EMV and Restaurants
*What you need to know!*

Mike English  
*Executive Director of Product Development*

Kristi Kuehn  
*Sr. Director, Compliance*

November 19, 2014
Agenda

- EMV overview
- Timelines
- Liability shifts – demystified
- Considerations
- EMV, Cardholder Security and PCI
EMV Overview

EMVCo
Owned & operated by
MasterCard UnionPay JCB American Express DISCOVER VISA

Improved security
= Decreased fraud

Global payment standard
= consistent experience worldwide

Building block for future technology
## What EMV is not…

<table>
<thead>
<tr>
<th>EMV ≠ Mandated / required</th>
<th>Merchant choice to implement!</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMV ≠ Protection against all chargebacks</td>
<td>Liability shift is for counterfeit &amp; lost/stolen only.</td>
</tr>
<tr>
<td>EMV ≠ Secure cardholder data</td>
<td>EMV does not protect or encrypt card numbers.</td>
</tr>
<tr>
<td>EMV ≠ PCI DSS</td>
<td>EMV protects against fraud, PCI focuses on security of sensitive data.</td>
</tr>
</tbody>
</table>
EMV News: Projections

“Only about 1% of the 1-billion-plus credit, debit and prepaid cards in the United States currently have an EMV chip.”

“By the end of 2015, 70% of U.S. credit cards and 41% of U.S. debit cards will be EMV enabled, says Aite Group.”

3 Data from EMV Migration Forum, September 2014 Meeting
EMV Progress

EMV card issuance

- Sam’s Club MasterCard
- Bank of America
- Barclaycard (Arrival Plus World Elite) MasterCard
- Chase (British Airways, Hyatt, Select, Palladium, Sapphire, Marriott) Visa
- Citi (AAdvantage, Hhonors) MasterCard
- Target REDcard MasterCard
- USAA
- Wells Fargo Platinum
- State Employee’s Credit Union (NC)
- United Nations Federal Credit Union

EMV card acceptance

- Walmart (enabled)
- Sears\(^1\)
- Target\(^1\)
- CVS\(^1\)

\(^1\) Announced accelerated roll-out (i.e. before October 2015)

References:
http://www.nerdwallet.com/blog/top-credit-cards/nerdwallets-best-emv-chip-credit-cards/
# Investments and Benefits of Implementing Chip Technology

## Investments

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Software upgrades</td>
</tr>
<tr>
<td>Hardware upgrade</td>
</tr>
<tr>
<td>Testing and certification</td>
</tr>
<tr>
<td>Time, resources, and training</td>
</tr>
</tbody>
</table>

## Benefits

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fewer disputes for fraud</td>
</tr>
<tr>
<td>Data becomes less attractive for hackers</td>
</tr>
<tr>
<td>Path to innovation</td>
</tr>
<tr>
<td>Consumer confidence</td>
</tr>
</tbody>
</table>
**U.S. EMV Timelines for Restaurants**

- **Oct-2012**: PCI validation relief¹
- **Apr-2013**: Processor support for chip processing
- **Oct-2013**: MC ADC relief takes effect (50%)
- **Oct-2015**: Liability shift
- **Oct-2015**: MC ADC relief (100%)
- **Oct-2016**: Visa GCAR relief

---

**Visa GCAR**: Global Compromised Account Recovery

**MasterCard ADC**: Account Data Compromise

¹ Applies to Level 1 & Level 2 merchants where 75% of transactions come from a dual interface, chip-enabled, terminal
There is **no mandate** for merchant to implement EMV!

Liability Shift = Potential Chargebacks

*Generally liability is going to shift to the party using the least secure technology*¹

¹ Rules outlined in following pages are as of September 2014
# Counterfeit Card Fraud Liability Shift

## American Express, Discover, MasterCard & Visa

<table>
<thead>
<tr>
<th>Current</th>
<th>October 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issuer</strong> liable&lt;sup&gt;1&lt;/sup&gt;</td>
<td>For chip cards, <strong>merchant</strong> liable if non-chip terminal</td>
</tr>
</tbody>
</table>

<sup>1</sup> A variety of factors play into liability, such as if the full track data was provided, but for simplicity purposes using the current general scenario
## Counterfeit Card Fraud Liability Examples

<table>
<thead>
<tr>
<th>Current</th>
<th>Mag stripe card + Mag stripe terminal = Issuer liable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>Mag stripe card + Mag stripe terminal = Issuer liable</td>
</tr>
<tr>
<td>Current</td>
<td>Mag stripe card + Chip² terminal = Issuer liable</td>
</tr>
<tr>
<td>Oct-2015 &amp; Beyond</td>
<td>Chip² card + Mag stripe terminal = Merchant liable</td>
</tr>
<tr>
<td>Oct-2015 &amp; Beyond</td>
<td>Chip² card + Chip² terminal = Issuer liable</td>
</tr>
</tbody>
</table>

