EMV and the October 2015 “Liability Shift”

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

When is the Liability Shift effective?  
As of October 1, 2015, merchants who cannot accept chip cards are fully responsible for any fraudulent or counterfeit transactions that may occur at the point-of-sale when chip cards are presented.

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 liability shift?  
The 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 that merchant, instead of the card issuing bank. If a counterfeit magnetic stripe card is presented at a chip certified terminal, the liability for the counterfeit fraud will remain the responsibility of the card issuer.

How do I protect my business?  
To protect your business from potential fraud liability you should upgrade your terminal system to a chip enabled system.

How does an increase in system costs to support EMV benefit my business?  
The new POS terminal system will help protect against fraud. It may also help cut down the number of disputes and chargebacks your business may receive.

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. The microchip provides an additional level of authenticity for the transaction.

Will I still be able to accept traditional credit and debit cards?  
Yes, terminals will still have a magnetic stripe swipe reader and you can continue to accept payment cards that are not chip-enabled.
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 a stand-alone terminal with an integrated PIN pad, or the terminal’s magnetic stripe reader.

Please note, if you opt to swipe the card because you could not support PIN entry, you may be subject to chargebacks for counterfeit cards or fraudulent activity beginning October 2015.

What happens if my customer enters an invalid PIN?
The transaction may be declined by the card issuer. Your customer may try the transaction again and sign the receipt instead of inputting a PIN. If the transaction is declined again, advise your customer to use an alternate form of payment and to contact their card issuer for assistance.

What happens if my customer has a chip card and the transaction does not work?
First, make sure the chip is inserted. If it is and the transaction still does not work, have the customer slide their card via the magnetic stripe swipe and sign the receipt. Please note, you should retain this receipt for your records.

Am I required to support EMV?
No, you are not required to support EMV in the U.S. at this time. However, the October 2015 liability shift and the potential ramifications counterfeit fraud could have on your business are items you should carefully consider.

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 shift to the least secure channels, including card-not-present environments. It’s important that CNP businesses be prepared for this shift, as proven in other regions that have already migrated toward chip card technology.

To more fully protect your business, it is recommended that you consider using additional fraud prevention measures in tandem with Address Verification and Card Validation Values (security code) checks, since the false positive exposure can be high with these tools alone. You should seek to strengthen the value of these tools by supporting additional technology to confirm and mitigate fraudulent activity.

What if I have more questions?
The Commercial Service Team is available at 1-800-724-7031, Monday – Friday, 8am – 6pm ET to help you with any additional questions you may have.