How Safe Are Mobile Payments?

MAC Webinar
March 16, 2017

Dave Lott
Payments Risk Expert
Federal Reserve Bank of Atlanta

The views expressed in this presentation are those of the presenters and do not necessarily reflect the views of the Federal Reserve Bank of Atlanta or the Federal Reserve System.

Presentation Development:
Marianne Crowe, Susan Pandy, Ph.D. - Payment Strategies Group, FRB - Boston
Dave Lott, Retail Payments Risk Forum, FRB - Atlanta
MAC is an organization of Bankcard professionals involved in the risk management side of Card Processing. We have members from Banks, ISOs, Card Associations and others related to the risk management side of the industry. MAC’s mission is to strengthen the payment ecosystem through ongoing education, communication and cooperation among acquirers, card brands and enforcement agencies.

To learn more about MAC or to become a member of MAC please visit the website below.

https://www.macmember.org/
Mobile Payments Industry Workgroup (MPIW)

– Collaborative effort of 40+ mobile payment industry experts
– Share perspectives on mobile topics of common concern, e.g. security, EMV migration, HCE, tokenization, nonbank solutions, regulation
– Form sub-groups; publish whitepapers for broader industry education

– FIs & card networks
– Merchants & third party processors
– Clearing/settlement orgs
– Online payment providers
– U.S. Treasury

– Mobile Network Operators (MNOs)
– Handset & chip manufacturers
– Mobile solution providers
– Industry trade associations:
  • CTIA, MAG, Connexus
  • Smart Card Alliance
Scope & Objectives

– Project driven by anticipated shift from CP to CNP fraud based on EMV chip card migration at POS
– Projected growth in e-commerce dollar/transaction volume and m-commerce growth share
– Use case development and analysis
  • Define mobile CNP use cases and framework for analysis
  • Understand how different CNP payment models work, primarily mobile browser and mobile app/in-app
  • Identify potential risks and security gaps across use cases
  • Identify security/authentication controls/solutions
  • Outline issues and recommendations
Estimated Quarterly U.S. E-commerce Sales as Percent of Total Retail Sales (2013-2016)

E-commerce Sales ($Mn)

2009 – 2015 Average Annual Growth = 22%

SOURCE: U.S. Census Bureau
M-commerce as a % of E-commerce

SOURCE: comScore m-Commerce Measurement
CNP Fraud Losses in EMV Countries 2004-2014

Sources: Data compiled from Financial Fraud Action UK, The Observatory for Payment Card Security, Canadian Bankers Association, and Australian Payments Clearing Association
Card Fraud Shift to the CNP Environment

CNP Fraud as a % of Total Fraud

Mobile Wallet Ecosystem

2006-2008
- Remote Payments - SMS & Internet
- PayPal Text to Buy
- Text Buy It
- Mobile App Stores
  - Apple
  - Android
- Contactless Cards
  - Visa payWave
  - MasterCard payPass
- Direct Carrier Billing

2009-2010
- Mobile Browser
- mPOS
- Proliferation of Mobile Apps

2011
- QR Codes
- LevelUp
- NFC + SE Mobile Wallet
- Mobile Prepaid

2012
- mPOS
- PayPal HERE
- NFC Wallet
- Digital Wallet
- Prepaid Account
- Mobile Bank Account

2013-2014
- NFC + HCE
- Beacon BLE
- Digital Wallet
- NFC + token
- Digital Wallet

2015-2016
- Merchant Apps
- Walmart Pay
- Fi Wallet
- NFC + HCE
- Virtual Swipe
- SAMSUNG pay
- Digital Wallet
New opportunities for compromise from malware and data breaches
Use Cases Evaluated

1. Guest check-out, no card-on-file (CoF) via mobile browser or mobile app

2. “Pay” Wallets: Mobile in-app with EMV identification and verification (ID&V), CoF
   – Payment token stored in SE, or for HCE – in TEE or Mobile OS

3. Cloud-based mobile wallets with CoF that use “Other Authentication” processes (PayPal, Amazon, retailer apps or mobile websites)
   – Consumer authenticates to Payment Service Provider (PSP) processing on behalf of merchant or directly to merchant via merchant mobile browser or app

4. Card network digital wallet CoF models (e.g., Visa Checkout, MasterPass, AmEx Express Checkout)
Use Case Functions Analyzed

1. Account creation
2. EMV ID&V (Use Cases 2 & 4 only)
3. Authentication
4. Integration of mobile device/operating system
5. Use of third party service providers

**Types of attacks mapped to functions in matrix:**

- Data breach, malware/virus, account takeover fraud, new account fraud, mobile device porting fraud, man-in-the-middle/browser attack, fingerprint spoofing, social engineering
Use Case 1: Guest Checkout via Mobile Browser or Mobile App (No Card-on-File)

