Hacking

This article is more than **1 year old**

Hackers got nearly 7 million people's data from 23andMe. The firm blamed users in 'very dumb' move

The company pointed at people who 'failed to update their passwords' as sensitive data was offered for sale on forums

23andMe's headquarters in Sunnyvale, California. Photograph: Justin Sullivan/Getty Images

Mack DeGeurin

Thu 15 Feb 2024 09.26 EST

Three years ago, a man in Florida named JL decided, on a whim, to send a tube of his spit to the genetic testing site 23andMe in exchange for an ancestry report. JL, like millions of other 23andMe participants before him, says he was often asked about his

ethnicity and craved a deeper insight into his identity. He said he was surprised by the diversity of his test results, which showed he had some Ashkenazi Jewish heritage.

JL said he didn't think much about the results until he learned of a huge breach at the company that exposed the data of nearly 7 million people, about half of the company's customers. Worse, he later learned of a hacker going by the pseudonym "Golem" who had offered to sell the names, addresses and genetic heritage reportedly belonging to 1 million 23andMe customers with similar Ashkenazi Jewish heritage on a shadowy dark web forum. Suddenly, JL worried his own flippant decision to catalog his genes could put him and his family at risk.

"I didn't know my family was going to potentially be a target," he said. "I may have put my family and myself in danger for something I did out of curiosity more than anything."

JL, who asked to only be identified by his initials due to the ongoing privacy issues, is one of two plaintiffs listed in a recent class-action lawsuit filed in California against 23andMe. Plaintiffs claim the company failed to adequately notify users of Jewish and Chinese heritage after they were allegedly targeted. The lawsuit claims hackers placed those users in "specially curated lists" that could have been sold to individuals looking to do harm.

23andMe has since confirmed hackers gained access to 14,000 user accounts over a span of five months last year, some of which revealed detailed, sensitive reports on users' health. The company revealed details on the exact types of data stolen in its months-long breach in a January data breach notification letter sent to California's attorney general earlier last month. Hackers accessed users' "uninterrupted raw genotype data" and other highly sensitive information, like health predisposition reports and carrier-status reports gleaned from the processing of a user's genetic information. Worse still, 23andMe confirmed the thieves also accessed other personal information from up to 5.5 million people who opted in to a feature that lets them find and connect with genetic relatives.

23andMe only publicly acknowledged the hackers' attacks after one user posted about the up-for-sale data on a 23andMe subreddit in early October. An investigation digging into the incident revealed hackers had actually been trying, sometimes successfully, to gain access since at least April 2023. The attacks had continued for nearly five months through the end of September. In an email sent to the Guardian, a 23andMe spokesperson said the company

did not “detect a breach” within 23andMe systems and instead attributed the incident to compromised recycled login credentials from certain users.

A far larger subsection of users had other, potentially less sensitive data exposed through 23andMe’s opt-in DNA relatives feature, which automatically lets the company share data between other users on the platform who they may be related to. In other words, hackers who gained access to a user’s account via the compromised passwords were also able to suck up data about potential relatives. The optional feature gives users insight into a variety of data points, including their relatives’ name, their predicted relationship, and the percentage of DNA shared with matches. It can also include an individual ancestry report, matching DNA segments, and uploaded photos.

Eli Wade-Scott, one of the attorneys representing JL in the class-action lawsuit, said these allegedly ethnicity-specific groupings could amount to a “hit list”. Jay Edelson, another attorney representing those users, worried those lists of users could look attractive to terrorists looking to identify people of Jewish heritage. He also said Chinese intelligence agencies, which have a history of surveilling and intimidating dissidents abroad, could use the data to target people critical of the government or even nation states.

> *“This is a total paradigm shift when it comes to the implications of a data breach”*
> **Jay Edelson**

“This is a total paradigm shift when it comes to the implications of a data breach,” Edelson added.

Months after it first became aware of the beach, 23andMe sent a letter to several customers taking legal action against the company. The company defended itself by saying there was no way the breach could lead to real-world problems: “The information that was potentially accessed cannot be used for any harm.” It also cast blame for the hack on users who “negligently recycled and failed to update their passwords”. Cybersecurity professionals refer to the weaponization of these repeated digital keys as “credential stuffing” attacks.

“Therefore,” 23andMe concluded, “the incident was not a result of 23andMe’s alleged failure to maintain reasonable security measures.”

But multiple attorneys and genetic privacy experts say the company should have seen such an attack coming and done far more to safeguard this highly sensitive, intimate data. “You shouldn’t be able to do an attack like this over the course of months and have nobody at 23andMe notice,” said Wade-Scott.

