EMV Liability Shift

By Joseph B. LaRocco

There will be a major EuroPay, MasterCard, and Visa (EMV) liability shift to merchants on October 1, 2015: merchants not using EMV-enabled credit card terminals or point of sale (POS) systems will bear the liability for credit cards bearing a computer chip when fraud is involved.

Although EMV compliance is not mandatory, the EMV liability shift is certain. Fraud involving credit card charges could be in the form of fake cards, stolen cards, or cards used without proper authority.

In order to meet EMV compliance requirements, businesses that accept credit card payments will need to have an EMV-enabled terminal or POS system that allows new credit cards with computer chips to be inserted into the terminal rather than being swiped.

The banks that are already in the process of issuing these new cards will determine what they want the cardholder to do once the card is inserted in the terminal for processing. The options are either 1) a cardholder types in the personal identification number (PIN) associated with that card, 2) a cardholder signs the receipt, or 3) no further action will be required. Some merchants who are already using these new EMV terminals may find that the terminals are not yet activated to process payments by insertion, and customers must still swipe the card as usual.

BuisnessInsider.com reports that credit and debit card fraud has caused billions of dollars in losses in the U.S.—$5.5 billion in 2012 and $7.1 billion in 2013. In fact, in 2013, 51 percent of global payment card fraud costs were attributable to the U.S. alone. While Europe is already on board and embracing the new technology to reduce fraud, U.S. merchants are lagging behind. In fact, it has been estimated that less than 50 percent of merchants in the U.S. will be in compliance with the EMV guidelines on October 1, 2015.

Who Is Liable?

Merchants using a terminal that only allows a credit card to be swiped and have a customer who fraudulently uses a credit card with the EMV chip bear the risk of loss for EMV liability. In many other cases, however, issuing banks will be liable.

For instance, an issuing bank will bear the risk of loss if a merchant still uses a terminal that only allows a credit card to be swiped and has a customer who fraudulently uses a card with no chip, just the magnetic strip on the back of the card.

If a merchant has an EMV-enabled terminal and a customer fraudulently uses a credit card with the EMV chip, the odds are very strong that the transaction will not go through. Even if it does, the issuing bank will bear the risk of loss because the merchant was using an EMV-enabled terminal.

Lastly, a merchant might use an EMV-enabled terminal but have a customer who uses a credit card with no chip, just the magnetic strip on the back of the card. The card is swiped, and the transaction goes through. In the case of a fraudulent transaction, the issuing bank will still bear the risk of loss for the transaction, not the merchant.

An App for That

In addition to considering EMV liability, merchants must also be aware of mobile apps that individuals are turning to more and more. Various mobile payment solutions will be coming online in addition to some of the ones highlighted below, so merchants should make sure that they can handle payment transactions being transmitted via near field communication (NFC). NFC transactions can be done wirelessly through a smartphone or EMV terminal.

Google Wallet, which has been around since 2011, is a mobile app that makes it easy to pay in stores, online, or to anyone in the U.S. with a Gmail email address. It works with any debit or credit card on every mobile carrier. Google Wallet lets users securely store payment information, transaction history, offers, and more, which are synced to the cloud. The app turns any mobile phone into a virtual wallet, so customers can use it to make purchases at any business that accepts Google Wallet. Payments are made by tapping the phone at the point of sale, using virtual versions of credit cards, loyalty cards, and Google Offers.

Apple Pay is an app that allows users to make payments using their iPhone 6 and iPhone Plus. It relies on fingerprint technology and tokenization for security. When the payment transaction takes place, the credit card information never passes through to the merchant's terminal. Rather, a symbol-based token is submitted and initiates the payment. In this manner, the risk of the customer's credit card data being stolen from the merchant's processing terminal is greatly reduced. One of the barriers for Apple Pay is its reliance on the infrastructure of the Visa and MasterCard payment system and need for terminals and POS systems to accept NFC transactions, but its strength lays in its fingerprint and tokenization technology.

Android Pay is in the works and was announced by Google Senior Vice President Sundar Pichai at the Unpacked event in Barcelona this March. Samsung has partnered with Loop Pay, a Boston-based mobile payment technology provider, to integrate payments into the very operating system of its new smartphone, which may give it an interesting edge. Loop Pay could provide Samsung with a strategic advantage because its technology enables users to make contactless payments with their phone at a traditional magnetic strip terminal, which are still the majority of terminals in use today.

Leasing or Buying EMV Capable Terminals or POS Systems

One thing merchants should keep in mind when purchasing a terminal or POS System is the overall cost. Most small to mid-sized merchants will have to upgrade their terminals and POS systems to accept these mobile payments. The expense of such an endeavor has left many smaller businesses reluctant to do so.

> Merchants should make sure that they can handle payment transactions being transmitted via near field communication (NFC). NFC transactions can be done wirelessly through a smartphone or EMV terminal.

Leasing the terminal or POS system is a viable option. Statistically, however, leasing is a major area of concern for merchants due to the amount merchants have to pay during a lease term, which, in some cases, can be as much as eight or 10 times the actual purchase price.

Always check around to find out what the actual price of the equipment would be if you either bought it from the sales agent or from a third party vendor. Whether you are leasing or buying, make sure that it is at least EMV-capable, meaning you can insert as well as swipe a credit card to process the transaction. Also, the terminal should be able to accept NFC-transmitted transactions.

If the sales agent is providing you with the equipment based on a no upfront cost program, be sure that you understand all the terms and conditions associated with that program, which may require that you do all your credit card processing with them for a fixed number of years. The program may also have an early termination fee if you switch processors before the end of the term.

Find out if the equipment can be used by another processor in case you switch processors and that the terminal is not locked. If the equipment is locked, ask if it can be unlocked for a fee and how much that fee will be. Merchants often run into this problem when they try to switch processors.

To Comply or Not to Comply? That Is the Question.

Although following with the new EMV compliance rules is not mandatory, each business should consider the risks of noncompliance. For instance, if the merchant sells big-ticket items and has had to deal with instances of credit card fraud in the past, the merchant will probably not want to risk a large chargeback that would have a noticeable impact on the bottom line. The cost of upgrading a terminal greatly outweighs the EMV financial liability the merchant would suffer.

Even smaller businesses would be foolish not to upgrade based on the overall cost of upgrading. The liability risk is too much, especially since in addition to chargebacks, they could face steep fines imposed by MasterCard and Visa. In order to get businesses ready, discounts and sales are currently widespread on the hardware. If a merchant waits, he or she will also most likely have to pay more, as the sales will be over.

Also, merchants with older POS systems may want to check the current market for new offerings which will allow them to 1) save money when replacing their POS system, 2) provide more versatility while being easy to use, and 3) allow a gift, loyalty, and promotional software program such as Fanfare to help them increase revenues and customer retentions. N

Joseph B. LaRocco is the Northeast Regional Director for LaRocca Integrated Solutions, Inc., which is powered by NXGEN Payment Services, a Registered MSP/ISO of Elavon, Inc., in Georgia. He advises numerous businesses on payment solutions, POS systems, and credit card fraud prevention. Joseph can be reached at joseph@laroccais.com.