Grocers, Get Ready for Sweeping Credit Card Changes

By Dennis Hoyt, CPA, Certified Treasury Professional

Credit and debit cards are changing — from the way data is stored on the cards, to how cards are processed, to who is held responsible for card fraud — and all of it will impact grocers.

By October 1, 2015, the big credit card companies — MasterCard, Visa, American Express, and Discover — want systems in place to replace magnetic stripe cards with chip-embedded cards, sometimes called smart cards. Companies are pushing for the switch because the U.S. is behind the rest of the developed world when it comes to fighting credit card fraud — making U.S. businesses a target for hackers, with Supervalu being the newest merchant to announce a data breach just last month.

Europe led the way with the switch to chip-based cards about 10 years ago; now most countries with advanced economies, including nearby Canada and Mexico, have converted as well. These countries follow Europay/MasterCard/Visa (EMV) standards for processing face-to-face card transactions (internet and mail-order/telephone-order environments are not included). These three companies got together in 1994 to start to develop the specifications to apply chip card technology in payment transactions; these are now known as the EMV standards

Why the Change?

The goal of the EMV standards is simply to lessen face-to-face card fraud, which has increased dramatically in the U.S over the years. The EMV process encompasses (a) a new type of card with a data chip embedded in it, (b) terminals capable of reading chip-based cards, and (c) systems in place to securely process transactions. To be EMV compliant and avoid the liability from a fraudulent card, merchants will need terminals and software that can read and process transactions from the new chip-based cards.

How is it Different?

The current magstripe card, used by the public for almost 50 years, is based on 1950's magnetic recording technology. In a simple transaction, the card is swiped through a terminal, with the static data on the card quickly read by the terminal.

The new chip card will have data embedded into the card — under a computer chip — that will be read *and updated* during the check-out process, when the card in inserted or "dipped" into a terminal capable of accepting the card.

That means shoppers will no longer simply swipe their cards; instead, they will insert them into a card reader where they will stay until the transaction is completed.

Because the chip-based card contains a cryptogram for processing, it will securely combine existing information on the cardholder and certain processing requirements along with transaction information from the terminal to create "rules." These rules must be approved by the terminal and then verified by the issuing bank before the card is accepted.

Chip-based cards can also support contactless card reading, where instead of swiping or dipping, cards are tapped or waved against a terminal scanner that can pick up the data from the embedded chip. However, most U.S. banks are only issuing contact cards right now.

With the new chip cards, processing will take a few seconds, after which the customer will either sign for the purchase (as typically done now) or key-enter a PIN number into the terminal. A common practice with debit cards, entering a PIN is a stronger control than signing and will likely be added as a credit card transaction requirement as well.

With this more secure processing *plus* a transaction counter on the card that will be updated during each transaction, both the processing and the data on the card will be dynamic, making it very difficult to counterfeit the card. Note, however, that during what will be a several *year* transition to these chip cards, the new cards will still have magstripe data on the back, enabling acceptance by merchants not yet having EMV-capable terminals.

How will Liability Change?

The liability for credit card fraud will be shifting — and it may be shifting on to you. Today, the *issuer* of credit cards usually absorbs the cost of credit card fraud. However, beginning October 1, 2015, the liability for any card fraud will shift to the *least EMV compliant party* (the card issuer, the card processor, or the merchant). Because the card processors have had to be EMV compliant since last year, that means if the card issuer has issued chip-based cards, but a merchant hasn't changed their system to accept chip-based cards, then the merchant would be liable.

How great is the Liability Risk?

Merchants with *non* EMV-capable terminals will be greater targets for card-related fraud, and the liability for counterfeit fraud will be borne by them. They also risk an increase in the interchange rate at some time in the future and *may possibly incur additional charges if their lack of preparedness causes a data breach.*

It's also possible for merchants with EMV-capable terminals to still be at risk because of the *backward-compatibility feature* of the terminals. That is, to support the continued existence of old magstripe cards for the next few years, the new terminals must still be able to read them. Therefore, card fraud using a combination of new terminals and old cards may still be possible, until old cards are no longer accepted by the merchant. *However, while the backward-compatibility feature may enable fraud, those EMV-capable merchants will not be liable because they have taken the steps to become EMV compliant.*

Potential Fraud Aside, What Else Can Grocers Expect?

New cards and a new POS system may cause slightly longer checkout times because the chip-based card will take a little more time for processing than a simple swipe. Some customers will need to be trained in how to insert the card into the terminal. If they remove it too quickly, there will be a processing error. And some may leave the store with the card still in the terminal since, unlike the magstripe card, the card will be leaving the customer's hand, making it easier to forget. Grocers will need to train employees to use the new equipment and to help shoppers as needed.

Of course training employees, replacing swiping devices, and upgrading POS systems will come with a cost to grocers; however, it's difficult to determine the exact price tag because there are many variables, including the current state of a grocer's POS system. However, the cost of new EMV-capable terminals alone will be in the range of $500 - $1,000 per terminal.

And now a benefit: For those merchants who install terminals capable of accepting both EMV contact (to dip) and EMV contactless (to tap) cards: If 75% of the card transactions originate from EMV terminals, then they will be exempt from the PCI DSS validation requirements each year. Merchants must still be PCI compliant; they just won't have to go through the annual validation steps.

What Should Grocers Do Now?

All grocers will eventually want to shift to EMV capable terminals and software; when to do so is the question. If you only sell mostly low-value, perishable items, your risk of merchandise theft via card is probably low — and may stay there. On the other hand, you may want to consider making the change sooner if:

■ You sell higher-dollar, easily resalable items (such as gift cards); this may make you a future fraud target;

■ You are concerned about a possible data breach (they don't just happen to large retailers);

■ Your processor agreement is set to expire in the next year or so. If so, you may be able to negotiate a good deal with your current or a new processor that includes the new terminals.

Dennis Hoyt is a Michigan-based treasury consultant working mostly with retailers and grocers. Areas of expertise include financing, cash management, credit cards, forecasting, and risk management. He can be reached at 616-656-7770 and DHoyt@HoytTreasury.com.