NEWMEYER & DILLION LLP

MASSIVE DATA BREACH MEANS IT IS TIME TO CHANGE YOUR PASSWORD. *AGAIN.*

By: Casey J. Quinn

January 24, 2019

Casey J. Quinn

Contact
702.777.7506
casey.quinn@ndlf.com

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

Once again, a massive data breach has caught the attention of the cybersecurity world. However, this data breach is different from other recent breaches that were from a single database (like the Marriott / Starwood guest database) because it brings together a collection of data across multiple sources. To avoid negative repercussions from this latest breach, it is recommended to determine whether your private information was compromised, and consider changing password habits.

Details of "Collection 1" Data Breach

A large collection of data recently surfaced on a cloud service site called Mega. The data, saved under a root folder named "Collection #1" included 12,000 separate files and 87 GB of data. News of Collection #1 began circulating on hacker websites when it became known that the files contained an enormous amount of email addresses and passwords. Web security expert Troy Hunt was alerted to Collection #1 and shared news of it through his websites troyhunt.com and haveIbeenpwned.com. Hunt's analysis of the files indicates that there are almost 773 million unique email addresses and around 21 million unique passwords in Collection #1. Although it is difficult to ascertain all the details, it appears from the files in Collection #1 that these emails and passwords possibly came from some 2,890 different sites. In short, Collection #1's availability means that anyone whose address or password is found in this collection is at risk.

Determine the Impact

How do you determine if your accounts were affected? First, visit Hunt's website at haveibeenpwned.com. For several years, Hunt has been compiling a collection of compromised addresses and passwords so that people can see if their accounts have been compromised. Hunt took the data from Collection #1 and added it to his database. Using a search box at haveibeenpwned.com allows you to search to see if your email has ever been compromised in a known breach. If your email has been affected, it will say "Oh no- you have been pwned." (FYI-"pwned" is pronounced like "poned" and is Internet/video game speak for being utterly defeated or gotten the best of someone.) You can scroll down to see which breaches your email address was in and whether that includes Collection #1. If your address shows you have been pwned, you should immediately change your password, and ensure that the e-mail address has not been used for any nefarious purpose.

The same site allows you to click on passwords and search a separate database to see if your passwords have ever been exposed. While you may be concerned about entering your password on this site, Mr. Hunt has taken precautions to ensure its safety. Although Hunt obtained passwords from the same sources as email addresses, they are kept in a separate

database so that you cannot identify which password goes with which email. Try searching your current password. If it says that your password has been pwned, it will tell you how many times that password has shown up in breaches. It does not necessarily mean your specific account was compromised, but it is safe to assume that if your password shows as pwned, again, you need to immediately change it.

How to Avoid E-mail / Password Compromise

Simple steps can protect you from potential e-mail or password compromise, as was seen with this massive breach. First, it is vitally important to update your password regularly, especially if you were exposed in this breach. Even if you were not affected, the release of these documents is a good reminder that you should consider using a password manager. As Hunt says, "[T]he only secure password is the one you can't remember." Password managers like Lastpass or 1Password give you the ability to use passwords you cannot remember. By having one strong master password, you can have the service store all your passwords for other sites. These services will also allow you to generate passwords - which strengthens the protection that a complex, sophisticated password offers – and you will only have to remember a single password.

Expect additional data breaches to continue to occur, as cyber thieves continue to prey on e-mail accounts that are easily hacked. Good cyber hygiene can help you avoid appearing on lists of breached information – and it starts with strong, regularly changed passwords.

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.