

PATTY MURRAY, WASHINGTON
ROBERT P. CASEY, JR., PENNSYLVANIA
TAMMY BALDWIN, WISCONSIN
CHRISTOPHER MURPHY, CONNECTICUT
TIM KAINE, VIRGINIA
MARGARET WOOD HASSAN, NEW HAMPSHIRE
TINA SMITH, MINNESOTA
BEN RAY LUJÁN, NEW MEXICO
JOHN W. HICKENLOOPER, COLORADO
EDWARD J. MARKEY, MASSACHUSETTS

BILL CASSIDY, LOUISIANA
RAND PAUL, KENTUCKY
SUSAN M. COLLINS, MAINE
LISA MURKOWSKI, ALASKA
MIKE BRAUN, INDIANA
ROGER MARSHALL, KANSAS
MITT ROMNEY, UTAH
TOMMY TUBERVILLE, ALABAMA
MARKWAYNE MULLIN, OKLAHOMA
TED BUDD, NORTH CAROLINA

United States Senate

COMMITTEE ON HEALTH, EDUCATION,
LABOR, AND PENSIONS

WASHINGTON, DC 20510-6300

WARREN GUNNELS, MAJORITY STAFF DIRECTOR
AMANDA LINCOLN, REPUBLICAN STAFF DIRECTOR

www.help.senate.gov

October 20, 2023

VIA ELECTRONIC TRANSMISSION

Ms. Anne Wojcicki
Chief Executive Officer
23andMe, Inc.

Dear Ms. Wojcicki:

I write with significant concern over the recently disclosed data breach at 23andMe that resulted in the unauthorized disclosure of 1.3 million customers' information being posted on the dark web, including one million customers identified as people of Ashkenazi Jewish descent and 300 million customers identified as people of Chinese heritage.¹ Data included name, sex, birth year, location, photos, health information, and genetic ancestry results.² Hackers shared the information online as a database entitled, "Ashkenazi DNA Data of Celebrities."³ Some entries included well known individuals, such as technology company CEOs.⁴ While 23andMe confirmed the breach on October 6, it has yet to provide details about when hackers first exploited vulnerability in its systems.

As one of the largest purveyors of direct-to-consumer genetic tests, 23andMe plays a particularly important role in protecting the identities and privacy of your customers.⁵ Genetic information, unlike financial information and other types of identifying information, cannot be changed in response to data breaches. Genetic information is particularly sensitive, carrying health and personally identifying information that can be used against its owners. To this point, one commenter on the posted list proclaimed, "Crazy, this could be used by Nazis."⁶ This posting comes at a time of increasing rates of global antisemitism and anti-Asian hate, which can be

¹ Kevin Collier, *23andMe user data targeting Ashkenazi Jews leaked online*, NBC News (Oct. 7, 2023), <https://www.nbcnews.com/news/us-news/23andme-user-data-targeting-ashkenazi-jews-leaked-online-rcna119324>.

² Lily Hay Newman, *23andMe User Data Stolen in Targeted Attack on Ashkenazi Jews*, Wired (Oct. 6, 2023), <https://www.wired.com/story/23andme-credential-stuffing-data-stolen/>. Jonathan Greig, *23andMe scraping incident leaked data on 1.3 million users of Ashkenazi and Chinese descent*, The Record (Oct. 6, 2023), <https://therecord.media/scraping-incident-genetic-testing-site>.

³ Wired.

⁴ *Id.*

⁵ Matt Binder, *More than 26 million people have added their DNA to four leading ancestry databases: report*, Mashable (February 12, 2019), <https://mashable.com/article/at-home-ancestry-test-boom>.

⁶ *23andMe user data targeting Ashkenazi Jews leaked online*.

leveraged to draw higher prices for the information and increase the threat from potential evildoers. Hackers offered these records for sale in the posting for between \$1 and \$10 each.⁷

Your company's own website describes the potential negative health implications of association with Ashkenazi Jewish ancestry, namely incidence of Gaucher disease, Canavan disease, Tay-Sachs disease, Crohn's disease, and breast, ovarian, and prostate cancer. Such information in the hands of employers, potential employers, foreign governments, hostile actors, and others could be used to discriminate against individuals associated with the group.⁸

The statement released by your company claims that 23andMe's systems did not experience a data security incident, but rather hackers gained access to user passwords and "scraped" more user information through the platform's DNA Relatives feature.⁹ Given that your company has 14 million users, the potential for sensitive user data breach is immense and could extend beyond this serious incident.¹⁰ It is critical that you take the necessary precautions to protect your customers from breaches that can have serious impacts on their livelihoods and wellbeing.

I ask that you answer the following questions, on a question-by-question basis, by **November 3, 2023**:

1. When did 23andMe become aware of the data breach? What protocols did 23andMe follow once it became aware of the data breach?
2. When did 23andMe notify users of the data breach? Which users did the company notify and how did it notify them?
3. What regulatory or contractual obligations and considerations are 23andMe subject to as holders of individual genetic data and the phenotypes evident from such data? Specifically, what privacy, security, and breach notification obligations?
4. What security protocols, both cyber and physical, does 23andMe have in place? Is 23andMe accredited by any privacy and security organizations? If so, which?
5. How often does 23andMe conduct audits on its privacy and security protocols? What were the results of the most recent audits?
6. Why are individual users given access to others' genetic information and profiles, such as through the DNA Relatives Feature? How much access do they have? What types of data belonging to others are accessible?

⁷ Antonio Pequeno IV, *23andMe User Data Stolen And Listed for Sale In Attack Targeting Ashkenazi Jews*, Forbes (Oct. 6, 2023), <https://www.forbes.com/sites/antoniopequenoiv/2023/10/06/23andme-user-data-stolen-and-listed-for-sale-in-attack-targeting-ashkenazi-jews/?sh=1af0ff995be1>.

⁸ *Understanding Ashkenazi Jewish Ancestry & Genetics for Your Health*, 23andMe (Jul. 20, 2023), <https://blog.23andme.com/articles/ashkenazi-ancestry-and-health>.

⁹ *Wired*.

¹⁰ *23andMe user data targeting Ashkenazi Jews leaked online*.

7. What search tools and algorithms does 23andMe use to allow large-scale downloads of user data based on specific demographics? How did hackers compile such a comprehensive list of impacted users to the dark web?
8. How was mass user data, allegedly hundreds of personal accounts per compromised user account, obtained by access to a few individual accounts?¹¹
9. 23andMe stated that the hackers that obtained unauthorized data violated its terms of service.¹² How many times has 23andMe found that an entity or an individual violated these terms in the past year and what are the consequences of such a violation?
10. What is 23andMe doing to remediate the impact of the data breach? How is the company compensating affected users?
11. What is 23andMe doing to prevent future data breaches or unauthorized disclosure of customer data?

Sincerely,



Bill Cassidy, M.D.

Ranking Member

Senate Committee on Health,

Education, Labor and Pensions

¹¹ *Id.*

¹² *Addressing Data Security Concerns*, 23andMe (October 9, 2023), <https://blog.23andme.com/articles/addressing-data-security-concerns>.