

A consumer's guide to 'chip' cards

The U.S. credit card industry is making a transition from traditional magnetic stripe credit and debit cards to cards with computer microchips in them.

You can do the same things with "chip" cards—from making purchases to getting cash at an ATM—but using them is a lot safer.

Here's what you need to know about the new "smartcards" in your wallet.

What's changing and why

In the U.S., all cards have a magnetic stripe on the back. This is how store payment terminals—where you swipe your card—process transactions. The data contained in the magnetic stripe never changes, so criminals have found ways to "read" and counterfeit cards. Until the owner or issuer discovered the unauthorized access, counterfeit cards could be used to make purchases or get cash if the criminal also had the PIN.

New credit and debit cards have the magnetic stripe and an embedded computer chip. (If your card has a chip, you'll see a small shiny metallic square on the front, above the first four digits of the account number.)

Each time you use a chip card at a merchant, the chip generates a unique transaction code needed for approval. The code is good only for that transaction. Because the security code is "dynamic" (always changing), it is much more difficult for someone to steal and use it.

Even if there were a merchant data breach or a theft of the chip information, a fraudster could not use that transaction code again, and the stolen data would be useless for counterfeit fraud. This is just one of the ways chip cards help to greatly reduce losses from credit card fraud.

Chip technology also provides a foundation for innovations such as mobile payments. The chip that makes NFC (near field communication) transactions possible and secure is the same technology used in chip cards.



Transition schedule

Some cardholders have already received a chip card. Many others can expect to receive replacements in their mailboxes by the end of 2015. And most others are expected to have them by the end of 2016.

If you want to know when your new chip card will arrive, contact your card issuer at the number on your card.

In order to take advantage of the increased security offered by the chip, merchants must install chip-enabled payment terminals. Many, if not most, merchants will have the terminals installed by October 2015. Others may add them later. Chip readers at ATMs and pay-at-the-pump gas stations are expected to arrive in 2016-2017.

In the meantime, since the new cards will have both the magnetic stripe and the chip, you will be able to use your new card in all the same places you've always used it—even if the merchant doesn't have a chip-ready terminal.

How to use a chip card

Using a chip card in a store will be a little different but just as easy. At checkout, instead of swiping the card along the side of the terminal, you insert the chip end of your card into a slot and leave it there until the transaction is completed. You will then sign for the payment, enter a PIN or pay and go just as you do today.

There will be no change in the way you use your card online or by phone. Until ATMs are equipped

to read chip cards, use your new card at the ATM the same way you do now.

Chip cards also work in other countries, either with or without a PIN. In many cases, such as subway ticket kiosks, international cards can be used without PINs.

Cardholder rights and protections

Chip cards provide the same consumer protections offered by traditional credit and debit cards. Card networks and financial institutions typically provide consumers zero liability for fraudulent transactions. Federal rules also provide basic protections.

Credit cards. Under the Fair Credit Billing Act (FCBA), you can dispute a credit card charge and withhold payment for that amount while it is being investigated.

Your maximum liability for unauthorized credit card charges under federal law is \$50. (Many credit card issuers offer zero liability, so they waive the \$50.) You are not responsible for any unauthorized charges if the card was used after you reported it missing, or if the charges were made with just the card number (while you still had possession of the card).

Debit cards. Under the Electronic Fund Transfer Act (EFTA), you are not responsible for any unauthorized transactions:

- that occur **after** you report your debit card missing, or
- resulting from a stolen card number (while you still had possession of the card) if you report them within 60 days of your statement being sent to you.

When reporting debit card fraud or unauthorized transactions, remember:

- Your maximum liability for unauthorized charges under federal law is \$50 if you report the loss or theft within two business days.
- Your liability increases to \$500 if you report it more than two days after you notice the loss or theft but less than 60 calendar days after your statement is sent to you.
- You could be liable for—lose—all the money taken from your account if you report loss or theft more than 60 days after your statement is sent.



Always report your card lost or stolen as soon as you notice it missing. Review your statement for unauthorized transactions as soon as you get it and report them immediately. This will help you limit your liability.

Learn more

For specific questions about your particular card, contact your card issuer at the number on your credit or debit card.

For general information about chip cards issued by the payment network whose logo appears on your card, visit the company online:

Visa

<http://www.VisaChip.com>

MasterCard

<http://www.mastercard.us/mchip/>

Discover

<http://discvr.co/1S7Wizu>

American Express

<http://amex.co/1FxKVNO> (chip-and-signature)

<http://amex.co/1R0KCNn> (chip-and-PIN)

Credit for this publication

"A consumer's guide to 'chip' cards" was created by Consumer Action with a grant from Visa Inc. It is part of the Consumer Action/Visa Inc. educational project **Know Your Card** (www.knowyourcard.org).

To learn more about Consumer Action, visit us online at www.consumer-action.org.

© Consumer Action 2015