Data Security

Why U.S. Retailers Are Still Vulnerable

- Businesses are behind schedule in upgrading card payment systems
- "We want to activate early if there are any problems or bugs"

After last year's massive security breaches at **Target** and **Neiman Marcus**, data security pros urged U.S. retailers to upgrade their credit and debit card technology to reduce fraud. Companies have been slow to embrace the more secure payment systems that have been widely used in Europe and Asia for years, mostly because of the expense and a lack of synchronization among retailers, credit card providers, and banks.

Many companies are behind schedule in updating their systems to comply with a chip-based smart card standard known as EMV (for Europay-MasterCard-Visa, the companies that first backed the technology). Credit card networks have set an October 2015 deadline for most U.S. merchants to upgrade their payment systems. EMV is considered more secure because it's harder to copy account numbers and security codes from chips than from the magnetic strips on most cards used in the U.S. EMV cards create a unique code for each transaction, making them more difficult to hack or counterfeit than striped cards.

Merchant Warehouse, which processes credit and debit card transactions for 80,000 U.S. merchants, projects that only about 60 percent of its clients' locations will be ready to accept chip-based cards by the deadline. Richard Crone, chief executive officer of payments advisory firm Crone Consulting, says more than half of U.S. merchants will miss the cutoff.

One reason for the delay is the upgrade's high cost—$500 to $1,000 per payment terminal, according to researcher Javelin Strategy & Research, a division of Greenwich Associates. Retailers are also concerned that the switch will slow checkout times and that it remains unclear how the EMV software will work with debit cards. "It is not a question of just turning it on," says Margaret Chabris, a spokeswoman for **7-Eleven**. "EMV specifications are still being finalized."

Still, some big retailers, including **Wal-Mart Stores**, **Kroger**, and Target, have pushed ahead with the upgrade. Wal-Mart started updating its payment terminals in U.S. stores eight years ago. The company says it has progressed slowly because of a lack of industry support, despite the clear benefits. "We saw the fact that it was being implemented in the U.K. and many other countries around the globe; we saw the fraud decrease once this solution was implemented," says Mike Cook, assistant treasurer at Wal-Mart.

All of Wal-Mart's 4,838 U.S. stores (including Sam's Clubs) have the chip-based hardware in place. Of those, 1,000 have turned it on. By yearend, Wal-Mart says, the new payment terminals will be running in all of the company's U.S. locations. "We want to activate early if there are any problems or bugs to be worked out," Cook says.

For terminals to provide added security, customers must have chip-enabled cards. "Part of the reason we haven't pushed faster is there're just no cards out there for acceptance," Cook says. Today, with about 1 billion cards in use in the U.S., just 20 million chip cards have been issued, according to Smart Card Alliance. Only 20 percent to 30 percent of U.S. card holders will have the new cards by the deadline, says Nick Holland, an analyst at Javelin.

The new cards can cost up to $2 each, compared with pennies for the magnetic-stripe models. "We've got 10 million cards in inventory out in the field," says Mark Putman, a senior vice president for First Data, which offers prepaid card services. "At $2, we are probably looking at a $20 million investment, which I am going to defer for as long as possible."

Retailers are willing to do their part to improve security, the National Retail Federation says, but banks and card companies also have a responsibility to update their systems. That includes making and issuing chip-enabled cards.

The price for not complying could be high. Credit card companies have said most retailers and banks will be liable for some fraudulent in-store transactions if they don't have the new system. Even so, "merchants aren't crazy about this migration to EMV, and many of them are fighting it tooth and nail," says Julie Conroy, an analyst at Aite Group.

—Olga Kharif and Bianca Vázquez Toness

The bottom line U.S. retailers and banks could be liable for fraudulent transactions if they don't adopt a new, more secure payment system.

Smarter Cards

EMV cards, known by their gold, squarish symbols, are inserted into a card payment terminal, where they stay securely until the transaction is complete.

Benefits

Security
The chips are harder for hackers to copy.

Data
A unique transaction code is generated each time the card is used.

Pitfalls

Adaptation
Consumers will have to be trained to use chip cards, and that could slow down store lines.

Price tag
Chip cards aren't cheap and require the installation of expensive new payment terminals in stores.

OBAMA: ROBYN BECK/AFP/GETTY IMAGES; CREDIT CARD: AARON FOSTER/GETTY IMAGES
ILLUSTRATION BY 731; PATEL: COURTESY OF AARON B. HO-SKELLY/PAYRANGE