Cards with microchips could become more common

February 11 2014

The "chip" is coming. Amid relentless revelations of cyberthieves stealing our credit card and other personal data, there's a renewed push to fortify the plastic cards sitting in millions of Americans' wallets.

Specifically, the buzz is about switching U.S. credit and debit cards to ones embedded with a tiny microchip containing a customer's data. Widely used in Europe, Asia and Latin America, these so-called smart cards have sharply curbed financial losses due to counterfeit, lost or stolen cards. Until now, they've been almost unheard of in the United States, but that's changing.

"There's no excuse for us not migrating to the chip," said California state Sen. Jerry Hill, a Democrat who recently explored introducing legislation to prod California retailers and financial institutions into embracing microchip technology more quickly. "Yes, there may be a cost, but if Mexico, Brazil, China and Europe can absorb it, so can we.

"We used to be the first with consumer technology and consumer protections," he added, "and now it looks like we're behind."

Data intrusions, like those that hit Target over the holidays, Raley's grocery chain last summer or crafts store Michael's in late January, inflict damage that doesn't go away overnight. Months afterward, they rattle consumers' confidence, bruise retailers' images and heap more fraud losses onto banks and credit unions.

Although data breaches take many forms and not every breach leads to credit or debit card fraud, the growing number of U.S. incidents is unsettling.

Last year, more than 740 million consumer records - credit card and Social Security numbers, email addresses and computer username/passwords - were exposed, making 2013 "the worst year" ever, according to the Online Trust Alliance, a Seattle-based nonprofit that tracks data breaches and advises businesses on how to prevent them.

"The magnitude, velocity and scope of these incidents is accelerating," said Craig Spiezle, the Online Trust Alliance's president. And it's no accident that high-volume retailers such as Target are getting hit. "Cybercriminals are being more precise and sophisticated about who they're targeting, in order to get the biggest payload."

Dealing with cybertheft of credit/debit card information is a costly, unnerving headache.

Anne Bartkiewicz of Sacramento, Calif., knows the hassle only too well. Last year, in June and October, two of her banks canceled and reissued her credit cards due to suspected data breaches. She had to redo all of her online bill payments, including her Amazon and Netflix accounts. This year, in January alone, she's already been notified of possible fraudulent activity by several banks and retailers, including Target, which offered her free credit monitoring.

"I've been inundated with it. It's been a pain," said Bartkiewicz, who said she's now monitoring her credit card statements online - daily.

Primarily because of the billion-dollar costs, the United States lags behind the rest of the world in adopting the global standard for microchipped cards, known as EMV (for Europay, MasterCard and Visa). Until now, no one wanted to be first.

A decade ago, Target explored the adoption of microchipped credit cards. But in 2004, the chain abandoned a planned $40 million, three-year rollout because it would slow customers' cash-register transactions, be costly to implement and would not offer enough payback, since Target would have been the only major U.S. retailer offering EMV cards.

That cost-benefit analysis is rapidly changing.

"It's inevitable, going to a chip-and-PIN technology instead of a magnetic stripe," said Bill Dombrowski, president and CEO of the California Retailers Association, which represents large retailers, department stores, fast-food outlets and other merchants.

In the past, he said, "America wasn't ready for it," but the increase in costly data breaches has changed attitudes about microchipped cards. "It's a proven technology," he said.

Nationally, financial institutions and merchants face an October 2015 deadline - handed out by American Express, Discover, MasterCard and Visa - that they must have EMV-equipped cards, readers and ATMs. Those who don't will have to cover fraud losses due to point-of-sale theft of customer data.

Meeting that deadline is no small undertaking. Nationwide, the cost of issuing some 510 million new EMV plastic cards, installing millions of EMV readers at retail outlets and converting tens of thousands of ATMs is estimated at roughly $8 billion, according to a 2011 study by First Data Corp., an Atlanta-based global payments processing company.

For industries such as grocery stores, where there's a card reader at every checkout lane, the switchover will be pricey. The Food Marketing Institute, which represents about 40,000 U.S. grocery stores and 25,000 pharmacies, say the new readers could cost around $1,000 apiece, plus additional costs for updating software and passing compliance audits.

"The underlying issue is: Who's going to front the cost?" said Dave Heylen, spokesman for the California Grocers Association. While bigger chains could more easily absorb the extra expense, it's more problematic for smaller, independent grocers, he said.

Some grocery chains, such as West Sacramento, Calif.-based Raley's, which operates 128 stores in California and Nevada, are diving in.

"We are already investing in technology that will enable us to (handle) chip-and-PIN-enabled cards for our customers," said Raley's spokeswoman Nicole Townsend, who declined to disclose the cost. "Our goal is to as quickly as possible get them in place, and certainly well before the (October 2015) deadline."

Last summer, Raley's announced that a portion of its computer network

was hit by a "complex criminal cyberattack" and warned customers to watch their credit card statements for suspicious activity. Recently, the grocery chain closed its investigation, which included both in-house and outside investigators.

"Our investigation has concluded but the results are inconclusive," Townsend said. "We may never know precisely what happened."

Because of that uncertainty, she maintains that the Raley's situation is vastly different than the kind of recent attacks on Target and Neiman Marcus.

Meanwhile, state and national lawmakers are exploring ways to protect consumers' data and privacy.

Last month, Hill of the California Senate held meetings with credit card companies, retailers and financial institutions to discuss a proposed bill that would "hold everyone's feet to the fire" to comply with the October 2015 deadline for switching to microchipped cards. But late last week, Hill's office said it shelved the bill after being advised that the state doesn't have legislative jurisdiction.

On Feb. 25, two state Senate committees will hold a hearing on protecting consumer data in retail transactions.

In Washington, D.C., this week, congressional hearings on data breaches are underway. On Tuesday, Target executives apologized for the exposure of 110 million consumer records and said they were moving to deploy EMV technology in early 2015, six months ahead of schedule.

Some banks are already there. Citibank, for one, issues microchipped credit cards that also carry a magnetic stripe, meaning they can be used in stores with either EMV or traditional card readers.

Others, like Wells Fargo, have hit the pause button. In 2011, Wells Fargo offered microchipped credit cards in a test run to 15,000 customers who were frequent travelers overseas, where the cards are the norm.

But today, since so few U.S. merchants use EMV technology, "there is little need for a full-scale rollout," Wells Fargo spokeswoman Julie Campbell said in an email. She said the company would re-evaluate as chip cards gain popularity among merchants.

EMV cards will not wipe out all types of cybertheft. Their main defense is against point-of-sale transactions, where consumers swipe their card at a store's cash register terminal. They don't, for example, protect against credit cards used online, where a consumer types in a credit card number .

"Will (smart cards) help? Absolutely. It's a step in the right direction," said Spiezle, "but it's not the end-all."

In preventing cybertheft of our private data, "We're all in this together," he said. If U.S. consumers, banks, retailers and regulators don't make "meaningful changes" in how we protect and share our personal data, "trust in any of our transactions will only continue to decline."