BELLE
MAY 2 WATCH TRAILER

The New York Times | http://nyti.ms/1fpqR3v

BUSINESS DAY

After Data Breach, Target Plans to Issue More Secure Chip-and-PIN Cards

By ELIZABETH A. HARRIS APRIL 29, 2014

Still pushing to right itself after an enormous data breach by cybercriminals, Target announced on Tuesday that it would switch its debit and credit cards over to a more secure technology by early next year, most likely making it the first major retailer in the country to do so.

The company also said on Tuesday that it had hired a new chief information officer to oversee the company's technology team and data security.

The new debit and credit card technology, called chip and PIN, is widely used in Europe and considered to be far more secure than most cards used in the United States, which rely on magnetic strips. While it does not address all fraud, the chip makes a card hard to duplicate, and the pin, or personal identification number, more difficult for a thief to use.

"The move toward chip and PIN had been a very slow process in the United States because so many players have to restructure everything," said Suzanne Martindale, a staff lawyer at Consumers Union. "We're hoping that Target moving in this direction will encourage other retailers and financial institutions to create more secure payment cards, because it's long overdue."

Target has said it would spend $100 million switching to the new system, which includes changing its branded credit and debit Redcards, as well as the cost of installing new payment terminals.

Company executives have been promoting the chip and PIN system industrywide since the breach, and in the wake of several prominent data hacks, the transition to this technology appears to have gained traction in recent months. In February, for example, JPMorgan Chase said it would begin issuing some chip-and-PIN-enabled credit cards this year.

Experts stress, however, that these cards would not have necessarily helped those whose data was stolen in the Target breach.

But Target is eager to lead the charge all the same as part of its monthslong effort to restore consumer confidence.

"Target is snakebit," said David Robertson, publisher of the Nilson Report, a trade publication about payment cards. "In this post-breach era, they're going to do everything they can to let their customers know that they're trying to be as security conscious as possible."

At the helm of Target's new cybersecurity apparatus will be Bob DeRodes, who has held senior technology positions at a variety of companies including Home Depot and Delta Air Lines, and has served as a consultant to several federal agencies, including the Homeland Security, Justice and Defense departments, Target said.

The previous head of technology at the retailer, Beth M. Jacob, resigned in March after facing questions about whether she had the appropriate training to oversee protection of the company's computer networks that housed huge amounts of private consumer data.

The company also outlined some of the security measures it had been adapting. In some instances, it has deployed advanced technology like white-listing, which allows only web traffic that the company knows is innocuous to enter its systems. In other cases, the company is adding more sophisticated security around its network, including for its payment systems and customer data, which security experts say the company should have done long ago.

"I believe Target has a tremendous opportunity to take the lessons learned from this incident and enhance our overall approach to data security and information technology," Gregg Steinhafel, Target's chief executive, said in a statement.

On Dec. 19, 2013, just days before Christmas and in the crush of the holiday shopping season, Target publicly acknowledged that credit and debit card information for 40 million customers had been exposed. A few weeks later, the company said a second batch of information, the personal information of some 70 million people, had been compromised as well. The company has since said it believed there was overlap of at least 12 million people in the two groups.

The company's earnings underscored how much the breach had hurt store traffic and sales. Its fourth-quarter profits were down 46 percent compared with

the same period the year before. During that quarter, the company said, it spent $61 million on breach-related expenses, and executives said they expected the costs to continue.

Several other retailers and a hotel company have also been hacked in recent months.

Data breaches at Neiman Marcus and the arts and crafts retailer Michaels are believed to have been committed by the same band of criminals in Eastern Europe that infiltrated Target, according to people involved in the investigation, who were not authorized to speak publicly.

Nicole Perlroth contributed reporting.

A version of this article appears in print on April 30, 2014, on page B3 of the New York edition with the headline: After Data Breach, Target Plans to Issue More Secure Chip-and-PIN Cards.

© 2014 The New York Times Company