

1 Rafey S. Balabanian (SBN 315962)
2 rbalabanian@edelson.com
3 EDELSON PC
4 150 California Street, 18th Floor
5 San Francisco, California 94111
6 Tel: 415.212.9300
7 Fax: 415.373.9435

8 *Counsel for Plaintiffs David Melvin, J.L., and the Putative Classes*

9 **UNITED STATES DISTRICT COURT**
10 **NORTHERN DISTRICT OF CALIFORNIA**
11 **SAN FRANCISCO DIVISION**

12 **DAVID MELVIN and J.L.**, individually and
13 on behalf of all others similarly situated,

14 *Plaintiffs,*

15 *v.*

16 **23ANDME, INC.**, a Delaware corporation,

17 *Defendant.*

18 Case No. _____

19 **CLASS ACTION COMPLAINT FOR:**

- 20 (1) **Negligence;**
- 21 (2) **Threat Assessment and Monitoring;**
- 22 (3) **Violation of Cal. Bus. & Prof. Code § 17200, et seq.;**
- 23 (4) **Violation of 410 ILCS 513, et seq.;**
Alaska Stat. § 18.13.010, et seq.; **Or. Rev. Stat. § 192.531, et seq.;** and
- 24 (5) **Declaratory Judgment.**

25 **DEMAND FOR JURY TRIAL**

26 Plaintiffs David Melvin and J.L., on behalf of themselves and all others similarly
27 situated, bring this class action complaint against Defendant 23andMe, Inc. (“23andMe”) and
28 allege as follows upon personal knowledge as to themselves and their own acts and
experiences, and, as to all other matters, upon information and belief.

INTRODUCTION

1. Genetic data is the “holy grail” of personal information. DNA can be used to
reveal an individual’s health, explore their family history, and even identify their ethnicity. But
genetic data can also be exploited for discriminatory and abusive purposes, from denying

1 individuals and their families employment opportunities or health and life insurance, to
2 creating “hit lists” of minorities and other vulnerable populations, like what shockingly has
3 happened here.

4 2. On December 5, 2023, one of the largest direct-to-consumer genetic testing
5 companies, 23andMe, notified 7 million customers that a “threat actor” accessed their accounts
6 without authorization “in early October” through a process called credential stuffing. From the
7 outset, 23andMe appeared to wash its hands of the situation, blaming its customers for reusing
8 passwords from other websites and telling them that it has no “indication that there was a data
9 security incident” within its systems.

10 3. What 23andMe knew—but concealed—from those 7 million customers was that
11 their private genetic information (“PGI”) was leaked on the dark web two months earlier on
12 October 1, 2023, along with their genetic heritage, ancestral origin, full names, home addresses,
13 profile pictures, and birth dates. Discovery will show that 23andMe delayed sending notice of
14 the breach to these 7 million customers so that it could first change its terms and conditions to
15 add onerous arbitration requirements that were specifically aimed at preventing them from
16 pursuing claims against the company.

17 4. As if this was not bad enough, 23andMe also concealed that Jewish and Chinese
18 customers were specifically targeted by the hacker and that their PGI was compiled into
19 specially curated lists that were shared and sold on the dark web and continue to be shared and
20 sold to this day. Discovery will show that 23andMe reviewed this data and confirmed it was
21 legitimate, but nonetheless concealed this information from its Jewish and Chinese customers.

22 5. This is not a typical data breach. The hacker leaked the list of over 1 million
23 Jewish customers expressly in retribution for the Israel-Hamas war, and was more than happy
24 to leak the list of 350,000 Chinese customers upon request from a user with the alias “Wuhan.”
25 These lists generated a huge amount of interest from hackers on the dark web from all over the
26 world and were shared and reshared an untold number of times.

27 6. The disclosure of the Jewish and Chinese lists threatens the safety and security
28 of those customers and subjects them to harassment, vandalism, assault, and discrimination.

1 And given the Chinese government’s long history of tracking Chinese citizens both in the
2 country and abroad in the United States, the data poses unique dangers for Chinese 23andMe
3 customers who may become targets of the Chinese government’s surveillance and intimidation
4 apparatus.

5 7. To this day, 23andMe has never told its 7 million compromised customers that
6 their PGI was disclosed on the dark web, and never told its Jewish and Chinese customers that
7 they were specifically targeted. These customers must be immediately notified of the true
8 nature of the breach so that they can protect themselves and take the steps necessary to remove
9 their PGI off Defendant’s platform if they so choose.

10 8. As explained below, 23andMe lied to customers about how it would protect their
11 data, failed to reasonably protect their data in accordance with industry standards, lied about
12 the scope and severity of the breach, failed to notify its Jewish and Chinese customers that they
13 were specifically targeted, and in the end, exposed them to a host of threats and dangers that
14 they’ll never see coming. These customers would not have purchased genetic testing kits or
15 provided their genetic information to 23andMe had they known that it would fail to protect
16 their data or conceal information critical to their safety and well-being.¹

17 9. Accordingly, Plaintiffs bring this class action on behalf of themselves, a
18 Vulnerable Persons Subclass, and a State Genetic Privacy Statute Subclass to hold 23andMe
19 accountable for its egregious misconduct and to force it to notify its customers, including
20 specifically its Jewish and Chinese customers, of the actual scope and extent of the breach.

21 **PARTIES**

22 10. Plaintiff David Melvin is a natural person and a citizen of the State of Illinois.

23 11. Plaintiff J.L. is a natural person and a citizen of the State of Florida.

24 12. Defendant 23andMe, Inc., is a Delaware corporation with its principal place of
25 business located at 349 Oyster Point Boulevard, San Francisco, California 94080.

26
27
28 ¹ There may be additional ethnic, racial, or otherwise vulnerable groups that were specifically targeted by the breach, which is an issue that counsel will explore through discovery.

1 **JURISDICTION AND VENUE**

2 13. This Court has original jurisdiction over this action under 28 U.S.C. §
3 1332(d)(2). The amount in controversy exceeds the sum or value of \$5 million, exclusive of
4 interests and costs, there are more than 100 members of the proposed Classes, and at least one
5 Class Member is a citizen of a state different from Defendant.

6 14. This Court has personal jurisdiction over Defendant because Defendant is
7 headquartered in California, its principal place of business is in California, and it regularly
8 conducts business in California.

9 15. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant
10 and/or its parents or affiliates are headquartered in this District and a substantial part of the
11 events or omissions giving rise to Plaintiffs’ claims occurred in this District.

12 **DIVISIONAL ASSIGNMENT**

13 16. Pursuant to Civil Local Rule 3-2(c)&(d), this case should be assigned to the San
14 Francisco Division because a substantial part of the events or omission giving rise to the claim
15 occurred within the county of San Mateo.

16 **STATEMENT OF FACTS**

17 **I. 23andMe Creates and Stores the Highly Sensitive Genetic Profile Reports of its**
18 **Customers.**

19 17. 23andMe is a leading biotechnology company founded with the mission “to help
20 people access, understand, and benefit from the human genome.” It offers a suite of services
21 including DNA analysis, genetic healthcare information, and genetic ancestry analysis services
22 and touts its ability to provide users with “direct access to genetic information.”

23 18. In order to use Defendant’s services, customers buy one of the various packages
24 that 23andMe offers, which currently range in prices from \$119 to \$298. Defendant analyzes
25 the DNA in the customer’s saliva sample and provides a detailed personalized report of their
26 genetic profile.

27 19. 23andMe creates reports for its customers that provide extraordinarily detailed
28 information derived from their individual genome—in other words, an intimate snapshot of

1 their genetic profile. The report includes the individual’s health risks and disease profile, which
2 can include predisposition and carrier status for certain cancers, Alzheimer’s disease, diabetes,
3 cystic fibrosis, sickle cell anemia, and other conditions. In addition to this information, reports
4 also include information about the individual’s ethnic and ancestral background, genetic health
5 risks, as well as pharmacogenetic information—how their body processes certain medications.

