Bank of Hawaii Merchant Services

EMV®
Europay, MasterCard and Visa
September 17, 2015

Agenda

• What is EMV?
• Why EMV
• Chip and PIN vs. Chip and Signature
• How to process a Chip Card
• Tampered Devices
• Liability Shift
What is EMV®?
Chip card and chip card specifications

• EMV®¹ commonly refers to payment cards that contain an embedded microchip.
  – The “chip” provides security features and other capabilities a card issuer may want to incorporate into their payment card program.

• EMV® encompasses specifications that are based on various standards and define the physical, electrical, data and application levels for financial payment transactions.

Why EMV®?
Smart card

• Reduced counterfeit fraud as seen in other countries at the point of interaction
  – Chip is harder to duplicate than the magnetic stripe

• Stronger cardholder authentication
  – Card Issuer determines preferred cardholder verification method (CVM) for each transaction
    o Signature
    o Online PIN (PIN verified by the card Issuer)
    o Offline PIN (PIN verified by the chip)
    o No CVM (typically less risky transactions)

• Contactless “wave” faster than swiping or inserting card.
Chip and PIN vs. Chip and Signature

When processing a chip card transaction, the issuer may request for the following information to authenticate the transaction at the Point-of-Sale.

• Issuer may require the cardholder to supply a 4-6 digit PIN number (Chip and PIN), this also applies to credit cards.
• Issuer may require the cardholder’s signature (Chip and Signature)
• Issuer may require both PIN and Signature (Chip – PIN and Signature)
• Transactions outside a cardholder’s home country may require a PIN. This may be a new experience for cardholders from Asia and Australia who don’t use a PIN in their home country but may need to enter a PIN when they come to Hawaii.

Chip Card Transactions

FD Terminals

• Payment card transaction behavior is driven by the information the card Issuer needs to process and approve or decline a transaction.
  – Contact chip card
    o Insert card face up into chip reader
    o Leave card in terminal
    o Enter PIN or sign receipt
    o Remove card
  – Contactless chip card
    o Wave card in front of contactless reader
    o Enter PIN or sign receipt, if prompted

Bank of Hawaii Confidential
Chip Card Transaction

• First Data Demonstration

Tampered Devices
PCI (Payment Card Industry) Standards

The devices (terminals and PIN Pads) must have physical security on the device where the terminal can detect if it’s being tampered.

The First Data terminals will prompt *VIOLATED*, at which point the device will have to be replaced.
October 1, 2015
Counterfeit Card and Lost or Stolen Fraud Liability shift, not mandate

- Liability shift applies to card-present transactions since the chip card must be read.
- Liability for transactions generally will shift to the party that has the weaker authentication method
  - Issuer if card does not have an EMV chip
  - Merchant if terminal does not read the EMV chip
- Liability shifts to Issuer for contactless card transactions, including Apple Pay
- Ecommerce and other card-not-present fraud expected increase as they become the weaker payment channel.

October 1, 2015
Counterfeit Card and Lost or Stolen Fraud Liability shift, not mandate

- The liability shifts are not mandates but are there for protection
- Bank of Hawaii wants to ensure merchant customers are aware of the liability shifts and take advantage of them
- The October 1, 2015 liability shift date still applies to merchants who are using Point-of-Sales, Cash register system or gateway. The liability will shift to the merchant if the POS device does not read the chip if a chip card is presented.
EMVCo

Major card brands

• EMV® originally referred to the founding organizations from 1994—Europay, MasterCard and Visa that established chip card standards.

• Today the EMV® trademark is owned by all of the equity owners of EMVCo: American Express, JCB, Discover, MasterCard, UnionPay, and Visa.

