

GOING SMART

U.S. IMPLEMENTATION OF SMART
PAYMENT CARDS ON THE HORIZON





Suppose you're on vacation in the United Kingdom and decide to buy something. You insert your credit card into a payment device, but nothing happens.

Unlike the United States, the United Kingdom uses computer-chip technology, meaning the standard American magnetic-stripe card is useless in the U.K.

Europe began its migration to embedded computer-chip cards for credit, debit and ATM in 2002, when EuroPay, MasterCard and Visa collaborated on EMV, the leading global standard for chip technology. The United Kingdom, Japan, Mexico, Canada and 80 other countries then spent the next decade transitioning to EMV-based cards.

Although the United States was an early adopter of the electronic payment card system based on the magnetic stripe, it has been slow to embrace embedded chips. Less than 1 percent of the cards issued in the United States today use embedded micro-chip technology, even though supporters say it's less susceptible to fraud than magnetic-stripe cards.

There are a number of reasons why EMV has been slow to gain acceptance in the United States. One reason U.S. merchants are reluctant to accept EMV is the expense of replacing the

current system. Card issuers are concerned about issuing millions of cards to reluctant U.S. cardholders.

That reluctance may change.

Discover, American Express, Visa and MasterCard recently announced plans to switch to EMV-compliant, computer-chip payment cards starting in 2015.

What is an EMV card?

There are two common types of EMV smart cards: contact and contactless.

The contact card, often called a chip-and-PIN card, looks like a standard plastic card, but is embedded with a special microchip that contains the same information in a standard card's magnetic stripe. Some smart cards have both a chip and a stripe.

When swiping a card, a consumer must enter a PIN to complete a purchase, similar to using a debit card. The transaction device first reads the microchip to first ensure the card is authentic. The card reader, through the chip, also verifies that the card belongs to the cardholder and the user's PIN approves the transaction.

A contactless card requires only close proximity to a card reader. Both the reader and the card have antennae, and the two



Discover, American Express, Visa and MasterCard recently announced plans to switch to EMV-compliant, computer-chip payment cards starting in 2015. The computer-chip cards will help the industry and consumers combat fraud.

communicate using radio frequencies. The frequency range is one-half inch to three inches. Most contactless cards derive power for the internal chip from this radio signal and are used for entering a building or making payments that require quick transactions without a PIN, such as a subway terminal.

Less common cards on the market are the dual-interface card, which has one chip that allows for both contact and contactless transactions, and the hybrid card, which has two chips, one with a contact interface and one with a contactless interface—the cardholder may use it for either a chip-and-PIN or a contactless transaction.

Smart cards use a process called dynamic authentication. The verification information

on a chip is encrypted and each transaction is assigned a specific code. This code generating process, supporters say, significantly reduces or even prevents thieves from copying and reusing payment verification information.

The widespread use of inexpensive wireless communications made EMV technology possible. The use of wireless PIN pads and readers let customers make transactions without the card leaving their sight.

With the standard magnetic-stripe card, verification information is static, meaning it doesn't change with each transaction, and most card readers are stationary and require a customer's signature. For example: A customer at a restaurant gives the server a card, which is taken to a stationary reader out of the customer's

sight. These out-of-sight transactions are when most card fraud occurs, industry experts say.

Combating fraud

According to the Smart Card Alliance—a nonprofit association that promotes the understanding, adoption, use and widespread application of smart card technology—static, signature authentication lets criminals who get their hands on victims' credit cards make purchases immediately. It's even easier online, where a criminal only needs the account number to make purchases.

And easily available technology enables thieves to wirelessly skim transaction verification information from magnetic-stripe cards, meaning even the most cautious cardholders, those using ATM cards with PINS, may have their information stolen.

Although the incidents of payment card fraud in the United States is small in proportion to the number of daily noncash transactions, Richard J. Sullivan, an economist with the Kansas City Fed, said this immense volume of payment transactions adds up to big losses due to fraud.

U.S. cardholders used more than 1 billion debit and credit cards in 2011, making 69 billion transactions valued at more than \$3.9 trillion. These payments accounted for about 50 percent of all noncash retail payments in the United States.

“Even a small fraction of that kind of volume can amount to billions of dollars in losses for banks and merchants,” Sullivan wrote in his latest research, “The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud.”

Year after year, payment card fraud in the United States results in billions of dollars in losses. In 2007, credit card fraud alone totaled \$16 billion.

The EMV smart card system could vastly change that amount because it aims to make it more difficult for criminals to counterfeit cards, obtain stored information on the chip

and make unauthorized intrusions.

“The fraudsters, phishers, hackers and pickpockets who thrive off payment card fraud may soon have their work cut out for them,” Sullivan said.

Sullivan points to France, the United Kingdom and the Netherlands as examples of how the introduction of the EMV-card could diminish fraud in the United States.

France started using computer-chip cards in 1992; however, the card issuers used static data authentication. Thieves learned to reprogram the cards so any PIN would approve a transaction. France upgraded to EMV cards in 2001 and began using dynamic authentication in 2005. The move helped cut counterfeit credit card fraud and fraud on lost or stolen cards, but this doesn't mean fraudulent credit card activity disappeared.

Not foolproof

Although some types of fraud decreased in France, Sullivan said thieves focused on the types of transactions with weaker authentication methods—orders by Internet, mail and telephone.

