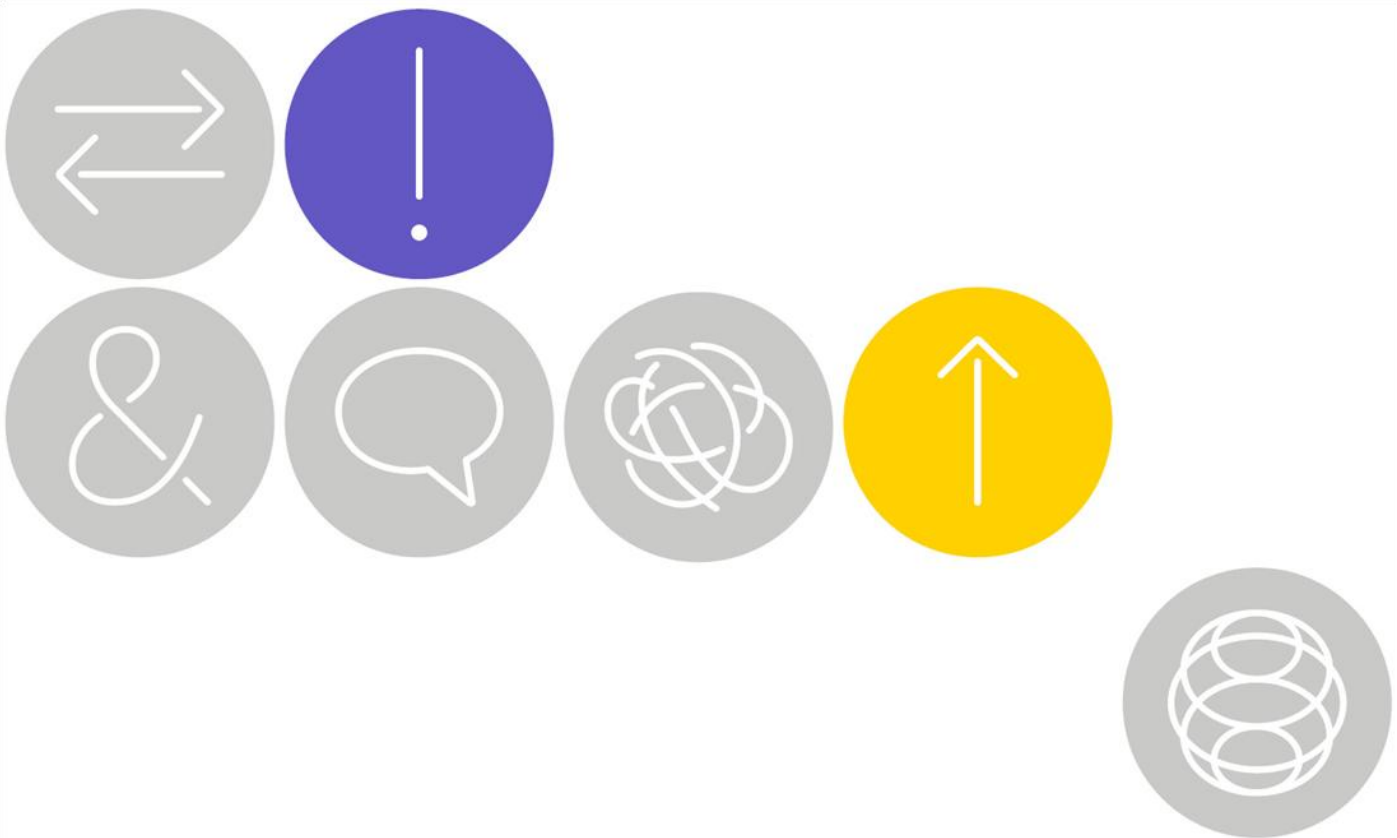


EMV Frequently Asked Questions for Merchants

May, 2014





EMV Overview

Q. What is EMV?

A. EMV is an Integrated Circuit Card Specifications for payment systems. It was developed jointly by Europay, MasterCard and Visa in the mid-1990s. EMV helps to facilitate interoperability between chip cards and terminals for both credit and debit transactions. EMV is also known as “Chip Cards”, “Smart Cards”, or “Chip and PIN”.

Q. What are the features of the Chip?

A. The chip stores information, performs processing, contains secure elements which store secret information and performs cryptographic functions.

