Foster Garvey

Duff on Hospitality Law

Credit Card Fraud Liability Shift is Here

on 10.1.15 | Posted in Payment Systems, Technology

Most credit and debit cards in the U.S., and the point of sale terminals and ATMs that read them, still use “magnetic stripe” technology. Magnetic stripes are obsolete and relatively insecure, allowing fraudulent practices such as “skimming” (acquiring cardholder and account data by “reading” the strip, and then making fraudulent transactions or counterfeit cards). Magnetic stripe-based technology also does not support secure data transmission through contact or near-field contactless interfaces, which is seen as impeding the emergence of fully mobile cardless payment modes in the U.S.

Outside the U.S., the story is different. In Asia, Europe, and now in Canada, the payment industry technical standard is “EMV,” which uses a “smart” microchip embedded in the card, and acceptance devices designed to support the chip-based standard. Although the U.S. is the largest user of payment cards in the world, it has been nearly the last country to adopt and implement EMV in payment card transactions.

Because the EMV standard (developed by three major global credit card issuers – Europay, MasterCard, Visa – specifically to combat fraud) is inherently more secure, the U.S. is now the “weak link.” Experts predict credit card fraud “migration” to the U.S. Statistics bear this out. According to a recent Accenture study, in countries (such as the U.K.) where EMV has been implemented, rates are declining, while in the U.S., they continue to rise. Part of the EMV business case is that chip-based payment technology enables “dual-interface” combinations of cards and contactless mobile payment. The need to replace the old magnetic-based point-of-sale acceptance devices in order to implement EMV also presents an opportunity to enable contactless and mobile-ready technology at the POS.

The estimated nationwide costs of converting to chip-based cards and POS acceptance devices are about $8 billion. That has been the primary obstacle to implementation of EMV in the U.S. But major credit card issuers, facing mounting fraud losses, are forcing processing banks and merchants to implement the switchover.

The first step in that forcing process occurred in 2013. As of April 2013, all major U.S. credit card associations, Visa, MasterCard, Discover and American Express, require “acquirers” (banks that contract with merchants to accept or acquire credit card payments from card-issuing banks), service providers, and sub-processors to have the capability to process any EMV POS transaction, both contact and contactless. These entities must adhere to payment network rules and complete approvals, in order to begin processing and passing additional

authorization data for EMV transactions.

October 1, 2015 Liability Shift

The next step is much more significant, and is now upon us. It directly affects any merchant who accepts credit or debit cards. Beginning today, on Oct. 1, 2015, MasterCard and Visa will shift liability for fraudulent counterfeit card transactions to the "non-EMV compliant" party. This means that, if a fraudulent transaction is made on a counterfeit card, and the merchant does not have EMV-compliant POS terminals, the merchant will be liable. If the merchant does have an EMV-compliant terminal, and the bank that issued the card issued a magnetic stripe card without an EMV chip, then the issuing bank will be liable.

Although most cards issued in the past couple of years in the U.S. are now chipped, according to most industry observers, many of America's businesses, particularly small businesses, are not ready for the shift to EMV, at the point of sale. Reasons include a lack of awareness, and a complex technical validation and certification process that is backlogged, and taking longer than expected.

There is a fair amount of fear and confusion about the Oct. 1 "liability shift." Practically speaking, the circumstances under which a merchant will be liable for a fraudulent transaction are fairly limited. First, the card must be a particular type of counterfeit: a phony magnetic strip type card, with tracking data copied onto the strip from a genuine chip card. Second, the merchant's POS terminal device must be incapable of reading a contact chip. That is the only situation a merchant can be liable when it has done nothing wrong other than not having the right type of terminal equipment. On the other hand, if a counterfeit card has a chip, and the merchant does not have a terminal capable of reading the chip, but authorizes the transaction anyway, it will be liable for that poor decision. In most other counterfeit card situations, the issuer remains liable. Furthermore, the "liability shift" applies only to "card present" types of transactions, where a customer presents a card at the point of sale. In fact, many observers think this will drive fraud to "card not present" exchanges, i.e. online transactions. Still, the risk is real, and for certain types of merchants (ones who depend heavily on face-to-face card transactions), could be significant.

Steps to Consider

While hardware upgrades can be expensive, and complicated in large organizations, the liability shift will make conversion to EMV-ready POS devices inevitable. Hospitality industry businesses would be well advised to:

- Begin implementing EMV now, if you haven't already begun;
- Ensure that your processing and POS equipment providers meet applicable EMV security and certification requirements; and if not, review contracts to determine if they can be

terminated in favor of an EMV-ready vendor;

- While upgrading to EMV, plan ahead, and consider deploying an integrated solution that will support some form of contactless mobile payment;
- Work with the banks that handle your merchant accounts and their POS device providers to find out how and when they are implementing EMV;
- Once EMV-ready terminals and related software are deployed, train front-office personnel on how “chip and pin” or “chip and sign” transactions work, and back office and IT personnel on configuration and validation requirements necessary to integrate EMV with legacy systems and work flows.

Larger organizations face a more complex CIO-level technology procurement and payments systems challenge, but there is no shortage of consultants and vendors focused on EMV implementation. Large or small, the change to EMV is already well underway.

Tags: chip-based cards, chip-based technology, contactless mobile payments, credit cards, debit cards, EMV standard, fraudulent counterfeit card transactions, liability shift, merchant, POS acceptance devices, skimming