THE WHO WHAT AND WHY OF EMV

An NCR white paper

These three little letters have been circling the retail industry for over a year—but what does EMV really mean? Learn about the key parts of this payment technology and how you can prepare your business to accept EMV payments.

1 Who does EMV affect?

2 What is EMV?

3 When will EMV be implemented?

4 Where will it be deployed?

5 Why is EMV important?

6 How does it work?

Sources: http://www.creditcards.com/ ; Payments Source, Payment Security Task Force, Visa, MasterCard, Smart Card Alliance, First Data, CreditCards.com research, Aite Group, PULSE, Yamika

The WHO

Who are the key players in this new transaction space? And how are they affected by the new EMV technology?

Consumers: Shoppers have replaced their previous magnetic stripe cards with new, smart chip cards provided by their bank. Instead of swiping their cards, they now insert (or dip) the cards into the payment machine. Their card stays in their possession during the entire transaction.

Consumers are on a learning curve with the new technology as well. It's important to provide them with easy to use software or well trained staff to help them ease into this new payment style.

1.2 billion

Estimated number of credit and debit cards that have to be upgraded to chip cards

The WHO

Retailer: As a merchant, it's almost impossible to think about EMV technology without thinking about the liability shift. As of October 1, 2015, if there is a fraudulent charge that could have been prevented by a smart chip card, the retailer is now liable as opposed to the bank. Retailers are now encouraged to make sure their POS software and equipment is EMV ready.

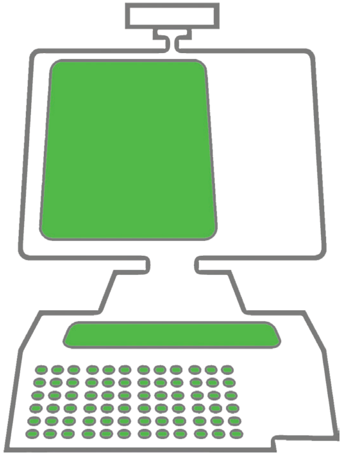
Banks: Banks are responsible for distributing new smart chip cards to their consumers. Also, with the new liability shift, banks are no longer liable for a fraudulent charge that could have been prevented by the smart chip card. Not only do banks have to convert their cards, but they have to prep their software to accept those new cards as well. Most of the larger banks have implemented the new technology but the toll of the change is causing smaller banks to update their systems more slowly.

The WHO

Payment Processors: Part of the complexity of creating EMV is that each payment processor has to be compatible with the new EMV functionality within POS software. Unlike previous certifications, each processor has to individually certify the POS payment software, payment hardware, and firmware on the payment hardware for use with EMV. The merchant must be running the proper make, model, and software version of all payment components in order to accept EMV payments. This complex testing is part of the reason why it's taking some time to roll out EMV functionality.

The WHO

POS System Companies: The point of sale software companies have experienced a steep learning curve with creating, installing and testing new EMV functionality software. With a lot of moving parts, this new technology is now a huge value added to point of sale technology.



15 million

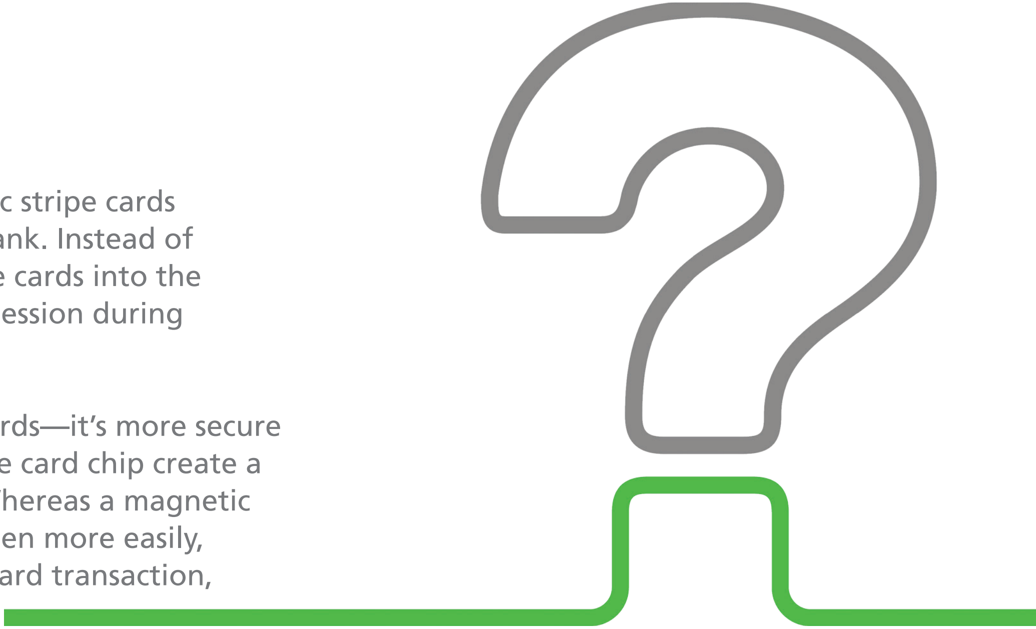
Estimated number of point-of-sale terminals that have to be upgraded to accept chip cards

