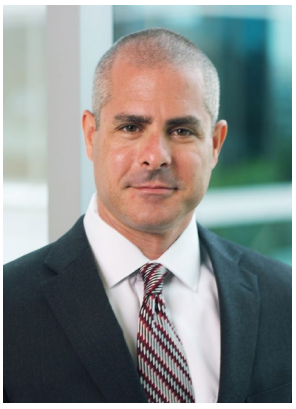
NEWMEYER & DILLION LLP

THE MARRIOTT BREACH: WHAT HAPPENED AND WHAT YOU SHOULD DO ABOUT IT

By: Joshua Bevitz and Casey Quinn

Friday, November 30, 2018



Joshua Bevitz

Contact

925.988.3226
joshua.bevitz@ndlf.com

Practice Areas

Business Litigation
Construction Litigation
Insurance Law
Privacy & Data Security
Real Estate Litigation

Casey Quinn

Contact

702.777.7506
casey.quinn@ndlf.com

Practice Areas

Appellate Law
Business Litigation
Construction Litigation
Insurance Law
Privacy & Data Security

Yet another unfortunate reminder that the threat to your privacy and your business by hackers is real and not close to abating. Marriott International Inc. announced today what may be the second largest data breach in history. If you are a consumer or a business, here is what you need to know about what happened and what steps you need to take if you are affected.

What Happened

On September 8, 2018, Marriott received an alert about an unauthorized attempt to access its Starwood guest reservation database. (Marriott acquired Starwood in September 2016.)

An investigation revealed that hackers had access to that database since 2014. The hackers not only copied private consumer data, but they also encrypted it before removing it. Marriott was not able decrypt the information until November 19, 2018.

At that time, Marriott determined that the stolen information includes various combinations of names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival/departure information, reservation dates, and communication preferences. The theft affects up to 327 million consumers who made reservations at a Starwood property. While Marriott had encrypted credit card information using Advanced Encryption Standard, Marriott cannot rule out the possibility that the hackers stole the encryption keys needed to decrypt that data.

What You Should Do About it

Marriott is in the process of sending e-mails on a rolling basis to affected consumers whose email addresses are in the Starwood guest reservation database. However, everyone should be proactive by calling Marriott's dedicated call center set up to answer questions about the incident (open 7 days a week: 1-877-273-9481; numbers for other countries are available at answers.kroll.com).

Those affected by the breach should do the following as soon as possible:

1. Change the passwords on all your accounts immediately;
2. Review your accounts for suspicious activity and be diligent about monitoring them going forward, including immediately contacting all of your banks and

credit card companies with any concerns;

3. Use a separate card for online transactions, which makes monitoring for suspicious activity less burdensome;
4. Visit answers.kroll.com to enroll in Webwatcher, which monitors websites and generates an alert if your personal information is found (Marriott will pay for one year of this service);
5. Be on heightened alert for phishing attempts when you review your e-mail; and
6. Review all of your accounts to determine whether you can and should delete unnecessary personal information.

Remember: Being Vigilant is the Key

What liability Marriott will face and whether insurance will cover the losses caused by the breach is an open question. However, this is another unfortunate reminder that consumers and businesses need to protect themselves from hackers. The losses from not doing so could prove catastrophic.

Joshua Bevitz is a partner in Newmeyer & Dillion's Walnut Creek office, and a member of the firm's Cybersecurity practice. As an experienced Insurance litigator, Josh advises his clients on proactive measures and potential pitfalls related to their cyber insurance policies. For questions on how you can protect your business, you can reach Joshua at Joshua.Bevitz@ndlf.com.

Casey Quinn is an associate in Newmeyer & Dillion's Las Vegas office, and a member of the firm's privacy & data security practice. Casey brings his substantial experience in complex business litigation to the table, helping businesses proactively navigate the legal landscape of cybersecurity. He can be reached at Casey.Quinn@ndlf.com.

ABOUT NEWMEYER & DILLION LLP

For almost 35 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business law, privacy & data security, employment, real estate, construction, insurance law and trial work, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by The Best Lawyers in America©, and Super Lawyers as top tier and some of the best lawyers in California, and have been given Martindale-Hubbell Peer Review's AV Preeminent® highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.