To Swipe or Not to Swipe ... That is the Retailer's Current Credit Card Dilemma

Mar 07 2016

Posted By: Chris A. Jenny & William R. West

Practice Area: Real Estate & Retail Real Estate

A day spent running errands around town can leave a consumer feeling confused. While the local grocery store chain would like a swipe of your credit card using the magnetic strip, Target and Walgreens insist that you "dip" your new chip-enabled credit card into the card reader. Currently, the lack of continuity on payment processing between retailers makes for a confusing checkout process. So why do some retailers insist you "dip" while others insist you "swipe?"

On October 1, 2015, the United States became one of the last countries in the world to make the switch from swipe-and-sign magnetic credit cards to chip-embedded cards (also known as the EMV standard, named for Europay, Mastercard and Visa, who first backed the technology.) EMV is a globally-accepted card payment standard that uses an embedded microchip to send a one-time unique code to process the payment, rendering duplication efforts for credit card fraud difficult, and thus payment more secure.

Along with the EMV switch came a shift in fraud liability for retailers. Prior to October 2015, liabilities for card-present fraudulent transactions were generally the responsibility of the card issuers. Now, for most major payment networks, (including American Express, Discover, Mastercard, and Visa) the liability for fraud depends on if the retailer is certified EMV compliant. (Gas pumps and ATMs will not experience the liability shift until 2017.)

Instances where a retailer may be liable for fraud include:

- Fraudulent transactions (including lost or stolen cards) using the magnetic strip on chip-enabled cards where the retailer does not use a point of sale (POS) system that is EMV compliant.
- A successful transaction using a magnetic stripe card that was counterfeited with data copied from a chip card, where the card is swiped at a point of service that is not chip-enabled.
- A successful transaction using a stolen chip-card that prefers input of a PIN, where the card is presented at a chip-enabled point of service and is processed with a signature instead of the PIN.
- "Friendly fraud" or "chargeback fraud" where a consumer may try to claim that it was not them who swiped a chip card at a retailer that is only using magnetic stripe technology.

Despite the shift in liability, retailers have been slow to adopt the new payment system, which explains the discrepancies in payment requirements between stores. A recent survey released in February of this year estimates that only 37 percent of U.S. retailers are ready to accept chip cards. Becoming EMV compliant may require a retailer to update their POS hardware system to accept chip-enabled cards, as well as software updates, which many small businesses might find to be an unwanted expense.

However, non-compliance with the EMV standards may have serious consequences. For example, Target, who was affected by a massive data breach in 2013, was compromised through their POS system where the perpetrators relied on malware to grab magnetic stripe card information to compromise millions of customer's data. The new shift in liability could cause a retailer to be entirely on the hook for a large-scale data breach or fraud perpetrated using an outdated POS system (such as a magnetic card skimmer.) It is important for all brick and mortar retailers, including small businesses, to focus on upgrading their POS payment systems to the EMV standard. Identity theft continues to be more problematic than ever before, and the potential cost of liability for a breach or fraudulent transaction is significantly higher than the investment in the new technology.