The WHAT

What exactly is EMV?

Shoppers have replaced their previous magnetic stripe cards with new, smart chip cards provided by their bank. Instead of swiping their cards, they now insert (or dip) the cards into the payment machine. Their card stays in their possession during the entire transaction.

EMV is enabled through a smart chip in new cards—it's more secure than previous magnetic stripe cards because the card chip create a unique transaction code every time it's used. Whereas a magnetic stripe card's data is unchanging and can be stolen more easily, if a hacker stole card information after a chip card transaction, they wouldn't be able to duplicate the data.

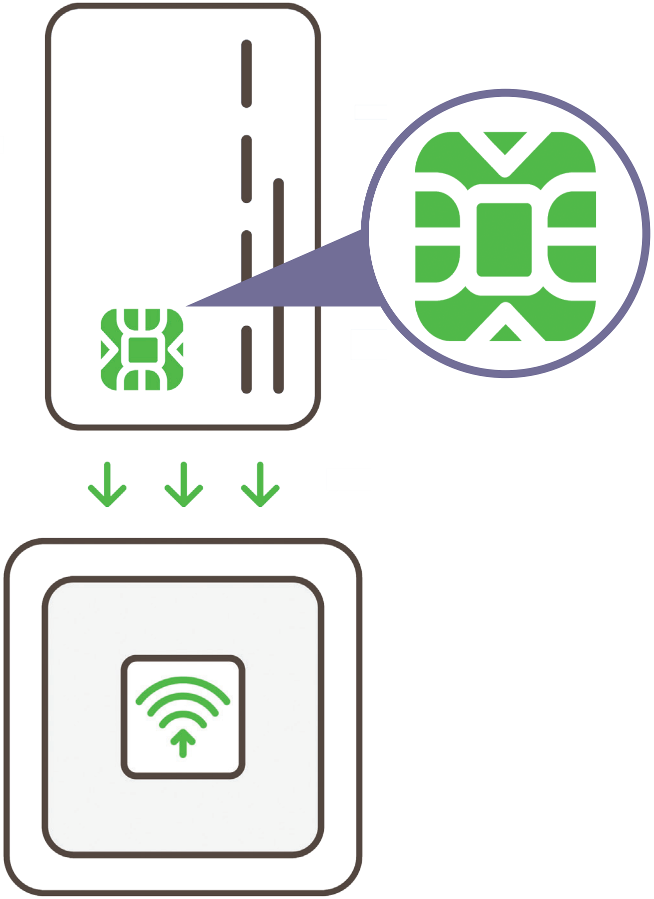


□ ■ □ □ □ □

The WHAT

What are the components of EMV?

- POS capable software
- Terminal reader
- Chip card - EMV enabled cards have several names, but all do the same thing. Some common names include:
  - Smart card
  - Chip card
  - Smart-chip card
  - Chip-enabled smart card
  - Chip-and-choice card (PIN or signature)
  - EMV smart card
  - EMV card



EMV Myth: If you don’t implement EMV, you are liable for all fraudulent electronic transactions.

If you don’t implement EMV, the merchant does not automatically incur liability for all fraudulent electronic transactions. The liability shift applies to whomever is not able to process EMV transactions. If the issuer does not provide EMV capable cards or the acquirer is unable to process EMV transactions the liability will apply to them instead of the merchant.