Barbara Prainsack, a University of Vienna professor for comparative policy, was herself a 23andMe customer. She said the company had a long time to protect itself and to establish data breach protocols. 23andMe, she said, seemed to have done neither: “This is almost a textbook case of how things should not be done.”

She added that blaming consumers for their own relatively minor security lapses is “morally and politically very dumb”.

23andMe users suing the company for negligence seem to agree. They say they never would have bought the company’s kits had they known how lax its security was. Since the breach, more than two dozen 23andMe users have brought forward individual and class-action lawsuits accusing the company of negligence and invasion of privacy. The specifics of each of the lawsuits vary, but each argues the company failed to “implement and maintain adequate security measures”.

“23andMe lied to customers about how it would protect their data, failed to reasonably protect their data in accordance with industry standards, lied about the scope and severity of the breach, failed to notify its Jewish and Chinese customers that they were specifically targeted, and in the end, exposed them to a host of threats and dangers that they’ll never see coming,” JL’s suit reads.

The slow-burning data breach scandal adds insult to injury to a company that has precipitously fallen from the highest rungs of Silicon Valley exceptionalism in recent years. The company went public in 2021 at a value of $3.5bn; now it is worth roughly $300m, a decline of 91%. 23andMe has never turned profit in its 18-year history. It may run out of cash by 2025. In only a few short years, the company that once seemed destined to become the “Google of spit” is struggling to remain on the Nasdaq in spite of co-founder and CEO Anne Wojcicki’s repeated attempts to quell investors’ concerns.

Experts said the downstream consequences of hackers accessing breached genetic data remains largely hypothetical. Still, they warned a bad actor armed with this type of information and enough motivation could potentially use it to identify an individual or blackmail them by threatening to reveal even more sensitive information. The possible combination of data gleaned from the 23andMe breach with other personal information could result in sophisticated identity fraud.

Murat Kantarcioglu, a professor of computer science at the University of Texas at Dallas said he could imagine a scenario where an attacker armed with data linking an individual to a previously unknown relative could blackmail them by threatening to make that connection public. Other data revealing a user's family history with mental health issues, Kantarcioglu said, could possibly be misused by an employer to pass over someone seeking a job or promotion.

At the time of writing, 23andMe requires two-factor authentication by default for all its users. That added layer of security, which critics had demanded for years, was only enabled by default after the breach. 23andMe says it also required all its customers to reset their passwords following the incident.

Muddying matters even further, legal experts believe 23andMe recently made subtle changes to its terms of service making it more difficult for victims to join together to pursue mass arbitration lawsuits, TechCrunch reported. Those changes reportedly came just two days before 23andMe officially disclosed the data breach. 23andMe denies accusations it altered its terms of service to dissuade lawsuits and has instead said it made the changes to make resolutions for disputes occur faster.

"Customers continue to retain the right to seek public injunctive relief," a 23andMe spokesperson said in an email.

"In the middle of the night, they [23andMe] changed their terms to game the system and make it basically impossible to bring any sort of large volume of arbitration," Edelson said. Cohen Milstead partner Doug McNamara described the maneuver as a "desperate attempt to dissuade and deter from suing [23andMe]" in a December interview with TechCrunch.

> *"The way that the information is being bought and sold, it's kind of Defcon One in the privacy world*
> Jay Edelson

Nearly a year has passed since hackers first tried gaining access to 23andMe users' accounts, but the company's legal and regulatory worries are probably just beginning. Aside from the metastasizing lawsuits, lawmakers are getting involved. In January, New Jersey Democratic representative Josh Gottheimer wrote a letter to FBI director Christopher Wray urging the agency to launch an investigation into the company to determine whether or not the exposed data could be used to target Jewish communities. That came on the heels of a letter sent to 23andMe by Arizona

attorney general Kris Mayes seeking additional data on the company's security protocols.

Experts fear the ripple effects of the 23andMe breach could extend beyond the company itself. Prainsack worries anxiety stemming from the breach may make people less likely to share personal health data, not just with 23andMe, but more traditional doctors as well. That lack of trust could make it more difficult to properly treat patients.

Kantarcioglu, from UT Dallas, said this probably wouldn't be the last data breach of its kind to affect genetic testing companies. "You have extremist groups calling for the death of Jews throughout the world, so it's hard to see how the stakes could be higher," Edelson, JL's attorney, said. "The way that the information is being bought and sold, it's kind of Defcon One in the privacy world."