Investigator Insight

“Chip”ping Away at Fraud

What does smart chip technology on credit/debit cards mean to you?

Have you heard the buzz about chip–enabled credit cards, debit cards and an October 2015 deadline? Perhaps you’ve already received new credit cards with a chip embedded on the front of the cards. Let’s take a look at the reason for the change and whether or not it affects your responsibility as the card user.

Merchants need to have point-of-service card readers to accept chip-enabled credit and debit cards (payment cards) by October 2015 to avoid liability for charges made if they accept a fraudulent payment card. Currently the financial loss caused by unauthorized use of a payment card (think lost or stolen) or use of a counterfeit payment card is felt by the financial institution that issued the card. From October forward, however, if a merchant doesn’t have the required system in place at point of service to accept a chip-enabled payment card and accepts a card payment by use of the magnetic stripe, the financial loss resulting from a fraudulent purchase falls on the merchant. If the card issuer hasn’t issued their cards with the smart chips embedded in them and a merchant accepts a fake card, then the loss falls on the financial institution that issued the payment card.

The smart chip technology, also known as EMV (Europe, Mastercard, Visa), in the embedded chip on the front of the payment card has been in use in Europe for several years. It has reportedly cut down on credit card fraud dramatically. Why? Unlike the magnetic stripe that holds static payment information, the chips on the newly issued payment cards provide a single-use authorization code each time the card is used to make a purchase. This makes for a more secure in-person transaction. Stolen payment card data can be added to the magnetic stripe on counterfeit cards and used for making purchases so moving to the chip-enabled cards—which are hard to clone—makes stealing large amounts of payment card data from retailers less valuable to the thief.

There are two types of chip-enabled cards: chip-and-signature and chip-and-PIN. Currently the chip-and-signature cards are more common in the U.S. but the chip-and-PIN card is more secure because it requires the consumer to enter a personal identification number or “PIN” while the card is in the card reader.

How does this affect you, the consumer? Prepare to change how you make a purchase with a payment card—no longer swiping the card's magnetic stripe but, instead, inserting the end of the card with the chip on it into the chip reader during the transaction and entering a personal identification number (PIN) or providing your signature.

Although the liability for an unauthorized transaction will depend on the circumstances of how the payment was accepted and whether or not the appropriate card readers were in place, the consumer still has the same responsibilities as they have today with regard to using and managing their payment cards.

Let's review what consumers should do:

- Even though there are not many merchants verifying anything when you use your payment cards, sign the back of your cards when they are received. Note the statement beside "Authorized Signature" on the back of the card. It reads "Not Valid Unless Signed." Mastercard and Visa security regulations require a signature.
- Check your accounts at least monthly, looking for unauthorized transactions and notifying the card issuer if any unauthorized transactions are found.
- Report the loss of a payment card to the card issuer immediately.
- Dispute any unauthorized charges right away. There are time limits related to reporting unauthorized transactions. While credit card fraud liability is capped at $50 by law, a debit card holder's liability depends upon how quickly the bank is notified of fraud after the consumer learns the debit card number was fraudulently used.
- Assign different PINs to each of their chipped cards. Then if your cards are lost or stolen, it is less likely that a thief would be able to use all of the cards if they were able to get hold of just one PIN.
- Be aware of "shoulder surfers"—those people who watch over your shoulder as you use your card and see your PIN. They could then steal your wallet to access that card and use it to make purchases.
- Use the same safeguards as are currently recommended for making purchases online or by phone and paying with a card. This includes, using secure websites and confirming the legitimacy of the business with which you are conducting business.