6 20. Beyond personalized reports, 23andMe also offers a “DNA Relatives” feature
7 that allows customers to share data with other customers and “explore the genetic similarities
8 and differences between you and family members.” Information shared through this feature
9 includes, but is not limited to, the name of individual account holders, percentage of shared
10 DNA and predicted relationships, ancestry reports, geographic location, family names, profile
11 pictures, birth years, family trees, and more.

12 **II. 23andMe Promised its Customers that it Would Protect Their Private Genetic**
13 **Information Using Security Measures that “Exceed” Industry Standards.**

14 21. To convince customers to pay money for its testing services, 23andMe promises
15 them that privacy and security are paramount to its business operations.

16 22. 23andMe recognizes the sensitive nature of genetic information and assures
17 customers that “your privacy comes first” and that “when you explore your DNA with
18 23andMe, you entrust us with important personal information. That’s why, since day one,
19 protecting your privacy has been our number one priority. We’re committed to providing you
20 with a safe place where you can learn about your DNA knowing your privacy is protected.”

21 23. 23andMe also tells customers that it is “a safe place to explore and understand
22 your genes,” because “Privacy and Security are woven into everything we do” and “respect for
23 customer privacy and transparency are core principles” that help “maintain customer trust.”

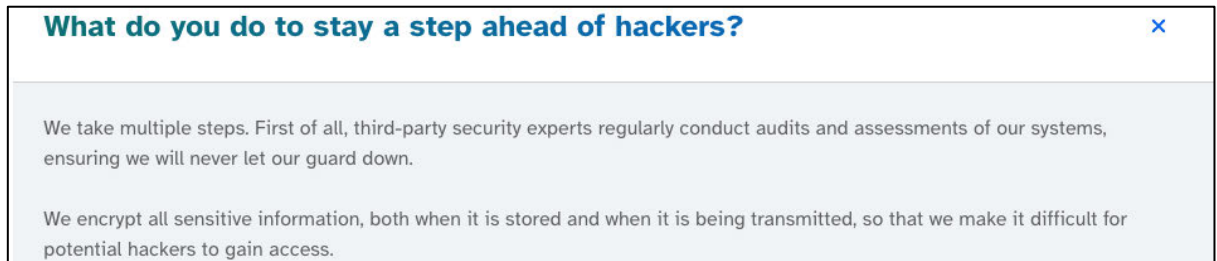
24 24. In its privacy policy, 23andMe acknowledges that it has obligations to protect
25 the data customers provide, stating, “we appreciate the level of trust [customers] put into us”
26 and telling customers it has implemented “physical, technical, and administrative measures
27 aimed at preventing unauthorized access to or disclosure of your Personal Information.”

28 25. In addition to recognizing the importance of privacy to its customers, 23andMe

1 represents that genetic information is “fiercely protected by security practices that are regularly
2 reviewed and updated.” It further states that “your genetic information deserves the highest
3 level of security, because without security, you can’t have privacy” and reiterates that it
4 “employs software, hardware, and physical security measures to protect [user] data.”

5 26. 23andMe further assures customers that its data security protocols “exceed
6 industry data protection standards,” that it “encrypt[s] all sensitive information,” and also
7 “conduct[s] regular assessments to identify security vulnerabilities and threats.”

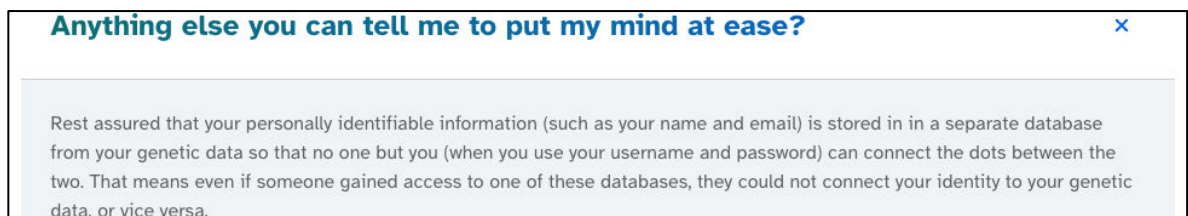
8 27. 23andMe also expressly tells users that it understands the threat of hackers and
9 the severity of the consequences of a potential data breach, as shown in Figure 1 below, which
10 is a screenshot from its website.



11
12
13
14
15 **(Figure 1.)**

16 28. On its blog, the company goes further, stating that “23andMe access combines
17 token-based, multi-factor authentication and strict least-privileged authorization controls.”

18 29. Defendant also tells potential customers that they should not be concerned about
19 their private genetic information being exposed because the company untethers its customers’
20 identities from the genetic data stored on its servers. In response to a hypothetical question,
21 “Anything else you can tell me to put my mind at ease,” Defendant promises that personally
22 identifiable information is segregated from genetic data, so that “no one but you . . . can
23 connect the dots between the two,” as shown in Figure 2 below, which is a screenshot from its
24 website.



25
26
27
28 **(Figure 2.)**

1 30. In other words, 23andMe assures customers that even if breached, their PGI will
2 remain protected and unconnected to their identities.

3 31. These statements are meant to assure customers that their PGI will not be at risk
4 of disclosure and that they have full control over how it is shared. This message is bolstered by
5 representations from 23andMe that “you are in control of your DNA and your data” and “we
6 give you full control to decide how your information is used and with whom it is shared.”

7 32. 23andMe’s customers chose to purchase the company’s services with the
8 expectation that it would comply with its promises to keep such information confidential and
9 secure from third parties.

10 33. While 23andMe assured customers of the numerous steps it takes to protect their
11 privacy, the data breach announced on October 6, 2023 has shown these representations to be
12 false, including the specific promises to anonymize PGI stored on its servers, protect PGI using
13 protocols that “exceed” industry standards, and actively monitor for suspicious activity.

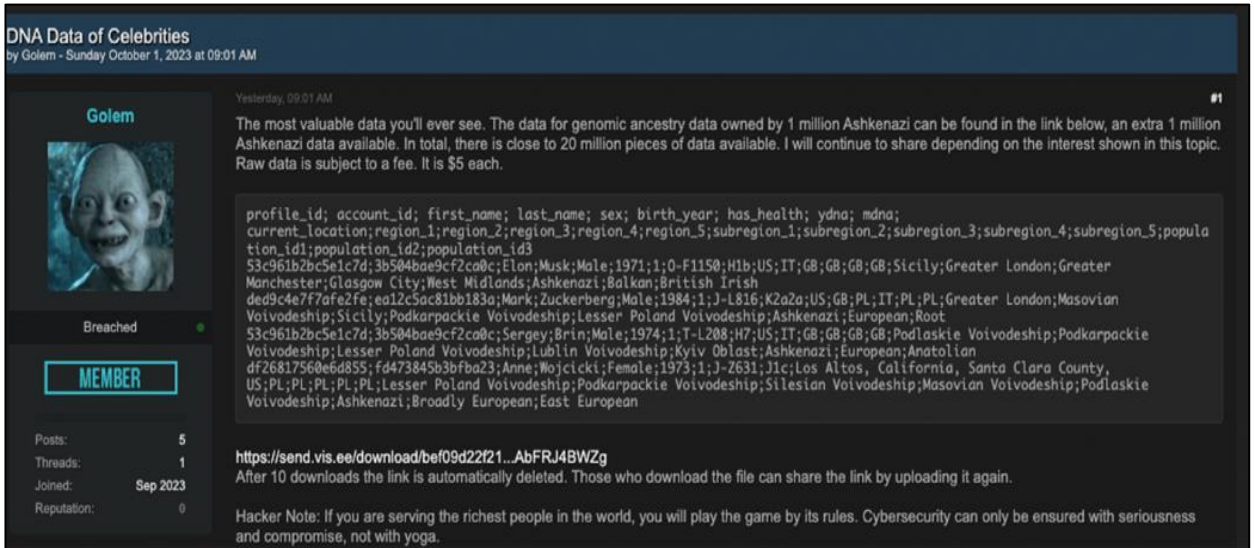
14 **III. Despite its Data Security Promises, 23andMe’s Customers’ Private Genetic**
15 **Information was Stolen and Used to Target Vulnerable Groups.**

16 34. Hackers use the “dark web” to buy, sell, and otherwise release stolen data. The
17 dark web is accessible via TOR (The Onion Router), which redirects traffic through thousands
18 of relays in order to anonymize the user’s internet activity and browsing. While using TOR, the
19 websites that are visited only log the IP address of the last TOR relay, as opposed to the user’s
20 actual IP address. TOR mainly consists of Onion sites that are similar to normal websites but
21 end with an address of “.onion.” These sites can only be visited through a TOR interface. Just
22 like the surface web, the dark web has various search engines that can be used to find content.

