EMV Implementation Guide
# Table of Contents

1. Introduction ............................................................................................................. 2
2. What is EMV? ............................................................................................................. 2
3. How is a chip card different? ..................................................................................... 2
4. How do EMV and chip cards provide security? ....................................................... 3
5. How does the liability shift work? ............................................................................. 4
6. Are contactless payments EMV compliant? ............................................................ 5
7. How is debit affected by the switch to EMV? .......................................................... 5
8. Do I need special equipment for EMV? ................................................................. 5
9. How will iQmetrix implement EMV? ........................................................................ 6
10. How does iQmetrix become certified for EMV? .................................................... 7
11. How does EMV affect my PCI compliance? ............................................................. 8
12. Will I need to provide training to customer facing employees? ............................. 9

Resources..................................................................................................................... 9
1. Introduction

EMV will be making its debut in the United States beginning in 2015. As it will be a required standard for payment security, this change carries many implications for retailers. iQmetrix intends to upgrade its current payment infrastructure to support and certify EMV compliance to enable acceptance across its entire customer base. Described within this guide are various answers to EMV questions iQmetrix has encountered during its strategic and development work towards EMV deployment. The purpose of this guide is to explain to retailers how EMV impacts them and how to ready themselves for new hardware and processes required for proper EMV implementation.

2. What is EMV?

EMV (Europay MasterCard Visa) is the name of the global standard for chip payment cards and is based on widely used and highly secure smart card technology. All EMV specifications are maintained by EMVCo, a working group that represents all major card brands. It is the global standard for card processing and has been in use in Europe for over a decade and in Canada for seven years. Use of EMV provides additional security over the current swipe card transaction model. Chip payment cards are standard-sized bank cards that have a microprocessor, or a mini computer embedded in the card that meet requirements of the EMV standard. Today, the U.S. is in the midst of migrating to chip payments. The U.S. market is larger than all of Europe’s payments markets combined, making it the largest individual market to convert to chip cards. After October 2015, the payment brands will shift the responsibility for any payment-transaction fraud to the party using the least secure technology. If neither or both parties are EMV compliant, the fraud liability remains the same as it is today.

3. How is a chip card different?

EMV is the global technology standard used on chip cards; and the term is synonymous with Chip cards. Chip cards are very similar to cards in use today but have a computer chip embedded into the left hand side of the card. All other features on the card remain the same: card brand, primary account number, card holder name and expiry on the front; magnetic track, CVV2, and signature line on the back. When chip cards are used for payment, the card must be inserted (chip up) into the slot on the payment device and remain there until the device displays “Please Remove Card” at the end of the transaction. This is required because of security features that modify data on the card once the transaction has completed. If a chip card is removed during a transaction, the process will fail and a reversal is sent to the card issuer to reverse the transaction. Some chip cards may require a PIN before approving the transaction while others will only require a signature. If a PIN is required, the payment terminal will automatically
ask the card holder to enter it. If the card only supports signature, the payment terminal (if it supports signature) will ask for a signature or print a signature line on the receipt. Signatures should be compared to the signature on the back of the card.

4. How do EMV and chip cards provide security?

The embedded microprocessor (computer) in a chip card provides strong transaction security features and other application capabilities not possible with traditional magnetic stripe cards. Chip payment technology prevents counterfeit card fraud in two ways:

- The first way is the storage of the cardholder data and security keys inside the chip. Even if chip data were to be copied, it could not be used to create another chip card using the same data.
- The second way is by a one-time, unique code, called a cryptogram, generated by the chip during each payment transaction. The cryptogram proves that the card is authentic and that the transaction data was unique to that card. Therefore, any use of the same unique card data would be detected by the issuer and the transaction denied.

EMV chip transaction data excludes other data needed for magnetic stripe transactions, so it cannot be used to make a fraudulent transaction in an EMV or magnetic stripe environment. Chip cards also allow for four types of cardholder verification methods (CVM):

- Chip and Signature: Customer signs to validate they are the cardholder – this prevents counterfeit card fraud.
- Chip and Offline PIN: Chip card and terminal validate the PIN on the device before proceeding to authorize the transaction – this prevents counterfeit, stolen, never received or issued card fraud.
- Chip and Online PIN: The PIN entered by the cardholder is sent online to the card issuer to validate the cardholder, then proceeds to authorize the transaction – this prevents counterfeit, stolen, never received or issued card fraud.
- No CVM: Frequently used for contactless EMV transactions. “No CVM” scenarios are still protected against counterfeit use and replay attacks with the data, but not from stolen reuse.
5. How does the liability shift work?

The October 2015 liability shift applies to all merchants and card issuers. There are two main types of fraud to consider for the shift, counterfeit and lost/stolen cards. Today, the card issuer would assume liability unless, through the chargeback mechanism, the merchant cannot prove they validated the card holder at the time of the transaction.

