Retail breaches could fuel push for safer cards

January 17 2014, by Joan Verdon

The Target credit and debit card and personal information breach, which last week was revealed to have affected more consumers than originally thought and which may be linked to attacks on other retailers, is expected to prompt U.S. retailers to speed up the adoption of more secure "chip cards" which are now used in Europe.

U.S. merchants and card issuers have been reluctant to take on the expense of switching to the smart-card technology already in place in most European countries. But the breach is demonstrating the danger of postponing the change.

Retailers and card companies are still using the equivalent of "eight-track tape from the 1960s" - magnetic strips on the backs of cards - when they should be using computerized chips, Matthew Shay, chairman and chief executive officer of the National Retail Federation said this week in an appearance on CNBC.

In full-page ads published in newspapers Monday, Minneapolis-based Target Inc. also said it would be pushing for the new technology. Target, which has faced criticism for its handling of the crisis, went on a public relations offensive Monday with the ads and an appearance by its chairman and CEO, Gregg Steinhafel, on CNBC.

The Target breach has switched the mood of the retail industry from complaining about the chip-card changeover to actively campaigning for it. It won't be cheap, and it won't come soon. The National Retail

Federation has estimated that full implementation of chip cards will take five years and cost more than $10 billion.

"It's going to heavily influence their decision-making over the next two years about where to put their priorities and their spending," said Randy Vanderhoof, executive director of the New Jersey-based Smart Card Alliance, an industry association created to promote the switch from magnetic strip credit and debit cards to chip cards - cards with embedded microprocessors with additional security features.

On Saturday, retailer Neiman Marcus confirmed that it learned in mid-December that cards used at its stores had been compromised, but did not disclose how many cards were involved. Neiman Marcus confirmed the breach in response to questions from security blogger Brian Krebs, who also broke the news of the Target breach.

Also Saturday, Reuters reported that, according to sources, at least three other major retailers, not identified, suffered smaller security breaches during the holiday season that may have been trial runs for the Target breach.

On Friday, Target announced that personal information, including email addresses, phone numbers and home addresses, had been stolen from 70 million customers, in addition to the 40 million credit and debit card numbers that had been compromised.

Steinhafel, in an interview with CNBC that aired Monday, said the company believed that no additional breaches would be revealed. He said Target would "make significant changes" to protect customers and "come out at the end of this a better company."

Steinhafel also said that investigators found malware on the company's point-of-sale systems that collected the card information. He defended

Target's decision to delay notification of customers for four days after the breach was discovered, saying those days were needed to fix the problem, begin the investigation and prepare employees to answer customer questions.

The United States Secret Service, responsible for the security of the nation's financial payment systems, is investigating the Target security lapse.

Steinhafel said on CNBC that the new smart-card technology should be adopted to make consumers less vulnerable.

U.S. retailers have balked at making the "huge financial investment to replace their card-acceptance infrastructure, and the back-end software-processing systems that are required to accept these more secure chip cards," Vanderhoof said. But the Target breach, which highlighted the cost to retailers in the form of "brand equity risk and reputational loss," is likely to convince retailers to make the change sooner than originally planned. Retailers have not agreed to an expedited date to switch.

The fact that personal information such as emails also was compromised indicates that the attack on Target's systems was more extensive than it originally appeared. When the news of the stolen credit and debit card numbers broke in December, security experts assumed the breach was confined to Target's point-of-sale system. The news of the stolen personal information probably means the breach extended deeper than the point-of-sale system.

The success that cyber-criminals have had in breaching existing payment systems convinced the leading credit card companies in 2011 and 2012 to begin establishing a timeline for the switch to the smart cards. MasterCard, Visa and other leading card brands have agreed to make October 2015 the target date for when retailers should be ready to accept

the chip-embedded cards.

That target date isn't a deadline by which all retailers must switch to systems that accept chip cards, but retailers will risk being held liable for fraud losses if they continue to use a less secure payment acceptance system.

The cards, also called EMV cards (short for Europay, MasterCard, Visa - the three payment card brands that developed the chip cards) were first created in 1996. More than 1.5 billion EMV cards have been issued since then, but most of those are being used in Europe. Only about 1 percent of the 1.2 billion cards in this country are chip cards, according to the Smart Card Alliance.

The smart cards have the capability of adding cardholder verification features, such as being able to recognize a PIN, a signature or even a biometric identifier, such as a fingerprint or an iris scan, that would prevent the cards from being used by a thief.

The U.S. has lagged behind Europe for two reasons, Vanderhoof said: It was easier to make the change in European countries, with fewer retailers and cardholders, and European countries had a bigger problem with payment-card information theft.

"As big and complex as the U.S. market is, it's also the most efficient at minimizing fraud losses and has the lowest rate of credit and debit card fraud as a percentage of total card transactions of any country in the world," Vanderhoof said. Card fraud has been estimated at $5 billion a year, he said, a fraction of the more than $16 trillion U.S. economy.

Previously, card issuers and retailers considered card fraud a manageable expense, and less costly than replacing the cards in the U.S. and the 10 million card readers in stores, Vanderhoof said. But the Target breach

has alarmed the industry, he said.

"Attention will be paid toward getting to the EMV standard faster than they may have considered in the past, because of recent events," he said.