23 35. Cybercrime forums such as Breach Forums are utilized by users on the dark web
24 to anonymously advertise and purchase stolen information, including stolen databases, leaks
25 from ransomware or other malicious software, and compromised accounts and passwords.

26 36. On October 1, 2023, a hacker using the alias “Golem” leaked the 23andMe DNA
27 and profile data of 1 million Ashkenazi Jews, including their full names, home addresses, and
28 birth dates on Breach Forums, calling it “[t]he most valuable data you’ll ever see,” as shown in

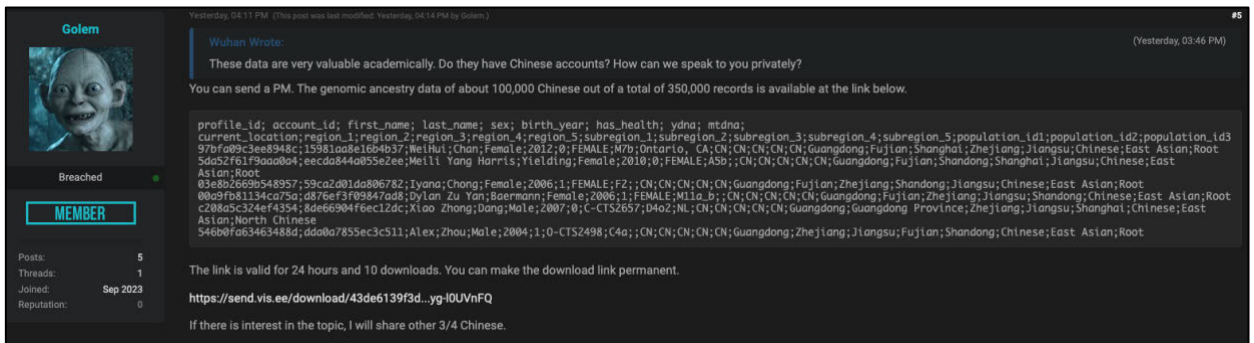
Figure 3 below, which is a screenshot from Breach Forums.



(Figure 3.)

37. Golem’s explicit targeting of Jewish 23andMe users is further conveyed by his use of the character “Gollum” from The Lord of the Rings—a creature driven by greed with ugly and outsized facial features—as his profile picture.

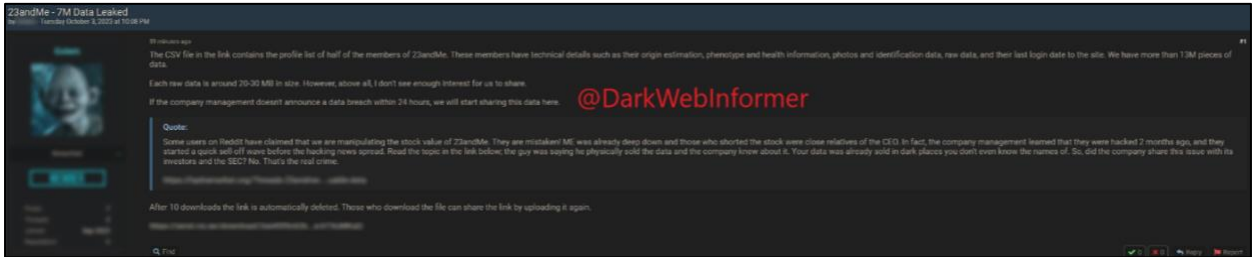
38. A few hours after leaking the Jewish 23andMe database, a user with the alias “Wuhan” replied and asked Golem if has “Chinese accounts,” indicated that such data is “very valuable academically,” and asked if they could “speak privately.” Golem responded with a link to the DNA and profile data of 100,000 Chinese customers. Golem also stated that he has a total of 350,000 DNA and profile records and that he would release them if there was interest, as shown in Figure 4 below, which is a screenshot from Breach Forums.



(Figure 4.)

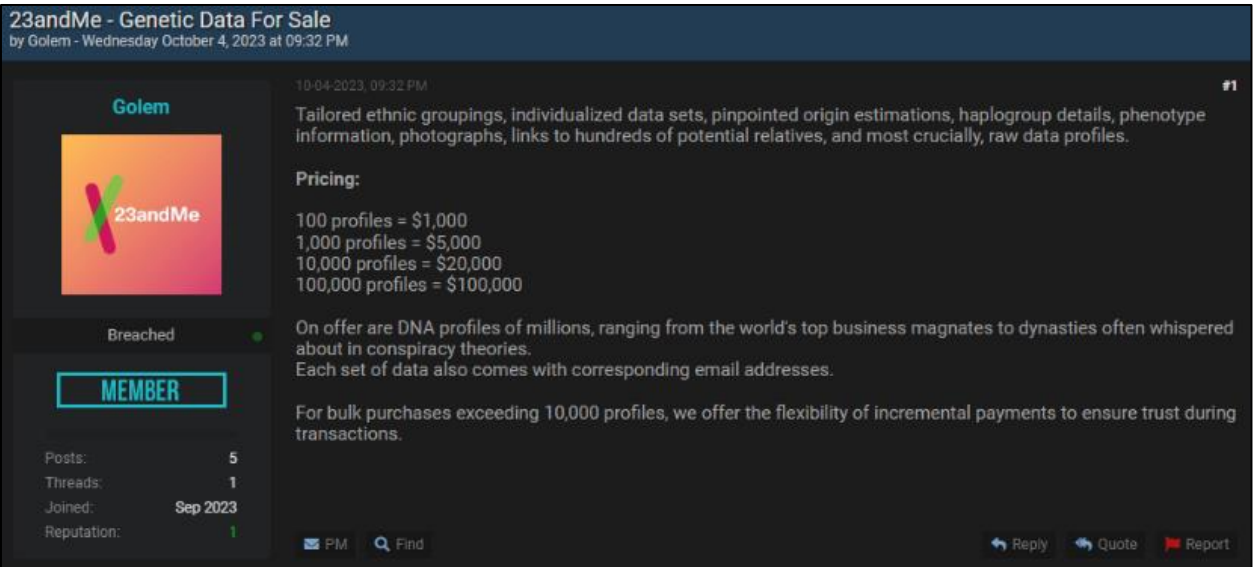
39. The next day, Golem leaked an even larger database of information including the DNA and profile data of 7 million users. Golem shared a link to the stolen data, writing, “the

1 CSV file in the link contains the profile list of half of the members of 23andMe . . . these
 2 members have technical details such as their origin estimation, phenotype and health
 3 information, photos and identification data, raw data, and their last login date to the site,” as
 4 shown in Figure 5 below, which is a screenshot from Breach Forums taken by Dark Web
 5 Informer:



