

Portland Press Herald

Thousands of Mainers' card data may have been stolen at Target

Customers in the state - up to 100,000 or more - are told to watch accounts for odd charges.

By J. Craig Anderson | December 19, 2013

Credit and debit card information for more than 100,000 Maine shoppers may have been compromised in the nationwide data breach that struck the retail giant Target this holiday season, but the exact number is open to question and state officials say they have no idea what it may be.

What is known is that for more than two weeks, data thieves stole credit and debit card numbers and security codes from every Target store in the country, affecting about 40 million consumers' accounts, the company revealed Thursday.

Cybersecurity analysts in Maine urged Target shoppers to review their bank and credit card account statements for fraudulent activity, and Gov. Paul LePage offered help from state officials with consumer information and guidance.

At the Target store in South Portland, Mia DiGiovanni of Portland said she loves shopping at the discount retailer but is concerned that it isn't doing enough to protect its customers.

"If somebody put that (card-reading) device in, then obviously they aren't keeping a good eye on what is going on," she said.

The card-data theft won't stop her from shopping at Target, she said, "if they can rectify the situation ... and assure people that it's never going to happen again."

DiGiovanni said she used a debit card to make purchases at Target in the period from Nov. 27 to Dec. 15, when thieves were stealing data from the company's systems. Under Maine law, businesses that suspect customers' payment-card data has been compromised must "conduct in good faith a reasonable and prompt investigation," and "give notice" that they suffered a breach. The law does not specify a time frame for that notification.

As of Thursday afternoon, Target had yet to notify DiGiovanni directly about the breach.

Carolyn Hemstedt of Brownfield said she had heard about the data theft but still decided to shop Thursday at the Target in South Portland.

"I feel confident that the transactions going through today are OK," Hemstedt said. "Have they totally taken care of the problem? No."

NUMBER OF MAINERS AFFECTED UNCLEAR

Minneapolis-based Target Brands Inc. said hackers stole information from as many as 40 million credit and debit cards that were used to make purchases at its stores in the U.S. beginning Nov. 27, as the holiday shopping season got into high gear. Card security was restored by Dec. 15, and transactions at Target are now safe, the company said in a news release. Online transactions at Target.com were not affected, the company said.

Target representatives have not specified how many customers in Maine were affected, and did not return calls seeking comment.

Without more specific information, it is difficult to determine how many Maine shoppers may have been affected.

If an equal number of cards were compromised at each of Target's roughly 1,800 U.S. stores, it would work out to about 111,000 at the retailer's five stores in Maine. Based on another estimate - that one in 10 Americans were affected by the breach - the number in Maine would total about 130,000.

Lloyd LaFountain III, superintendent of the state Bureau of Financial Institutions, said the actual number of Mainers affected is probably lower, based on the assumption that Target stores in Maine have less customer traffic on average than stores in more densely populated states.

The stolen data included each card holder's name, card number, expiration date and three-digit security code, according to Target. That's all a thief would need to sell the information on the black market or use it to drain card holders' accounts, local analysts said.

Target customers in Maine should monitor activity on potentially compromised accounts and contact the card issuer immediately if they notice fraudulent transactions, they said.

Just because a card number is compromised doesn't mean the card holder will become a victim of identity theft, said Maine Assistant Attorney General Linda Conti.

"They shouldn't assume ... that they have to get a new card," Conti said. "In fact, the bank will issue a new card if they think it is necessary."

Gov. LePage issued a statement warning Mainers who shopped at Target recently to be vigilant and seek help from the state Department of Professional and Financial Regulation.

"I encourage people to closely monitor their credit and debit card statements, and to contact the financial institution that issued the card promptly if questionable charges appear," LePage said.

Joshua Silver, a shareholder in the Portland law firm BeThoursarnstein Shur and a cybersecurity specialist, said Mainers who are affected by the breach are likely to receive notification from the issuers of their cards within the next 30 to 60 days.

When necessary, a card issuer may automatically cancel compromised cards and issue new ones, he said.

Target may offer services, such as a year of free credit monitoring, to help customers deal with the data breach, Silver said.

Card-data theft from retailers and other businesses has become “incredibly common,” he said, but only the larger incidents draw media attention.

“There are breaches on much smaller scales that happen every single day,” Silver said.

HOW DATA IS OFTEN STOLEN, SOLD

Edward Sihler, another cybersecurity expert in Maine, said data thieves usually infect a retailer’s point-of-sale system with malware, computer programs that capture card information and transmit it over the Internet to the hackers.

Given that Target is a huge company with tremendous resources for data security, it’s likely the card-number theft was an inside job, said Sihler, technical director of the Maine Cybersecurity Center at the University of Southern Maine.

“It’s entirely possible it’s a disgruntled employee,” he said.

The tools needed to pull off a card-data heist are for sale on the Internet, Sihler said. “You don’t have to be a rocket scientist to do this,” he said.

Once the card data has been obtained, it can be sold on black-market websites for about \$1 per card, Sihler said.

The data can be used to make purchases online, he said. Thieves are particularly fond of buying gift cards because they can be sold for cash, he said.

Debit cards are even more vulnerable than credit cards, Sihler said, because the information can be used to make counterfeit cards that work in ATMs.