TRAUB LIEBERMAN

October 28, 2015

The EMV (Chip/Pin) Liability Shift is Here

As of October 1, 2015, retailers that have not implemented Point of Sale (“POS”) payment terminals that support EMV- or Chip/Pin-enabled cards with embedded chip technology over the traditional magnetic stripe cards, face a shift in liability for fraud charges assessed by the payment card industry (“PCI”).

The EMV- (**E**uroPay, **M**asterCard, **V**isa) enabled cards have an embedded microprocessor chip that creates a unique authentication code for each transaction that is issued with either a personal identification number or a cardholder’s signature. In other words, only the transaction itself is authenticated and none of the payment card information or personal data stored on the card's magnetic stripe is ever accessed by the merchant.

Image not found or type unknown
chip

Until now, it has been the card issuers (and not the merchant) liable for fraudulent purchases on magnetic stripe cards swiped at a POS terminal. After this month’s liability shift, the liability for such losses falls to whichever party is the *least* EMV compliant in the fraudulent transaction. If the bank issued EMV-compliant cards but the retailer’s terminal is not using EMV technology, the liability falls to the merchant. If the merchant’s POS terminal is fully compliant, but the card issued by the merchant bank is not, the merchant bank will be liable. If all parties are EMV compliant the liability falls back to the card issuer.

There is significance to retailers which must carefully weigh the costs of upgrading to an EMV-compliant payment system with the increased risk of POS data breaches and the recent PCI liability shift. Some card brands offer specific incentives to upgrade. As a footnote, retail fuel merchants (gas stations) have an additional two years to move to the new technology before the “liability shift” takes effect.

While the EMV-enabled cards may provide an added layer of protection in the context of card-present transactions, EMV does not really mitigate cyber risks for on-line merchants or “card-not-present” transactions. The EMV cards themselves can still be counterfeited.

Finally, EMV technology is NOT required by the PCI-DSS v3.1. Implementing EMV does not automatically satisfy general PCI-DSS requirements. EMV compliant merchants still have exposure if there is a finding of PCI-DSS non-compliance at the time of a data breach.