10 **(Figure 5.)**

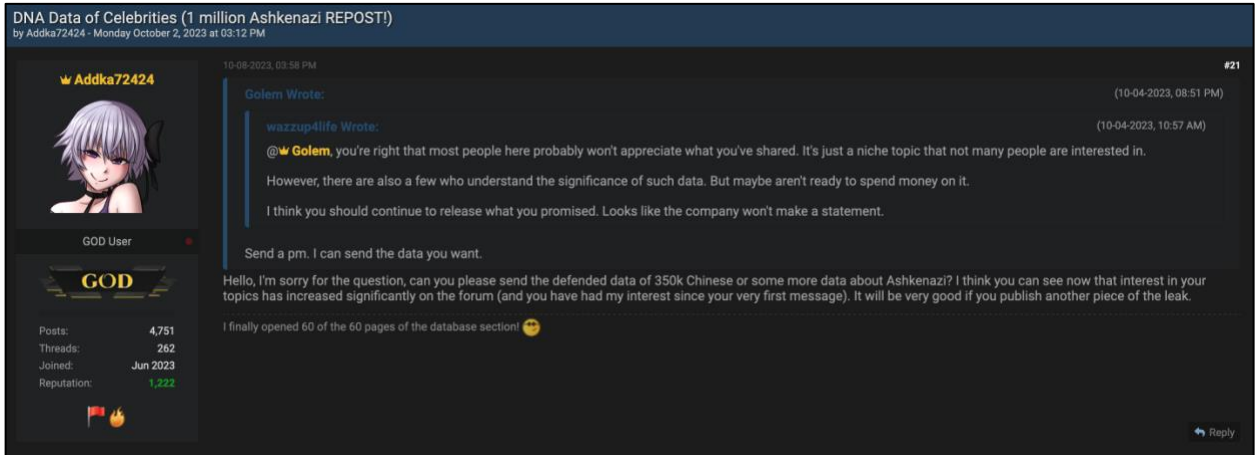
11 40. On October 3, 2023, Golem posted pricing for “[t]ailored ethnic groupings,
 12 individualized data sets, pinpointed origin estimations, haplogroup details, phenotype
 13 information, photographs, links to hundreds of potential relatives, and most crucially, raw data
 14 profiles,” as shown in Figure 6 below, which is a screenshot from Breach Forums.



24 **(Figure 6.)**

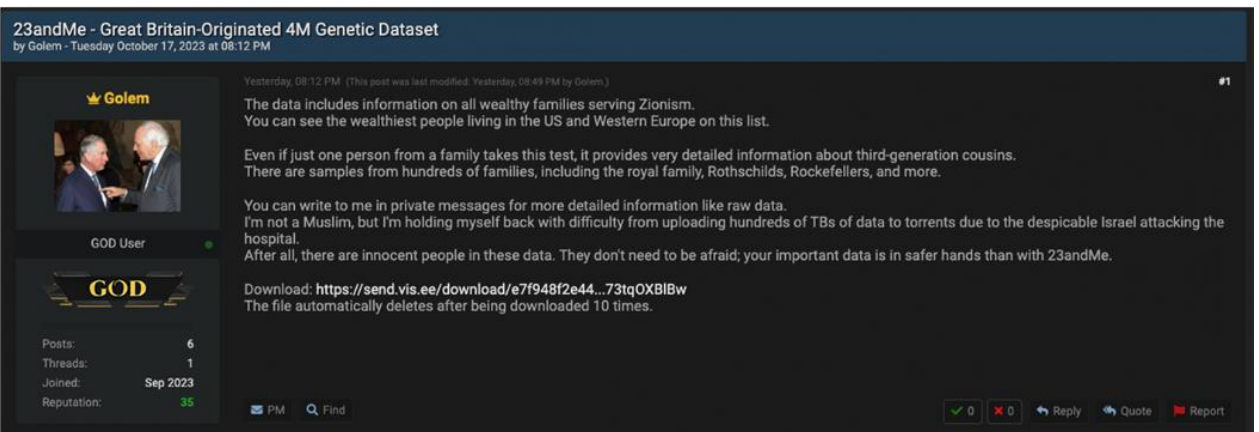
25 41. The Jewish and Chinese leaks were met with immediate and overwhelming
 26 interest from other Breach Forum users. For example, on October 8, 2023, “Addka72424”
 27 replied to Golem, stating, “I think you can see now that interest in your topics has increased
 28 significantly on the forum (and you have had my interest since your very first message)” and

1 asking, “can you please send the defeneded data of 350k Chinese or some more data about
 2 Ashkenazi?” as shown in Figure 7 below, which is a screenshot from Breach Forums.



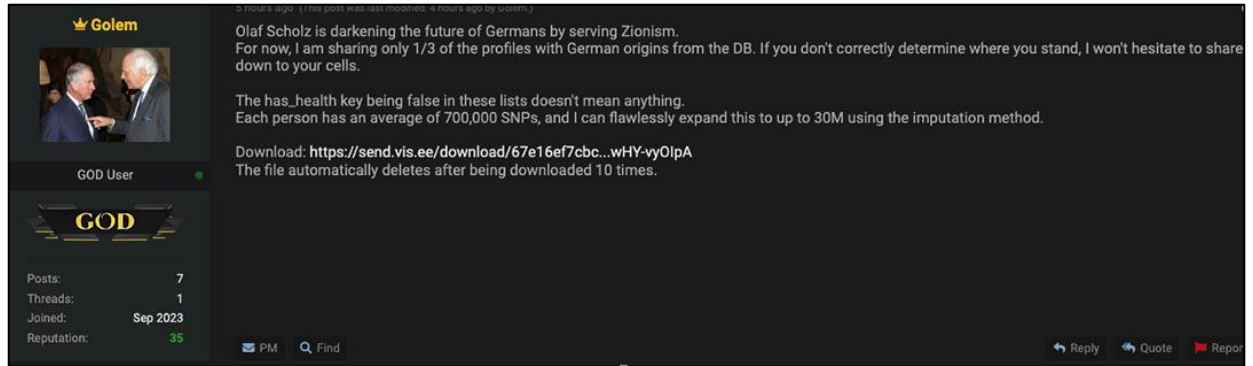
10 **(Figure 7.)**

11 42. On October 17, Golem posted another thread titled “23andMe – Great Britain-
 12 Originated 4M Genetic Dataset,” that expounded on his apparent antisemitic agenda and
 13 included data about “wealthy families serving Zionism” and stated, “I’m not a Muslim, but I’m
 14 holding myself back with difficulty from uploading hundreds of TBs of data to torrents due to
 15 the despicable Israel attacking the hospital,” shown below in Figure 8, which is a screenshot
 16 from Breach Forums.



24 **(Figure 8.)**

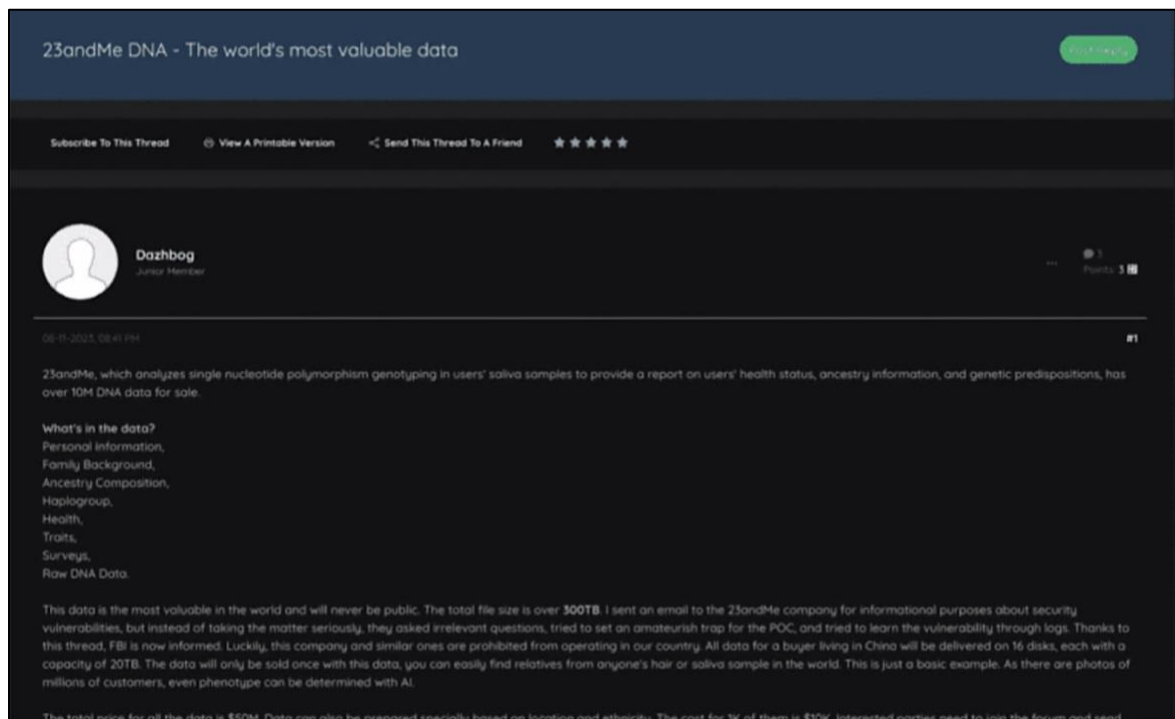
25 44. One day later—after German Chancellor Olaf Scholz expressed solidarity with
 26 Israel at a press conference in Tel Aviv with Israeli Prime Minister Benjamin Netanyahu—
 27 Golem posted another message stating that “Olaf Scholz is darkening the future of Germans by
 28 serving Zionism,” as shown in Figure 9 below, which is a screenshot from Breach Forums.



