

WHAT HAPPENED



5.2 Million People

The personal information — including names, addresses, phone numbers, email addresses, loyalty member data, DOB and additional linked travel preference information.



Unknown CC Data Impact

As of March 31, the company publicly said they do not believe payment data was compromised in the breach.



14 Months Since Last Breach

The last data breach from Marriott came from Starwood, which was announced Dec. 4, 2018. That breach impacted PII of 383M guests , including 5M encrypted credit cards & 8M credit card records.



~6 Weeks of Data Exposure

The company believed the breach activity began in mid-January 2020, and was discovered at the end of February 2020.

WHAT YOU NEED TO KNOW

- Marriott sent emails to guests involved.
- Marriott has also set up a dedicated website — www.mysupport.marriott.com — and call center resources with additional information for guests.
- Guest information is believed to have been breached using the login credentials of two employees at an unnamed franchise property.
- The company has implemented heightened monitoring and has notified relevant authorities for investigation.
- Marriott officials said there is “no reason” to believe payment data was stolen.

Rippleshot's Take: The Potential Fraud Fallout

Although it is not believed at this time that payment data was exposed in Marriott's latest data breach, the true impact from the incident is the potential fallout that can occur as a result of a massive amount of exposed PII data. Card fraud/compromised card fraud may not be impacted, but other types of fraud may rise, including: **Synthetic Fraud**, **Account Takeover** and **New Account Opening Fraud**.

The True Financial Impact

- In the last year alone, exposed consumer PII records rose 126%.
- New account fraud account for ~\$3.4B, and by 2021, industry estimates peg synthetic fraud to account for 40% of all credit card charge offs — costing lenders \$6 Billion annually.
- Dark Web crime rings are increasing as the availability of exposed PII grows substantially.
- Mobile account takeover fraud is up 56% in the past year to more than 679,000 incidents.

Breached PII Linked to the Above Financial Impact:

- **Contact Details:** Name, mailing address, email address, and phone numbers
- **Loyalty Account Information:** Account number and points balance, but not passwords
- **Additional Personal Details:** Company, gender, and birthday day and month
- **Partnerships and Affiliations:** Linked airline loyalty programs and numbers
- **Travel Preferences:** Stay/room preferences and language preference

For Rippleshot Clients: We don't currently anticipate a spike in compromised cards, and have no recommended actions. We will continue to monitor the incident and will send updates as new information becomes available.