Credit Card Fraud: EMV compliance and shift of liability as of October 1

PUBLISHED ON
October 1, 2015

As of October 1, 2015, all major credit card companies in the United States (including, Visa, MasterCard, Discover and American Express) will impose a liability shift for counterfeit presentation of payment cards.

In the past, card issuers (including, banks, credit unions and other financial institutions) generally accepted all liability for counterfeit payment card transactions, including those transactions where the payment card is presented by the holder (known as "card present" transactions). But on October 1, 2015, the liability for counterfeit, "card present" transactions generally shifted to the party (either the issuer or the merchant) that does not support modern "chip" technologies, including EMV "chip" cards ("EMV"stands for EuroPay, MasterCard and Visa). So, for example, if a merchant accepts a payment with a "chip" card and processes the transaction using a magnetic-only card reader, the merchant is now responsible for replacing the funds from fraud losses, not the card issuer.

This deadline appears to be the "carrot on a stick" needed by card issuers to entice businesses to adopt the more-secure, modern "chip" technologies. Annual costs of payment card fraud in the United States alone are estimated at $8.6 billion per year, and industry experts believe that figure will rise to at least $10 billion by the end of 2015. However, despite the availability of "chip" technology for several years, the Small Business Administration estimates that as of this past January 1, 2015, only 3% of all payment cards in the United States contained "chip" technology. It is expected that as a result of this liability shift and other contributing factors, that the percentage of payment cards containing "chip" technology will jump to closer to 40% by year end.

Most new cards will be enabled with both "chip" and magnetic strip technology to facilitate the transition phase. And the liability shift does not change the liability for online purchases, "card present" transactions conducted using lost or stolen cards, or "card present" transactions conducted using cards that only offer magnetic strips. Issuers will continue to be liable for payment fraud that occurs with these types of transactions. Furthermore, gas stations have an additional two-year period (until October 1, 2017) to convert their automated fuel dispensers, before their liability on counterfeit cards is shifted.

The push for "chip" technology is because it is far better than the existing, magnetic technology in preventing fraud. Magnetic cards store "static" data (information that does not change). So, if data is stolen from a magnetic card, the data can be copied and replicated onto one or more "cloned cards" and used to make purchases or withdraw cash. By comparison, "chip" cards generate a unique encrypted code for each transaction, making it virtually impossible to replicate and, therefore, much more secure than magnetic cards when read by a "chip" technology processing device.

The downside of "chip" technology and EMV compliance is cost. "Chip" cards are more expensive for issuers to manufacture. In addition, financial institutions may also need to upgrade their automated teller machines and merchants must upgrade to "chip" technology equipment and reader systems to accept in-store card payments that are protected with "chip" technology. Merchants must decide whether avoiding exposure to fraud liability is worth the difficulty and expense of the chip reader upgrade. Their decision may depend upon their unique risk of exposure to card fraud.

Overall, there is no doubt that the switch to "chip" technology will go much further in preventing payment card fraud than the current, magnetic technology allows. However, since online transactions (frequently referred to as "card not present" transactions) are not directly affected by "chip" technology, it is anticipated that fraudsters will re-focus their time and efforts toward online fraud and merchants may wish to take additional security precautions for higher value and/or higher risk online transactions.

WRITTEN BY:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com