(Figure 9.)

45. Reports show that there may have also been an additional and entirely separate breach of 23andMe’s servers by a different threat actor several months before the genetic information was posted to Breach Forums on October 1, 2023.

46. On August 11, 2023, a person using the alias “Dazhbog” posted a message titled, “23andMe DNA – the world’s most valuable data,” on a hacker forum called Hydra Market offering to sell 300 TB of 23andMe data for \$50 million and stating that “all data for a buyer living in China will be delivered on 16 disks, each with a capacity of 20 TB,” as shown in Figure 10 below, which is a screenshot from Hydra Market:



(Figure 10.)

47. On August 12, 2023, Dazhbog uploaded a sample of genetic data for one million

1 23andMe customers in the United States, noting the leak contained the DNA profiles of 10
2 million Americans. The hacker claimed to have contacted 23andMe at that time—a relatively
3 common extortion practice—but “instead of taking the matter seriously, [the company] asked
4 irrelevant questions.”

5 48. At this time, Plaintiffs do not know if the Dazhbog leak contained authentic
6 23andMe customer information or if 23andMe was even aware of the posting, as it never
7 publicly acknowledged the post or notified its customers about it. Plaintiffs are also unaware at
8 this time as to whether the Dazhbog and Golem leaks are related in any way. These matters will
9 be explored through discovery.

10 49. But the fact that there is evidence of a potential additional breach of 23andMe’s
11 customers’ genetic information that occurred two months earlier is nonetheless extremely
12 concerning, especially given that Dazhbog provided specific instructions about how he would
13 safely deliver this data to China and that it was offered at a price point (\$50 million) that would
14 only be relevant actors on the global stage, such as the Chinese government. People that might
15 be considered “dissidents” to the Chinese government abroad were rightly terrified of this
16 revelation, given the government’s practice of keeping minute tabs on individuals even in other
17 countries.

18 50. The disclosure of the Jewish and Chinese customer lists threatens the safety and
19 security of those customers and subjects them to harassment, vandalism, assault, intimidation,
20 and discrimination.

21 51. According to the Anti-Defamation League (“ADL”), antisemitic incidents
22 skyrocketed after Hamas carried out a terror attack in Israel on October 7, 2023. Between
23 October 7 and December 7, the ADL recorded a total of 2,031 antisemitic incidents, up from
24 465 incidents during the same period in 2022, representing a 337% increase year-over-year.²
25 This includes 40 incidents of physical assault, 337 incidents of vandalism, and 749 incidents of
26

27 ² Press Release, ADL, *ADL Reports Unprecedented Rise in Antisemitic Incidents Post-Oct. 7*
28 (Dec. 11, 2023) <https://www.adl.org/resources/press-release/adl-reports-unprecedented-rise-antisemitic-incidents-post-oct-7>.

1 verbal or written harassment, and a fatality that occurred at an anti-Israel protest in Los
2 Angeles, where a Jewish man was killed after being hit in the head by a pro-Palestinian
3 protester.

4 52. A recent ResumeBuilder survey found that 25% of hiring managers are less
5 likely to move forward with Jewish candidates, 32% reported that antisemitism is common in
6 their workplace, and 23% admitted their belief that their industry should have fewer Jewish
7 employees.³

8 53. In a January 11, 2024 letter to the FBI, U.S. Congressman Josh Gottheimer—a
9 member of the House Permanent Select Committee on Intelligence—raised the alarm about the
10 possibility that the lists could be used for domestic terrorism and expressed an urgent need “to
11 protect the information, locations, and lives of the American Jewish population”:

12 I am concerned that the leaked data could empower Hamas, their supporters, and
13 various international extremist groups to target the American Jewish population and
14 their families. The threat of violent domestic extremism poses a significant danger
15 to America’s Jewish community.

16 54. Likewise, Arizona Attorney General Kris Mayes recently sent a letter to
17 23andMe expressing her concerns for the safety of its Jewish and Chinese customers:

18 The recent increase in all hate crimes across the country, especially antisemitic and
19 anti-Asian hate crimes, means that this is a particularly dangerous time for the
20 targeted sale of information of individuals identifying and belonging to specific
21 racial or ethnic groups—information that 23andMe profits from analyzing.

22 55. Given the Chinese government’s long history of tracking Chinese citizens both
23 in the country and abroad in the United States, the data breach poses unique dangers for
24 23andMe customers of Chinese ancestry who may become targets of the Chinese government’s
25 surveillance and intimidation apparatus.

26 56. In fact, a secret Chinese police station was recently discovered in New York City
27 that was tasked with monitoring and coercing Chinese expatriates.⁴ The station was part of an

28 ³ *1 in 4 hiring managers say they are less likely to move forward with Jewish applicants*,
ResumeBuilder, <https://www.resumebuilder.com/1-in-4-hiring-managers-say-they-are-less-likely-to-move-forward-with-jewish-applicants/> (last updated Jan. 9, 2024).

⁴ Perry Stein and Joseph Menn, *U.S. alleges secret Chinese police post in NYC, online tracking of dissidents*, The Washington Post (Apr. 17, 2023), <https://www.washingtonpost.com/national-security/2023/04/17/chinese-police-new-york-social-media/>.

1 extensive network that the Chinese government uses to silence dissent and exert control of
2 Chinese nationals and dissidents in the United States.

3 57. This breach also raises the specter of Chinese nationals being coerced within the
4 vast ambit of China’s social credit system, which can severely limit personal freedoms based
5 on behavior. The system can dictate one’s access to services, freedom of movement, and even
6 influence social standing. The pervasive nature of this system means that the compromised data
7 from 23andMe could place individuals and their families under even greater scrutiny,
8 potentially leading to punitive measures that extend beyond China’s borders.

9 58. To this day, Defendant has failed to notify any of its Ashkenazi Jewish or
10 Chinese customers that their DNA, genetic reports, and personal information has been leaked
11 on Breach Forums and shared with an untold number of hackers.

12 59. For customers of Ashkenazi Jewish and Chinese ancestry, the stakes could not
13 be higher. The uncertainty surrounding which other ethnic or religious groups may be targeted
14 with the leaked PGI database only adds to the distress. In a climate where cyber threats loom
15 large, the possibility that hackers could aggregate and trade sensitive genetic information about
16 vulnerable communities represents a harrowing breach of trust and personal security.

17 **IV. Instead of Taking Responsibility for its Deficient Data Security Measures,**
18 **23andMe Drastically Downplayed the Breach and Blamed its Customers.**

19 60. Though its customers’ PGI was posted on Breach Forums on October 1, 2023,
20 23andMe waited 5 days before announcing through a vaguely drafted blog post that it “recently
21 learned that certain 23andMe customer profile information . . . was compiled from individual
22 23andMe.com accounts without the account users’ authorization” as a result of “threat actors”
23 being able to “access certain accounts” (the “October 6 Announcement”).

24 61. The October 6 Announcement failed to provide any details on the number of
25 customers affected by the breach, and most importantly, failed to mention that the hacker
26 leaked the DNA and profile information of 7 million customers on the dark web or that the
27 hacker disclosed specially curated lists of Jewish and Chinese customers. In fact, to this day,
28 23andMe has never told its customers about the Breach Forums leak, even though its

1 spokesperson has confirmed for multiple media outlets that the leak contained genuine data.

