No quick solution to payment card hacking

February 21 2014

Consumers shell-shocked by the escalating size and frequency of payment card hacks like the one that recently struck Target aren't likely to get much relief any time soon.

If anything, security experts say, the situation will worsen for American shoppers before it improves, if it ever does.

The U.S. relies largely on payment cards with magnetic strips - described by one retail trade group as "antiquated" and especially prone to fraud - instead of more secure systems already in place in most other countries. The vulnerability makes the United States a prime target for hackers.

A belated switch to credit cards with encrypted chips is set to kick in next year, but security experts are skeptical of its ability to keep cybercriminals at bay. And despite the growing costs of payment card hacks, the retailers, card companies and banks responsible for safeguarding consumers' financial information continue to butt heads over how best to stem the losses.

Amid the finger-pointing, politicians are weighing whether the government needs to get involved in ensuring greater payment card security.

President Barack Obama took a step in that direction last week by unveiling guidelines aimed at prodding companies that oversee essential services such as banking to better protect themselves from cyberattacks. The release came a week after Congress held a series of hearings

demanding that retail and financial industry leaders explain how they planned to secure customer information.

Security experts fret that failure to act could threaten consumer trust in the plastic cards that drive the national economy.

"This has the potential for people to question the viability of our payment system," said Venky Ganesan, a venture capitalist with Menlo Ventures, who focuses on cybersecurity investments. "If people lose faith in the payments system, you're going to have the economy gum up."

Though e-commerce is a fast-rising sector, sales in bricks-and-mortar stores still account for 94 percent of all U.S. retail purchases, according to Javelin Strategy & Research. Credit and debit cards are used in half of those transactions.

Last year, nearly 70 billion payments, worth about $4 trillion, were made with credit, debit and prepaid cards in the U.S., according to industry tracker Nilson Report.

The Target breach was a stark reminder of just how vulnerable those plastic cards are.

Cybercriminals accessed credit and ATM card numbers of about 40 million customers and also stole personal information from up to 70 million shoppers by hacking the card readers. Soon after, major breaches were also discovered at Neiman Marcus and Michael's.

The information was then sold on the black market and used for fraudulent charges, the amount of which investigators are still trying to determine. Credit card consumers are not liable for the fraudulent charges made with the stolen information, but some are having to spend

hours repairing dinged credit scores or clearing up a transaction.

The costs to banks and retailers are mounting in the aftermath.

The Target hack alone has cost credit unions up to $30 million to reissue cards and staff up call centers to handle consumer inquiries, according to the Credit Union National Association. Member banks of the Consumer Bankers Association have reissued more than 17.2 million payment cards, at a cost of $172 million. A report from Jefferies & Co. calculated that Target could face penalties of $400 million to $1.1 billion from the payment card industry because of the breach.

Still, the thefts came as no shock to security industry insiders. A study from Verizon Enterprise Solutions released last week found that just 11 percent of merchants are fully compliant with credit card security standards.

"That's a surprise, because the standard is not about rocket science," said Rodolphe Simonetti, managing director of payment card industry services for Verizon.

These thefts are just the tip of a very large iceberg. The Secret Service cybercrime investigations team has arrested more than 4,900 suspects associated with $1.37 billion in fraud losses in the last four years.

Banks managed to stop about $13 billion in attempted fraud last year, according to the American Bankers Association. But there were still more than 600 breaches during that period, a 30 percent year-over-year increase, according to the Identity Theft Resource Center.

Cleaning up the mess will be complex and costly. And a consensus on how to do it remains elusive.

The U.S. is an island when it comes to plastic cards with personal financial information stored on magnetic strips - a tool in use since the 1960s. Most other countries ditched the cards years ago in favor of a version known as EMV, a chip-based means of securing payment transactions developed by Europay, MasterCard and Visa.

Without this added layer of security, American credit cards have become easy pickings for thieves who swipe the data and sell it to counterfeit card makers.

"All the issues we are seeing are the result of the legacy systems we have in place," said Alphonse Pascual, a senior analyst for Javelin. "This information can be stolen by anyone."

Rather than push the costly EMV technology, credit card companies joined forces in 2006 to create the Payment Card Industry Security Standards Council. The council was charged with facilitating the adoption of tighter protections against the theft of consumer data.

Some credit the group for improving security and creating investigation and reporting standards. Many criticize the council as being too passive.

Either way, Troy Leach, PCI's chief technology officer, insisted during the recent congressional hearings that the group is better equipped than legislators to handle data security.

"High-profile events such as the recent breaches are a legitimate area of inquiry for the Congress, but should not serve as a justification to impose new government regulations," he said.

Already, Sen. Patrick Leahy, D-Vt., has reintroduced the Personal Data Privacy and Security Act, which he first sponsored in 2005. The bill would create, in part, new rules for data breach notification and securing

customers' personal information.

The payments industry has set a 2015 deadline to implement the chip technology in U.S. cards.

But the timetable isn't a requirement. Instead, credit card companies are compelling retailers and banks to make the switch by refusing to foot the bill for fraud that could have been prevented by EMV cards after the deadline.

Target recently said it will accept EMV cards by early 2015 and accelerate its investment in chip technology.

But many retailers are balking at the estimated $20 billion to $35 billion they'll have to spend to replace their point-of-sale technology, including the $9 billion to $15 billion in terminals that would have to be swapped out.

In addition, retailers want cards that also require personal identification numbers but complain that banks are calling for chip-and-signature cards, which are more easily counterfeited.

Mallory Duncan, general counsel for the NRF, calls such cards a "half-baked solution" or "like locking the front door and leaving the back open."

"It's a very expensive transition," Duncan said. "No one wants to spend billions of dollars to swap out equipment if there won't be chip-and-PIN cards."

And EMV may be just a partial stopgap, said many security experts, who note that the cards would not have prevented the kind of data breach that occurred at Target.

And although adoption of the cards cut back payment card fraud in Europe, some countries have recently begun to see an increase in fraud online, where EMV's protections aren't effective.

"Fraud is like a balloon," Pascual said. "You squeeze one end, and it pops up in another. I don't like seeing EMV thrown out as a panacea."

Many security companies are pressing for more radical shifts, encouraging tactics such as greater encryption of data and biometric shields, such as fingerprint scanners.

Many, though, are just bracing for the next attack.

"This is the largest economy, and most of the largest merchants in the world are here - it's the best place to commit fraud," said Sterne Agee financial technology analyst Jennifer Dugan. "They're trying to get it done before the doors close and all that data is rendered less usable to them post-EMV."