Marriott security breach exposed data of up to 500M guests (Update)

30 November 2018, by Michelle Chapman And Mae Anderson

This Feb. 1, 2010, file photo, shows the Westin Philadelphia hotel in Philadelphia. The information of as many as 500 million guests at Starwood hotels has been compromised and Marriott said that it's discovered that unauthorized access to data within its Starwood network has been taking place since 2014. The company said Friday, Nov. 30, 2018, that credit card numbers and expiration dates of some guests may have been taken. (AP Photo/Matt Rourke, File)

A security breach inside the Marriott hotel empire compromised the information of as many as 500 million guests worldwide, exposing their credit card numbers, passport numbers and birth dates for as long as four years, the company said Friday.

The crisis quickly emerged as one of the largest data breaches on record. By comparison, last year's startling Equifax hack affected more than 145 million people.

Analysts were alarmed by the length of time the breach had been going on. Many security breaches span months, an average of 90 to 200 days, but this one began in 2014.

The affected hotel brands were operated by Starwood before it was acquired by Marriott in 2016. They include W Hotels, St. Regis, Sheraton, Westin, Element, Aloft, The Luxury Collection, Le Méridien and Four Points. Starwood-branded timeshare properties were also included.

None of the Marriott-branded chains were threatened.

For as many as two-thirds of those affected, the exposed data could include mailing addresses, phone numbers, email addresses and passport numbers. Also included might be Starwood Preferred Guest account information, date of birth, gender, arrival and departure times and reservation dates.

Credit card numbers and expiration dates of some guests may have been taken, according to the company.

"We fell short of what our guests deserve and what we expect of ourselves," CEO Arne Sorenson said in a statement. "We are doing everything we can to support our guests, and using lessons learned to be better moving forward."

It isn't common for passport numbers to be part of a hack, but it is not unheard of. Hong Kong-based airline Cathay Pacific Airways said in October that 9.4 million passengers' information had been breached, including passport numbers.

Passport numbers can be added to full sets of data about a person that bad actors sell on the black market, leading to identity theft. And while the credit card industry can cancel accounts and issue new cards within days, it is a much more difficult process, often steeped in government bureaucracy, to get a new passport.

In this July 31, 2013, file photo, the logo for the W Hotel, owned by Starwood Hotels & Resorts Worldwide, is seen in New York's Times Square. The information of as many as 500 million guests at Starwood hotels has been compromised and Marriott said that it's discovered that unauthorized access to data within its Starwood network has been taking place since 2014. The company said Friday, Nov. 30, 2018, that credit card numbers and expiration dates of some guests may have been taken. (AP Photo/Mark Lennihan, File)

But one redeeming factor about passports is that they are often required to be seen in person, said Ryan Wilk of NuData Security. "It's a highly secure document with a lot of security features," he said.

Email notifications for those who may have been affected begin rolling out Friday.

The 500 million figure includes the number of guests who made a reservation at one of the affected hotels. But it could also include a single person who booked multiple stays, the company said.

Asked for more details, Marriott spokesman Jeff Flaherty said Friday that the company has not finished identifying duplicate information in the database.

When the merger was first announced in 2015, Starwood had 21 million people in its loyalty program. The company manages more than 6,700 properties across the globe, most in North America.

While the first impulse for those potentially affected by the breach could be to check credit cards, security experts say other information in the database could be more damaging.

"The names, addresses, passport numbers and other sensitive personal information that was exposed is of greater concern than the payment info, which was encrypted," said analyst Ted Rossman of CreditCards.com. "People should be concerned that criminals could use this info to open fraudulent accounts in their names."

An internal security tool signaled a potential breach in early September, but the company was unable to decrypt the information that would define what data had possibly been exposed until last week.

Marriott, based in Bethesda, Maryland, said in a regulatory filing that it's premature to estimate what financial impact the breach will have on the company. It noted that it does have cyber insurance, and is working with its insurance carriers to assess coverage.

The Starwood breach stands out among even the largest security hacks on record.

In this Tuesday, April 30, 2013, file photo, a man works on a new Marriott sign in front of the former Peabody Hotel in Little Rock, Ark. Marriott says the information of up to 500 million guests at its Starwood hotels has been compromised. It said Friday, Nov. 30, 2018, that there was a breach of its database in September, but also found out through an investigation that there has been unauthorized access to the Starwood network since

2014. (AP Photo/Danny Johnston, File)

Yahoo had data breaches in 2013 and 2014 that affected about 3 billion accounts. Target also had an incident in 2013 that affected more than 41 million customer payment card accounts and exposed contact information for more than 60 million customers.

Elected officials were quick to call for action.

The New York attorney general opened an investigation. Virginia Sen. Mark Warner, co-founder of the Senate cybersecurity caucus and the top Democrat on the Senate Intelligence Committee, said that the U.S. needs laws that will limit the data companies can collect on its customers.

"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," Warner said in a prepared statement.

Marriott has had a rocky process of merging its computer system with Starwood computers. Members of both loyalty programs have complained about missing points, glitches with stays crediting to their accounts and problems with free nights earned from credit cards not appearing.

Sorenson said that Marriott is still trying to phase out Starwood systems.

Marriott has set up a website and call center for anyone who thinks that they are at risk.

APA citation: Marriott security breach exposed data of up to 500M guests (Update) (2018, November 30) retrieved 22 May 2019 from https://phys.org/news/2018-11-marriott-million-guests-affected-hack.html