Data breach at Saks, Lord & Taylor compromises customer payment data

The retail stores' parent company said customers would not be liable for charges and would be offered free identity protection services.

by Tim Stelloh / Apr.01.2018 / 11:49 AM ET / Updated Apr.01.2018 / 2:59 PM ET

People walk by the Saks Fifth Avenue store in New York.Shannon Stapleton / Reuters file

The owner of Lord & Taylor and Saks said Sunday that a data breach at its department stores compromised customer payment data.

In a statement, Hudson's Bay Company said the breach hit Saks Off 5th, Saks Fifth Avenue and Lord & Taylor stores in North America.

"HBC has identified the issue, and has taken steps to contain it," the statement said.

The company did not immediately provide additional details about how many customers were impacted, but it said they would not be liable for charges and would be offered free identity protection services.

The cyber security firm that says it uncovered the breach, Gemini Advisory, said in a post Sunday that more than 5 million credit and debit cards were stolen and that 125,000 of them were for sale on the dark web — apparently one of the largest breaches to hit a retail company.

The group behind the hack, Joker's Stash, may have been stealing the information since last May, the firm said, and the majority of the data was taken from stores in New York and New Jersey.

Gemini's chief technology officer, Dmitry Chorine, told NBC News that his company reached out to HBC's internal security team on Friday after the data was discovered on criminal forums and message boards.

"We never heard from them," Chorine said. He added: "The breach was way too big for us to sit on."

An HBC spokeswoman could not immediately provide comment.

Chorine said that Joker's Stash is among the biggest players in the hacking world, carrying out attacks on Omni Hotels and Resorts, Chipotle, Whole Foods and others.

The group is well-funded and could have as many as 2,000 members — software developers and money launderers, operational security personnel and executives, he said, adding that it is controlled by Russian-speakers though they aren't necessarily Russian.

"It could be the Ukraine, Belarus, Kazakhstan — no one knows where they live," Chorine said. "Every law enforcement agency is looking for them."

Chorine said the group uses phishing e-mails and malware to access and harvest information from computer networks. It also uses unconventional surveillance methods, such as hiring a "mystery shopper" from Craigslist, for instance, who unwittingly helps reveal if a retail store is using an outdated credit card machine.

This may have been the case with the latest breach, Chorine said, suggesting that not all of HBC's stores had upgraded credit card systems.