Q. Why EMV?

A. EMV protects against counterfeit fraud through authentication of unique data that resides on chip cards, smart phones, and other devices. EMV also provides risk management parameters at the card level and offers both online and offline PIN to help protect against fraud due to lost and stolen cards.

Q. What changes with EMV for a merchant?

A. Many different parts of the payment process changes when moving from a magnetic stripe transaction to an EMV transaction:

1. The process flow of a transaction changes due to the use of dynamic authentication of the card
2. To achieve the dynamic authentication, an EMV capable terminal is required with an EMV reader. Merchants may also support contactless transaction devices when updating to the EMV reader.
3. In order to complete the transaction, the card will have to stay in contact with the chip reader throughout the entire transaction.
4. With the addition of dynamic authentication, there are new message requirements including Data Element 55 that carries the EMV information.

Q. When will chip cards start to show up at US merchants?

A. There are over 1 billion EMV cards in the world today. Merchants have probably already seen an EMV card and did not realize it. Most EMV cards still have a mag-stripe on the back of the card, so while the cards are at US merchants the current process on how they are used has not changed. If a merchant is in a tourism market, EMV cards have probably been presented many times since most other developed countries in the world are using EMV.



Q. What is the transaction flow of an EMV Transaction?

A. The following is an overview of the EMV transaction flow:

1. Application Selection
 - The card and the terminal decide which applications stored on the chip will be used when processing the transaction
2. Initiate Application Processing and Read Application Data
 - After all applications are identified the terminal reads all data related to the selected application.
3. Offline Data Authentication
 - If the card and terminal support Offline Data Authentication, they work together to validate the authenticity of the card.
4. Processing Restrictions
 - Checks are performed to confirm the chip is allowed to do the transaction requested.
5. Cardholder Verification
 - Cardholder verification is determined based on the card and the terminal. The verification may be Offline PIN, Online PIN, Signature or No CVM.
6. Terminal Risk Management
 - The terminal performs several checks (such as floor limit) to determine whether there is a requirement for online processing.
7. Terminal Action Analysis
 - The terminal will then request to go online or it will request an offline approval.
8. Card Action Analysis
 - The card will decide if it will approve the transaction offline or go online.
9. Online Processing
 - If the chip requests to go online the terminal builds an online request for authorization and online card authentication; the transaction request is then forwarded to the selected payment authorizer.
10. Completion and script processing
 - Transaction completed and all issuing scripting back to the card occurs.



Transactions

Q. Will customers with magnetic stripe cards be able to use EMV terminals?

A. Yes, the EMV terminals certified by Vantiv will also have a magnetic stripe card reader.

Q. Can an EMV card be used in a magnetic stripe terminal?

A. Yes, for the foreseeable future credit and debit cards will be issued with a chip on the front of the card and the familiar magnetic stripe on the back of the card so that chip cards can be backwards compatible with existing non-EMV capable devices.

Q. Do EMV transactions take longer to process than magnetic stripe transactions?

A. EMV transaction times are highly dependent on how the issuer has personalized the card and how the merchant configures the terminal. If the card or the terminal has not been configured in an efficient manner, transaction times will increase. If the card and terminal are properly “tuned” the actual transaction time should be close to what a merchant experiences today. However, the overall time in lane will increase due to the additional interaction the cardholder has with the transaction.

Q. What are issuer scripts and how will they affect my transaction processing?

A. Issuer scripts are small files sent from the issuer to the card as part of the authorization response message. They will not affect transaction processing and merchants cannot implement means to prevent them from being sent to the card.

Q. Since the customer has to leave their card in the terminal during the transaction, what can be done to reduce the number of cards forgotten in the terminal?

A. Vantiv recommends that merchants do not print the customer’s receipt until after the card has been removed from the card reader and/or program the terminal to produce an audible beep when the card should be removed.

Q. What is a dual-interface card?

A. A dual-interface card is one that supports both contact (via the chip plate on the front of the card) and contactless transaction processing via an embedded antenna and transmitter.



Visa:

Cardholder Receipt Requirements

- EMV and Visa require that the terminal should always print the AID and Application Label (or Application Preferred Name) on the receipt.

Discover:

- When printing a receipt, the terminal must be fully compliant to [EMV 4.2-4, Section 11.4], as well as the relevant operating regulations, policies, and agreements.

