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

# Forever 21 Says Unencrypted Payment Card Data Breached

By **Allison Grande**

*Law360, New York (November 16, 2017, 10:58 PM EST)* -- Forever 21 customers who swiped their payment cards between March and October at certain retail locations that weren't using encryption and tokenization methods that the company rolled out two years ago may have had their personal information compromised in a recently discovered data breach, the apparel retailer said Tuesday.

According to a notice posted on its website, Forever 21 immediately launched an investigation of its payment card systems and engaged a "leading security and forensics firm to assist" after recently receiving a report from an unidentified third party, which suggested that there may have been "unauthorized access" to data from payment cards that were used at "certain" stores for eight months beginning in March.

"Because of the encryption and tokenization solutions that Forever 21 implemented in [point-of-sale payment systems] in 2015, it appears that only certain point-of-sale devices in some Forever 21 stores were affected when the encryption on those devices was not operating," the company said. Tokenization refers to the process of replacing sensitive data with unique identification symbols to boost the security of that data.

Because the investigation is still ongoing, the company said it was still "too early" to provide additional details about the incident, including exactly what information was compromised, who was behind the intrusion, and how many customers and stores were impacted. The California-based retailer, which was founded in 1984, operates more than 815 stores in 57 countries, including the U.S., Australia, Brazil, Canada, China, France, Germany and the U.K., with more than 500 of these locations being in the U.S.

Forever 21 said it would provide an update "as it gets further clarity on the specific stores and time frames that may have been involved" and advised customers to closely monitor their payment card statements and immediately notify the bank that issued their card if they spot unauthorized charges. The company added that under payment card network rules, cardholders generally are not responsible for fraudulent charges that are reported in a timely fashion.

"We regret that this incident occurred and apologize for any inconvenience," the company added. "We will continue to work to address this matter."

As with most companies and organizations that experience major data breaches, Forever 21 is expected to face scrutiny from class action plaintiffs, regulators and lawmakers, and the answer to lingering

questions about the scope of the breach and how hackers found their way into the system is likely to play a major role in determining how these inquiries shake out, according to Marcus Christian, a Mayer Brown LLP cybersecurity and data privacy partner and former executive assistant U.S. attorney at the U.S. Attorney's Office for the Southern District of Florida.

"I don't think we'll find that Forever 21 made no investment in cybersecurity," Christian said. "I'm sure they have made that investment and that they are to some extent a victim here. But how they're treated and viewed moving forward will depend on the facts that come out and, like others, they'll take the lessons learned here and try to do a better job in the future."

Among the biggest question marks are how much of the retailer's vast footprint had been impacted by the breach, how long the breach may have gone undetected, to what extent the compromised data was encrypted, and whether the retailer was fully compliant with rules such as the Payment Card Industry's data security standards for merchants that accepts payment cards.

While the exact structure of Forever 21's system remains unknown, only portions of information held by companies may be protected by encryption for a variety of reasons, including that one part of the system didn't get the necessary technology upgrade or that vulnerabilities that were created when two systems came together through a merger or other change in corporate structure.

"Sometimes mistakes happen, and in the course leave certain areas of a system vulnerable," Christian noted, adding that the bigger the breach turns out to be, the more eyes that are likely to be focused on it.

The suspected breach at Forever 21 comes in the wake of a flurry of intrusions that have been reported in recent years by both companies in a range of industry sectors, including Target, Home Depot, Kmart, Yahoo, Arby's, Chipotle and Sonic, and major government organizations such as the U.S. Office of Personnel Management and the Internal Revenue Service.

Credit reporting giant Equifax and the U.S. Securities and Exchange Commission joined these ranks in September, when Equifax announced that the personal identification and financial information of roughly 145.5 million Americans had been compromised and the SEC followed up less than two weeks later by revealing that its electronic filing system for public company disclosures had been breached last year and that the information that was taken "may have provided the basis for illicit gain through trading."

Congressional lawmakers responded to these incidents by holding a wave of hearings and introducing several bills aimed at making good on long-standing efforts to codify federal breach notification and data security standards to offset a patchwork of state laws.

A coalition of Democratic senators took the latest stab on Tuesday by introducing the Consumer Privacy Protection Act of 2017. Under the legislation, which was spearheaded by Sen. Patrick Leahy of Vermont and six other lawmakers with a reputation for cybersecurity advocacy, businesses would be required to report data breaches "as expediently as possible" and implement baseline data security standards to protect customers' financial account information, biometric data, login credentials, geolocation information and other sensitive records.

Christian noted that even though the Forever 21 breach and similar retail hacks that have come before it have largely impacted payment cards and not more sensitive information like biometric data and Social

Security numbers that are far more difficult to replace, they are still taken seriously by stakeholders ranging from consumers to regulators such as the Federal Trade Commission to state attorneys general.

"There's an environment now where sometimes people get a little bit numb, but the Equifax breach, given that it affected so much of the U.S. population, got people paying attention to these incidents," he said.

While legislation specifically to address incidents like the Forever 21 hack is unlikely, questions are likely to be posed about the data security standards and best practices that are currently in place, including the highly anticipated switch a few years ago to what was billed as more secure chip and pin technology, and how well those efforts are protecting consumers' financial data.

"Notwithstanding the PCI standards and the other significant standards being in place, there have been breaches," Christian added. "While payment card breaches haven't necessarily been the biggest news in data breaches as of late because of some of the other kinds of information that has been hacked in other breaches, they're not extinct and people can still make money off of them. Threat actors are opportunists, and they're looking for open doors or doors that are easier to get into, and they'll go through there."

--Editing by Bruce Goldman.