CHIP CARDS

Frequently Asked Questions

How do I know that I have a chip card?

Look for a chip on your credit or debit card. It is a small, metallic square on the front of the payment card. You still have a magnetic stripe on the back of the card so you can use it at retailers that don't yet accept chip cards.

Do I have to pay for a chip card?

Banks are issuing chip cards to cardholders at no cost. You do not have to pay anything.

How do I use my chip card?

Insert your card into the chip-enabled terminal with the chip first, facing up. Leave the card in the terminal until the transaction is complete. You may be prompted to sign your name. If there isn't a chip-enabled terminal, use the card the traditional way and swipe.

If fraud happens on my credit card and I don't have a chip card, am I liable for the transaction?

No. Whether you dip or swipe, you still are not held liable for fraudulent purchases as long as you reported the fraudulent transaction as soon as you noticed it.

What happened on October 1? Why is that date important?

Until October 1, 2015 banks had been required to pay for credit and debit card fraud. Now, whoever has the oldest technology when counterfeit fraud occurs—bank or merchant—determines who covers the fraud costs. Consumers still have zero-liability and are protected from all fraudulent transactions regardless of if they swipe or dip their card to make a transaction.

What does EMV stand for?

It stands for "Europay, MasterCard, Visa." They are the three companies that originally created the standard.

Will chip cards guarantee my credit card information is not stolen?

Chip cards are an important step for keeping your data safe because they make counterfeit fraud virtually impossible. However, no single technology will prevent fraud. Chips are only part of the greater effort being made by banks and networks to combat thieves and hackers.

A lot of media has focused on credit card data being stolen. How does data get stolen?

There have been numerous large-scale breaches at retailers over the past few years that exposed their customers' credit card information. Data breaches at places like Target or Home Depot happen when criminals hack into their computer system and steal customer information.

People talk about Tokenization as the next technology that will protect credit cards. What is it?

Tokenization is an important feature that some mobile wallets, such as Apple Pay, use. Tokenization works by replacing sensitive consumer account information at the cash register or online with a random string of letters, characters and numbers called a "token." The token is only used for that one transaction, rendering the information less useful to criminals if it is stolen.

American Bankers Association®