What You Need To Know About EMVs

Are you a swiper or a dipper? Chances are, you have at least one EMV chip-enabled card in your wallet.

EMV, which stands for Europay, Mastercard and Visa, and has been used for years throughout the world, was introduced in the U.S. about 18 months ago. The cards are also called smart cards, chip cards, smart-chip cards and chip-enabled smart cards.

Here's what you need to know about the new generation of cards.

1.) Increased protection against fraud

The number one reason the U.S. is making the switch to chip cards is to curb rampant credit card fraud. Things have gotten really bad - before the switch, the U.S. was home to nearly half of the world's credit card fraud!

Experts pin the high rate of fraud on the outdated system the U.S. had been using. The magnetic strips on your old credit and debit cards store static, unchanging data. That means anyone who gets their hands on that data can do whatever they want with it, like racking up huge bills, emptying accounts and taking out loans in your name.

In contrast, EMV cards create a unique transaction code for each purchase you make. That code cannot be used again, so even if a fraudster steals the chip information from a point of sale, they won't be able to use that transaction number for another purchase. The data transmitted during each transaction is also encrypted, adding more to the security measures it offers.

EMV technology will not prevent data breaches from occurring, but it will make it much harder for criminals to profit from what they steal. Experts are hopeful this shift will significantly reduce credit card fraud in the U.S., and studies show that U.S. counterfeit fraud rates have already decreased. According to Visa, chip-enabled merchants saw a 52% drop in counterfeit fraud from 2015 to 2016.

2.) How it works

Like their counterparts, chip cards are processed through the two steps of card-reading and verification. However, there's no quick swipe involved. Instead, you'll be asked to insert, or dip, your card into a terminal slot, and then leave it there as you wait for the transaction to process.

When your card is dipped, data is transmitted from the card chip and the issuing financial institution to verify the card's legitimacy and to create the unique transaction code. This process will take a bit longer than a swipe.

Aside for dipping, EMV cards can also support contactless card reading, also known as near field communication, or NFC. NFC-equipped cards are tapped against a terminal scanner, which reads the data from the card's embedded computer chip.

Contactless transactions are faster and more consumer-friendly than dipping; all you need to do is tap! Unfortunately, though, the equipment needed to scan them is expensive, so this option is not yet widely available.

After you've inserted your card into the payment terminal, the card acts just like your ordinary magnetic-stripe card. You may be asked for a PIN or a signature, which will be transmitted to the payment terminal for

verification and approval. If your merchant is not equipped with a chip-card reader, your EMV card can also be read with an ordinary swipe.

You may find yourself at a point-of-sale terminal, unsure of whether to dip or swipe. No worries - the terminal will guide you. If you enter a card into a chip-reader slot that hasn't been activated, it'll prompt you to swipe your card. Likewise, if you try swiping instead of inserting into an activated chip-reader, you'll be prompted to dip your card instead.

3.) Fraud liability changes

The shift to EMV presents several changes for merchants and financial institutions. Issuing new cards and purchasing new processing technology is an expensive undertaking.

But there's more than just cost involved. The switch to EMV represents new liability rules.

Though fraud is harder to pull off with chip cards, it's still possible. In the event that an EMV card is frauded, who is held responsible?

The rule with transactions conducted using counterfeit or stolen magnetic-strip cards is pretty straightforward: consumer losses fall back on the payment processor or issuing financial institution, depending on the card's terms and conditions.

Card chip-fraud works somewhat differently. Since the Oct. 1, 2015 deadline created by the four major U.S. credit card companies, the liability for card fraud has shifted to whichever party is the least EMV-compliant in the transaction. This means if the merchant is not equipped with chip-card reading equipment, they will be held responsible. If the consumer's financial institution has not provided them with an EMV card, they're footing the bill.

So, while replacing payment processors and issuing new cards is an initially expensive venture, it will save businesses and financial institutions the huge cost of being held responsible for fraud payouts in the long run.

4.) Increase in online fraud

The EMV transition is not all good news on the fraud front. Though it helped cut in-store fraud in 2016, it also gave consumers a false sense of security, spiking online fraud. Chip card or magnetic strip, for an online purchase, makes no difference at all. When buying something on the internet, it's up to you to be extra vigilant and ensure you aren't being frauded.

Fortunately, protecting yourself against online fraud is easy. First, always shop with a reputable retailer and read reviews before sharing your card information. Never give personal information over email, or authorize a wireless money transfer for a website or merchant if you are not familiar with them. Also, consider using tokenized systems like ApplePay, where your personal information is transformed into a numerical token instead of an actual card number.