processing of mobile and digital tokenized payment transactions under various schemes
- Payment tokenization removes original payment account credential (PAN) from transaction process
  - Replaces PAN with substitute value to use in mobile/digital financial transactions in lieu of PAN
  - Follows EMV token spec
  - Token renders payment card data meaningless to hackers
  - Not mathematically reversible - only Token Vault owner (token service provider) can de-tokenize
  - Format fits legacy payment account credentials (PAN)
- Security tokenization
  - Replaces underlying sensitive value (PAN) with a non-sensitive token value post-authorization for data-at-rest stored in merchant/acquirer database
  - Reduces risk of potential compromise and non-compliance with PCI.
  - Chargebacks and payment reconciliation can take place without handling payment data
  - Supported by PCI SSC, X9 (119-2), Proprietary merchant/acquirer model
Apple Pay use case: How payment token secures mobile credentials

1. Tap iPhone on NFC-enabled terminal. Authenticate with fingerprint or passcode. Transmit token & dynamic cryptogram to POS terminal.

2. Tokenized PAN & cryptogram sent to network via merchant acquirer.

3. TSP de-tokenizes token. Sends real PAN (encrypted) to card issuer.

4. TSP re-tokenizes PAN. Sends token back to merchant terminal (via acquirer) to complete transaction.
Mobile/digital wallets expand to e-commerce channel with new security challenges

<table>
<thead>
<tr>
<th>Mobile/Digital Wallets</th>
<th>Technologies</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘PAY’ Wallets</td>
<td>NFC + eSE</td>
<td>Apple Pay</td>
</tr>
<tr>
<td></td>
<td>NFC + HCE</td>
<td>Samsung Pay</td>
</tr>
<tr>
<td></td>
<td>NFC + TEE / MST</td>
<td></td>
</tr>
<tr>
<td>Merchant-centric</td>
<td>Cloud + QR Code</td>
<td>Walmart Pay, Starbucks, CurrentC</td>
</tr>
<tr>
<td>Payment Service Providers</td>
<td>Cloud</td>
<td>Amazon Payments, PayPal</td>
</tr>
<tr>
<td>Banks</td>
<td>Cloud</td>
<td>CapitalOne, WF, PayPay</td>
</tr>
<tr>
<td>Card Networks</td>
<td>NFC + HCE</td>
<td>Masterpass, Visa Checkout</td>
</tr>
</tbody>
</table>
EMV card migration does not address CNP fraud

CNP Fraud by Country

- UK
- France
- Canada
- Australia

U.S. Credit Card Third Party Fraud Losses

Actuals (estimated) vs Forecast

- CNP
- Counterfeit
- Lost/Stolen/NR
- Application Fraud
- ATO

Source: Retail Payments Risk Forum, FRB Atlanta, 2015
Source: Early Warning Analyst Estimates, 2015
Mobile payments is driving up CNP/e-commerce volume

8.1% of total U.S. retail sales in Q2 2016 from ecommerce

Source: U.S. Census Bureau; comScore mcommerce Measurement, 2016
Conducted assessment of m-commerce models in CNP environment

• Goal to understand and compare risks and security controls of m-commerce wallet models

• Analyzed four mobile CNP use cases
  – Guest checkout via mobile browser and app (no CoF)
  – Mobile in-app with EMV ID&V (Apple Pay, Android Pay, Samsung Pay)
  – Cloud-based wallets using other authentication approaches (PayPal, Amazon)
  – Card network digital wallet (Visa Checkout, Masterpass, AmEx Express Checkout)
Mobile CNP Assessment

- Looked at critical points of vulnerability across use cases
  - Account creation
  - EMV ID&V*
  - Authentication*
  - Mobile device and operating system integration
  - Use of third-party service providers
- Identified possible mitigation solutions and tools across use cases
  - Authentication
  - Use of dynamic cryptograms
  - Encryption
  - Security and payment tokenization
  - 3D–Secure 2.0

*Considered most vulnerable even though they are risk controls
Payment tokenization moving to online and in-app CNP payments

MasterCard to integrate fully tokenized checkout experience within MasterPass-enabled bank issued wallets using MDES

- Replaces PAN with a payment token for consumer credit & debit, commercial and prepaid cards stored in MasterPass
- Tokens are unique to each bank-connected MasterPass wallet,
- Similar to tokens used at POS, following the EMV token spec.
Risk-based authentication improves ecommerce security

**EMVCo 3DS**
- Secure communication protocol
- Enables real-time cardholder authentication directly between merchant and issuer
- Liability for fraudulent transactions shifts to issuer

**3DS 1.0**
- Never broadly adopted in U.S.
- All transactions authenticated
- Cardholder must enroll

**Will U.S. merchants and issuers implement 3DS 2.0?**
- Authenticates ONLY when risk exceeds predetermined level
- Reduces customer abandonment, improves check-out speed and convenience
Recommendations

- Extend payment tokenization model to CNP e-commerce and cloud-based wallets to remove PAN from clear
- Simplify integration of payment and security tokens on merchant back-end
- Implement end-to-end encryption with tokenization at POS and CNP
- Monitor potential social engineering fraud during enrollment with ID&V
- Use multi-layered and other authentication tools, including MFA, biometrics (fingerprint), enhanced risk based methods (3DS V2.0)
- Large merchants, FIs & providers should share expertise/best practices in CNP risk management with less sophisticated, smaller e-commerce merchants
- Manage m-commerce as a separate channel from e-commerce
- Collaborate on standards and best practices for mobile payments in CNP environment