2 62. Instead of providing this critical information or explaining what steps were being
3 taken to remedy its data security vulnerabilities, 23andMe’s October 6 Announcement shifted
4 the blame to its customers, telling them that the breach was the result of “threat actors [who]
5 were able to access certain accounts in instances where users recycled login credentials—that
6 is, usernames and passwords that were used on 23andMe.com were the same as those used on
7 other websites that have been previously hacked.” 23andMe also reassured that customer data
8 is adequately protected on its system, reiterating that “At 23andMe, we take security seriously.
9 We exceed industry data protection standards and have achieved three different ISO
10 certifications to demonstrate the strength of our security program. We actively and routinely
11 monitor and audit our systems to ensure that your data is protected.”

12 63. Over the next two months, 23andMe released a handful of minor updates that
13 failed to provide any meaningful or substantive information about the breach. For example,
14 23andMe updated its October 6 Announcement on October 20, 2023 to say that “As part of the
15 ongoing security investigation, we have temporarily disabled some features within the DNA
16 Relatives tool as an additional precaution to protect the privacy of our customers,” and again on
17 November 6, 2023 to say that “[s]tarting today, we are requiring all customers to utilize email
18 2-step verification (2SV) as an added layer of protection for their account.” The updates were
19 silent about the scope and extend of the breach, despite that it already had actual knowledge
20 that the DNA and profile information of 7 million customers was leaked on Breach Forums.

21 64. Two months later, on December 1, 2023, Defendant updated its October 6
22 Announcement to report that “23andMe has completed its investigation, assisted by third-party
23 forensic experts,” and is finally “in the process of notifying affected customers.” In other
24 words, 23andMe waited a full two months before it informed 7 million customers that they
25 were directly impacted by the data breach, and even then, the section titled “How does this
26 impact you?” was so vague and confusing that it raised more questions than it answered, as
27 shown in Figure 11 below, which is a screenshot of that section from 23andMe’s December 1,
28 2023 email notice:

How does this impact you?

After further review, we have identified your DNA Relatives profile as one that was impacted in this incident. Specifically, there was unauthorized access to one or more 23andMe accounts that were connected to you through DNA Relatives. As a result, the DNA Relatives profile information you provided in this feature was exposed to the threat actor. You can see a full list of the types of information that you may have included in your profile [here](#). You can view what information is currently included in your DNA Relatives profile and make changes [here](#).

(Figure 11.)

65. Amazingly, Defendant again concealed the Breach Forums leak and again failed to notify customers with Ashkenazi Jewish or Chinese ancestry that they were specifically targeted by hackers.

66. On December 5, 2023, Defendant provided a final blog update to its October 6 Announcement:

As our investigation comes to a close, we wanted to share the details of what took place and our findings.

In early October, we learned that a threat actor accessed a select number of individual 23andMe.com accounts through a process called credential stuffing. That is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously compromised or otherwise available. We do not have any indication that there was a data security incident within our systems, or that 23andMe was the source of the account credentials used in these attacks.

The threat actor used the compromised accounts to access information shared with these accounts. Specifically, DNA Relatives profiles connected to these compromised accounts, which consist of information that a customer chooses to make available to their genetic relatives when they opt in to participate in 23andMe's DNA Relatives feature. A DNA Relatives profile includes information such as display name, predicted relationships, and percentage of DNA shared with matches. You can find a full list of the types of information included in a DNA Relatives profile [here](#).

Additionally, through the compromised accounts, the threat actor accessed a feature called Family Tree, which includes a limited subset of DNA Relatives profile information. The Family Tree feature does not include ancestry information such as the percentage of DNA shared with genetic matches or ancestry reports.

1 Additional Details

- 2 ○ The threat actor was able to access less than 0.1%, or roughly 14,000 user
3 accounts, of the existing 14 million 23andMe customers through credential
4 stuffing.
- 5 ○ The threat actor used the compromised credential stuffed accounts to access the
6 information included in a significant number of DNA Relatives profiles
7 (approximately 5.5 million) and Family Tree feature profiles (approximately
8 1.4 million), each of which were connected to the compromised accounts.

9 Since detecting the incident, we emailed all customers to notify them of the
10 investigation and are continuing to notify impacted customers, based on applicable
11 laws. We also required every 23andMe customer to reset their password. In
12 addition, 23andMe now requires all new and existing customers to login using two-
13 step verification. Protecting our customers' data privacy and security remains a top
14 priority for 23andMe, and we will continue to invest in protecting our systems and
15 data.

16 67. 23andMe's final public announcement fell woefully short of providing any
17 information about the breach and again failed to warn victims that their private information had
18 already been leaked on Breach Forums. By failing to disclose this critical information,
19 23andMe lied to its customers about the scope and severity of the breach.

20 68. Further, despite having actual knowledge that the hacker curated and leaked lists
21 of Jewish and Chinese customers on the dark web, a 23andMe spokesperson told the New York
22 Times on December 4, 2023 that "we have not learned of any reports of inappropriate use of
23 the data after the leak."⁵ Likewise, 23andMe's attorney, Ian Ballon, went even further in a
24 December 11, 2023 letter to attorneys representing certain 23andMe customers, stating, "the
25 information that was potentially accessed cannot be used for any harm."⁶ These were false
26 statements that were intended to mislead 23andMe's customers and investors.

27 **V. Despite Blaming its Customers, the Circumstances of the Breach Show that**
28 **23andMe Failed to Implement Basic Security and Threat Detection Measures.**

69. The facts underlying the breach, as well as the October 6 Announcement and all

26 ⁵ Rebecca Carballo, *Data Breach at 23andMe Affects 6.9 Million Profiles, Company Says*,
New York Times (Dec. 4, 2023), [https://www.nytimes.com/2023/12/04/us/23andme-hack-
data.html](https://www.nytimes.com/2023/12/04/us/23andme-hack-data.html).

27 ⁶ Letter from Ian C. Ballon, Attorney for 23andMe, to Hassan A. Zavareei (Dec. 11, 2023)
28 available at [https://www.documentcloud.org/documents/24252535-response-letter-to-tycko-
zavareei-llp](https://www.documentcloud.org/documents/24252535-response-letter-to-tycko-zavareei-llp).

1 updates thereafter, demonstrate that 23andMe abjectly failed to implement reasonable and
2 adequate security measures prior to the October 6 Announcement by (1) failing to implement
3 reasonable policies and procedures to detect suspicious activity; (2) failing to adequately
4 anticipate and prevent reasonably foreseeable hacking threats; (3) failing to properly assess the
5 security and privacy risk of dangerous product features (such as DNA Relatives); and (4)
6 failing to respond to public discussions of leaks of data in Defendant's possession.

7 70. First, 23andMe very obviously failed to take the proper steps to detect and
8 prevent the unauthorized access. Credential stuffing generally has a very low rate of success at
9 around 0.1%—meaning a threat actor will succeed only once for every thousand attempts to
10 use a recycled password from a large list.⁷ The fact that 23andMe admits roughly 14,000
11 accounts were successfully accessed means the threat actor likely made around *14 million*
12 *failed login attempts*. If 23andMe had even basic threat detection tools in place, it would have
13 detected such a large pattern of suspicious activity in real time and had ample opportunity to
14 shut it down. Similarly, the automated process by a threat actor to access 5-7 million DNA
15 Relatives profiles also presents a very obvious anomalous pattern of access that would appear
16 very different from normal user activity to threat detection protocols.

17 71. Had 23andMe implemented adequate monitoring systems in line with industry
18 guidance, it could have detected these patterns of activity at the onset of the compromise and
19 taken steps to prevent further malicious logins as well the further access to and eventual
20 exfiltration of its customers' highly sensitive genetic data.