Counterfeit Fraud Shift:

- Visa, MasterCard, American Express and Discover are participating.
- Merchants are not liable if they use an EMV-capable payment terminal that can accept contact or contactless chip cards. If the payment terminal is not EMV-capable, it is treated as a swipe card.
- Cards without chip (swipe card) remain the same as they are today – it is up to the merchant to verify the card holder and assume the liability for this type of fraud.

<table>
<thead>
<tr>
<th>Card Capability</th>
<th>Payment Terminal Capability</th>
<th>Fallback Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chip and PIN</td>
<td>Issuer</td>
<td>Merchant</td>
</tr>
<tr>
<td>Chip and Signature</td>
<td>Issuer</td>
<td>Merchant</td>
</tr>
<tr>
<td>Magnetic Stripe</td>
<td>Issuer</td>
<td>Issuer</td>
</tr>
</tbody>
</table>

Lost and Stolen Fraud Shift:

- MasterCard and Discover are participating.
- Merchants are not liable if they use an EMV-capable payment terminal that can accept PIN entry when processing chip cards. Merchants are also not liable if a lost/stolen PIN was used at the EMV-capable payment terminal.

<table>
<thead>
<tr>
<th>Card Capability</th>
<th>Payment Terminal Capability</th>
<th>Fallback Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chip and PIN</td>
<td>Issuer</td>
<td>Merchant</td>
</tr>
<tr>
<td>Chip and Signature</td>
<td>Issuer</td>
<td>Issuer</td>
</tr>
<tr>
<td>Magnetic Stripe</td>
<td>Issuer</td>
<td>Issuer</td>
</tr>
</tbody>
</table>
Please note: Merchants using a terminal capable of chip and PIN cardholder verification will be covered under both types of liability shift.

6. Are contactless payments EMV-compliant?

Contactless cards and NFC-based mobile wallets work in either EMV or magnetic-stripe mode and depend on the capabilities of the terminal. All major card brands have developed an implementation of contactless payment and iQmetrix will be certified for both contact and contactless EMV. If a card is not passing EMV-compliant information (i.e. some contactless cards are not EMV-compliant), it would be considered a swipe transaction for liability shift concerns.

7. How is debit affected by the switch to EMV?

Debit cards are moving to EMV, however, the change has been slower than for credit based cards. While major credit-branded debit cards have announced a specification required to support them at the terminal, U.S. debit networks are taking longer to establish this specification. At the time of this writing, the debit specification has been released to processors/acquirers who then need to build acceptance into their solutions. Once they have completed their work, they will release documents outlining the specification that iQmetrix will consume in order to support EMV debit. To date, there has been no announcement of a liability shift for debit transactions. However, an announcement is expected in October 2015 along with the credit liability shift.

8. Do I need special equipment for EMV?

In order to accept EMV, you will need to use an EMV-capable terminal that iQmetrix has developed for and certified with, along with the processor you use and EMVco (payment card brands). At the time of this writing, iQmetrix will support the VeriFone MX915 for EMV certification with all the processors with which they are
partnered. iQmetrix expects more devices to be added to the list as the EMV liability shift nears. iQmetrix will likely also support an Ingenico line of devices including the ISC250 counter top devices and ISMP/ICMP mobile devices. Using an off-the-shelf EMV device will not be supported by iQmetrix software applications.

9. How will iQmetrix implement EMV?

iQmetrix started the process of becoming EMV compliant over the last year. This included hiring knowledgeable staff to head the EMV technology push, as well as training for all payment developers and testing staff for EMV specific projects. iQmetrix worked with industry leaders to build out its path to EMV, including device integration, contact and contactless support, and realistic timelines for certification to be completed before the 2015 credit card liability shift. As with all industry pushes, iQmetrix is following and monitoring the migration in detail to ensure it meets the needs of merchants and provides an excellent experience at the point of payment. For the most part, RQ users should not see any change in how the system works. Only how the consumer uses their card should change.

EMV debit is almost ready for consumption but delays within the domestic debit group have caused delays in iQmetrix’s processors’ ability to build out the required infrastructure to support it. iQmetrix expects that its partner processors will be ready to release their EMV debit documents in early Q2 of 2015 and the company’s development effort will begin shortly after that. iQmetrix’s choice of devices will support both credit and debit EMV.

As iQmetrix completes development of EMV components, they will be included in RQ releases. Once development has been wrapped up, iQmetrix will begin the certification effort for all its processing partners. For more information on certification, see the “How does iQmetrix become certified for EMV?” section below.

