The Marriott Data Breach

December 4, 2018
by Seena Gressin
Attorney, Division of Consumer & Business Education, FTC

Marriott International says that a breach of its Starwood guest reservation database exposed the personal information of up to 500 million people. If your information was exposed, there are steps you can take to help guard against its misuse.

According to Marriott, the hackers accessed people's names, addresses, phone numbers, email addresses, passport numbers, dates of birth, gender, Starwood loyalty program account information, and reservation information. For some, they also stole payment card numbers and expiration dates. Marriott says the payment card numbers were encrypted, but it does not yet know if the hackers also stole the information needed to decrypt them.

The hotel chain says the breach began in 2014 and anyone who made a reservation at a Starwood property on or before September 10, 2018 could be affected. Starwood brands include W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Le Méridien Hotels & Resorts, and other hotel and timeshare properties.

The company set up an informational website, https://answers.kroll.com, and a call center, 877-273-9481, to answer questions. It says affected customers also can sign up for a year of free services that will monitor websites that criminals use to share people's personal information. Marriott says the service will alert customers if their information shows up on the websites, and will also include fraud loss reimbursement and other services.

If your information was exposed, take advantage of the free monitoring service, and consider taking these additional steps:

- **Check your credit reports** from Equifax, Experian, and TransUnion — for free — by visiting annualcreditreport.com. Accounts or activity that you don't recognize could signal identity theft. Visit IdentityTheft.gov to find out what to do.

- **Review your payment card statements carefully.** Look for credit or debit card charges you don't recognize. If you find fraudulent charges, contact your credit card company or bank right away, report the fraud, and request a new payment card number.

- **Place a** fraud alert **on your credit files.** A fraud alert warns creditors that you may be an identity theft victim and that they should verify that anyone seeking credit in your name really is you. A fraud alert is free and lasts a year.

- **Consider placing a free** credit freeze **on your credit reports.** A credit freeze makes it harder for someone to open a new account in your name. Keep in mind that it won't stop a thief from making charges to your existing accounts.

  Marriott says it will send some customers emails with a link to its informational website. Often, phishing scammers try to take advantage of situations like this. They pose as legitimate companies and send emails with links to fake websites to try to trick people into sharing their personal information. Marriott says its email will not have any attachments or request any information. Still, the safest bet is to access the informational website by typing in the address, https://answers.kroll.com .

  To learn more about protecting yourself after a data breach, visit IdentityTheft.gov/databreach.