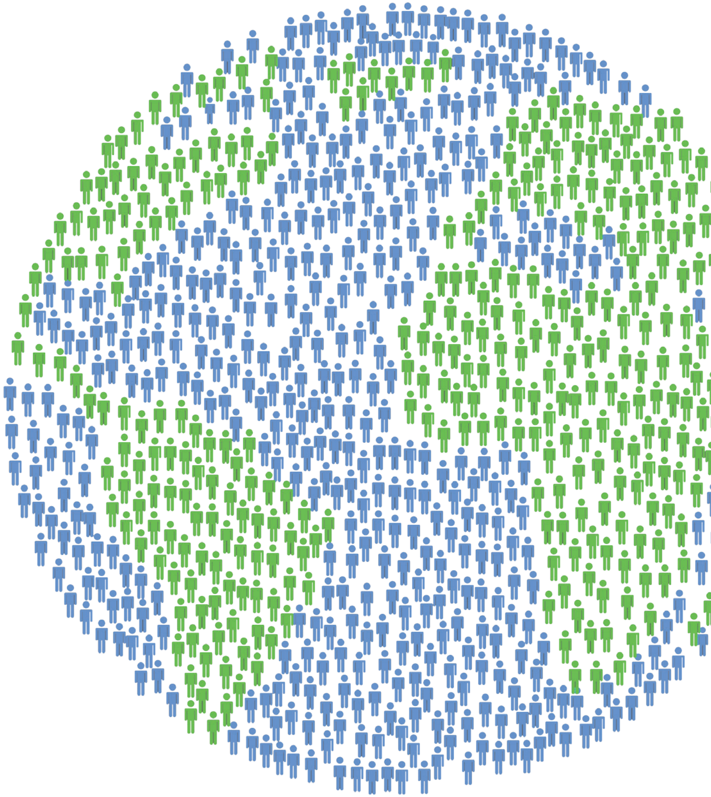
For the liability to shift to the merchant, an EMV card must be processed at the site by an acquirer that supports EMV transactions on a payment terminal that does not support EMV.

The WHERE

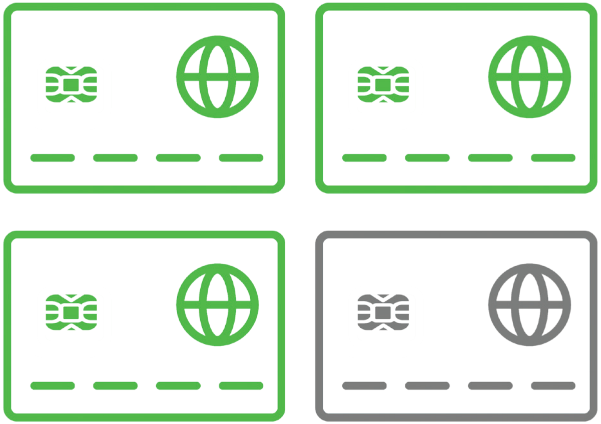
EMV technology has been used for years internationally and is now being introduced into the United States to help prevent fraudulent transactions.

While EMV has been used for years internationally, cards issued in the US are typically programmed differently than in other parts of the world. Most notably US issued credit cards usually, but not always, require only a signature for the cardholder verification method (CVM). Cards issued in the US may sometimes prompt for signature or PIN as the card, device and network negotiate the proper requirements for each transaction. As a result, the typical “signature for credit, PIN for debit” thinking is no longer always the case.

Any business that accepts cards as a payment transaction is now encouraged to install EMV capable software. Grocery stores, gas stations, restaurants and any industry in the retail space are focused on EMV functionality.



The WHEN



EMV will take years to fully roll out and install across businesses in the United States. As of the October 1, 2015 liability shift date, less than 5% of US merchants were prepared to accept EMV cards. With such a complex system, merchants will be focused on rolling out EMV over the foreseeable future.

75% Percentage of US. debit cards that will be issued as EMV cards by the end of 2016

28-30% Estimated percentage of merchant locations currently ready to process chip card payment, per MasterCard and Visa estimates.

EMV Myth: EMV provides P2P Capabilities:

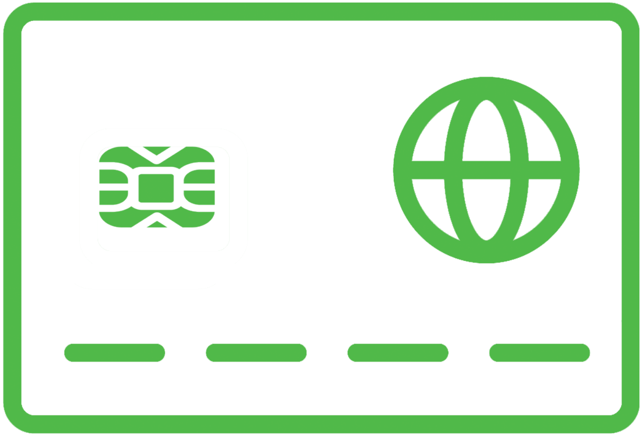
EMV and Point-to-Point Encryption (P2P) are two separate technologies that address different security concerns and require independent implementations. P2PE helps protect card data and keeping it from being readable in the event a merchant’s system is breached. EMV does not encrypt card data, as you noted. EMV data without P2PE is transmitted in clear text, but the dynamic CVV code makes any card data that is stolen less valuable, since it can’t be used elsewhere. It’s worth noting that P2PE protects both EMV and traditional MSR swipe transactions.

