What is EMV?

“EMV® is a global standard for credit and debit payment cards based on chip card technology” taking its name from the card schemes Europay, MasterCard, and Visa - the original card schemes that developed it. EMV cards come with an embedded microprocessor that provides heightened transaction security, card authentication and additional capabilities not possible with traditional magnetic stripe cards.

How does EMV technology benefit merchants?

EMV increases security and fraud protection against counterfeit, lost or stolen payment cards. EMV also enables interoperability with the global payments infrastructure. In other words, EMV cards can be used with any EMV-enabled terminal anywhere in the world.

How does EMV help prevent fraud?

The chip on the EMV card is very difficult to duplicate. Each EMV-enabled card contains an embedded smart chip that is programmed by the card issuer to create a unique cryptogram (an encrypted code) for every transaction. This code represents a randomly generated numeral provided by the POS terminal at the time that the purchase amount is keyed in by the cashier. When an EMV chip is used in a transaction, a cardholder verification is triggered and becomes required for authentication via Chip & PIN or Chip & Signature. If connectivity with the card issuer is unavailable during a transaction, the chip determines whether the transaction can be processed offline.

What determines whether an EMV card is Chip and PIN or Chip and Signature?

While Chip and PIN cards will be the norm, some card issuing banks have chosen to issue EMV cards with Chip and Signature. EMV enabled terminals will read the chip on each card presented for payment and determine whether a PIN or Signature is needed based on the card issuer.
What is the timing for EMV in the United States?

October 1, 2015 marks the date on which fraud liability shifts for all non-EMV enabled POS devices (except for automated fuel dispensers at gas stations). U.S. Banks have already started issuing EMV-enabled cards. It is expected that there will be 166 million EMV credit cards and 105 million EMV debit and prepaid cards in circulation by the end of 2015. It is also estimated that 70% of the issuers in the U.S. will have implemented EMV cards by 1st quarter of 2016.

What does the liability shift mean?

Starting October 1, 2015, the party that provides an EMV payment acceptance option will be protected from financial liability originating from counterfeit, lost or stolen card-present transactions. For example, if a chip card is presented to a merchant who has not implemented an EMV-enabled terminal, liability for any counterfeit or fraudulent transactions will shift to the merchant. If a counterfeit magnetic stripe card (non-EMV chip card) is presented at an EMV-enabled terminal, liability will remain with the card issuer.

Am I required to support EMV?

You are not required by law to support EMV at this time. However, you may be putting yourself and your customers at risk, as fraud liability migrates to non-EMV enabled parties. Fraudsters will be targeting businesses who haven’t implemented an EMV solution. BluePay recommends ensuring that your POS terminal(s) are chip-capable and that your payment processing application can accept EMV chip cards.

Who is enforcing EMV?

There is no government entity or authority that is overseeing or enforcing migration to EMV in the US. However, the Payment Card Industry Security Standards Council (PCI SSC) and EMVCo, the official EMV standard governing body, are collaborating with major card issuers on EMV chip technology adoption and implementation in the US. As such, all merchants who are accepting electronic card payments will be required to continue meeting PCI security compliance processes and be subject to the liability shift set forth by card issuers.

How are EMV transactions different?

With EMV, customers will no longer hand over their payment card to a store associate or cashier for processing. Rather, a customer will keep the card in possession at all times. Instead of swiping the card, as traditional magnetic stripe cards allow, the customer will insert the card into the EMV reader and leave the card in the terminal until prompted to remove it.
What happens if merchants don’t upgrade their POS system to EMV?

Starting October 1, 2015, the merchant whose POS system is not EMV-enabled will assume full liability risk for fraudulent card-present transactions when processing chip cards on a non EMV-enabled terminal. Also, migration to EMV is a perfect opportunity for merchants to enhance their electronic payment acceptance by adding additional payment forms including PIN debit, NFC (ex. Apple Pay), and introducing other value-added programs to engage with their customers.

Why do businesses have to worry about counterfeit, lost or stolen card fraud?

As recently published and widely covered card breaches at several large-national retailers in the US have illustrated, card fraud can be extremely costly and damaging to a brand. For a small business, such an incident could be catastrophic. In addition to minimizing the risk of fraud, merchants implementing EMV chip payments in neighboring countries, including Canada and Mexico, have reported significant decreases in fraudulent transactions.

What can merchants do now to prepare for EMV?

To migrate and successfully adopt EMV chip card technology, merchants should identify if the current hardware they are using to process payments is EMV compatible. Many new terminals have a chip card reader included, where only an external pin pad device is needed to enable EMV acceptance. Merchants who are unsure about the compatibility of their current solution or who want more information should contact the BluePay Merchant Services Department to identify what is needed to process EMV payments.

We are here to help you prepare your business for EMV. Please contact us today for any additional questions or concerns.

merchantservices@bluepay.com | 866-739-8324

BluePay
www.bluepay.com