October 2014

Heartland

EMV and Restaurants:

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 stands for the European MasterCard Visa consortium that developed new payment card technology, utilizing embedded chips. 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. That security is further enhanced when used in conjunction with a PIN (personal identification number).

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 more difficult to economically counterfeit.

Today, there are more than 1.5 billion EMV cards deployed in more than 120 countries on four continents. "By the end of 2015, 70% of U.S. credit cards and 41% of U.S. debit cards will be EMV-enabled, says Aite Group."[2] The United States will be the last developed country to migrate to EMV.

Accepting EMV at Your Location

Restaurants 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 merchants to accept EMV cards is contactless, where the card is tapped at the terminal or PIN pad's contactless reader for payment acceptance. Restaurants should work closely with their point-of-sale provider to determine EMV-enabled point-of-sale options.

What Benefits Does EMV Provide for Merchants?

Restaurants that implement an EMV solution may benefit from a reduction in card present fraud, decreased requests for copies, and fewer disputes, as well as the unrelated but valuable 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.

[2] http://www.finextra.com/news/announcement.aspx?pressreleaseid=55560&topic=payments

What Is the Liability Shift?

Visa, MasterCard, Discover and American Express have mandated liability shifts for fraudulent transactions effective October 1, 2015. Generally, liability will shift to the party using the least secure technology.

For counterfeit fraud, liability will shift to a restaurant when a counterfeit mag strip from a chip card is used at a mag stripe terminal. The merchant has not upgraded to EMV and is therefore less secure.

For lost and stolen fraud on MasterCard, Discover and American Express cards, liability will shift to restaurants when a lost or stolen *chip and PIN* card is used at a less secure terminal. For Visa, the issuer will continue to be liable for lost and stolen fraud.

Is EMV Practical for a Restaurant?

At first glance, the financial value to a restaurant is questionable, as one must consider the liability shift mandated by the card brands and the volume of fraudulent cards that a small business receives today versus the cost of installing an EMV-enabled terminal. However, incidents of fraudulent cards being presented at small business locations will increase as national chains 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 merchants with an EMV solution.

Restaurants will want to be viewed as a secure place to dine and will be influenced by the growing awareness of their customers. 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 small merchants. 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.

There are behavioral and operational issues to overcome at QSR and fast casual concepts as well as casual and fine dining concepts. QSRs and fast casual operations will need to re-engineer their counter operations and where applicable, their drive-thru outlets. Casual and fine dining establishments will have to assist servers and customers to adjust to paying at the table.

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 still 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.

Tip Management with EMV

While EMV dual message transactions will still allow tip adjustments when used as a *chip and PIN*, restaurants will want to streamline EMV card acceptance. Operationally, the following might be a best practice:

- When an EMV card is tendered and a PIN is required, it is a best practice to include the tip during the transaction.
- When an EMV card is tendered and signature is requested, the customer can sign the receipt and tip is added later.
- In the event that the customer card tendered only supports PIN, and the restaurant only supports *chip and signature* or no customer verification method, restaurants may ask for another form of tender.

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, which is used today at some quick service restaurants. 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 restaurant's terminal or POS system's capabilities.

Customer Convenient Payment

The following are pay-at-the-table considerations for restaurants implementing EMV:

Chip and signature	▪ Follows current payment process ▪ Minimal expense
Stand-beside payment	▪ Purpose-built unit with EMV and NFC ▪ Wallet acceptance ▪ Stand-beside or semi-integrated
Kiosk at the table	▪ Requires iPad or Android at each table with enclosure and readers ▪ Power, battery life and security are concerns
Purpose-built mobile	▪ Smartphone and sled, which is a cover encasing the smartphone to provide payment acceptance ▪ Integrated with POS system or stand-beside
Mobile device for ordering and payment	▪ Smartphone and sled ▪ Integrated with POS system

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 a restaurant 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.