7/10/2019

Nate kebede

Data Protection - CYBS-6350-040

Links: <https://krebsonsecurity.com/2019/06/labcorp-7-7m-consumers-hit-in-collections-firm-breach/>

<https://gdpr.report/news/2019/06/10/data-breaches-us-healthcare/>

Summary

A recent breach that targeted the American Medical Collection Agency (AMCA) is the latest example of a breach that a little-known company could hold vast quantities of sensitive data that is being shared or stored in ways that were beyond the control of affected consumers. AMCA is a New York-based third-party billing collections firm that aggressively collects debt for a range of businesses including medical labs, hospitals, telecom companies, marketers, and toll agencies. The Diagnostic lab testing firm Quest Diagnostics, and medical testing giant, LabCorp were also clients of AMCA. The exploited weaknesses of AMCA allowed hackers to breach its payment page and compromise its network, which led to the victimization of millions of consumers. The firm informed Quest about the breach on May 14, 2019, but it took two weeks for the vendor to determine the number of affected people and the type of information lost. It later identified that the personal, financial, and medical data of nearly 12 million Quest patients was breached. The exposed data included SSN, medical history information, credit card numbers and bank account information, service accounts, and balance information. Days after, LabCorp also announced that it had been breached. The breach persisted between August 1, 2018, to March 30, 2019. It was identified that the personal and financial data of 7.7 million consumers, including first and last name, DOB, address, bank account information, service account, and balance information, was exposed. From a data protection perspective, the vendor, AMACA could have protected the data in the following ways: Access control: control in depth using technical systems to prevent an unauthorized user from accessing personal and financial information. Compliance and Legal: following PCI DSS and HIPAA guidelines, and ensuring that the correct security measures are always in place. Cryptography: encrypting PII that was compromised via unauthorized access. Network design: segmenting the network and implementing robust network authentication methods including two-factor authentication, and perhaps through Non-Collection: data such as SSN shouldn’t be collected in the first place if not needed.