21 72. 23andMe also failed to adequately anticipate and prevent reasonably foreseeable
22 hacking threats. Credential-stuffing attacks are a common security threat that have garnered a
23 significant amount of attention due to breaches at other large companies by hackers using
24 recycled user passwords. For this type of attack, hackers often buy credentials from these
25 previous breaches, knowing that users often reuse passwords. 23andMe was well aware of the
26

27 ⁷ CloudFlare, *What is Credential Stuffing?* <https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/#:~:text=Statistically%20speaking%2C%20credential%20stuffing%20attacks,they%20will%20succeed%20roughly%20once> (last visited Jan. 23, 2024).
28

1 threat of this type of attack and even posted warnings in its privacy policies writing, “[b]e
2 mindful of keeping your password and other authentication information safe from third parties,
3 and immediately notify 23andMe of any unauthorized use of your login credentials.” Despite
4 this knowledge, 23andMe apparently placed the burden on users of the platform to report
5 unusual activity, when it could have proactively protected customer information by requiring
6 them to use multi-factor authentication for their accounts—a feature that had been optional on
7 the platform since 2019.

8 73. In fact, 23andMe implicitly admitted that the breach could have been prevented
9 with two-step verification. On November 6, 2023—more than a month after the Breach Forum
10 leak—23andMe finally began requiring customers to use two-step verification because it
11 “provides an extra layer of security and can prevent bad actors from accessing an account
12 through recycled passwords.” Many companies have had mandatory two-step verification in
13 place for years. Ring, a leading manufacturer of home security systems and cameras, added the
14 requirement roughly four years ago. Had 23andMe implemented industry standard protections
15 (or “exceed” them as promised), it would have required two-step verification prior to this
16 breach.

17 74. Beyond two-step verification, the Open Source Foundation for Application
18 Security (“OWASP”), a peer-reviewed industry resource, provides a number of basic, industry
19 standard measures that 23andMe could have implemented to protect against a credential-
20 stuffing attack including, implementing a Completely Automated Public Turing test to tell
21 Computers and Humans Apart (CAPTCHA) for each login attempt, blocking known malicious
22 or abusive IP addresses or devices, or even requiring users to create a username as opposed to
23 an email address (which would have been listed in illicit information obtained by hackers to
24 conduct a credential-stuffing attack).⁸ Had 23andMe implemented *any* of these security
25 processes, the credential-stuffing attack could have been thwarted entirely.

26
27
28 ⁸ *Credential Stuffing Prevention Cheat Sheet*, OWASP, https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html (last visited Jan. 23, 2024).

1 75. Before the breach, 23andMe also failed to inform users of the increased risks of
2 using the DNA Relatives feature. 23andMe knew or should have known through a risk
3 assessment that the DNA Relatives function could compromise the integrity of numerous
4 customer profiles if a single associated account was breached. Nevertheless, there were no
5 additional safeguards, protections, or warnings in place to alert users to increased threats when
6 using this feature. If users had known of the potential for the widespread compromise of user
7 accounts through this feature, they would have likely opted out.

8 76. The unauthorized acquisition of such a massive amount of user data during the
9 breach further showed that 23andMe failed to institute reasonable security measures to prevent
10 or detect the attack including, monitoring for unusual login patterns and rates, utilizing up-to-
11 date audit and traceability tools to monitor for suspicious activity, as well as threat detection
12 and monitoring alerts that trigger when in real time data is exfiltrated at large volumes. Any of
13 these basic security measures would have detected and mitigated the credential-stuffing attack
14 and unauthorized data scraping of the DNA Relatives function.

15 77. While 23andMe publicly touted that it was certified in information security
16 standards such as ISO/IEC 27001:2013, 27018, and 27701, it failed to upgrade its certifications
17 to the newer 2022 versions, which contained pertinent policies that could have addressed the
18 potential sources of the breach described here. For example, the new controls in updated
19 versions include topics of threat intelligence, data leakage prevention, and monitoring
20 activities, all of which are relevant to this breach.⁹

21 78. 23andMe also knew or should have known about industry best practices aimed at
22 preventing common data security threats, including a credential-stuffing attack. OWASP Top
23 10, a peer-reviewed industry standard document, highlighted the top web vulnerabilities against
24 which companies should defend themselves.¹⁰ Among these threats, the category
25 “Identification and Authentication Failures” highlights security weakness that “permit
26

27 ⁹ *ISO/IEC 27001 & ISO/IEC 27002:2022: What You Need to Know*, PECB (Mar. 23, 2022)
28 <https://pecb.com/past-webinars/isoiec-27001--isoiec-270022022-what-you-need-to-know>.

¹⁰ *OWASP Top 10: 2021*, OWASP, <https://owasp.org/Top10/> (last visited Jan. 23, 2024).

1 automated attacks such as credential stuffing.”¹¹ Another category, “Security Logging and
2 Monitoring Features” outlines best practices to “detect, escalate, and respond to active
3 breaches” including appropriate alerting thresholds, monitoring logins and high-value
4 transactions, and monitoring suspicious activities.¹²

5 79. 23andMe also failed to comply with guidance promulgated by the Federal Trade
6 Commission (“FTC”) to ensure businesses handling confidential consumer information
7 implement adequate data security practices.¹³ With respect to detecting data breaches, in
8 particular, the FTC recommends businesses use an intrusion detection system, monitor all
9 incoming traffic to the networks for unusual activity, monitor for large amounts of data being
10 transmitted from their systems, update systems frequently, and have a response plan prepared
11 in the event of a breach. The failure to employ reasonable and appropriate measures to protect
12 against unauthorized access to confidential consumer data is considered an unfair act or
13 practice prohibited pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45, and state law
14 equivalents.

15 80. Finally, 23andMe failed to implement digital threat monitoring systems to obtain
16 visibility into the surface web (the regular open internet), the deep web (sites that require
17 logins), and the dark web (sites only accessible via special software such as TOR). The main
18

19 ¹¹ A07:2021—*Identification and Authentications Failures*, OWASP,
20 https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ (last visited
21 Jan. 23, 2024).

22 ¹² A09:2021 — *Security Logging and Monitoring Failures*, OWASP,
23 https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/ (last visited
24 Jan. 23, 2024).

25 ¹³ The FTC has also issued guidance related to security principles and standard practices for
26 businesses handling confidential information. These include but are not limited to: (a) taking
27 inventory of the personal customer information they collect and store; (b) properly disposing of
28 personal information and only keeping it for as long as necessary; (c) protecting confidential
information through physical security, electronic security (including encryption and
authentication), and employee training; (d) understanding their network’s vulnerabilities; and
(e) implementing policies to correct security problems. *See Protecting Personal Information: A
Guide for Business*, FTC (Oct. 2016), [https://www.ftc.gov/business-
guidance/resources/protecting-personal-information-guide-business](https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business); *see also Policy Statement
of the FTC on Biometric Information and Section 5 of the FTC Act*, FTC (May 18, 2023),
https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf (including
genetic information within the definition of “biometric information” which must be protected
by reasonable security measures to prevent unauthorized access).

1 purpose of such monitoring is to gain early warning to better anticipate and detect a breach.
2 Many companies run their own threat intelligence programs and others either rely completely
3 on a third party or use that third party to augment their existing program.

4 81. The surface web can be scanned by simply using various search engine operators
5 to look for a particular company name or product identifying them. Google can also be used to
6 set alerts to fire if a particular keyword is mentioned on the surface web. Searching the deep
7 web often involves creating logins to various known cybercriminal sites and checking forums
8 for particular mentions. Just like the surface web, the dark web has various search engines that
9 can be used to find content. Additionally, threat intelligence sources often provide large lists of
10 various cybercrime related Onion sites.

11 82. If consumers had known that 23andMe failed to comply with its own security
12 statements, industry best practices, and reasonable security standards, they would not have
13 purchased or chosen to entrust 23andMe with highly confidential information such as their
14 genetic or personal information.

15 83. While the 23andMe had the resources necessary to prevent, or at the very least,
16 detect and mitigate the breach, it neglected to abide by its own terms and security promises,
17 failed to implement basic measures designed to anticipate and prevent reasonably foreseeable
18 hacking threats, and failed to implement reasonable policies to detect suspicious activity.

