KRIS MAYES
ATTORNEY GENERAL

OFFICE OF THE ARIZONA ATTORNEY GENERAL

STATE OF ARIZONA

January 4, 2024

Jacquie Cooke
General Counsel and Privacy Officer
23andMe Inc.
349 Oyster Point Boulevard
South San Francisco, CA 94080

Re: Data Breach

Dear Ms. Cooke:

On October 6, 2023, your company, 23andMe, Inc. ("23andMe") disclosed that a release of "customer profile information," shared through your company's DNA Relatives feature, had occurred without the account users' authorization. On December 5, 2023, after 23andMe's investigation concluded, it announced that the data breach may have affected as many as 6.9 million individual 23andMe customers. A threat actor predictably engaged in "credential stuffing" by re-using usernames and passwords that previously had been compromised or were otherwise available to access 14,000 individual customer accounts, which included their name, sex, date of birth, geographical location, and genetic ancestry results. Through these compromised accounts, the threat actor accessed personal information ("PI") from an additional 5.5 million individuals who used 23andMe's "DNA Relatives" feature, including each individual's name, birth year, relationship labels, the percentage of DNA shared with relatives, ancestry reports, and self-reported location, and another 1.4 million people who used the Family Tree feature that displays a subset of the information available in the DNA Relatives feature.

Additionally, I understand that the 23andMe breach resulted in the publication of the data of one million users of Ashkenazi Jewish heritage and 100,000 users of Chinese ancestry. The information was sold on the dark web for $1 to $10 per individual account. Two weeks later, the data of another four million users was reportedly advertised on the same forum where the first set of data was published. The recent increase in all hate crimes across the country, especially antisemitic and anti-Asian hate crimes, means that this is a particularly dangerous time for the targeted sale of information of individuals identifying and belonging to specific racial or ethnic groups—information that 23andMe profits from analyzing.

23andMe has yet to submit a breach notification to the Attorney General under the Arizona data breach notification statute, A.R.S. § 18-552. The statute requires an entity experiencing a breach of PI to notify all affected Arizona residents within 45 days of the determination that a breach occurred.[1] If the breach affects more than 1,000 Arizona residents, the entity must also notify the Attorney General, the Director of the Arizona Department of

[1] A.R.S. § 18-552(B)(1).

Homeland Security,[2] and the three largest nationwide consumer reporting agencies within 45 days of the breach determination.[3] Your company announced that it had completed its investigation and commenced customer notifications on December 1, 2023.

I am concerned whether 23andMe is adequately protecting Arizonans' personal information and fairly treating Arizona consumers, who are protected by Arizona's data breach notification statute, the Genetic Information Privacy Act,[4] and the Arizona Consumer Fraud Act ("ACFA").[5] Consumers trust 23andMe in part because it claims to protect sensitive information about users through various data protections. These advertised protections include, among others, exceeding "industry" data protection standards, encrypting all sensitive information, and conducting regular assessments to identify security vulnerabilities and threats.[6] And while 23andMe earns significant revenues from its direct-to-consumer DNA report services, its research services unit provides another revenue stream derived from using consumers' genetic data in affiliation with pharmaceutical companies, essentially turning people's genetic data into a product. Though the breach happened through a "credential stuffing" attack, such attacks are predictable events that data security architects should anticipate, particularly if they boast of data security measures while seeking consent from consumers to collect, use, and sell data. Further, a December 5, 2023 Wired article about the breach cited U.S. National Security Agency Director of Cybersecurity Rob Joyce's X feed, in which Joyce noted that some users who used unique email addresses for their 23andMe accounts were still subject to credential stuffing attacks, begging the question of how those email addresses had been compromised in the first place. If they were unique email addresses, they could not have been exposed in another breach incident or via data scraping. Your company's consumers either deserve to know how 23andMe's privacy protections failed to protect their data, or whether your advertised data protections were exaggerated or outright false.

23andMe is in the business of collecting and analyzing the most unique and invaluable of information from individuals: their genetic data. The massive amount of data that was breached and is being sold on the dark web presents a serious harm to consumers who trusted 23andMe with their PI. Accordingly, I am requesting the following answers and information:

1. Identify the total number of individuals whose data was affected by this incident, including the number of Arizona residents.