Amex:

- Transaction Data Source (e.g. Swiped, Manual Entry, Chip) – Mandatory
- AID – Mandatory
- Application Preferred Name – Conditional (Where the application preferred name is present and the Terminal supports the relevant Issuer code table index, then this data element is mandatory)
- Payment Brand Name/Application Label – Mandatory
- PIN Statement (Only required for PIN) e.g., PIN Verified, PIN Locked – Conditional
- Cryptogram Type/Value – Preferred (best practice)



Processing

Q. When do I need to be EMV compliant?

A. While there is no specific mandate from the card brands to be EMV compliant, merchants need to be EMV certified (or using pre-certified devices) by October, 2015 in order to avoid any impact from the counterfeit fraud liability shift.

Q. What EMV changes are there to the Vantiv authorization and clearing message specifications?

A. EMV requires additional data elements to be included in the authorization message. The majority of the EMV relevant data is contained in Field 55 of the ISO 8583 message specification (Note: The field name containing the EMV data may vary among different message specs, but “Field 55” is the commonly used term in the industry). There are new values for the POS Entry Mode and Additional POS Data fields. The clearing message will contain new data elements, but the authorization message is the source of this data. The Vantiv message format specifications have been updated to include the requirements of all the networks. Merchants will need to populate the data elements created between the card and the terminal into the message format and pass the entire message to Vantiv and Vantiv will parse out the data to the networks.

Q. What is “offline” processing?

A. There are a few different offline processes that are possible with EMV; Offline CAM (Card Authentication Method), Offline PIN and Offline Approval. In Offline CAM, the card provides a digital signature that the terminal can verify using public key cryptography to determine if the card is genuine. This is considered offline since the terminal determines the card’s validity without going online to the issuer. Offline PIN is a cardholder verification method (CVM). Similar to Online PIN, it is used to verify the cardholder is a legitimate user of the card. In Offline PIN, the card uses a PIN stored in secure memory on the chip to compare to the PIN entered by the cardholder. The PIN may be sent in plain text or encrypted. In Offline Approval, the card and the terminal run through a series of risk management steps to determine whether to approve the transaction, decline the transaction or send the transaction online for decisioning. It is anticipated that the majority of implementations in the U.S. will initially not support Offline Approval and will always go online.

Q. What is “fallback”?

A. There are two types of fallback; technical fallback and CVM (Cardholder Verification Method) fallback (or PIN Bypass). Technical fallback occurs when there is an issue with the card or the terminal that prevents the two from successfully communicating. If the terminal cannot read the chip, the transaction can “fallback” to a magnetic stripe or key-entered transaction. Depending on how the terminal is configured, multiple attempts to read the chip may be required before fallback is allowed. CVM fallback



occurs when the cardholder cancels out of entering their PIN (PIN Bypass) in favor of a signature transaction. Whether or not this is allowed depends on the configuration of the terminal.

Q. What happens to the Terminal Verification Results during technical fallback?

A. Technical fall back is based on the terminal and card not being able to communicate. If the terminal cannot read the chip, the terminal will "allow" the card to be swiped. In this case, there would be no TVR since there was no interaction between the chip and the terminal to create the TVR.

Q. Does EMV impact Reauthorization?

A. Reauthorization occurs after the card is no longer in the terminal, but EMV data such as the cryptogram needs to be passed to Vantiv for the reauthorization attempt.

Q. Does EMV impact Full Matching?

A. Full matching is the process whereby a settlement record is compared to its corresponding authorization request and any missing data in the settlement record is populated from data in the authorization request where available. Full matching will not be supported for EMV transactions.

Q. Does EMV impact Least Cost Routing (BIN Matching)?

A. At this point, transaction routing will still be based on the BIN (or an extended BIN). The debit solution framework released by the EMF allows merchants to continue to enjoy the benefits of least cost routing.

Q. Does the adoption of EMV eliminate the need for end-to-end encryption or tokenization?

A. No, since EMV does not encrypt all of the transaction data (including the PAN), end-to-end encryption and tokenization are still valuable tools in securing payment data.

