Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Saks, Lord & Taylor Confirm Payment Card Data Breach

By **Allison Grande**

*Law360 (April 2, 2018, 11:07 PM EDT)* -- The parent company of Saks Fifth Avenue and Lord & Taylor disclosed Sunday that personal information for shoppers who swiped their payment cards at retail locations in North America may have been compromised in a recent data security breach, with one cybersecurity firm estimating the number of affected customers at 5 million.

In a notice posted on the retailers' websites, the Canadian retail business group Hudson's Bay Co. said that it had recently become aware of a data security problem involving customer payment card data at Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor stores in North America.

While the company offered no estimate of how many stores or payment cards may have been involved, the New York-based cybersecurity firm Gemini Advisory said in a blog post Sunday that it had "confirmed with a high degree of confidence" that the more than 5 million stolen credit and debit cards that the hacking syndicate JokerStash, also known as Fin7, said it was releasing for sale on the dark web on March 28 had been taken from Saks Fifth Avenue and Lord & Taylor customers.

Gemini Advisory added that its preliminary analysis suggested criminals had been siphoning the payment card information between May 2017 and the present, and that it believed that the entire Lord & Taylor network and 83 Saks Fifth Avenue locations had been compromised, with the majority of pilfered cards obtained from New York and New Jersey locations.

The Hudson's Bay Co. refused to verify details or the alleged link between the stolen payment cards and its customers, saying that the investigation was continuing and that it "wanted to reach out to our customers quickly to assure them that they will not be liable for fraudulent charges that may result from this matter."

"Once we have more clarity around the facts, we will notify our customers quickly and will offer those impacted free identity protection services, including credit and web monitoring," the company said, adding that it encouraged its customers to review their account statements and contact their card issuers immediately if they identified activity or transactions they did not recognize.

While Hudson's Bay Co. did not say when it learned of the breach, the company stressed that it had identified the problem, taken steps to contain it, and believed that "it no longer poses a risk to customers shopping at our stores."

The retailer said there was no indication that the breach affected its e-commerce or other digital platforms, Hudson's Bay, Home Outfitters, or HBC Europe, and that it was continuing to work "rapidly" with data security investigators to "get our customers the information they need," in addition to working with law enforcement authorities and payment card companies.

The security breach follows a flurry of intrusions reported in recent years by companies in a range of industry sectors, including similar payment card breaches at Neiman Marcus, Kmart, Wendy's, Arby's, Chipotle, Sonic, Target and Home Depot, and by major government organizations such as the U.S. Office of Personnel Management and the Internal Revenue Service.

Gemini Advisory noted that Fin7, the hacking syndicate that has released 125,000 of the 5 million payment card records that are believed to belong primarily to Lord & Taylor and Saks customers, has had a "long streak of successful high-profile breaches, including Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels and many more."

Mayer Brown LLP partner Stephen Lilley, who is not involved with the breach response, told Law360 Monday that while details revealed about the breach appear to be consistent with what has happened in previous breaches, it was notable that the announcement by Gemini Advisory, rather than Hudson's Bay Co. itself, seemed to be the driving force behind Sunday's disclosure.

"Ideally what happens from a company's perspective is to learn about the breach themselves and investigate it thoroughly and identify and close out the vulnerability before notify the public about what happened," Lilley said. "It's a bit unfortunate for the companies in this case that they seem to have been informed about the breach because the cards showed up on a criminal forum and were reported on by the cybersecurity company."

While it is not unusual for security researchers or the media to beat companies to disclosure or even discovery, this puts companies in the position of having to address the public fallout and manage a complex forensic investigation at the same time, according to Lilley.

This chain of events "emphasizes the value of having a good incident response plan in place and having practiced both the type of scenario where you discover it and have the ability to put your ducks in a row before it gets out and the scenario where you don't," Lilley said.

Having a well thought-out and proven incident response plan that works in a company's culture can also help reduce the liability that stems from the crush of consumer, investor and financial institution class actions; regulatory investigations; and disputes with payment card networks that often follow such breaches, Lilley said.

"At the end of the day, there's a lot of criminals who want to make money off of stealing credit card information, so it's going to be a risk that comes with accepting credit card payments for a while," Lilley said.

--Editing by Peter Rozovsky.

---