Merchants beware: You could be on the hook for the next data breach

James J. Giszczak, Richard W. Cline, Dominic A. Paluzzi, Adam C. Smith | Wednesday, August 12, 2015

Starting Oct. 1, 2015, credit card companies and banks will enforce new terms in their acceptance guidelines, commonly known as liability shift provisions. These provisions are based on the rollout of Europay, MasterCard and Visa (EMV) technology. If there is an incident of fraud after October 1, the entity, either merchant or card issuer, utilizing inferior non-EMV technology will be held liable.

EMV is overseen by American Express, Discover, JCB, MasterCard, UnionPay, and Visa. EMV operates through the use of card dipping. A consumer dips his or her card into the bottom portion of a terminal, leaves the card in place, and removes the card when prompted. During that process, an imbedded chip communicates with the terminal by sending a unique transaction code. The EMV chip is the reason credit card companies and banks are sending out new cards. Utilizing EMV technology requires customers to have an EMV credit card and merchants to have EMV card terminals available.

Card dipping is different from swiping a credit or debit card; the EMV unique code can be used only once, whereas the account number transmitted when swiping a credit or debit card is used for every transaction. The obsolescence of the unique EMV code will theoretically prevent hackers from obtaining card account numbers because that unique code, not an account number, is being transmitted.

How does the fraud liability shift after October 1? If credit card fraud occurs and a customer is using an EMV credit card but the merchant failed to obtain an EMV terminal for the customer to use, the merchant will be liable. If credit card fraud occurs in one of the following circumstances, the credit card company or

bank will be liable:

- The customer and the merchant are utilizing EMV technology.
- Neither the customer nor the merchant are utilizing EMV technology.
- The merchant has an EMV terminal available, but the customer is not using an EMV card.

It is important to note EMV technology is not required or even available for online credit card purchases – also known as card-not-present transactions. Thus, the liability shift will not impact such purchases. However, merchants that allow online card transactions should know how this change could affect them. Prognosticators have warned that online merchants will likely see an uptick in online transaction fraud once EMV technology is implemented in point-of-sale transactions. Marc Castrechini, vice president of product management and solution engineering at Merchant Warehouse, has advised that because EMV technology will greatly frustrate point-of-sale fraud, fraudsters will likely migrate to hacking card-not-present transactions. Therefore, online merchants should take this as an opportunity to assess their current transaction processes to ensure they are using the most current fraud prevention tools, such as address verification, card verification, and tokenization.

What you should know

If you are a merchant, you should begin the process of obtaining EMV card terminals now, and have them available for your customers to use by October 1. If you don't, you take the considerable risk of incurring liability for credit card fraud, as some courts have held that customers affected by data breaches have standing to bring class action lawsuits **based only on the threat of future harm**, without any actual loss. Many cardholders already have an EMV chip card, which means if you have EMV technology you should start training employees on the new card dipping process.

Though EMV technology likely will stifle or frustrate point-of-sale credit card fraud, card-not-present fraud will likely increase dramatically. If you allow such transactions, recognize the propensity of such increased fraud and implement all possible fraud prevention measures to curb those risks.

For more information, please contact one of the attorneys listed below.

James J. Giszczak

Richard W. Cline

Dominic A. Paluzzi

Adam C. Smith

Merchants beware: You could be on the hook for the next data breach