October 2014

Heartland

EMV and Educational Institutions:

What you need to know

Mike English
Executive Director, Product Development
Heartland Payment Systems

The goal of this white paper is to educate the reader about EMV and the potential benefits of implementing an EMV solution, and to provide high-level information that will guide you to successfully implement EMV for payment acceptance.

What Is EMV?

EMV is a set of standards designed to protect debit and credit cards that are accepted at the point of sale, as well as ATM transactions. The EMV standards were formed by Europay, MasterCard and Visa in 1993. EMV standards define the interaction at the physical, electrical, data and application levels between an integrated circuit (IC) chip embedded in a plastic card and the point-of-sale terminal or device that reads the IC card for processing EMV financial transactions.

EMV chip-based payment cards, also known as smartcards, contain an embedded microprocessor, a type of small computer. The microprocessor chip contains the information needed to use the card for payment, and is protected by various security features. Chip cards are a more secure alternative to traditional magnetic stripe payment cards.

EMV's payment security approach is based on smartcard technology that adds dynamic security data to the transaction stream, authenticating that the card is present at the point of purchase. Additionally, every card contains its own microprocessor chip, making the cards nearly impossible to economically counterfeit.

Today, there are more than 1.5 billion EMV cards deployed in more than 120 countries on four continents. The United States will be the last developed country to migrate to EMV.

Accepting EMV at Your Location

Educational institutions are able to accept EMV cards in two ways. One method is to insert the EMV card into a card reader that is integrated in the terminal or PIN pad. This is referred to as an EMV contact transaction. Another way for a school to accept EMV cards is contactless, where the card is tapped at the terminal or PIN pad's contactless reader for payment acceptance.

What Benefits Does EMV Provide for Merchants?

Educational institutions that implement an EMV solution may benefit from a reduction in card fraud, decreased requests for copies in relation to chargebacks, and fewer disputes, as well as the opportunity to update terminals for other capabilities like Near Field Communication (NFC)[1] contactless acceptance.

[1] Near Field Communication (NFC) is a short-range wireless connectivity technology (also known as ISO 18092) that provides intuitive, simple and safe communication between electronic devices.

What Is the Liability Shift?

Visa, MasterCard, Discover and American Express have mandated that liability for fraudulent cards will shift to the issuer or business/acquirer on October 1, 2015, whichever one is not accepting EMV transactions and using strong customer verification methods. This liability is for fraudulent transactions committed with a counterfeit EMV card at the point of sale.

Additionally, MasterCard, Discover and American Express have announced a shift as it relates to lost and stolen chip cards. Liability falls to the party that supports the less secure form of cardholder verification. PIN is the highest form of cardholder verification.

Recently, Visa has announced a shift of lost/stolen liability to the issuer for chip card transactions completed at unattended chip-capable terminals that support no cardholder verification. Apparently, this is to encourage merchants that deploy unattended chip terminals to support no verification for Visa in addition to PIN for the other brands.

Is EMV Practical for an Educational Institution Provider?

At first glance, the financial value to an educational institution is questionable, as one must consider the liability shift mandated by the card brands and the volume of fraudulent cards that a typical business receives today versus the cost of installing an EMV-enabled terminal. However, incidents of fraudulent cards being presented at small retail locations will increase as national merchants move forward with implementing EMV and criminals begin to seek out non-EMV supporting businesses. Cardholders will eventually recognize the security improvements offered by EMV, and will look to make purchases from institutions, businesses and merchants with an EMV solution.

Educational institutions will want to be viewed as a safe place to conduct commerce and will be influenced by the growing awareness of their students and those visiting the campus. Additionally, EMV—specifically contactless EMV—brings NFC acceptance with it, and marketing opportunities such as the ones provided by Apple Pay, Softcard, Google Wallet, and other mobile wallet programs. Eventually, NFC might be a driving force along with other point-of-touch technologies, such as QR codes.

So, in the long run, the answer is yes—EMV will be practical and beneficial for educational institutions. Most new terminals being sold today have an integrated EMV contact reader, so it will be simpler for a merchant to start accepting EMV when it is time.

Is EMV Secure?

