Costly shift to new credit cards won't fix security issues

March 3, 2015 By: Nandita Bose Reuters

http://finance.yahoo.com/news/costly-shift-credit-cards-wont-120000448.html

CHICAGO, March 3 (Reuters) - New technology about to be deployed by credit card companies will require U.S. consumers to carry a new kind of card and retailers across the nation to upgrade payment terminals. But despite a price tag of $8.65 billion, the shift will address only a narrow range of security issues.

Credit card companies have set an October deadline for the switch to chip-enabled cards, which come with embedded computer chips that make them far more difficult to clone. Counterfeit cards, however, account for only about 37 percent of credit card fraud, and the new technology will be nearly as vulnerable to other kinds of hacking and cyber attacks as current swipe-card systems, security experts say.

Moreover, U.S. banks and card companies will not issue personal identification numbers (PINs) with the new credit cards, an additional security measure that would render stolen or lost cards virtually useless when making in-person purchases at a retail outlet. Instead, they will stick with the present system of requiring signatures.

Anre Williams, president of global merchants services at American Express, cited cost and complexity as reasons for not issuing PIN numbers, which would require a much larger investment by card issuers. "It is the PIN management system that takes the effort," Williams said, in part because of the additional customer support it requires.

Chip technology has been widely used in Europe for nearly two decades, but banks there typically require PINs. Even so, the technology leaves data unprotected at three key points, security experts say: When it enters a payment terminal, when it is transmitted through a processor, and when it is stored in a retailer's information systems. It also does not protect online transactions.

"The simplest way to circumvent chip-and-PIN is to use a stolen card number to make an online purchase," said Paul Kleinschnitz, a senior vice-president for cyber security solutions at card processor First Data Corp.

Analysts predict that credit card fraud at brick-and-mortar retailers will fall after the introduction of chip-enabled cards, but that online fraud will rise, as has happened in other countries using the technology. Research and consulting firm Aite Group estimates U.S. online card fraud will more than double to $6.6 billion from $3.3 billion between 2015 and 2018.

Retailers and security experts say it would make more sense for the United States to jump instead to a more secure system, such as point-to-point encryption. This technology is superior to chip-and-PIN, which first was deployed about 20 years ago, because it scrambles data to make it unreadable from the moment a transaction starts.

But the newer technology would cost as much as twice what the chip card transition will cost, and does not have the older technology's long track record.

Moreover, some security experts say that mobile payment services such as Apple Pay, a service from Apple that stores data on the cloud, have the potential in coming years to secure payments without the need to swipe or tap a card at all.

LIABILITY FOR BREACHES

The dispute over the effectiveness of dueling payment security systems offers insight into a broader battle over who bears liability for breaches: retailers or the financial firms that extend the credit.

Currently, card issuers are generally liable for fraudulent charges. After the October deadline, if a retailer is not using a terminal that can read the new cards and a security breach occurs involving a chip card, the retailer will be liable, though consumers will still deal with their banks in the event of a fraudulent charge. If the retailer is chip-and-PIN enabled, the card issuer will be liable.

The liability issue has engendered anger on the part of some retailers, but it has also provided an incentive for compliance with the new standards.

"When banks and card companies are only concerned about shifting the liability to the retailer, you have to comply first," Brooks Brothers Chief Executive Officer Claudio Del Vecchio said. "And then think of solutions that will fix your problems."

The clothing retailer expects to meet the October deadline, but Del Vecchio declined to give details on the cost involved.

Banks and card companies argue that chip-enabled cards are a needed first step toward defending against the use of lost, stolen, or counterfeit cards. "The first thing we need to do as a country is secure face-to-face transactions," said Carolyn Balfany, senior vice-president of product delivery for MasterCard, one of the companies involved in setting the new standards known as EMV, which stands for Europay, MasterCard and Visa.

And there are reasons that banks and card companies haven't yet embraced newer, more secure systems.

"A payment standard that is accepted globally will substantially reduce transaction costs for them," Rick Dakin, chief executive officer of cybersecurity risk and compliance firm Coalfire. "Also they have already done the heavy lifting for EMV so they are ready and pushing for it," he said.

Dakin, who is advising a group of banks on payment security, said no industry standard exists for the newer point-to-point encryption systems, and banks and card companies are hesitant to make large-scale investments before the standards are set.

Banks and card companies said a chip card alone can make stolen data less useful for hackers and the technology has worked in reducing counterfeit card fraud in Europe and elsewhere.

Security experts said the shift cannot prevent massive consumer data breaches of the sort that recently hit Target and Home Depot. But the technology will make it more difficult to use stolen data.

BIG SPEND

With the October deadline approaching and the upgrade costs hitting retailers' income statements, some merchants remain unaware of the required changes, while others have renewed their focus on the shortcomings of chip technology.

"As the deadline approaches, retailers realize they are stuck with this massive investment they have to make for a technology that does not solve the problem," Dakin said.

The installation of 15 million payment terminals that can read chip cards in the U.S. will cost approximately $6.75 billion. Banks are expected to spend some $1.4 billion to issue new cards and another $.5 billion to upgrade their Automated Teller Machines according to Javelin Strategy & Research.

The upgrade of a single payment terminal to chip-and-PIN capability costs between $500 and $3000, depending on features. It would cost between $1000 and $4000 to install a point-to-point encryption terminal, security experts said.

"The problem now is how do we allocate our capital in a way that addresses EMV first and then immediately find the funds to upgrade again and install a better solution," said Grant Shih, vice president for IT development at kids clothing retailer Carter's Inc.

For some small merchants, however, the problem is even more basic: Knowing what will be expected of them in October.

Six of 10 small retailers in Chicago interviewed by Reuters said they had no idea about the deadline later this year and have no plans to upgrade their payment terminals. Three others said they had heard about the shift, but that their businesses were small and hadn't had problems with fraud that would justify the expense of installing new equipment. Only one business owner said she would like to upgrade terminals, though she says cost is an impediment.

Anne Manion, owner of the women's clothing and accessories boutique Girl Hour said she doesn't think small businesses are as exposed to data breaches as large retailers are, but she is still thinking about reaching out to her bank about upgrading terminals at two of her stores.

"The cost implications are important and I'm going to wait and see if by the end of the year there is a way to rent these terminals instead of buying them," she said. Manion already pays a $500 fee every month for the two card terminals she now has.

The Retail Merchants Association said it believes a majority of small retailers are aware of the risks from card fraud but haven't started making the required investments yet. The group is developing a plan to explain the shift in liability and will start reaching out to smaller merchants soon.

"Many small retailers have a tendency to wait until the very last minute until they realize they absolutely have to spend that money because for them cash is king," said Sarah Paxton Vice Chairman of the Retail Merchants Association, in Richmond VA.

(Reporting by Nandita Bose, Editing by David Greising, Peter Henderson and Sue Horton)