Nearly 7 Million Consumers Impacted by 23andMe Data Breach

On Oct. 6, 2023, a genetic testing company offering ancestry and health reports, 23andMe, announced that its consumers' data was listed on the dark web. Interestingly, many prominent figures such as Mark Zuckerberg, Elon Musk and Sergey Brin's personal information was listed for sale.

23andMe claimed there had not been any vulnerabilities in its network, but rather the hacker used credential stuffing to access its consumers' accounts. Credential stuffing is a technique in which hackers use credentials found on databases for compromised accounts to break into additional accounts where the same credentials were used. To put it simply, 23andMe consumers used the same username and password for multiple websites and one of those websites was breached. In total, the hackers accessed data belonging to about 14,000 users, which is about 0.1% of 23andMe's customers.

The hacker was able to access additional accounts by using the "DNA Relatives" feature on the website, which allows consumers to share data with potential relatives. These "additional accounts" that were impacted by the breach totaled 6.9 million consumers. Some of the data that was stolen and offered for sale included name, date of birth, genetic information, gender, profile pictures and geographical locations. In defense of the data leak, 23andMe explained that it monitors accounts for unauthorized access and provided users with the option of multifactor authentication (MFA).

Class Action

On Oct. 9, 2023, a class action lawsuit was filed against 23andMe alleging negligence, invasion of privacy/intrusion upon seclusion, unjust enrichment and breach of implied contract. According to the complaint, the victims now face an increased risk of identity theft and fraud and suffered from out-of-pocket expenses due to responding to the breach, the decrease in value of their personal data, lost time, and did not receive their benefit of the bargain with 23andMe. Additionally, the complaint alleges that 23andMe failed to implement reasonable and appropriate safeguards to protect users' data, such as monitoring unauthorized access to accounts and adequately training its employees.

Since the breach, 23andMe has updated its terms of service to prevent impacted users from suing or pursuing class actions against it. 23andMe updated its "Dispute Resolution and Arbitration" section which includes a mandatory arbitration clause and requires users to explicitly opt-out of the new terms within 30 days or will be deemed to have agreed to the new terms. This change is notable in that arbitrators are not required to follow legal precedent or procedure. Additionally, arbitration negotiations and awards are generally private, and thus, the records will not be available to the public.

Takeaways

Notably, the type of genetic information that 23andMe collects is not protected under the Health Insurance Portability and Accountability Act (HIPAA). As a result, third-party sharing is allowed under 23andMe's privacy policy. Thus, potential users of genetic testing kits should know that their personal

and sensitive genetic information may not be protected and therefore could fall into the hands of cybercriminals and/or posted in the Dark Web. Additionally, the sharing of genetic information has the potential to place the burden on the consumer to manage their personal data.

This data breach has demonstrated the importance of having unique and complex passwords. Indeed, the National Institute of Standards and Technology (NIST) recommends user-created passphrases be of at least eight characters, auto-generated passphrases be of at least six characters. NIST also recommends users should be able to create passwords at least 64 characters. Notably, the NIST recommendations should set a minimum bar for creating unique and difficult to hack passphrases. The use of credential stuffing is common and the easiest way for a hacker to gain access to multiple accounts. To ensure maximum security, it is best to think of a complicated password that includes phrases, symbols and numbers. Lastly, consumers should enable MFA on any online account that stores their personal information. MFA makes it more difficult for a hacker to gain access to online accounts because it requires another layer of verification to confirm the account owner's identity.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters, including HIPAA and other privacy authorities. If you have any questions about the information presented in this memo, please contact Jessica L. Copeland, CIPP/US or any attorney in Bond's cybersecurity and data privacy practice.

**Special thanks to Associate Trainee Victoria M. Okraszewski for her assistance in the preparation of this blast. Victoria is not yet admitted to practice law.*