2. Please provide a breakdown of the categories of PI compromised for the impacted Arizona residents.

3. Indicate when the impacted Arizona residents received or will receive notice informing them that their PI was compromised as a result of the data breach. Please also indicate whether 23andMe plans to submit notice of this incident to our office and if so, when such notice will be provided. If not, please explain why.

4. Please explain whether any Arizona residents' information was made available on

[2] A.R.S. § 18-552(B)(2)(b).
[3] A.R.S. § 18-552(B)(2)(a).
[4] A.R.S. § 44-8001 *et seq.*
[5] A.R.S. § 44-1521 *et seq.*
[6] https://www.23andme.com/privacy/

the dark web and whether this information includes their genetic ancestry information.

5. Produce copies of all versions of 23andMe's comprehensive security program, as that term is defined by A.R.S. § 44-8002(A)(4) of the Genetic Information Privacy Act, in place for the period of June 1, 2023 through October 15, 2023.

6. Please explain how the PI or data at issue was stored on the systems involved and any safeguards in place at the time of the breach to protect such information from unauthorized access or acquisition.

7. Please describe any safeguards put into place by 23andMe to prevent or detect "credential stuffing" attacks on your system. Please also include 23andMe's methods for detecting the use of bots.

8. Please provide further detail on the breach timeline, including when the data exfiltration began and ended, and when 23andMe discovered the breach.

9. Please provide information on the further security measures implemented after discovery of the breach to protect user data in addition to requiring users to reset their passwords on October 9 and later switching from optional to required use of multi-factor authentication to access accounts on November 6, and explain why these security measures were not required prior to the breach.

10. Please describe how 23andMe defines "industry data protection standards" and detail the data protection setup, policies, and procedures that your company has implemented to exceed those standards. This explanation should include:

    a. A description of the "industry" against which 23andMe measures itself.

    b. Whether these standards include principles of risk assessment, gap analysis, internal and external audits, data segmentation, and third-party certification.

    c. How 23andMe's policies and procedures before the breach incident complied with those standards.

11. Explain whether the data compromised during the subject breach was contained within your information security management system supporting 23andMe's "IT Consulting, Managed Services and Cloud Services" that you advertise as ISO 27001:2013 certified. If so, please state whether you know of any other companies in your "industry" that currently conform to the newer ISO 27001:2022 revision and its heightened security protocols.

12. Please detail the type and frequency of the assessments 23andMe uses to identify security vulnerabilities and threats that it claims it regularly conducts.

13. Please describe the standard of encryption that 23andMe to protect sensitive data, along with what data your company includes in its definition of "sensitive data."

14. Please provide a copy of any internal or third-party investigative report or audit performed by or for 23andMe related to this breach.

15. Please describe the process or processes that 23andMe uses to obtain consent from users for the "DNA Relatives" feature. Please include screenshots of exact disclosures or click-through screens that have been shown to users prior to receiving their consent to opt into the "DNA Relatives" feature.

16. Please provide any plan, policies, and/or procedure that 23andMe currently has in place, or is developing, to prevent the reoccurrence of a data security incident and a timeline for implementing the plans, policies, or procedures.

17. Please describe the policies that 23andMe has put in place for both internal and external reporting requirements when your company suffers a data breach.

18. Please explain whether you plan to provide consumers whose PI was compromised any compensation or data monitoring services as a result of the breach.

19. Please provide the plans or policies that 23andMe has for the use and disposal of users' PI, if any.

20. Explain why 23andMe amended its terms of service for consumers since the breach was discovered, to prevent collective or class arbitration.[7] Clarify whether this does anything to improve 23andMe's data security practices or ensure that Arizona consumers are less likely to be harmed by future breaches, or whether this instead disincentivizes 23andMe from taking any proactive steps to protect the public.

21. Provide the name and contact information for a point of contact at the appropriate agency corresponding with the "federal law enforcement officials" 23andMe claimed to be working with in its October 9, 2023 update on the breach incident.

Sincerely,

Kris Mayes
Arizona Attorney General

[7] https://www.hipaajournal.com/23andme-updates-terms-of-service-to-prevent-class-action-lawsuits/