1 Same applies for all brands
2 With or without PIN capabilities
## Counterfeit Card Fraud Liability Examples

<table>
<thead>
<tr>
<th>Current</th>
<th>Mag stripe card</th>
<th>+</th>
<th>To summarize...</th>
<th>Liability for fraud shifts <strong>to the merchant</strong> when a <strong>counterfeit mag stripe from a chip card</strong> is used at a <strong>mag stripe terminal</strong> after Oct-2015/2017</th>
<th>Issuer liable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mag stripe card</td>
<td>+</td>
<td></td>
<td>Issuer liable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mag stripe card</td>
<td>+</td>
<td></td>
<td>Issuer liable</td>
<td></td>
</tr>
<tr>
<td>Oct-2015 &amp; Beyond</td>
<td>Chip&lt;sup&gt;2&lt;/sup&gt; card</td>
<td>+</td>
<td>Mag stripe terminal</td>
<td>Merchant liable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chip&lt;sup&gt;2&lt;/sup&gt; card</td>
<td>+</td>
<td>Chip&lt;sup&gt;2&lt;/sup&gt; terminal</td>
<td>Issuer liable</td>
<td></td>
</tr>
</tbody>
</table>

1. Same applies for all brands
2. With or without PIN capabilities
# Lost/Stolen Card Fraud Liability Shift

## American Express, Discover & MasterCard

<table>
<thead>
<tr>
<th>Current</th>
<th>October 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issuer</strong> liable(^2)</td>
<td>For chip &amp; PIN cards, <strong>merchant</strong> liable if terminal is less secure</td>
</tr>
</tbody>
</table>

Visa rules on lost and stolen fraud are different than the other card brands and will be covered later in the presentation.

---

\(^1\) Applies to face to face transactions

\(^2\) A variety of factors play into liability, such as if the full track data was provided, but for simplicity purposes using the current general scenario
**Lost/Stolen Card Fraud Liability Examples:**

**American Express, Discover & MasterCard**

<table>
<thead>
<tr>
<th>Current</th>
<th>Mag stripe card + Mag stripe terminal = Issuer liable</th>
<th>Mag stripe card + Mag stripe terminal = Issuer liable</th>
<th>Mag stripe card + Chip terminal = Issuer liable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct-2015 &amp; Beyond</td>
<td>Chip &amp; PIN card + Mag stripe terminal = Merchant liable</td>
<td>Chip &amp; Sig card + Mag stripe terminal = Issuer liable</td>
<td>Chip &amp; Sig card + Chip &amp; PIN terminal = Issuer liable</td>
</tr>
<tr>
<td></td>
<td>Chip &amp; PIN card + Chip &amp; PIN terminal = Merchant liable</td>
<td>Chip &amp; PIN card + Chip &amp; PIN terminal = Issuer liable</td>
<td>Chip &amp; PIN card + Chip &amp; PIN terminal = Issuer liable</td>
</tr>
</tbody>
</table>

1 Applies to face to face transactions
2 Visa rules are different; the issuer is responsible for lost & stolen; see details for Visa later in presentation
### Lost/Stolen Card Fraud Liability Examples: American Express, Discover & MasterCard

<table>
<thead>
<tr>
<th>Current</th>
<th>Oct-2015 &amp; Beyond</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mag stripe card + Mag stripe terminal = Issuer liable</td>
<td>Chip &amp; PIN card + Mag stripe terminal = Merchant liable</td>
</tr>
<tr>
<td>Mag stripe card + Mag stripe terminal = Issuer liable</td>
<td>Chip &amp; Sig card + Mag stripe terminal = Issuer liable</td>
</tr>
<tr>
<td>Mag stripe card + Mag stripe terminal = Issuer liable</td>
<td>Chip &amp; Sig card + Chip &amp; PIN terminal = Issuer liable</td>
</tr>
<tr>
<td>Chip &amp; PIN card + Mag stripe terminal = Merchant liable</td>
<td>Chip &amp; Sig card + Chip &amp; PIN terminal = Issuer liable</td>
</tr>
</tbody>
</table>

*To summarize...* Liability shifts **to the a restaurant** when a **lost or stolen chip & PIN card** is used at a **less secure terminal** after Oct-2015.

