NEWMEYER & DILLION LLP

QUEST DIAGNOSTICS DISCLOSES DATA BREACH THAT MAY HAVE EXPOSED THE PERSONAL INFORMATION OF NEARLY 12 MILLION PATIENTS

By: Daniel Schneider

June 10, 2019

Daniel Schneider

Contact
949.854.7000
daniel.schneider@ndlf.com

Practice Areas
Privacy & Data Security
Business Litigation
Construction Litigation
Real Estate Litigation

In a recent filing with the U.S. Securities and Exchange Commission, Quest Diagnostics disclosed that nearly 12 million patients may have had their personal and financial data exposed as a result of a breach that occurred through its billing collection vendor, American Medical Collection Agency. On May 14, 2019, AMCA informed Quest that it identified "potential unauthorized activity" on its web payment page that allowed an "unauthorized user" to gain access to millions of social security numbers, credit card numbers, bank account information and other sensitive data between August 1, 2018 and March 30, 2019 according to the filing.

While no laboratory test results were exposed because Quest does not provide that data to AMCA, this breach sheds light on the fact that data held by medical companies is becoming an increasingly common target for cybercriminals. Although Quest reported that it has not yet been able to verify the accuracy of the information received from AMCA since the investigation is on-going, Quest has since suspended sending any further collection requests to AMCA out of an abundance of caution.

Be Proactive: Monitor & Vet

For patients of Quest that are concerned about their own information:

- Make a habit of monitoring bank account and credit card statements to catch any unauthorized charges. If you find any unauthorized activity, report it immediately. Many banks allow users to set up text-message alerts for every transaction over a specified amount.
- Consider requesting a credit freeze with each of the three major consumer credit bureaus in an effort to watch if your social security number has been stolen. A credit freeze will not affect credit scores, but it will prevent credit reports from being accessed and used by cybercriminals to do such things as applying for loans in your name.

For business owners that are similarly concerned about their own stores of user and customer information, the Quest breach is a stark reminder to make sure that the proper safeguards to protect user and customer information are being implemented. Additionally, outside vendors and contractors that will have access to user data should be properly vetted to ensure that they have the appropriate security in place to protect user data.

The Quest breach is yet another in the long-line of significant data breaches that the citizens of our country have endured. Unfortunately, these breaches will continue to occur – thus obligating both businesses and consumers to guard personal information in the most effective manner possible.

Daniel Schneider is a partner in Newmeyer & Dillion's Privacy & Data Security group. Focused on advocating on behalf of clients when cyber threats inevitably happen, Dan also advises on best practices to help protect the company and mitigate future concerns. Dan can be reached at daniel.schneider@ndlf.com.