EMV *is* secure. EMV's payment security approach is based on smartcard technology that adds dynamic security data to the transaction stream, rendering replay of payment transactions unpractical. Additionally, every card contains its own microprocessor chip, making the cards nearly impossible to economically counterfeit. Using EMV improves the security of payment transactions in three areas:

- Dynamic card authentication protects against counterfeit cards.
- Cardholder verification using PIN authenticates the cardholder and protects against acceptance of lost and stolen cards.
- Transaction authorization using issuer-defined rules to authorize transactions reduces the chance for transaction interception or "man-in-the-middle" attacks.

EMV cards contain a secure integrated chip that is tamper-resistant and includes a variety of hardware and software capabilities that immediately detect and react to tampering attempts, thus countering possible attacks. However, EMV does not encrypt the cardholder account number or other transaction information that hackers can monetize, thus the need for additional security. Additionally, each EMV card issued in the U.S. will carry a magnetic stripe that could be skimmed and used fraudulently.

Heartland Secure

Heartland Secure™ is a comprehensive card data security solution that combines three powerful technologies, working in tandem, to provide merchants with the highest level of security available to protect against card-present data fraud. Featuring the only warranty of its kind in the payments industry, this exclusive solution is designed to provide businesses with security against point-of-sale (POS) intrusions, insider misuse, and other common sources of data fraud, by eliminating the opportunity for criminals to monetize card data.

Offered to Heartland customers for no extra service fees, Heartland Secure combines:

- EMV electronic chip card technology to authenticate that a consumer's card is genuine;
- Heartland's E3™ end-to-end encryption technology, which immediately encrypts card data as it is entered so that no one else can read it; and
- Tokenization technology, which replaces card data with "tokens" that can be used for returns and repeat purchases, but are unusable by outsiders and have no value.

Heartland SECURE

How Do E3 and Tokenization Work with EMV?

E3 encrypts the cardholder information, making card data indiscernible as it enters the payment cycle. In the event of firewalls or network security being breached, hackers and criminals gain nothing of commercial value. With E3, captured and encrypted card data cannot be used to make counterfeit cards or fraudulent phone/mail/online purchases. Magnetic stripe swiped and EMV transactions are encrypted prior to leaving the terminal so the transactions and cardholder information is sent encrypted through your network, over the Internet, and to Heartland without being readable. Tokenization eliminates the need to refer to a customer card number for returns, voids, card on file, and recurring transactions. Both E3 and tokenization combine with EMV to provide optimal transactions.

How Are EMV Transactions Authorized?

EMV transactions can be authorized online and offline. EMV transactions authorized online are verified though an online connection from the merchant's terminal or point-of-sale system to card issuers, via an acquirer like Heartland Payment Systems. This process is much like today's magnetic stripe-based transactions in the U.S., where transactions are authorized online. EMV offline transactions are authorized through authentication of the card and the merchant EMV acceptance device (point of sale or terminal). MasterCard and Discover have announced their support for offline authorization, but Visa does not support offline authorization for U.S.-issued chip cards. Chances are that your transactions will be authorized in an online mode and you will not need to be concerned about offline authorization.

How Are Cardholders Verified?

Use of PIN is a common EMV cardholder verification method (CVM) that authenticates the cardholder and protects against the merchant's acceptance of a lost or stolen card. When a cardholder's pin is used to validate who they say they are, it is called *chip and PIN*. In addition to chip and PIN, other customer verification methods include signature verification and no customer verification. The U.S. will most likely migrate to *chip and choice*, which indicates PIN, signature and no customer verification method. Selection of other appropriate customer verification methods will depend on how customers pay for goods and services at your location today, speed of checkout, customer convenience, and the need for chargeback protection, as well as the educational institution's terminal or POS system's capabilities.

What Is the Technology Innovation Program (TIP) and Does It Apply to Me?

Effective October 2012, Visa's TIP provides qualifying merchants—Level 1 and Level 2 merchants that process more than 1 million Visa transactions annually—PCI audit relief when 75% of the merchant's Visa transactions originate at a dual-interface EMV chip-enabled terminal. However, all merchants must continue to comply with PCI DSS. MasterCard offers a similar program to Visa. It is important to note that whether you are a Level 1 merchant processing more than 1 million transactions a year, or an educational institution processing 10,000 transactions annually, you are still responsible for being PCI compliant.

Questions?

If you have questions about EMV, lowering your cost of payments, how to better manage your store network, improving transaction security, payroll management or anything related to payment processing, please reach out to us at heartlandpaymentsystems.com/about/contact us.