THE WALL STREET JOURNAL.

http://www.wsj.com/articles/starwood-reports-payment-information-data-breach-1448033469

BUSINESS | MARKETS

Starwood Reports Payment-Information Data Breach

Company sees no indication that its guest-reservation system or loyalty-rewards program were compromised

The Sheraton Birmingham Hotel in Alabama was among the locations that Starwood said had been affected by a data breach. *PHOTO: STARWOOD HOTELS & RESORTS*

By **ROBIN SIDEL** and **CRAIG KARMIN**

Updated Nov. 20, 2015 5:40 p.m. ET

Starwood Hotels & Resorts Worldwide Inc. said hackers stole customer credit-card and debit-card information during a data breach that lasted nearly eight months and affected 54 locations, including a number of luxury properties.

The breach was the latest in a wave of hacking attacks targeting the hotel industry.

The company said malicious software, known as malware, infiltrated payment systems at in-hotel restaurants and gift shops, collecting customer names, card numbers, security codes and expiration dates.

The breach affected luxury hotels, including the Phoenician Resort in Scottsdale, Ariz., and the St. Regis Bal Harbour Resort in Bal Harbour, Fla., as well as properties that are part of the Sheraton, Westin and W chains.

The company didn't disclose how many card accounts were exposed in the breach that targeted some of the hotels for months at a time.

"Protecting our customers' information is critically important to Starwood, and we take this issue extremely seriously," said Sergio Rivera, Starwood's president in the Americas.

The disclosure came just days after Starwood announced that it was being acquired by Marriott International Inc. for $12.2 billion in a deal that would create the world's largest hotel company. A Marriott spokesman said his company was aware of the Starwood security breach before it reached the agreement to acquire Starwood, but he declined to comment further.

The Trump Hotel Collection recently notified its customers of a potential breach. A spokeswoman said the company found no evidence that customer information was taken but "out of an abundance of caution we provided notice of the incident to our clients."

The payments industry is trying to reduce such data breaches by replacing traditional cards that have magnetic strips with more secure cards that have computer chips. Merchants are installing devices to accept such cards following a recent change in which they may be financially responsible for fraudulent transactions.

Consumers aren't liable for unauthorized purchases made on their cards, but breaches can cause significant aggravation if swindlers use the stolen information to create counterfeit cards.

Max Rayner, a partner at travel and hospitality consultancy Hudson Crossing, said hotels have been focusing on how to secure their central reservation systems but "people haven't paid adequate attention" to the point-of-sale devices that were hacked at Starwood and other companies.

"It's not just the hospitality industry," he added. "It's one of the most common credit-card attacks."

He cited restaurants and unattended gas stations as other prime targets. These businesses could protect themselves by locking the point-of-sale device after hours and changing passwords.

Starwood said the attacks didn't affect the hotel reservation system. Customers who stayed at hotels but didn't use restaurants or shops weren't affected, Jessica Doyle, Starwood's director of corporate communications, said.

The recent attacks have prompted Visa Inc. to focus on companies that set up and maintain so-called point-of-sale for merchants, including restaurants. The payments network said it has seen a "considerable increase" in malware that gets unauthorized access to the payment systems via these companies, which are called integrators.

Starting in March, Visa will require certain merchants that want to accept its credit and debit cards to use integrators that have received a special certification. The rule will be expanded to include all merchants in January 2017.

It is so far unclear whether the Starwood attacks are tied to the services provided by integrators.

The integrators pose little risk to merchants if they are properly secured, but recently "cyber criminals have exploited inadequate security controls to gain unauthorized access to a substantial number of merchant (point-of-sale) systems and payment card data," Visa said in a security alert issued in June.

Starwood provided details of the breaches, showing that hackers took aim at certain hotels for a specific amount of time and then moved onto other properties.

The first exposure occurred Nov. 5, 2014, at the Sheraton Walt Disney World Dolphin hotel in Orlando, according to a list provided by the company. That breach exposed customers until April 13.

Nearly 35 of the hotels were first exposed March 2, according to the list. Most of those attacks lasted for about six weeks, although the Westin Cincinnati was exposed for nearly four months.

Starwood said there is no indication the guest-reservation system or loyalty-rewards program were compromised. Starwood also said there is no evidence that other information such as contact information or personal identification numbers were accessed.

Starwood said the malware no longer presents a threat to customers using payment cards at its hotels.

Write to Robin Sidel at robin.sidel@wsj.com and Craig Karmin at craig.karmin@wsj.com