---

1 Applies to face to face transactions
# Lost/Stolen Card Fraud Liability Shift

**Visa**[^1]

<table>
<thead>
<tr>
<th>Current</th>
<th>October 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issuer liable</strong>[^2]</td>
<td>No change</td>
</tr>
</tbody>
</table>

[^1]: Applies to face to face transactions
[^2]: A variety of factors play into liability, such as if the full track data was provided, but for simplicity purposes using the current general scenario
Lost/Stolen Card Fraud Liability Examples: Visa\(^1\)

<table>
<thead>
<tr>
<th>Current</th>
<th>Mag stripe card</th>
<th>+</th>
<th>Mag stripe terminal</th>
<th>=</th>
<th>Issuer liable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct-2015 &amp; Beyond</td>
<td>Mag stripe card</td>
<td>+</td>
<td>Mag stripe terminal</td>
<td>=</td>
<td>Issuer liable</td>
</tr>
<tr>
<td></td>
<td>Chip &amp; PIN card</td>
<td>+</td>
<td>Mag stripe terminal</td>
<td>=</td>
<td>Issuer liable</td>
</tr>
<tr>
<td></td>
<td>Chip &amp; Sig card</td>
<td>+</td>
<td>Mag stripe terminal</td>
<td>=</td>
<td>Issuer liable</td>
</tr>
<tr>
<td></td>
<td>Chip &amp; Sig card</td>
<td>+</td>
<td>Chip &amp; PIN terminal</td>
<td>=</td>
<td>Issuer liable</td>
</tr>
<tr>
<td></td>
<td>Chip &amp; PIN card</td>
<td>+</td>
<td>Chip &amp; PIN terminal</td>
<td>=</td>
<td>Issuer liable</td>
</tr>
<tr>
<td></td>
<td>Chip &amp; PIN card</td>
<td>+</td>
<td>Chip &amp; PIN terminal</td>
<td>=</td>
<td>Issuer liable</td>
</tr>
</tbody>
</table>

\(^1\) Applies to face to face transactions
# Lost/Stolen Card Fraud Liability Examples: Visa

<table>
<thead>
<tr>
<th>Current</th>
<th>Current Mag stripe card + Current Mag stripe terminal = Issuer liable</th>
</tr>
</thead>
</table>

**To summarize...**

A restaurant is **never liable** for **lost and stolen** card fraud with a Visa product.

---

\(^1\) Applies to face to face transactions
POS Considerations

Supported Cardholder Verification Method (CVM)

- PIN
- Signature
- **No Signature** (such as implemented at a QSR; also called no CVM)

NFC / Contactless Support

- Is speed of service a need?
- Do you serve a demographics that is looking to mobile payments?
Process Adjustments

- Staff training
- Customer verification method
- Intuitive for the cardholder
  - Tap, swipe or insert?
  - Patron comfort factor
  - Forgotten cards?
- Additional time per transaction
- Position yourself for future technology considerations such as NFC, BLE, QR codes and others
Next Steps

- Seek education and updates from a trusted advisor …
  - Your processor, acquirer or ISO
  - Your POS or terminal provider
  - The NRA & Heartland email helpline – AskMeAboutEMV@e-hps.com
- Reference materials provided by NRA & Heartland
  - EMV & Restaurants, What you need to know
  - How to Successfully Implement EMV Payment Acceptance
- Evaluate your existing environment
  - Can you update your POS and what is the cost
  - Location and demographics that are best for EMV
  - Chargeback ratios
  - PCI, EMV and cardholder security
EMV Card and Security

Validating the Cardholder
Offline or online PIN validate the cardholder

Card Authentication
- Authorization Request Cryptogram verifies the card is authentic
- Authorization Response Cryptogram verifies the issuer is authentic to the card

Combating Replays
The Application Transaction Counter combat replay attacks

Validating Card Use
Transaction Certificate (TC) value that provides evidence to the issuer that the card was present and was used for payment
EMV and Cardholder Security

- Implementing the EMVco and Card Brand EMV specifications leaves a customer’s primary account number (PAN) and discretionary data exposed

- In the event that crimeware has found its way into the retailer’s POS system or network, the cardholder data could be stolen and used fraudulently

- Every EMV card being issues in the US includes a magstripe

- Visa has provided no “sun set” date on magstripe support 

1 Visa International Operating Regulations (Public version), 15 April 2013, page 421, reference ID#: 150413-010410-0004832
EMV, E3 and Tokenization

- EMV card is inserted in The terminal and encrypted
- Transaction wrapped in SSL encryption
- Cardholder data decrypted in a PCI compliant data center for authorization
- Single use token returned to POS (reference number)

Watch for a future NRA & Heartland webinar on technology!
Mitigating Risk!

- EMV and encryption remove ability to skim and monetize card data through combinations of verification and encryption
- EMV and encryption eliminate “man-in-the-middle” attacks
- Encryption and tokenization remove card data from the businesses’ environment
- Encryption eliminates the risk of monetizing stolen card data
- Encryption and tokenization are a definitive response to “all organizations should assume they’ve been hacked”
- Encryption and tokenization reduce a merchant’s PCI scope as per a Coalfire study
QUESTIONS?

Kristi Kuehn  
*Sr. Director, Compliance*  
kristi.kuehn@e-hps.com  
(972)295-8928

Mike English  
*Executive Director of Product Development*  
michael/english@e-hps.com  
(877)798-9656 x2756