• User not required to create account to complete a purchase; i.e., no PII/PAN stored with retailer.
• User manually enters PAN/PII via mobile browser/app for each purchase.
• **66% of top 100 retailers offer guest checkout** – many consumers reluctant to share personal information with merchant for privacy/security reasons.
• **Authentication is biggest challenge** for merchants because they do not know the customer as they do with registered customers.
• Important for online merchants to **encrypt** consumer data as it is entered and during transmission – via mobile browser or mobile app.
• Merchants (mostly large) are exploring tools to help with authentication, such as collecting the device ID.
• **Probability of risk from fraud attacks/threats is MEDIUM to HIGH** across all components but can be effectively managed by merchants with proper tools/fraud detection systems.
Use Case 2: Mobile In-App with EMV ID&V ("Pay" Wallets)

- Wallets follow the EMV tokenization spec and use payment tokenization, dynamic cryptograms, issuer ID&V and other controls to secure these models.
  - Require consumer enrollment where payment credentials are vetted using issuer ID&V before a token is provisioned to the mobile phone (wallet).
  - For each mobile in-app purchase, user authenticates on mobile device using fingerprint or a passcode/PIN.
  - Additional authentication data from mobile device: geolocation, device ID is used to recognize suspicious transactions.
  - Secure mobile OS/device architecture – hardware only (Apple), software only (Android), or hybrid (Samsung)
  - **Probability of risk from fraud attacks/threats is LOW** across all components, although **new account fraud** was initially **MEDIUM** but is now low because of vulnerabilities in early implementations with weak ID&V processes having been addressed.
Use Case 3: Cloud-Based CoF Models using Other Authentication Processes (Amazon, PayPal, larger online merchants)

- User creates account and enrolls a payment method with Payment Service Provider (PSP), such as Amazon or PayPal, that processes on behalf of merchant, or directly with online merchant.
- To authenticate to PSP, user selects that option on participating merchant’s mobile website or mobile app and enters his PSP login credentials to complete purchase.
  - Payment credentials not shared with merchant.
- To authenticate with merchant, user logs in to his merchant account which uses payment credentials stored on file (i.e., CoF) to pay for his online purchases.
- Other authentication processes for risk management.
  - Use sophisticated risk engines that analyze data to develop a risk score to determine whether to allow/decline transaction.
Use Case 3: Cloud-Based CoF Models using Other Authentication Processes (cont.)

• Vulnerable to account takeover fraud (ATO), one of largest growing attacks (See Kount and ThreatMetrix studies).

• Most common data stolen is usernames and passwords, the fraudster can attempt to access multiple consumer online accounts and overtake them.

• While several risks of attacks may be high, PSPs such as these and larger merchants use sophisticated risk modeling using customer profile info, behavioral analytics, transaction monitoring and other authentication methods to reduce risk of fraud.
Use Case 4: Card Network Digital Wallet CoF Models using Other ID&V

- AmEx, MasterCard and Visa offer CoF digital wallet services.
- Merchants add wallet to their mobile browser or mobile app checkout carts but do not store consumer credentials.
- User creates account on digital wallet service website (via mobile device browser) (AmEx is slightly different).
  - Provides first/last name, email or mobile phone number and password.
  - Is verified by clicking on out-of-band message sent to email address
  - Adds other personal information and payment credentials to account manually or by scanning card using mobile device camera
  - CVC must be entered manually
  - To purchase, user logs in to the digital wallet service to authenticate and authorize their purchase
- MasterCard and Visa provision a payment token to user’s digital wallet.
# Use Case Attack Vectors and Risk Assessment

<table>
<thead>
<tr>
<th>Function of CNP Transaction</th>
<th>Use Case 1</th>
<th>Use Case 2</th>
<th>Use Case 3</th>
<th>Use Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Probability</td>
<td>Magnitude</td>
<td>Probability</td>
<td>Magnitude</td>
</tr>
<tr>
<td>Account Creation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Breach Risk</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Malware/Virus</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Account Takeover Fraud</td>
<td>L</td>
<td>L</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>New Account Fraud</td>
<td>L - M</td>
<td>L</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Device Porting Fraud</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>EMV (ID&amp;V)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Engineering Fraud</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile man-in-the-middle attack</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Mobile man-in-the-browser attack</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Malware</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Fingerprint Spoofing</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Fingerprint Sensor Spying Attack</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Spoofed authentication</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Mobile Device / OS Integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Rooting/Jailbreaking</td>
<td>M - H</td>
<td>L</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>Lost/Stolen Phone</td>
<td>H</td>
<td>L</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Malware/Virus</td>
<td>H</td>
<td>L</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Use of Third Party Providers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Breach Risk</td>
<td>M</td>
<td>H</td>
<td>L</td>
<td>L</td>
</tr>
</tbody>
</table>

### Probability Magnitude
- M: Medium
- L: Low
- H: High
CNP Security Controls & Methods

- Authentication
- Tokenization (Payment and Security)
- ID&V
- 3D Secure 2.0
- Encryption
- Dynamic cryptograms
Gaps & Issues Across Use Cases

- Tokenization Approaches
- Use of End-to-End Encryption
- EMV ID&V and Other Authentication Approaches
- Level and Sophistication of Customer Authentication Methods
Recommendations

