US a laggard in adopting more secure credit cards

December 24 2013, by Chris O'brien

The massive data breach at Target last week has again highlighted how the United States remains a relatively insecure backwater when it comes to credit-card technology.

Over the last decade, most countries have moved toward using credit cards that carry information on embeddable microchips rather than magnetic strips. The additional encryption on so-called smart cards has made the kind of brazen data thefts suffered by Target almost impossible to pull off in most other countries.

Because the United States is one of the few places yet to widely deploy such technology, the nation has increasingly become the focus of hackers seeking to steal such information. The stolen data can easily be turned into phony credit cards that are sold on black markets around the world.

"The U.S. is one of the last markets to convert from the magnetic stripe," Randy Vanderhoof, director of the EMV Migration Forum. "There's fewer places in the world where that stolen data could be used. So the U.S. becomes more of a high-value target."

EMV stands for Europay, MasterCard and Visa and is the technology standard that involves placing an integrated circuit of some kind into a credit card. Most European and Asian countries began adopting the technology a decade ago, pushed by regulators in those countries.

About 80 countries use smart credit cards, which allow for greater encryption and security. By comparison, only about 1 percent of credit cards issued in the U.S. contain such technology.

Smart cards in most countries are so widely adopted that U.S. travelers are increasingly running into problems using their magnetic stripe cards when they travel abroad. Banks and credit card companies often advise customers to request a smart credit card they can use for foreign travel.

The reason such technology has been embraced is simple: Hacking into a system to collect information on a chip and then creating a counterfeit credit card using similar technology is too complicated. As a result, hackers have increasingly turned to the U.S., where the cards are significantly easier to duplicate because information is stored on a common magnetic strip.

"The U.S. is slowly issuing these cards to users," said Joram Borenstein, vice president of Nice Actimize, which helps companies analyze their security systems. "It's harder to commit fraud against these cards. You have to steal the chip information, and that's a lot more difficult."

The reasons the U.S. lags so badly in adopting smart cards are complicated, experts said. In part, there hasn't been the political will to demand that businesses and financial institutions make the change. Analysts also say the payment processing system in the U.S. is more complicated, with merchants, credit companies and banks reluctant to spend the big bucks it would take to convert a system with 1 billion credit cards to EMV from magnetic stripes.

"It's a function of our system of government and culture," said Ben Woolsey, director of marketing and consumer research for CreditCards.com, which enables consumers to compare credit card offers. "Moving in that direction is going to be costly for the card

industry and retailers."

The good news for consumers is that the U.S. is indeed moving to embrace smart credit cards. In the last couple of years major card issuers have laid out road maps for upgrading the card technology, and many have set out to achieve this by October 2015.

At that point, major credit card companies will change their rules about who is liable for fraudulent purchases caused by security breaches. Under the new rules, the entity in the payment chain - merchant, credit card, banks - deemed to have the weakest security will be liable. Credit card companies can't make anyone adopt the technology, but they're giving them a hard nudge.

"The road map and larger migration has provided issuers and merchants with the flexibility to manage their business and technology decisions," Jim Issokson, a MasterCard spokesman, said in a statement. "The decision on if, how and when EMV will be implemented has been and will continue to be made independently by each issuer and merchant."

Still, it will take a while for the switch to happen.

Vanderhoof's organization estimates there are 10 million to 15 million smart credit cards now in the United States, less than 1 percent of all credit cards. It projects that number to grow to 50 million to 70 million by 2014. In addition, because the changeover is more costly and complicated for gas stations, they have until October 2017 to make the change. Several observers noted that it's possible the latest breach at Target will provide additional financial and political momentum to make the switch happen faster, though Vanderhoof cautioned it was too soon to say for sure.

"What we really need to do is make the investment in this new chip

technology so there's no value in stealing that information," Vanderhoof said.

Will Pelgrin, chief executive and president of the Center for Internet Security, said the new technology would be a big step forward in fighting fraud. But he also cautioned against thinking it would solve every problem. Hackers, he noted, are constantly evolving their strategies, and companies need to remain vigilant and continue to invest in securing and monitoring their networks even when the smart card era takes hold.