

Merchants: Are You Ready for the October 2015 Credit Card Liability Shift?

AS A REMINDER, MERCHANTS MUST UPGRADE THEIR CREDIT CARD PROCESSING SYSTEMS TO “CHIP AND PIN” TECHNOLOGY BY OCTOBER 2015, OR THE LIABILITY FOR FRAUDULENT TRANSACTIONS WILL SHIFT FROM THE BANKS TO MERCHANTS IF THE MERCHANTS HAVE NOT UPGRADED THEIR SYSTEMS.

In response to the recent major data breaches of companies like Target, Home Depot, and Neiman Marcus, the major credit card companies and merchants have begun to upgrade their credit card processing systems to Chip and PIN, which is a more secure system than the “Swipe and Sign” systems historically used by most merchants in the United States.

Swipe and Sign System is Vulnerable to Hackers

Currently, credit cards in the U.S. have a magnetic strip which is swiped and read by the retailers’ machine; a receipt is then generated which the customer signs as an additional measure of security. Under this system, hackers need merely steal the card itself or the magnetic strip’s information (by installing either a malware program or a physical data “skimmer” on machines), and signatures are rarely if ever checked.

For example, the Target and Home Depot hackers installed malware which stole customers’ credit card numbers, which were used to print duplicate cards to be used just like the originals.

Chip and PIN Offers Increased Security

Under the more secure Chip and PIN system, each credit or debit card has an embedded microchip which contains the information traditionally stored in a magnetic strip. The customer inserts the card into a chip reading machine, and a unique cryptographically-secured transaction code is generated for each purchase; the microchip is encrypted, which prevents thieves from copying a person’s credit card information like they can with a magnetic strip.

For those that upgrade to using PIN’s instead of signatures, the customers would also enter their secret PIN number (as currently seen with debit cards) to complete the transaction. Thus, if hackers

steal the card, they will not have the PIN, and even if they steal the PIN, they will not have the transaction code required to make an in-store purchase.

Chip and PIN technology is already commonly used overseas and has been for several years; frequent travelers may have already had to obtain a chip card for use abroad.

How Does the Liability Shift Affect Merchants?

Visa and MasterCard, along with other major companies, are now widely issuing cards with embedded chips (many of which are still compatible with older magnetic strip machines). Under the old liability system, the card company was liable for fraudulent transactions.

However, beginning in October of 2015, the liability will shift to whoever has the lesser technology, the card company or the merchant. Thus, for example, if a hacker steals a customer’s information and uses it to make a fraudulent Swipe and Sign transaction on an outdated machine, the merchant using the older machine will be fully liable to the customer if the card also had a chip.

Card companies claim the shift is simply intended to encourage merchants to upgrade, but it could be costly or even fatal to businesses caught unprepared. In order to ensure the security of customer information and avoid potentially disastrous liability, all merchants should upgrade to Chip and PIN machines as soon as feasible. ■



Brett Henderson and Steve Hymas are attorneys in the Privacy and Data Integrity Practice Group at Downey Brand in Sacramento, California. The focus of their practice is on representing

clients with complex business technology transactions including assessing and minimizing the risks associated with gathering, transferring and storing of sensitive data.