Q. Are Tokenization and Point-to-Point Encryption (P2PE) options with EMV?

A. Vantiv will support EMV with P2PE and Tokenization in 2014.

Q. How does EMV affect interchange?

A. At this point, EMV has no impact on the interchange qualification of a transaction.



Q. How does EMV impact my card not present business?

A. Card not present transactions are currently not in the scope of EMV. Since there is no card-terminal interaction, no cryptogram is created (a cryptogram is an alphanumeric value that is the result of data elements entered into an algorithm and then encrypted commonly used to validate data integrity). However, the industry is exploring options for using EMV features in online/CNP environments.

Q. How does EMV work with tablet-based POS systems?

A. A wired or wireless PIN pad (WPP) that will accept an EMV card and NFC (Near Field Communication) for wireless will be connected to the tablet. The purchase amount would be transmitted to the PIN pad which would in turn prompt for card insertion/PIN and communicate the transaction to the Vantiv front end or the merchant's host depending on how the system is configured.

Q. Does EMV require a PIN be entered on credit as well as debit transactions?

A. Whether or not PIN is on credit is up to the issuer. Visa has stated that they feel EMV with signature is sufficient, but MasterCard has shown support for PIN. The risk of not supporting PIN is that the merchant could still have chargeback liability if the card supports PIN, but the terminal only supports signature. There is no PIN requirement with the U.S. implementation of the chip, and the issuer will determine if the card will support PIN. Vantiv will support both PIN and signature. MasterCard has also shown support for PIN on credit as the preferred CVM (Cardholder Verification Method). MasterCard, American Express and Discover's liability shifts are based on the highest security level, which means the liability will shift if the card supports PIN but the terminal only supports signature.



PCI (Payment Card Industry)

Q. How does EMV impact PCI requirements?

A. Merchants are still required to maintain on-going PCI compliance, but may be eligible for a waiver of the annual PCI Validation process.

Q. What merchants are eligible for the PCI Validation waiver?

A. MasterCard's program is open to PCI DSS Level 1 & 2 merchants. Visa, Discover and American Express do not call out specific levels, but the annual validation is only required of Level 1 & 2 merchants. In addition, 75% of the merchant's transactions must be processed through EMV-enabled terminals. However, this does not mean that 75% of the transactions must be EMV transactions. The transactions, whether EMV or magnetic stripe, just have to process through EMV-enabled terminals. The terminals must also support both contact and contactless transactions.

Q. Are any EMV-specific fields in the scope of PCI?

A. Tag 57 contains the Track 2 equivalent data. Other than that, there is no other PCI relevant data.

Q. Is there a new PCI SAQ version for merchants with EMV compliant terminals?

A. At this time, there is no unique SAQ for EMV. However, EMVCo has engaged with the PCI Council to identify areas of collaboration.



Terminals

Q. How are devices in an integrated environment supported for EMV?

A. Integrated devices will require the merchant to complete an EMV terminal certification with Vantiv. The merchant will continue to manage the download of applications and updates as they do today. Vantiv is also working with the card brands on a streamlined certification program to make the process more manageable for the merchants and their software partners.

Q. How will existing devices be updated to support EMV?

A. If the terminal is EMV-capable (i.e. it already has an EMV card reader), it can be downloaded with an EMV application once the application is certified. If the terminal is EMV-compatible (i.e. it doesn't have a chip card reader, but can accept an EMV application), the merchant will need a peripheral card reader and download.

Q. Will the magnetic-stripe reader be removed from EMV terminals?

A. No, for the foreseeable future mag-stripe reader will continue to be a feature on EMV terminals. This will allow EMV terminals to process transactions from the large base of magnetic stripe cards in the market and support fallback (terminal can't read the chip) transactions.

Q. What keys are needed for EMV and how are they managed?

A. EMV uses Public Key Infrastructure for Offline data authentication. Unlike PIN keys, the EMV keys can be downloaded like a terminal parameter. The public keys in the terminal are used to facilitate secure communication with the EMV apps on the cards for offline processing. The terminal may authenticate the card is valid using the certificate authority's public keys. The keys are owned and distributed by the card brands so a terminal that supports all four of the major networks would need keys from each one. These keys change periodically and will need to be pushed down to the terminals like any POS update. However, the payment networks each have a set of keys that include keys of 1152 bits, 1408 bits and 1984 bits in length and the 1984 bit keys represent the maximum size that can be accommodated within the EMV structure. So for the members of EMVCo, all expected keys have been published. If all keys are installed at the time of terminal deployment, it is expected that no further key installation will be required, which reduces the logistics of introducing new keys.