- Consider mobile commerce as a new channel
- Use multi-layered and multifactor authentication controls
- Develop a strategy to minimize magstripe cards
- Industry collaboration on information sharing and customer education
- Share best practices from m-commerce use case analysis
- Collaboration on standards and best practices to mitigate mobile CNP fraud
Questions & Discussion

Whitepaper available on FRB-Boston website:
SAVE THE DATE

MAC 2017 Annual Conference
March 21 – 23, 2017
SLS Hotel - Las Vegas, NV

Don’t miss the premier payments industry risk conference. Register today at www.macmember.org
APPENDIX
Use Case 1: Guest Checkout Transaction Flow

1. Consumer opens browser or merchant mobile app (already installed on device), populates shopping cart, proceeds to the checkout process and selects “guest checkout.”
2. Consumer enters PAN, expiration date, and CVC (optional depending on merchant). Encrypted transaction data is transmitted to Merchant Server where it is decrypted using private key.
3. Merchant may use additional risk management tools before transmitting transaction to the Acquirer.
4. Acquirer logs transactions and sends to respective Card Network.
5. Card Network transmits to Card Issuer for authorization.
6. Authorization decision sent back by Card Issuer to Card Network.
7. Card Network sends authorization decision to Acquirer.
9. Transaction status message sent to consumer’s mobile phone including truncated PAN (depending on merchant configuration and consumer notification preferences).
Use Case 2: Mobile In-App With EMV ID&V - Enrollment

1. Customer downloads mobile wallet application into their smartphone and requests a token through the Mobile Wallet Provider be issued for a payment card. Card number manually entered or captured through camera.
2. Wallet service provider requests a payment token from the Card Network sending PAN and other verifying data.
3. Card Network requests approval from the Card Issuer or stands in for Issuer.
5. If approved, the Card Network creates a Payment Token linked to the PAN and stores in their Token Data Vault.
6. Card Network sends response to request back to the Wallet Provider.
7. Payment Token is stored in mobile wallet in lieu of card PAN.
Use Case 2: Mobile in-app with EMV ID&V – Purchase Transaction

1. Token has been preloaded into mobile wallet through the payment credential enrollment process. Customer opens merchant application and identifies goods/services for purchases which are placed in cart. Customer selects the mobile wallet payment option, enters/verifies billing and shipping address.

2. Encrypted transaction data including payment token is transmitted to Merchant Server via mobile cellular network where it is decrypted using private key.

3. Merchant may perform additional risk management processes before sending to the Merchant Acquirer.

4. Transaction is logged and sent to appropriate card network.

5. Card Network:
   a) Accesses Token Vault to look-up true PAN
   b) Token Vault sends PAN for transmittal to Issuer for authorization

6. Card Network:
   a) Sends authorization request with PAN to Issuer
   b) Authorization decision sent back by Issuer

7. Card Network still using token sends authorization decision to Acquirer.


9. Transaction status message sent to mobile phone.
Use Case 3: Cloud-Based CoF Models using Other Authentication Processes

1. To make a purchase, consumer logs in to the PSP or merchant’s mobile website or app to authenticate himself, selects goods and proceeds to checkout.

2. If Consumer uses a PSP for payment to the merchant, then the PSP recreates the original PAN from a security token stored on file and creates a transaction message that is sent to the Acquirer.
   - If the Consumer is using the CoF stored with the merchant, the authorization request is sent from the Merchant Server to the Acquirer.

3. Acquirer sends the request to the Card Network.

4. Card Network sends the request to the Card Issuer for authorization.

5. Card Issuer sends authorization decision back to the Card Network.

6. Card Network sends response to back to the Acquirer or the PSP.

7. Acquirer or PSP sends response back to Merchant.

8. PSP or Merchant sends confirmation/decline message to Consumer.

• Assumes consumer has previously created a wallet and login credentials with the PSP or merchant and has enrolled payment credential(s)/designated the default payment method for future purchases.

• Once an account has been created with a PSP or merchant, the payment credential is stored in an encrypted form or through a security tokenization process as a “card-on-file.”
Use Case 4: Card Network Digital Wallet CoF Models Using Other ID&V

- Assumes consumer has previously enrolled for a digital wallet with a card network.

1. To make a purchase (1): (a) Consumer logs in to the PSP or merchant’s mobile website or mobile app to authenticate himself; or (b) Consumer proceeds with purchase using “guest checkout” on a PSP or merchant website/app. Consumer selects goods, proceeds to checkout, and selects preferred card network digital wallet. Assumes merchant integration with wallet to display “Wallet Checkout” logo on its website/app.

2. Consumer logs in to card network digital wallet to confirm shipping information and authorize payment. Some models may invoke 3DS if determined that stepped-up authentication is needed by the Bank Issuer (e.g., sending a OTP to the consumer for verification).

3. Acquirer sends the authorization request to the Card Network via API or ISO messaging (not all networks may offer an API).

4. Card Network sends the authorization request to Issuing Bank for a decision.

5. Issuing Bank sends authorization decision back to the Card Network.


7. Acquirer/Merchant sends confirmation message to Consumer based on consumer preferences and merchant system configuration.