The WHY

What are the benefits of installing EMV functionality?

- Less opportunity for fraudulent charges. Merchants and consumers will be able to make and process payments in a more secure environment.

- Reduced liability. As of October 1, 2015 the liability for card—present fraud shifted to whichever party is the least EMV-compliant in a fraudulent payment transaction, thus, the liability will more than likely shift to the merchant. Any merchant that is not EMV capable could incur a very high cost if there is a data breach.



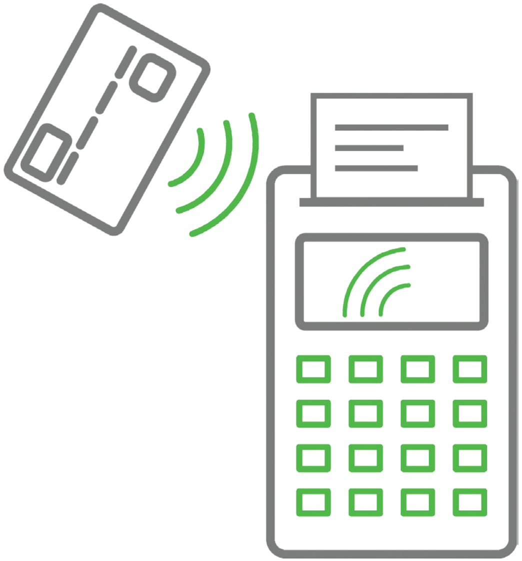
EMV Myth: EMV protects your retail location from a data security breach.

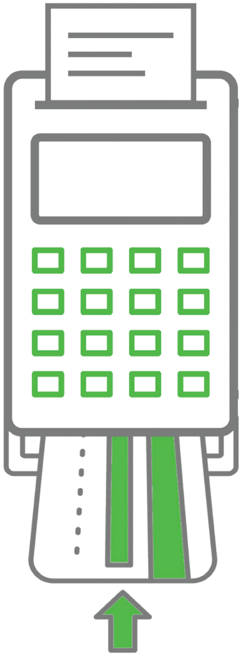
Remember—implementing EMV alone will not protect your retail location from being hacked. While EMV helps protect you from counterfeit card use, it’s not the end-all, be-all of payment card data security. There are measures that you can put into place that are not provided by EMV—such as encrypting credit card data as it passes through your network—that will safeguard your retail location from a data breach as well as give you greater peace-of-mind.

The HOW

How does the card work?

Dipping: Instead of swiping a card, customers insert an EMV card into the POS terminal, much like an ATM. Inserting the card and removing it is called "dipping." Sometimes consumers will still need to enter a PIN code depending on if the card is debit or credit.





Contactless: When using a contactless card, there is no dipping. The card is "tapped" or "waved" against the POS terminal. One quick tap establishes connection and verifies authorization. This technology is starting to be widely accepted in Europe but it will still take some time to rollout in the United States.

The HOW

And how can I, as a retailer, make my business EMV ready?

Begin with talking to your point of sale provider. They are the experts in this new field of technology and will recommend the necessary steps for your business to implement EMV.

$500-$1,000 Average cost of an EMV-compliant point-of-sale terminal

Why NCR?

NCR Corporation (NYSE: NCR) is the global leader in consumer transaction technologies, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables more than 550 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Duluth, Georgia with over 30,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries. The company encourages investors to visit its web site which is updated regularly with financial and other important information about NCR.

NCR Corporation | 3097 Satellite Boulevard . Duluth, Georgia 30096 . USA

NCR continually improves products as new technologies and components become available. NCR, therefore, reserves the right to change specifications without prior notice. All features, functions and operations described herein may not be marketed by NCR in all parts of the world. Consult your NCR representative or NCR office for the latest information. All brand and product names appearing in this document are trademarks, registered trademarks or service marks of their respective holders.

www.ncr.com