How Android Pay and EMV Could Make Credit Card Fraud a Thing of the Past

December 1, 2015 - Written By Darla Sutrich

Up until a few years ago, most credit card processing services were content with the status quo of credit card security — a magnetic stripe and a signature. But now things are changing, thanks to massive data breaches like the 2013 Target breech that compromised the personal information of up to 70 million people. These kinds of breeches are expensive for credit card companies, merchants, and consumers alike, and now everyone is more wary of credit card fraud than ever.

That's why Visa and Mastercard are finally issuing EMV-equipped cards in the United States. These cards each bear a secure chip that protects the consumer's personal information from fraud. They've been standard in most other countries for a long time, and now they're making an appearance in the U.S.

But EMV-equipped cards aren't the only option you'll have at the checkout. Google's Android Pay now allows customers to pay for goods and services at participating stores directly from their phones, and some say this technology is even more secure than EMV.

How EMV Protects Against Card Fraud

"EMV" stands for Europay, Mastercard, and Visa, the three credit card processors that originated this secure payment technology. EMV chips in credit and debit cards eliminate the threat of fraud presented by criminals stealing credit card information. With the old-fashioned magnetic stripe system, it's pretty easy for criminals to steal credit card information and use it to create a counterfeit card with the stolen information in its magnetic stripe.

With the EMV technology, however, it's a lot more expensive and difficult for criminals to create counterfeit cards. To understand why, you have to understand how EMV chips work. These chips are actually microprocessors that create a unique transaction code each time the card is used. Even if criminals steal that information, it won't do them any good. Once you get your new EMV credit and debit cards, you won't have to worry about criminals hacking into merchant databases to steal your credit card information.

Most countries using EMV technology opted for a chip-and-PIN system, meaning that when consumers in those countries use their cards, they have to enter a PIN at the terminal to verify their identity. U.S. credit card issuers have opted for the chip-and-signature approach, meaning that users will need to verify their identity as they always have, by signing their name to a receipt. While this might make the transition to EMV technology easier for many card users, it still leaves consumers vulnerable to the threat of card theft.

Under the chip-and-PIN system, thieves can't use a stolen card unless they somehow get hold of the PIN that goes with it. Under the chip-and-signature system, thieves can still use a fraudulent signature to make purchases with a stolen card.

Why Android Pay May Be More Secure

Android Pay is Google's answer to Apple Pay. The app, formerly Google Wallet, will be preinstalled on most Android phones starting this year. The digital wallet will allow users to pay for goods and services from 700,000 physical merchants and 1,000 apps using American Express, Visa, Mastercard, or a checking account.
Users will be able to pay at any merchant with an NFC terminal equipped to process smart phone payments, and since most merchants are updating their payment terminals to comply with new EMV-technology rules, many may go ahead and install NFC-compliant terminals, too.

Many say that Android Pay is even more secure than EMV-equipped credit and debit cards. That's because the service doesn't use your real card information to complete transactions. Instead, it creates a virtual account number that allows you to complete your transaction without compromising your personal information. Each time a purchase is made with the app, you'll receive a confirmation that contains information about where the purchase was made, and from which merchant.

With the help of these confirmations, you'll be able to monitor your account for suspicious payment activity. And you won't have to worry about criminals stealing your phone in order to use your payment app. Thanks to the Android Device Manager, you can lock your phone, change the password, and remove any personal information from the device if it is stolen, to protect your payment information.

Thanks to the adoption of more secure payment technologies, it's getting harder and harder for thieves to steal your personal information. While the days of credit card fraud aren't quite over, enterprising criminals may soon find themselves wishing more people carried cash.