US gets chance to catch up on credit card security

September 9 2011, By PETER SVENSSON , AP Technology Writer

Two bank smart cards are displayed in London, Friday, Sept. 9, 2011. Smart cards with built-in chips, are the equivalent of a safe: they can hide information so it can only be unlocked with the right key. Because the important information is hidden, the cards can't be copied. The cards are recognizable by the fingernail-sized gold contacts embedded on one side. Through the contacts, a chip inside the card can transmit information to a terminal when slid into a slot. (AP Photo/Martin Cleaver)

The next time you swipe your credit card at check-out, consider this: It's a ritual the rest of the world deems outdated and unsafe.

The United States is the only developed country still hanging on to credit

and debit cards with those black magnetic stripes, the kind you swipe through retail terminals. The rest of the industrialized world has switched -or is in the process of switching- to "smart" chip-based cards.

The problem with that black magnetic stripe on the back of your credit card is that it's about as secure as writing your account information on a postcard: everything is in the clear and can be copied. Card fraud, and the measures taken to prevent it, costs U.S. merchants, banks and consumers billions each year.

The smart cards can't be copied, which greatly reduces the potential for fraud. Smart cards with built-in chips are the equivalent of a safe: they can hide information so it can only be unlocked with the right key. Because the important information is hidden, the cards can't be replicated.

But the stripes have been so entrenched in the vast U.S. payment system that banks, payment processors and retailers have failed to reach consensus on how to revamp it, leaving the U.S. behind the rest of the world.

"The card system in this country has been dysfunctional for a long time," says Mallory Duncan, general counsel of the National Retail Federation. "We have far, far too much fraud because we have a very antiquated payment system relative to the rest of the world. This is something they should have fixed a long time ago."

Yet even here, there are now serious moves to swap conventional cards for smart cards in a few years.

Last month, Visa announced new policies that will give U.S. banks a reason to issue smart cards and stores several reasons to accept them, starting in 2015.

Eric Schindewolf, product manager for smart cards at Wells Fargo & Co., says Visa's announcement is a "watershed" moment.

"I think that the U.S. has reached a tipping point. You'll begin to see more and more smart cards in the hands of U.S. consumers," Schindewolf says.

Smart cards are recognizable by the fingernail-sized gold contacts embedded on one side. Through the contacts, a chip inside the card can transmit information to a terminal when slid into a slot.

Here's how a smart card works in practice: When it's time to settle the bill at "Le Gaspard de la Nuit," a tiny restaurant just off the Place de la Bastille in Paris, the waiter brings to the table a wireless payment terminal. The customer inserts his chip-equipped "smart" credit card and enters his code on the keypad.

Voila! The foie gras is paid for without the card leaving the customer's sight, and the combination of chip and PIN code kept the transaction safe from fraud.

The U.S. payments industry has so far been locked up in a "chicken and egg" quandary, Schindewolf says. Stores had little reason to install terminals for smart cards if banks didn't issue them, and aside from some contactless cards, banks didn't issue them because stores wouldn't accept them.

The impasse has left U.S. businesses and consumers struggling with higher fraud rates. Richard Sullivan, the senior economist in payments research at the Federal Reserve Bank of Kansas City, says that in 2006, 9 cents out every $100 paid by card in the U.S. ended up in the pockets of criminals. The comparable figure for Spain was 2 cents. Sullivan believes the use of smart cards there is a big reason for the difference.

Other factors play a role, too. Spaniards, for instance, are less likely to shop online.

Javelin Strategy & Research puts the amount of fraud based on stolen card numbers in the U.S. at $14 billion. Fraud based on new card accounts created using stolen identities adds billions more - the total cost of identity fraud in the country is $37 billion.

Visa's move comes as industry experts are warning that U.S. merchants are set to become targets for fraudsters in other countries where payment systems already have tighter security. Since counterfeit magnetic-stripe cards are now difficult to use in other countries, these criminals will probably ship the cards to the U.S.

That prospect is especially worrisome now that Mexico and Canada, are adopting smart cards, experts say.

"There's already evidence that that type of channel for fraud is increasing in the U.S.," says Sullivan.

The U.S.'s status as a holdout has also started to cause problems for travelers. While most European stores and restaurants still accept magnetic-stripe cards, Americans are finding that their credit cards don't work in European automated kiosks, like the ones that sell tickets for the Paris Metro. Some U.S. banks, like Wells Fargo, have started issuing smart cards to customers who travel abroad.

Next year, Visa will start dangling this carrot in front of store owners: If they replace most of their terminals with ones that accept smart cards, they will no longer need to have their payment-system security checked every year. U.S. stores spend hundreds of millions of dollars a year for these audits, according to the NRF.

In an even more momentous shift, in 2015 Visa is shifting the liability for a certain kind of fraud from the banks to stores.

The specific case is this: If a customer presents a smart card in a store that can't accept it, then it will fall back to using the backup magnetic stripe on the card. If that transaction turns out to be fraudulent, the payment processor will be liable, and in practice, make the store eat the loss. Today, the bank would be liable for the fraud.

The change means that banks will have an incentive to put chip-based cards in their customers' hands, since their fraud liability will be reduced when the cards are used. For their part, stores will have a reason to install smart card terminals, because otherwise, their fraud costs could increase.

Javelin puts the cost of moving to chip-based cards at about $8 billion, mostly for upgrading payment terminals in stores.

The retail federation's Duncan calls Visa's move a necessary step, but not a fully satisfactory one. One of the shortcoming he sees is that it doesn't mandate the use of PIN codes with smart cards, so even if the cards can't be copied, they could still be used on a signature basis if stolen.

Smart cards won't help secure online payments either, at least not initially, so that will remain an avenue for fraudsters. But they could help secure online transactions if paired with computers that can communicate with the chips, perhaps through accessory card readers. (American Express issued PC readers for its Blue smart card in 1999. But the "smart" features on the card were proprietary to Amex, and saw very little use.)

Phone makers are also starting to build smart-card chips into cellphones, which could then be used in place of cards at "contactless" terminals and perhaps help secure online shopping done through the phone.

The world's largest retailer, Wal-Mart Stores Inc. can't wait for smart cards to come fast enough. It's frustrated with the gaping security holes in the current payment system and wants to save money on card-acceptance fees that are inflated by fraud.

Wal-Mart has already installed terminals with slots for smart cards in all its U.S. stores, and it's working on getting the behind-the-scenes software working, so it can start accepting payments. It, too, sees PIN codes as essential to the security of the system.

"Signatures are a waste of time," says Jamie Henry, senior director of payment services at the company. "They add no value to anyone."