

EMV



Frequently Asked Questions About EMV Technology

Q. “What is EMV?”

A. EMV is the current global standard for payment processing with credit and debit cards. It will soon become the standard in the United States as well. Currently, cardholder information is stored on a magnetic stripe on the back of the card. With EMV, that information, and more, is stored in a chip embedded in the front of the card.

Q. “Do you support EMV-compatible equipment?”

A. Yes, we offer the most up-to-date equipment available on the market; merchants may upgrade their equipment now to prepare for EMV acceptance as soon as it becomes standard.

Q. “How does EMV work?”

A. EMV is chip-based transaction processing that focuses on the security of point-of-sale (POS) transactions, with an end goal of reducing duplicate card fraud and enabling other cardholder validation methods. Rather than swiping a magnetic stripe card through the magnetic stripe reader, customers insert the card into the chip reader to enable the POS equipment to interact with the chip in the card.

Q. “What is duplicate card fraud?”

A. Duplicate card fraud — also known as counterfeit card fraud — includes such illegal acts as cloning a card or copying the cardholder information stored on it. Cloning a credit card takes seconds: While a card is being handled for payment, a dishonest staff member can swipe the card’s magnetic stripe data and download it onto a computer or other device; then a duplicate card is made, enabling criminals to process credit card transactions using stolen card information.

Q. “How does EMV protect against duplicate card fraud?”

A. When an EMV-enabled payment card is inserted into the chip reader, security information such as PAN/track data and dynamic CVV are presented to be used in the authorization request. This dynamic CVV changes for each transaction and is validated against what is expected at the card issuer host.

Q. “What other benefits does EMV offer?”

A. Most foreign countries issue only chip cards, and many major U.S. card providers are now beginning to issue them as well. The ability to accept a chip card may mean the difference between card swipe rates and hand-keyed transaction rates. In addition, the ability to accept EMV cards can provide a potential increase in revenue through acceptance of foreign visitors’ cards. And merchants may save money through the future liability shift.





Frequently Asked Questions (cont.)

Q. “What is the liability shift and how does it impact merchants?”

A. In order to reduce duplicate card fraud, the associations have mandated a liability shift that will occur in the next few years. This means that whichever party causes a contact chip transaction to not occur will be financially liable for any resulting card-present counterfeit fraud losses. So if a merchant does not have equipment that can support chip technology and this is the cause of the fraud, that merchant will be financially liable.

Q. “What is the difference between a contact card and a contactless card?”

A. Contact cards communicate with the card reader over a contact plate; this plate must come into contact with the terminal, usually via a dip reader. Contactless cards communicate with radio frequency (RFID) or near field communication (NFC). Dual interface cards combine both technologies and can communicate either way (contact or contactless).

Q. “Why is the ability to accept contactless cards important?”

A. MasterCard® and Discover® have mandated that in order to avoid the liability shift, merchants must have the ability to accept EMV cards and must support both contact and contactless interfaces.

Q. “How does EMV impact PCI compliance?”

A. Merchants are still required to achieve and maintain PCI compliance. Annual SAQ completion and quarterly external vulnerability scanning requirements remain in effect.

Q. “Why are equipment upgrades necessary?”

A. Utilizing the most current EMV capable devices — with a chip slot — on the market today ensures that the merchant can enable EMV via a simple download once EMV-capable applications become available. Merchants that purchase the most current technology will be able to add compatible peripheral devices with contactless functionality once they become available; this will put merchants in the position to fully achieve compliance and be ready for the future liability shift.

Q. “I have some more questions that are specific to my business. Where can I get more information and answers?”

A. We will be happy to answer your questions and provide all the information you need. Just contact your business development representative.

