DNA Diagnostics Center Settles Data Breach with Ohio and Pennsylvania Attorneys General

March 21, 2023

On February 16, 2023, the Attorneys General of Ohio and Pennsylvania announced a settlement with Ohio-based DNA Diagnostics Center ("DDC") for a 2021 data breach which involved 2.1 million residents nationwide, including the social security numbers of over 45,000 Ohio and Pennsylvania residents. As a part of the settlement, which resolves alleged violations of Ohio and Pennsylvania consumer protection laws, DDC will pay $400,000 in fines and will be required to implement improved security practices.

DDC, one of the world's largest private DNA testing companies, suffered the breach in November 2021. The breach involved databases that were not used for any active business purpose, but had been acquired by DDC as a part of a 2012 acquisition of Orchid Cellmark. These databases contained the personal information of over 2 million individuals who received DNA testing services between 2004 and 2012, including names, payment information, and social security numbers. DDC claims it was unaware that this data was transferred as a part of its acquisition of Orchid.

DDC allegedly received indications of suspicious activity in the database from a security vendor as early as May 2021, but did not activate its incident response plan until August 2021 after the vendor identified signs of malware. The malware was loaded onto DDC's network by threat actors that ultimately facilitated the extraction of patient data, which was subsequently used to extort a payment from DDC in exchange for its promised deletion. In its internal investigation of the incident, DDC found that an unauthorized third party had logged in via VPN on May 24 using a DDC account, having harvested credentials from a domain controller that provided password information for each account in the network. The Assurance of Voluntary Compliance ("AOC") noted that at the time the hacker accessed the VPN, DDC had recently migrated to a different VPN, meaning no one should have been using the VPN that the hackers used. Furthermore, the AOD notes that the threat actor used a decommissioned server to exfiltrate the data.

Prior to the breach, DDC conducted an inventory assessment and penetration test on its systems, however, the legacy databases that stored sensitive personal information in plain text were not identified, as the assessments singularly focused on active customer data.

The Ohio and Pennsylvania Attorneys General alleged that DDC engaged in deceptive or unfair business practices by making material misrepresentations in its customer-facing privacy policy concerning its safeguarding of its customers' personal information. The policy represented that the company implemented "reasonable measures to detect and prevent unauthorized access to [DDC's] computer network."

The settlement requires DDC to develop, implement, and maintain a comprehensive information

security program that is reasonably designed to safeguard the security, integrity, and confidentiality of the company's collected, stored, transmitted, and/or maintained personal information. Additionally, DDC's information security program must include documented methods and criteria for handling information security risks to such personal information. On an annual basis, the company must also conduct comprehensive risk assessments, provide security awareness training to appropriate personnel, and evaluate the overall effectiveness of its information security program.

The settlement specifically requires DDC to implement the following safeguards:

- The assessment of risks associated with acquired technical assets (e.g., systems applications, or devices) containing personal information and the subsequent removal of such information serving no legitimate business purpose or utility to consumers;
- Personal information must be transmitted and stored so that it is only accessible to people and systems that need such information for a legitimate business purpose;
- The maintenance of an updated data/asset inventory of DDC's entire network and the disabling and/or removal of any unnecessary assets;
- The implementation of an incident response plan that mandates DDC employees to respond to any alerts generated from the company's security monitoring systems, along with the documentation of actions to such alerts;
- The detection, investigation, containment, response to, eradication, and recovery from security incidents within reasonable time periods;
- Authentication protocols to ensure that people and systems utilizing credentials are who they purport to be, including through multi-factor authentication, one-time passcodes, and location specific requirements;
- The implementation and maintenance of logging and log monitoring policies and procedures designed to collect, manage, and analyze security logs and monitor where the company stores personal information (to identify, understand, or recover from an attack);
- The maintenance and support of up-to-date software on DDC's network; and
- Technical measures for the detection and response to suspicious network activity within DDC's network, which may include log correlation and alerting, file integrity monitoring, data integrity monitoring, SIEM systems, intrusion detection and prevention systems, and threat management systems.

Takeaways

With this settlement, we get insight into the corrective actions that two different Attorneys General believe are appropriate to prevent future incidents from occurring. Data breaches are often caused by a string of security failures as is alleged to have happened here, including: ignored security alerts, failure to monitor network activity, such as the VPN used by the threat actor that should have no longer been in use, failure to adequately data map thoroughly enough to know that the Orchid systems needed to be in scope for penetration testing, and the failure to properly decommission a server that allowed the hackers to exfiltrate data. However, with such specific injunctive terms, this settlement provides businesses with a good example of how Attorneys General interpret the requirement that they implement "reasonable" safeguards for personal information. It's also a

reminder that companies should review their privacy policies and other public-facing representations regarding their security statements, and ensure they aren’t making promises that they aren’t living up to.