
# EMV — Only Part of the Answer

It's important to understand that EMV® may be a little misrepresented from the perspective of fraud prevention. If you've listened to news programs lately, it's claimed EMV encrypts all data on a card preventing a fraudster from stealing and reusing the card data. The idea of EMV being a universal cure for all card fraud is somewhat misguided. Certainly, EMV protects against the stealing of chip data and creating counterfeit chip cards, but it doesn't protect against fraud occurring from card-not-present (CNP) channels, such as Internet or mobile transactions. In the case where a card has both a chip and magnetic stripe, it doesn't protect the card from being lost or stolen, or magnetic stripe counterfeit card fraud.

## WHAT EMV DOES FOR FRAUD PREVENTION

EMV has a multi-tiered security approach that leverages a dynamic, one-time, per-transaction data attribute called a cryptogram to validate the card. In contrast, the magnetic stripe card has repeatable, static data (CVV, CVC) stored on the magnetic stripe. Combine card validation (something you have) with a PIN (something you know), and a merchant can be confident the card is neither counterfeit nor stolen (this would exclude friendly fraud). If the industry had already fully migrated to chip, meaning all terminals and all cards support chip, counterfeit card fraud would practically disappear because it's nearly impossible to counterfeit a chip card.

## WHAT EMV DOESN'T DO FOR FRAUD PREVENTION

If a merchant moves to EMV today, the merchant's terminals will still be required to support traditional magnetic stripe transactions for the foreseeable future. During the migration period, all EMV cards will be hybrid — containing both the chip and the static magnetic stripe data encoded on the back of the card — for use at merchants that haven't migrated to EMV. The magnetic stripe data is also encoded on the chip and sent in the clear during transaction messages. A fraudster can then copy the data off the magnetic stripe or intercept the message and create a counterfeit magnetic stripe card. Since many merchants don't require PINs, and instead use a signature or no cardholder verification at all, the PIN doesn't have to be stolen to commit this type of fraud. So, until all of the magnetic stripe terminals are replaced by EMV-only terminals (i.e. having chip only and no magnetic stripe capability), a fraudster can steal data from a chip card or a magnetic stripe card.

In addition, many e-commerce websites don't require or prompt the cardholder for CVC2/CVV2 data from the back of the card, so fraudsters can use the stolen magnetic stripe data to commit e-commerce mail or telephone order fraud. EMV doesn't address the fraudulent use of payment data when there's no direct connection, such as when the data is entered into an e-commerce application, given over the phone, or through the mail — in other words, CNP situations.

Iowa State Savings Bank