ChargeItPro
The ABC's of EMV – Frequently Asked Questions

What is EMV?
Why is EMV being implemented in the United States?
Am I required to support EMV?
How is an EMV card different from a traditional payment card?
Will I need to buy new hardware to accept EMV cards?
Will I still be able to accept traditional credit and debit cards?
How does EMV chip technology work?
How will chip cards impact the checkout experience at my business?
What is the EMV liability shift and how may that affect me?
What does EMV migration mean for card-not-present (CNP) merchants?
What if I have more questions?

What is EMV?

Simply put, EMV (also referred to as chip-and-PIN, chip-and-signature, chip-and-choice, or generally as chip technology) is the most recent advancement in a global initiative to combat fraud and protect sensitive payment data in the card-present environment.

EMV cards are embedded with a microprocessor chip that stores and protects cardholder data. A cardholder's confidential data is more secure on a chip-enabled payment card as it supports dynamic authentication (dynamic values existing within the chip itself that, when verified by the point-of-sale device, ensure the authenticity of the card). EMV technology was introduced in Europe in 1992 and is used throughout the world with more than a billion chip cards in circulation today.

Why is EMV being implemented in the United States?

Credit Card fraud continues to increase in the United States. Current magnetic stripe cards can be easily copied (skimmed) with inexpensive card reading devices allowing criminals to reproduce counterfeit cards. The use of EMV cards is expected to significantly reduce credit card fraud. This benefits both the merchant as well as the card holder.

Am I required to support EMV?

No, you are not required to support EMV in the United States at this time. While EMV cards will continue to have a magnetic stripe to ensure customer can continue to pay on existing hardware, you need to consider that even if your organization hasn't been targeted by high levels of card present fraud in the past, you may be putting yourself at risk in the future, as fraud will migrate to the weakest technology (magnetic stripe) Therefore, you may want to

ensure that your payment processing application and hardware can support EMV card acceptance.

How is an EMV card different from a traditional payment card?

An EMV card looks just like a traditional card with an embedded chip in addition to the standard magnetic stripe on the back of the card. What you see on the card is not the actual microchip but a protective overlay. The microchip provides an additional level of authenticity for the transaction.

Will I need to buy new hardware to accept EMV cards?

To take full advantage of the EMV secure technology you will need to make a one-time investment in new EMV capable hardware. This hardware is available now and ChargeItPro is dedicated to making this transition as painless as possible. Speak to your ChargeItPro representative about your options.

Will I still be able to accept traditional credit and debit cards?

Yes, any hardware provided to you by ChargeItPro will allow you to continue to accept payment cards that are not EMV-enabled.

How does EMV chip technology work?

EMV-enabled hardware will communicate with the processor chip inside the customer's credit card to determine whether or not the card is authentic. Generally, the EMV hardware will prompt the customer to sign or enter a PIN to validate their identity. This process enhances the authentication of both the card and cardholder, effectively reducing the possibility that your business will accept a counterfeit card or be held liable for a fraud-related chargeback.

How will chip cards impact the checkout experience at my business?
To process a chip card transaction, follow these four simple steps:
- Identify whether the card is an EMV card.
- If it's an EMV card, the customer should then insert it into the EMV card reader (slot on the bottom-front of the terminal) and leave it there until the transaction is complete.
- Follow the prompts displayed on the terminal.
- Let the customer complete the transaction by keying in a PIN or signing the receipt.

What is the EMV liability shift and how may that affect me?
Effective October 1, 2015, Visa, MasterCard, Amex, and Discover will institute a liability shift for all POS devices, excluding fuel pumps. With the liability shift, if an EMV card is presented to a merchant that has not adopted a terminal that is certified for EMV card acceptance, liability for counterfeit fraud may shift to the merchant's acquirer – **who may then pass this fee back to the merchant**. The liability shift encourages EMV adoption since any EMV-on-EMV transaction (EMV card read by EMV certified hardware) provides the dynamic authentication data that helps to better protect all parties. In addition, if a counterfeit magnetic stripe card is presented at a chip certified terminal, the liability for the counterfeit fraud will be the responsibility of the card issuer.

What does EMV migration mean for card-not-present (CNP) merchants?
As EMV technology is adopted in the card present space, it is expected that fraud will also shift to the least secure channels, which includes mail order, telephone orders and internet sales. It is important that CNP businesses be prepared for this anticipated shift, as experienced in other regions that have already migrated toward EMV technology. The tools you have in place now may no longer be advanced enough to protect you and your customers. It is recommended that you avoid the use of Address Verification (AVS) and Card Validation Values (CVV) checks as your sole fraud detector since the false positive exposure can be high with these tools alone. You should consider strengthening the value of these tools by supporting additional technology to confirm and mitigate fraudulent activity.

What if I have more questions?
Contact your ChargeItPro sales representative at 800-989-2135 or sales@chargeitpro.com.