Q. When do the keys expire?

A. EMVCo recommends certificate expiration dates. Networks have accepted these recommendations to date, but could choose their own dates if they so desired.



- 1152-bit keys are recommended to have an expiry date of 31 December 2017
- 1408-bit keys are recommended to have an anticipated lifetime to at least 31 December 2023*
- 1984-bit keys are recommended to have an anticipated lifetime to at least 31 December 2023*
- (*The 1408-bit and 1984-bit dates are only “anticipated lifetimes” since EMVCo does not project expiration dates beyond a ten year horizon.)

Q. What terminals will Vantiv support for EMV?

A. The following devices are on the Vantiv roadmap for EMV support:

- Equinox T4205sc, T4210sc, T4220sc, Apollo Series
- Ingenico iCT220, iCT250, iWL222, iWL252, iWL255 – GPRS (all versions of all models), iPP320 PIN Pad
- VeriFone Vx510 (4MB or greater), Vx520 (all versions), Vx570 (all versions)
 - Vx 805 and Vx 820 PIN Pads can also be connected to any of the above devices

Q. Are the mobile card readers that Vantiv deploys EMV-compliant?

A. No, at this time the mobile card readers do not support EMV transactions. However, there are EMV-compliant mobile card readers beginning to enter the market and EMV support is on the Mobile roadmap.



Testing and Certification

Q. When can merchants begin their certification process?

A. Updated message specifications have been released and merchants (or their software partner) can begin making coding changes now. Hardware that is capable of accepting chip cards can also be procured. We anticipate certifications to begin in Q2/Q3 2014.

Q. Will Vantiv offer EMV certification test kits for merchants?

A. EMV certification test kits will be available for Merchants to purchase beginning in Q2/Q3 2014.

Q. If a merchant certifies a path and uses the exact same full path in other locations, does the merchant need to recertify the same path?

A. No, a merchant does not need to recertify if there have been no new changes to the path.

Q. Is Vantiv going to specify which PIN pads/customer facing devices must be used for EMV?

A. Vantiv will pre-certify a number of devices for small to medium-sized business for countertop use, but will not dictate the device types larger merchants or merchants utilizing a payments middleware will use for supporting EMV. The merchant's ISV should provide them with a list of supported devices that can be used for EMV in conjunction with their POS path. This will need to be discussed between the ISV and the merchant.

Q. Are there any technical requirements the device must meet in order to be considered eligible for certification with EMV?

A. Devices must have a current EMVCo kernel levels 1 and 2 certification and have a minimum of PCI PTS 1.3 certification. However, PCI PTS 3.0 or higher is recommended.

Q. I am an existing merchant and am going to be certifying PIN Debit; can I also certify EMV at the same time?

A. No, Vantiv will not certify existing merchants for additional features/functionality in conjunction with EMV. EMV certification must be done as a separate certification.

**New merchants will be required to have a base/standard certification with a separate/secondary certification for EMV.*



Q. How will the eMAF data be changed to include the EMV information?

A. The eMAF will be updated to include the following data elements:

- EMV-capable card
- EMV-capable terminal
- EMV transaction
- Offline authorized

In addition, two new POS Entry Mode values will be supported:

- 01 – Fallback from EMV to manual entry
- 80 – Fallback from EMV to mag-stripe



Support

Q. What EMV changes are there to Direct?

A. Transaction research and chargeback pages will be updated to include additional fields/values that will identify:

- If the card used in the transaction was EMV-capable
- If the terminal used in the transaction was EMV-capable
- If the transaction processed as EMV
- If the transaction was processed “offline”
- If the transaction was processed as “fallback”

Q. What infrastructure changes are needed to support the larger EMV message size?

A. Due to the increased size of the messages, Vantiv evaluated all aspects of our processing to make sure our systems could handle the increase in data. We looked at everything from the max messages buffer sizes to available disk space and made changes as needed. The exact changes Vantiv made would be specific to our systems and wouldn't translate to any specific merchant's system. Each merchant will need to evaluate their systems to determine the impact of the increased amount of data.

Q. Will disputes processors be able to determine if a transaction was EMV or not?

A. Yes, using the screen changes in Direct, disputes processors will be able to determine if the transaction was processed as EMV, if the card was EMV-capable and if the terminal was EMV-capable. Additional updates to disputes-specific screens may also be made in the future, if needed.