U.S. retailer Michaels warns of possible payment card breach

By Jim Finkle

(Reuters) - Michaels Companies Inc, the biggest U.S. arts and crafts retailer, said it is investigating a possible security breach on its payment card network and advised customers to check their financial statements for fraudulent activity.

If confirmed, it would mark the second known data breach since 2011 at Michaels, which is preparing to sell shares in an initial public offering.

"We are concerned there may have been a data security attack on Michaels that may have affected our customers' payment card information," Michaels Chief Executive Chuck Rubin said in a statement on Saturday. "We are taking aggressive action to determine the nature and scope of the issue."

The warning comes in the wake of a massive data breach at Target Corp over the holiday shopping season, and suggests that hackers may be attacking U.S. retailers in a spree the extent of which is yet to be fully understood.

Target last month said hackers had stolen some 40 million payment card records and accessed 70 million customers' records. Luxury retailer Neiman Marcus has also disclosed a data breach that compromised data from about 1.1 million cards.

The U.S. Federal Bureau of Investigation last week warned retailers to expect more attacks and said the agency has reviewed 20 incidents over the past year that were similar to the recent breaches.

Michaels said federal investigators and an outside forensics firm were investigating to determine if there had been a breach. The company said it decided to warn the public and launch a probe into the matter after hearing that there had been an increase in fraud involving cards of customers who had shopped at its stores.

It was not immediately clear how many cards might have been affected, when an attack might have occurred, or whether the systems were currently compromised. A Michaels representative declined to elaborate on the statement.

U.S. Secret Service spokesman Edwin Donovan told Reuters his agency was investigating the matter.

PLANNING TO GO PUBLIC

Michaels, whose major investors are Blackstone Group LP and Bain Capital LP, last year filed documents with the U.S. Securities Exchange Commission to go public. The company resubmitted its IPO documents late last month following a restructuring.

In a high-profile 2011 attack, hackers replaced some 84 PIN pads on payment-card terminals at a small number of Michaels stores, resulting in the theft of about 94,000 payment card numbers, according to Department of Justice attorneys who eventually prosecuted two men charged in that case.

Last year the Irving, Texas-based retailer settled a class-action consumer lawsuit related to the matter, without admitting to any wrongdoing.

Michaels disclosed the 2011 attack in an S-1 registration statement that it filed with the Securities and Exchange in March of last year.

"This is devastating for them because this is the second time in a row," said Gartner security analyst Avivah Litan. "The public and the credit card companies are going to slap their wrist twice as hard because they'll say they haven't learned their lesson and that they can't be trusted."

But that criticism might be tempered somewhat, given that other retailers have been breached, Litan said.

The FBI has warned retailers about cyber criminals using "memory-parsing" software, also known as "RAM scrapers." When a customer swipes a payment card at checkout, the computer grabs data from the magnetic strip and transfers it to the retailer's payment processing provider. While the data is encrypted during the process, RAM scrapers extract the information from the computer's live memory, where it briefly appears in plain text.

RAM scraping technology has been around for a long time, but its use has increased in recent years and cyber criminals have added features to make it more difficult for victims to detect the malicious software on their networks.

"They have gotten much more sophisticated," said Daniel Clemens, chief executive of the cyber security firm Packet Ninjas, whose firm investigates credit card breaches at retailers. "We are in a cycle where the incidence of these attacks will just continue to grow."

(Reporting by Jim Finkle. Additional reporting by Mark Hosenball; Editing by James Dalgleish, Gunna Dickson and Tiffany Wu)