

EMV and the Proposed October 2015 “Liability Shift”

This document was created to provide more information on Europay, Mastercard® and Visa® (“EMV”) and the proposed October 2015 “Liability Shift” deadline.

What is EMV?

EMV™ chip technology is the global standard for credit card and debit card payments. Named after its original developers (Europay, Mastercard® and Visa®), this chip technology features payment instruments (cards, mobile phones, etc.) with embedded microprocessor chips that store and protect cardholder data. This standard has many names worldwide and may also be referred to as: “chip and PIN”, “chip and signature”, “chip and choice” or “chip technology”.

What is chip technology?

Chip technology is an evolution in our payment system that will help to increase cardholder security and reduce fraud and fraud-related chargebacks. Chip cards are standard bank cards embedded with a micro-computer chip. Some may require a Personal Identification Number (“PIN”) instead of a signature to complete the transaction process.

What is the pending liability shift?

The pending October 2015 liability shift states that if a chip card is presented to a merchant that has not adopted a chip enabled terminal, liability for counterfeit fraud may shift to the merchant acquirers, such as M&T Bank, instead of the card issuing bank. In accordance with the merchant agreement, this cost is the merchant’s responsibility. This liability shift encourages the adoption of chip enabled terminal since any chip-on-chip transaction (chip card read by a chip certified terminal) provides the dynamic authentication data that helps to protect all parties. 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.

How does EMV chip technology work?

Your EMV-enabled point-of-sale device will communicate with the chip inside the customer's smart card to determine whether or not the card is authentic. The terminal will then 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. It is important to note that the card will remain in your point-of-sale device for the length of the sale so your device should be put in a place that is easy for your customer to access.

What makes EMV different than the traditional magnetic stripe card payment?

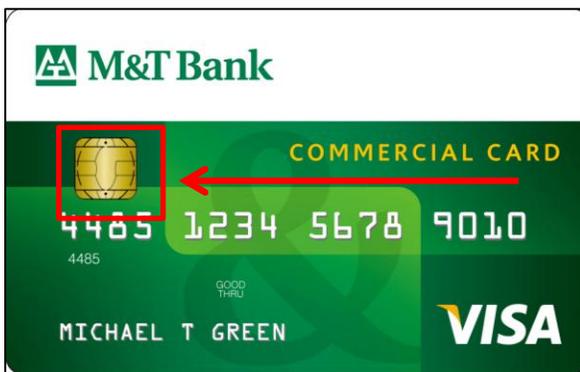
EMV is a global initiative to combat fraud and protect sensitive payment data in the card-present environment. Card data from a traditional magnetic stripe cards can be copied (skimmed) with a simple and inexpensive card reading device – enabling criminals to reproduce counterfeit cards for use in both card present and card-not-present environments. Chip technology is effective in combating counterfeit fraud with its dynamic authentication capabilities (dynamic values existing within the chip itself that, when verified by the point-of-sale device, ensure the authenticity of the card).

Why should I invest in chip card acceptance now?

Preventing the growth of fraudulent activity is one of the main reasons the payment industry is moving toward EMV. Chip cards make it difficult for fraud organizations to target cardholders and businesses alike. As a result, more and more chip cards are being introduced by U.S. financial institutions in order to support and switch over to this technology.

How is a chip card different from a traditional payment card?

A chip payment card looks like a traditional card with an embedded chip (see image below), 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 still be able to accept traditional credit and debit cards?

Terminals will still have a magnetic stripe swipe reader and you can continue to accept payment cards that are not chip-enabled. Chip cards will still have a magnetic stripe during the U.S. migration to EMV, to ensure that customers can continue to pay until all merchants have been given the time to upgrade their equipment.

How will chip cards impact the checkout experience?

To process a chip card transaction, follow these four simple steps:

1. Identify whether the card is a chip card.
2. If it's a chip card, the customer should then insert it into the chip card reader (slot on the bottom-front of the terminal) and leave it there until the transaction is complete.
3. Follow the prompts displayed on the terminal.
4. Let the customer complete the transaction by keying in a PIN or signing the receipt.

How do I know if I need a PIN pad or not?

The card issuing bank sets the requirement for PIN entry at each individual card level. It is in your best interest to use a PIN entry device at your place of business to ensure that protective measures are taken; however, it is not a requirement that you have a PIN entry device. You can still accept the card using the magnetic stripe reader.

Of importance, if you opted to swipe the card because you could not support PIN entry, you may be subject to chargebacks for counterfeit cards or fraudulent activity beginning in October 2015.

Am I required to support EMV?

No, you are not required to support EMV in the U.S. at this time. However, the pending October 2015 liability shift is an item you should consider and the ramifications to your business.

What does EMV migration mean for card-not-present (“CNP”) merchants?

As EMV is adopted in the card present space, it is expected that fraud will also shift to the least secure channels, including card-not-present environments. It's important that CNP businesses be prepared for this anticipated shift, as experienced in other regions that have already migrated toward chip card technology.

As fraud migrates online and fraudsters continue to get more sophisticated, the tools you have in place now may no longer be advanced enough to protect you and your customers. Strategy is key, and it's imperative to take the extra measures to know good customers and good customer behavior (beyond just Address Verification and Cardholder Verification Value checking). It is recommended that you avoid the use of Address Verification and card validation values (security code) 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.

Is this technology unique to the United States?

No. Chip technology standard for payments was first used in France in 1992. Today, there are more than 1 billion chip cards used around the world. The U.S. is one of the few industrialized nations that have not fully transitioned to this technology standard.

What if I have more questions?

The Commercial Service Team is available at 1-800-724-2240, Monday – Friday, 8am – 6pm ET, to help your business with any additional questions.