Key Components to EMV development:

<table>
<thead>
<tr>
<th>Component</th>
<th>Status</th>
<th>Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>iQmetrix Payment API</td>
<td>Ready</td>
<td>Nov. 2014</td>
</tr>
<tr>
<td>MX915 EMV Integration</td>
<td>On Track</td>
<td>Early Jan. 2015</td>
</tr>
<tr>
<td>Paymentech EMV Message Spec (Class B)</td>
<td>On Track</td>
<td>Early Feb. 2015</td>
</tr>
<tr>
<td>Elavon EMV Message Spec (Class B)</td>
<td>On Track</td>
<td>Mid Feb. 2015</td>
</tr>
<tr>
<td>Heartland EMV Message Spec (Class B)</td>
<td>On Track</td>
<td>Mid Feb. 2015</td>
</tr>
</tbody>
</table>
10. How does iQmetrix become certified for EMV?

Initially, iQmetrix will complete a new Class B certification with each processor/acquirer. Once this is complete, it will enter the EMVco payment brand certification. iQmetrix will work with each acquirer to run EMVco test cases using the industry approved Collis test kit. When completed, the acquirer portion of data obtained from the tests is submitted for approval by EMVco. The time from starting Class B to EMVco approval is expected to last up to 150 days; iQmetrix plans to launch simultaneous certifications in order to complete the process as quickly as possible. Once certifications are received, iQmetrix will enable the components for use at the workstation. These EMVco certifications cover the entire transaction flow from the device to the issuer, to ensure proper procedures and management of EMV data throughout the transaction lifecycle. A new certificate must be obtained for each new device iQmetrix chooses to support.

Certification Timelines:

<table>
<thead>
<tr>
<th>Component</th>
<th>Status</th>
<th>Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paymentech EMVco certification MX915</td>
<td>On Track</td>
<td>Late Aug. 2015</td>
</tr>
<tr>
<td>Elavon EMVco Certification MX915</td>
<td>On Track</td>
<td>Late Aug. 2015</td>
</tr>
<tr>
<td>Heartland EMVco Certification MX915</td>
<td>On Track</td>
<td>Early Sept. 2015</td>
</tr>
<tr>
<td>First Data EMVco Certification MX915</td>
<td>On Track</td>
<td>Mid Sept. 2015</td>
</tr>
</tbody>
</table>

*Once certification is complete, iQmetrix can enable the service the next day.
11. How does EMV affect my PCI compliance?

While EMV transactions provide enhanced security, card data is still present on the card. Additionally, cards with problem chips could lead merchants to require a swipe and run a transaction as a “fallback” – in that case, full card data is read and the enhanced security of EMV can’t be enforced. All card-accepting merchants will still be required to be PCI-DSS compliant and when required, and an audit must be performed to obtain certification. Compliance vs. certification is based on the number of transactions and the network you’ve built to support your stores.

EMV acceptance does have the opportunity of some PCI relief, in particular, to the audit portion of your PCI program. See the chart below for PCI relief from each card brand.

<table>
<thead>
<tr>
<th>Card Brand</th>
<th>% of EMV Transactions Required</th>
<th>Relief</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa</td>
<td>75%</td>
<td>More than 75% of transactions from an EMV compliant POS terminal, merchant may apply for relief from the audit requirement of their PCI compliance.</td>
</tr>
<tr>
<td>MasterCard</td>
<td>75%</td>
<td>More than 75% of transactions originate from EMV compliant POS terminals, the merchant is relieved of the audit requirement of their PCI compliance.</td>
</tr>
<tr>
<td>American Express</td>
<td>75%</td>
<td>Merchants will be eligible to receive relief from PCI Data Security Standard (DSS) reporting requirements if the merchants’ POS acceptance locations, where 75% of their transactions occur, are enabled to process American Express EMV chip-based contact and contactless transactions.</td>
</tr>
</tbody>
</table>

*You should review your PCI compliance options with your security assessor or auditor before taking actions that could put you out of compliance.
12. Will I need to provide training to customer facing employees?

While the operations of RQ will remain consistent with the current experience at the point of payment, there are new devices, prompts and procedures for your customers to follow. These prompts and procedures should be similar for each of iQmetrix’s partner processors, but different card issuers can allow for different types of cardholder verification. Some may ask for a PIN and when used, signatures are not required, while others will only require a signature to complete the transaction. In either case, the PIN pad display should guide the customer and the RQ display will guide the employee on what to do next. Each acquirer/processor provides additional information about EMV acceptance and procedures for proper EMV acceptance at the terminal.

Resources

EMVco: http://www.emvco.com/

EMV Connection: http://www.emv-connection.com/

Chase Paymentech: https://www.chasepaymentech.com/faq_emv_chip_card_technology.html


Heartland: http://www.heartlandpaymentsystems.com/Heartland/files/e0/e08a3e0d-1738-4593-a84d-8143e2601e0a.pdf

First Data (Bank of America): http://www.firstdata.com/emv/emv-for-merchants.html