

Chip Card FAQs

Q: *What is all this EMV hoopla all about?*

A: On October 1, the card networks had a major change in their operating rules regarding the party that would be held responsible for counterfeit card fraud. As of that date, for credit and debit card transactions at a merchant's location, the party that has not upgraded to accept EMV—or chip—cards will assume the liability. If both parties have upgraded, then there will be no liability shift.

Q: *What's so wonderful about this card?*

A: The EMV card provides a number of enhanced security features thanks to the embedded secure microprocessor chip. Upon the card's issuance, the chip contains secure data that serve as card credentials. This information is highly resistant to attacks of card skimming or cloning. During an EMV transaction, the card is authenticated as being genuine and the transaction includes unique, dynamic data. These data prevent the possibility of the transaction data being intercepted and used to conduct additional transactions.

Q: *My payment card doesn't have a chip on it. Does that mean I can't use it anymore?*

A: No. While financial institutions have started reissuing credit and debit cards containing the chip, it is expected that it will be well into 2017 before most consumers' cards are enhanced with the chip.

Q: *If the computer chip is so wonderful, why does the card I received still have the magnetic strip on the back?*

A: Since it will take time for all merchants to swap out their terminals to be able to handle the chip, it is necessary for the card to still be able to use the magnetic strip to conduct transactions.

Q: *Will I still swipe the card the same way at merchant locations?*

A: No. This is the biggest change for consumers. Instead of swiping the card through the terminal reader, the customer will insert, or "dip," the card into the terminal and leave it there for the duration of the transaction since the terminal must maintain contact with the card to complete the transaction. The terminal beeps when it's all right to remove the card. The terminal screen also instructs the customer to remove the card.

Q: *What happens if I remove my chip card before the transaction is complete?*

A: Generally, removing the card during the transaction cancels the transaction. The merchant should instruct the customer how to successfully complete the transaction.

Q: *Are ATMs going through this change as well?*

A: While a very small number of ATMs have been enhanced to accept EMV cards, the liability-shift timetable for ATMs doesn't occur before October 2016.

Q: *What about the card readers at fuel pumps?*

A: The liability shift for fuel pumps doesn't take place until October 1, 2017. This delay is because of the increased cost and complexity related to the conversion.

Q: *I have heard that EMV technology is more than 20 years old. Isn't there more modern card security technology on the market?*

A: While the EMV specifications were first released more than 20 years ago, they have been frequently upgraded and improved. Although the U.S. market has some unique requirements regarding debit cards, the EMV specifications represent a way to achieve global interoperability for credit and debit card transactions.

Q: *Will chip cards completely solve the card fraud problem?*

A: No. There are many different types of card fraud, and EMV addresses only counterfeit card fraud in a card-present environment. Other types of card fraud that are being addressed by other solutions other than EMV include lost or stolen cards and card-not-present (internet, telephone, or mail order) fraud.

Q: *What is the anticipated overall impact of chip card migration?*

A: As seen in other countries, the additional security provided by chip cards will significantly reduce counterfeit card fraud. Since the fraudsters will not go away, it is expected that card-not-present fraud as well as check and fraudulent account applications will come under increased attack. This shift has been seen in other countries, and efforts have been under way in the United States to employ additional techniques to mitigate the risk of fraud in this scenario.