RISK INSIGHTS

OLSON & OLSON Ltd

The Credit Card Liability Shift—What Merchants Need to Know

EMV is the acronym for Europay, Mastercard and Visa—the three credit card companies responsible for pioneering a new credit card technology in the 1990s. Though they were the first innovators, since then, all major credit card companies have adopted the technology, which has been in widespread use in Europe and elsewhere in the world for several years. On Oct. 1, 2015, that same standard will come to the United States as credit card companies enact the "EMV liability shift."

In the simplest terms, this means that the cost of fraudulent charges on certain kinds of credit and debit card transactions will be determined solely by the technology used in the transaction. Whoever has the least EMV-compliant technology—either the merchant processing the transaction or the card issuer—will be liable for the costs of the fraudulent charge.

Such a shift could have huge financial implications for businesses, especially since card issuers have typically borne the bulk of fraud liability. To minimize the impact of this shift on your business, it's important to understand what EMV is, why it's being adopted as the new standard and what the new technology will and won't do in terms of minimizing risk.

Understanding the New Technology

EMV replaces the old standard of encoding cardholder information—the magnetic stripe on the back of the card—with a microprocessor chip that's embedded **within** the card. Customers then punch in a personal identification number (PIN), much like a debit card, or sign for the transaction in the same way customers currently do with magnetic stripe cards.

EMV cards offer major security benefits. Specifically, in contrast to their magnetic stripe counterparts, EMV chip cards are almost impossible to clone. On magnetic stripe cards, thieves can steal cardholder information using a device called a "skimmer." On EMV chip cards, cardholder information is stored in a microprocessor that generates a unique signature for every transaction, effectively "communicating" its authenticity every time it's scanned. In fact, in countries that have adopted the EMV standard, the use of counterfeit cards has dropped nearly to zero.

Whoever has the least EMV-compliant technology—either the merchant processing the transaction or the card issuer—will be liable for the costs of the fraudulent charge.

EMV Migration – What Businesses Need to Do

There are certain steps a business will have to take in order to become EMV compliant. These can take time, so starting as soon as possible is the best strategy.

- **Examine Hardware**: Some businesses that have upgraded point-of-sale (POS) card readers in the

past few years might find them capable of reading EMV cards. Many businesses, however, will have to upgrade their existing hardware.

- **Consult With Third Parties**: Businesses should contact their merchant acquirers, payment processors and independent software vendors. These third parties can help by offering specific recommendations and solutions that fit with each individual business's needs.

- **Purchase and Certify New Hardware**: The merchant acquirer or payment processor should be able to tell a business what certification, if any, that business might need.

    - Often, if the card reader isn't heavily customized, the acquirer or processor may have already taken care of certification.

    - If, however, the card reader is highly integrated into the business's POS, that business might need to obtain proper certifications. In some cases, the same policy can cover multiple events.

    - Certification takes time. Level 3 certification, for instance, can take anywhere from a couple of weeks to several months.

- **Decide on Chip-and-PIN or Chip-and-signature:** Businesses should also consider whether the terminals they purchase can handle chip-and-PIN transactions or only chip-and signature transactions. At the moment, most card companies are issuing chip-and-signature cards. However, it's likely that chip-and-PIN will be the standard in a few years. Rather than update hardware twice, it might make sense to make that investment now.

- **Implement Internal Training**: EMV cards are processed a bit differently than magnetic stripe cards, so it's important that employees understand the differences:

    - The total amount of the transaction must be entered into the terminal **before** the card is inserted.

    - An EMV card must remain inserted in the terminal for the entire duration of the transaction.

- **Educate Customers**: Most businesses will be far more knowledgeable on the new technology than their customers. Teaching employees how to instruct customers on using their new EMV cards will be essential in making the transition as smooth as possible.

Important Exclusions to EMV

The liability shift only applies to card-present, face-to-face transactions. Currently, there's a separate liability shift, scheduled for October 2017, for ATM withdrawals and automated fuel dispensers.

Card-not-present (CNP) transactions won't be affected by the liability shift. That means that even if a business has an EMV-compliant terminal, if the card information is manually entered, or if the transaction occurs on the internet, the business will usually be responsible for the costs associated with a fraudulent transaction.

It's also worth noting that many EMV cards will also have a magnetic stripe in addition to the chip. If a business uses the stripe to read the card rather than use the chip, it will assume liability, regardless of whether the terminal is EMV compliant or not.

Putting it All Together

EMV is a technology designed to reduce losses and should be thought of as another piece of your business's overall security strategy. For more information on how to assess and mitigate your business's risks, contact Olson & Olson, Ltd today.