• EMVCo maintains the EMV® Specifications and related testing processes.
October 1, 2015

Counterfeit card liability shift

- The counterfeit liability shifts for Accel, American Express, China UnionPay, Discover, MasterCard, NYCE Payments Network, SHAZAM Network, STAR Network and Visa networks for the U.S. are summarized in the following chart:

<table>
<thead>
<tr>
<th>Chip Capability: Card</th>
<th>Chip Capability: POS</th>
<th>Counterfeit Liability after October 2015 Lies with:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magnetic stripe only card</td>
<td>Terminal not enabled for contact chip</td>
<td>Issuer</td>
</tr>
<tr>
<td>Magnetic stripe only card</td>
<td>Contact-chip-enabled</td>
<td>Issuer</td>
</tr>
<tr>
<td>Chip card</td>
<td>Contact-chip-enabled</td>
<td>Issuer</td>
</tr>
<tr>
<td>Counterfeit magnetic stripe card with track data copied from a chip card</td>
<td>Terminal not enabled for contact chip</td>
<td>Acquirer/Merchant</td>
</tr>
<tr>
<td>Counterfeit magnetic stripe card with track data copied from a chip card</td>
<td>Contact-chip-enabled</td>
<td>Issuer</td>
</tr>
</tbody>
</table>

*Data from a contact chip card.

October 1, 2015

Lost or Stolen Fraud liability shift

- The lost or stolen liability shifts for American Express, Discover and MasterCard for the U.S. are summarized in the following chart:

<table>
<thead>
<tr>
<th>Chip Capability: Card</th>
<th>Chip Capability: POS</th>
<th>Lost/Stolen Liability after October 2015 Lies with:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magnetic stripe card</td>
<td>Any terminal type</td>
<td>Issuer*</td>
</tr>
<tr>
<td>Chip card, PIN-prefering CVM (online or offline)</td>
<td>Terminal not enabled for contact chip</td>
<td>Acquirer/Merchant**</td>
</tr>
<tr>
<td>Chip card, signature-prefering CVM</td>
<td>Terminal not enabled for contact chip</td>
<td>Issuer***</td>
</tr>
<tr>
<td>Chip card, signature-prefering CVM</td>
<td>Contact-chip-enabled, signature CVM (no PIN capability)</td>
<td>Issuer</td>
</tr>
<tr>
<td>Chip card, PIN-prefering CVM (online or offline)</td>
<td>Contact-chip-enabled, signature CVM (no PIN capability)</td>
<td>Acquirer/Merchant</td>
</tr>
<tr>
<td>Chip card, signature-prefering CVM</td>
<td>Contact-chip-enabled, PIN CVM (online and/or offline)</td>
<td>Issuer</td>
</tr>
<tr>
<td>Chip card, PIN-prefering CVM (online or offline)</td>
<td>Contact-chip-enabled, PIN CVM (online and/or offline)****</td>
<td>Issuer</td>
</tr>
</tbody>
</table>


Bank of Hawaii Confidential.
October 1, 2015
Lost or Stolen Fraud liability shift

* Magnetic stripe liability shift rules apply.
** If PIN was prompted and approved, magnetic stripe liability rules apply.
*** Loss or stolen liability shift applies to any legitimate card that are lost or stolen based on issuer determination.
**** Payment networks have slightly different policies. In the U.S., if MasterCard and Discover, if a merchant decides to support PIN, the terminal must support both online and offline PIN. In the U.S., for American Express, the merchant terminal can support either offline PIN, online PIN or both. In all three cases, the issuer retains liability if a fraudulent lost or stolen PIN-preferred chip card is used at a chip-able terminal that supports PIN.


Further reading
Resources

• EMVCo
  – www.emvco.com

• EMV Migration Forum
  – www.emv-connection.com
Installation date

- Please follow the terminal set up instructions on the next slide to install on September 21.
- Once you have completed the installation, you are ready to use your chip enabled terminal.

Terminal set up

1. Remove the back cover from the terminal.
2. Plug in the phone line into the blue ‘Phone line port’ located on the back of the terminal.
3. If you have a PIN pad, plug in the PIN pad cord into the top USB port.
4. Lastly, plug in the power cord into the terminal which is located on the side of the terminal.