

The Virgin Islands Consortium

Data Of 500 Million Marriott Guests Exposed Through Hack

Business / **Published On December 01, 2018 11:11 AM /**

Ernice Gilbert **December 01, 2018**



The personal data -- to include credit cards, addresses and at times even passport numbers -- of Marriott Hotel guests was compromised by hackers, Marriott International confirmed on Friday. The hack amounts to one of the largest breaches of personal data in U.S. history, rivaled only by the 2013 Yahoo Breach, which affected some three billion user accounts.

Marriott International said hackers breached its Starwood reservation system and had stolen personal data of its guests. It was not clear whether the Marriott brands in St. Thomas and St. John were part of the compromised data, but the breach affected customers who made reservations for Marriott-owned Starwood hotel brands from 2014

to September 2018, including Sheraton, Westin, W Hotels, St. Regis, Four Points, Aloft, Le Méridien, Tribute, Design Hotels, Elements and the Luxury Collection, according to the New York Times.

The Marriott brands in St. Thomas along with Westin in St. John have the SPG, or "Starwood Preferred Guest" logo atop the right side of their pages on the main Marriott website. The Westin St. John page even provides a link to more information about the security breach. (See screenshots below.)



Marriott's Frenchman

📍 7338 Estate Bakkerøe, St. Thomas 008

Overview

Photos

Villas & Rooms

Deals

Di

Dates

Sat, Dec 1, 2018 - Sun, Dec 2, 2018



Rooms & Guests

1 Room: 1 Ad



For more information on the Starwood guest reservation database security

[SPG.com](#) ▾ / [Westin Hotels & Resorts](#) / [Great Cruz Bay](#) / [Resort](#)

WESTIN[®]
HOTELS & RESORTS

The Westin St. John Re

📍 300B Chocolate Hole, Great Cruz Bay 0

[Overview](#)

[Photos](#)

[Rooms](#)

[Deals](#)

[Spa](#)

Dates

Sat, Dec 1, 2018 - Sun, Dec 2, 2018 ▾

Rooms & Guests

1 Room: 1 Adu



Marriott brands Residence Inn and the Ritz-Carlton operate on a separate reservation system. Marriott has plans to merge that system with Starwood's, according to The Times.

Stolen were the addresses, phone numbers, birth dates, email addresses and encrypted credit card details of hotel customers, as well as the travel histories and passport numbers of a smaller group of guests.

"We deeply regret this incident," said Arne Sorenson, Marriott's president and chief executive, in a statement. "We fell short of what our guests deserve and what we expect of ourselves."

Marriott said it had set up a [website](#) and call center whereby it would communicate with guests. The company on Friday said it would attempt to reach its customers to inform them of the breach.

The firm is offering one year of free enrollment in a service called Web Watcher to people who live in the United States, Canada and Britain. As described by Marriott, Web Watcher is a service that keeps an eye on websites where thieves swap and sell personal information and then alerts people if anyone is selling their information.

The intrusion went unnoticed for four years by Starwood, which Marriott purchased in 2016 for \$13.6 billion. It was discovered in early September, when a security tool alerted Marriott of unauthorized attempts to access the Starwood guest reservation database. After the alert, Marriott hired outside security firms to perform an investigation, which concluded that hackers had compromised the Starwood system since 2014.

The Federal Bureau of Investigation said on Friday that it was aware of the breach and was monitoring the matter. It added that any suspected instances of identity theft should be reported to the F.B.I.'s Internet Crime Complaint Center at www.ic3.gov.

Several lawsuits were filed against Marriott on Friday, and investigations were announced by New York's attorney general, Barbara D. Underwood, and European regulators, according to The Times.

Marriott told shareholders that it did not expect the breach would affect its long-term financial prospects. Even so, Marriott's stock price fell more than 5 percent on Friday, following the announcement of the breach.

According to The Times, lawmakers said the episode was yet another example of why the United States needs data privacy laws that punish companies for failing to keep customers' information private.

"It is past time we enact data security laws that ensure companies account for security costs rather than making their consumers shoulder the burden and harms resulting from these lapses," Senator Mark R. Warner, a Democrat from Virginia, said in a statement.