The Observatory for Payment Card Security, a French forum focused on the payment card system, reported that by 2010, fraud on Internet, mail and telephone transactions was the top source of payment fraud in France, and although it increased in 2011, it accounted to only 8.4 percent of the total value of all French card payments.

French authorities now encourage merchants to use 3D secure payments, which requires a cardholder to register a payment card with the issuer and creates a PIN for Internet purchases.

Although payment card fraud has declined, French authorities still battle card-present fraud. This transaction involves the card being present at a transaction. Authorities contribute the increase to thieves being able to obtain PINs for the card.

The United Kingdom also faced great losses

due to fraudulent payment card transactions. The U.K. first converted to a dual payment card that had both a chip and magnetic stripe. The Netherlands followed the same transition process, and criminals in both countries took advantage by making counterfeit cards with a magnetic stripe that could be used at ATMs and with merchants that still accepted magnetic-stripe cards.

After 2008, the United Kingdom saw a steep decline in payment card fraud as the European mainland converted to EMV cards, more merchants accepted the cards and 3D authentication was implemented for Internet transactions.

The Netherlands, which took longer to make the conversion, experienced \$56 million in fraud in 2011 with dual chip-stripe cards. The country has now converted to EMV cards, but still faces fraud problems because some cards still have both a chip and a stripe.

Future fraud

Although conversions to the EMV system cut down on stolen and counterfeit card fraud in Europe, thieves still find ways to take advantage of payment card systems.

A new trend is infiltration of payment processing databases by hackers intent on

capturing card and PIN information. Seven individuals were arrested in May after thieves hacked into a database for prepaid debit cards and stole \$45 million from ATMs around the world.

Although fraud will be a concern, research shows that EMV-compliant cards currently are the best deterrent.

For example: if the United States' conversion to smart cards follows the same patterns as in Europe, fraud losses could decrease by 40 percent, Sullivan said.

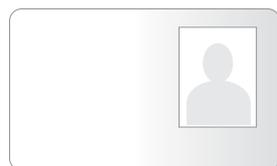
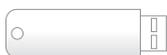
Implementing U.S. smart cards

The learning curve and expense of altering the payment system have been the biggest obstacles to implementing chip technology in the United States.

Other countries' smaller, less-complex financial systems made for easier implementation of EMV. For example: Canada's recent conversion to EMV only took agreement by the five primary financial institutions to change the entire card market.

The United States has the world's largest economy with more than 10,000 card issuers, a million merchants and 8 million point-of-sale devices that accept cards, according to the Smart Card Alliance.

SMART TECHNOLOGY USES



Microchip technology is used in unconnected tokens, one-time password devices, USB tokens, payment cards, employee badges, SIM/UICC for cell phones, electronic passports and identity credentials.



Critics say the combination of the cost of altering the payments system and lack of consumer acceptance, means conversion to an EMV-compliant system could take longer and may not be as successful as in other countries.

Americans carry an average of four cards. Having to remember a PIN for each card may become a frustration that consumers won't accept, especially when a cardholder enters the wrong PIN and a transaction is denied and recorded as suspicious.

This possible scenario prompted Visa and MasterCard to support both a chip-and-PIN and chip-and-stripe option in the United States.

The main incentive for banks outside the United States to issue chip-and-PIN or EMV-based cards was the liability shift.

Ross Anderson, a professor of security engineering at the University of Cambridge, said in a recent interview that the EMV system instituted a higher level security, so if a PIN was used in a fraudulent purchase, the fault for a disputed transaction would fall on the customer and the merchant; while the bank would have no liability.

That shift in liability has not worked, Anderson said, and several countries have already taken action to protect consumers.

In the United States, however, the liability shift wouldn't completely work because of Regulation E.

The goal of the Regulation E is to protect individual consumers who engage in electronic fund transfers. This limits a consumer's liability for loss, theft or other unauthorized transaction to \$50; if the consumer fails to notify the depository institution in a timely fashion, however, the amount may be \$500 or unlimited. In 2006, U.S. card issuers bore a 59 percent share of fraudulent losses and merchants assumed the other 41 percent of liability.

Some American card companies already offer chip-and-PIN cards to American customers who frequently travel abroad or

corporations that do business overseas, and some card companies offer customers a chip-and-signature option. Overseas travelers, however, occasionally report problems using chip-and-signature cards at unmanned kiosks, *Traveler* magazine reported.

Contactless cards also are in use in the United States, but mainly as security devices, such as for keyless entry. And the few contactless payment cards in use have limited acceptance.

Randy Vanderhoof, director of the Smart Card Alliance, said in a recent interview that businesses only make investments in wholesale system changes if there's a substantial return on investment. Recouping billions of dollars in fraud losses could be that incentive in the United States, he added.

But currently the United States does not have a comprehensive system for collecting and reporting statistics on payment fraud, Sullivan said.

"Timely information on the sources of fraud allows policymakers and the card payment industry to respond swiftly and effectively to new attacks," Sullivan wrote.

This also allows both regulators and the industry to measure the levels and sources of fraud and identify who pays the price, and how much, for the nation's fraud losses.



KEVIN WRIGHT, TEN EDITOR

FURTHER RESOURCES

"The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud,"

by Richard J. Sullivan.

www.kansascityfed.org/publicat/econrev/pdf/13q1Sullivan.pdf.

COMMENTS/QUESTIONS are welcome and should be sent to teneditors@kc.frb.org.