19 **VI. As a Company Storing Highly Valuable Private Genetic Information, 23andMe**
20 **Knew or Should Have Known that it Would Likely be Targeted by Hackers.**

21 84. 23andMe was not only entrusted with protecting users' personal information but
22 also their highly sensitive genetic information. While the unauthorized disclosure of personal
23 information can have significant consequences, the unauthorized disclosure of genetic
24 information compounds these issues and poses unique risks that have the potential to inflict
25 permanent and irreparable harm.

26 85. 23andMe knew that its data security obligations were important given the
27 increase in cyberattacks targeting companies that store confidential consumer information. For
28 example, the Identity Theft Resource Center estimated that as of the third quarter of 2023, there

1 were approximately 2,116 reported data breaches impacting over 233 million people.

2 86. Research has shown that personal data has high commercial value on the dark
3 web, where information such as names, addresses, phone numbers, and credit history of
4 individuals sells for between \$40 and \$200.¹⁴ Beyond the monetization of individual-level
5 information, reports have also documented the significant commercial value of access to the
6 breached databases of companies.

7 87. Beyond its obligations regarding personal information, 23andMe knew or should
8 have known that the unauthorized disclosure of genetic information poses an even higher risk
9 to consumers because it is immutable, thereby making its disclosure harder, if not impossible,
10 to cure. This immutability also makes genetic data highly attractive to third parties. Genetic
11 data is unique in the value it represents to both a victim of a data breach and the hacker
12 obtaining the data because, “[o]nce digital genetic data is stolen or disclosed, it cannot be
13 reissued or changed in the same manner as other information types. A single human whole
14 genome sequence can cost hundreds to thousands of dollars per sample, and when amassed,
15 genetic information of large cohorts can be worth millions of dollars. This positions human
16 genetic information systems as likely targets for cyber and physical attacks. . . .”¹⁵

17 88. The National Counterintelligence and Security Center has warned consumers
18 about the risks posed by the disclosure of genetic information, advising, “your DNA is the most
19 valuable thing you own. It holds the most intimate details of your past, present, and potential
20 future—whether you are prone to addiction or high-risk for cancer.”¹⁶

21 89. In addition to risks posed to individual customers, researchers have noted that
22

23 ¹⁴ *In the Dark*, VPN OVERVIEW, [https://vpnoverview.com/privacy/anonymous-browsing/in-](https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/)
24 [the-dark/](https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/) (last visited Jan. 15, 2024).

25 ¹⁵ Garrett Schumacher, et al., *Genetic Information Insecurity as State of the Art*, 8 FRONTIERS
26 IN BIOENGINEERING AND BIOTECHNOLOGY 591980 (Dec. 8, 2020),
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7768984/#:~:text=Once%20digital%20genetic%20data%20is,dollars1%20%2C2%20%2C3>.

27 ¹⁶ Nat’l Counterintel. and Sec. Ctr., *China’s Collection of Genomic and Other Healthcare*
28 *Data from America: Risks to Privacy and U.S. Economic and National Security*, Dir. of Nat’l
Intel. (Feb. 2021),
https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf.

1 one person’s genetic information has implications for his or her family members and that the
2 misuse of genetic information could have intergenerational effects that are far broader than any
3 individual incident of unauthorized use.¹⁷ In their words, “[s]ince genomic data contains
4 information about a family; the impact of a breach of such data also affects the person’s close
5 and distant biological relatives, making it more significant as compared to attributes such as
6 name, date of birth, and address of an individual.”

7 90. The unauthorized use of genetic information can have devastating consequences
8 for victims. It can be used to discriminate against, blackmail, and target victims based on
9 characteristics such as ethnicity, race, or genetic predispositions.

10 **VII. Facts Relating to Plaintiffs Melvin and J.L.**

11 91. Plaintiff Melvin purchased a 23andMe DNA kit in or around 2010 for \$400 and
12 provided a sample of his genetic material to 23andMe for testing. At all relevant times, Plaintiff
13 Melvin’s PGI was stored and maintained on 23andMe’s computer systems.

14 92. 23andMe notified Plaintiff Melvin in December 2023 that a threat actor
15 compromised his account and accessed his PGI. Plaintiff Melvin was never told that his PGI
16 was leaked on the dark web.

17 93. Plaintiff J.L. purchased a 23andMe DNA kit in or around 2021 and provided a
18 sample of his genetic material to 23andMe for testing. Through this testing, Plaintiff J.L.
19 learned that he has Ashkenazi Jewish ancestry. At all relevant times, Plaintiff J.L.’s PGI was
20 stored and maintained on 23andMe’s computer systems.

21 94. 23andMe notified Plaintiff J.L. in December 2023 that a threat actor
22 compromised his account and accessed his PGI. Plaintiff J.L. was never told that his PGI was
23 leaked on the dark web or that a hacker compiled and leaked lists of Ashkenazi Jewish
24 customers on the dark web.

25 95. Plaintiff J.L. is now gravely concerned about the ramifications of appearing on a

26
27 ¹⁷ Saadia Arshad, et al., *Analysis of Security and Privacy Challenges for DNA-Genomics*
28 *Applications and Databases*, 119 J. OF BIOMEDICAL INFORMATICS 103815 (July 2021),
<https://www.sciencedirect.com/science/article/pii/S1532046421001441#:~:text=Since%20geno mic%20data%20contains%20information,and%20address%20of%20an%20individual.>

1 list that is potentially being sold to terrorists on the dark web. He is also gravely concerned that
2 he will become the target of harassment, intimidation, vandalism, assault, and discrimination.

3 **CLASS ALLEGATIONS**

4 96. Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and
5 (b)(3) of the Federal Rules of Civil Procedure on behalf of themselves and the following
6 Classes:

7 **Nationwide Class**: All individuals in the United States whose PGI was accessed
8 by third parties, without consent, as a result of the data breach announced by
9 23andMe on October 6, 2023.

10 **Vulnerable Persons Subclass**: All individuals in the Nationwide Class who are
11 identified by their PGI as having Ashkenazi Jewish heritage or Chinese ancestry.¹⁸

12 **State Genetic Privacy Statute Subclass**: All individuals in the Nationwide Class
13 who reside in Illinois, Oregon, or Alaska.

14 97. Excluded from the Classes are the following individuals and/or entities:
15 23andMe and 23andMe's parents, subsidiaries, affiliates, officers, and directors and any entity
16 in which Defendant has a controlling interest, all individuals who make a timely election to be
17 excluded from this proceeding using the correct protocol for opting out, any and all federal,
18 state or local governments, including but not limited to its departments, agencies, divisions,
19 bureaus, boards, sections, groups, counsel, and/or subdivisions, and all judges assigned to hear
20 any aspect of this litigation, as well as their immediate family members.

21 98. Plaintiffs reserve the right to amend the above class definitions or to propose
22 other subclasses in subsequent pleadings and motions for class certification.

23 99. This action has been brought and may properly be maintained as a class action
24 under Fed. R. Civ. P. 23 because there is a well-defined community of interest in the litigation
25 and membership of the proposed Classes is readily ascertainable.

26 100. **Numerosity**: A class action is the only available method for the fair and efficient
27 adjudication of this controversy. The members of the Class are so numerous that joinder of all
28 members is impractical, if not impossible. Defendant has publicly announced that millions of

¹⁸ Plaintiff J.L. reserves the right to expand this definition to include any additional ethnic, racial, or otherwise vulnerable populations that were specifically targeted through the breach.

1 accounts were affected by the breach. Membership in the Class will be determined by analysis
2 of 23andMe's records and/or through the records made publicly available by the bad actor(s).

3 101. Commonality: Plaintiffs and Class Members share a community of interest in
4 that there are numerous common questions and issues of fact and law which predominate over
5 any questions and issues solely affecting individual members, including, but not limited to:

6 (a) Whether 23andMe had a legal duty to Plaintiffs and the Class to exercise
7 reasonable care in collecting, storing, using and/or safeguarding their PGI;

8 (b) Whether 23andMe breached that duty when it failed to take adequate
9 and reasonable measures to ensure its data systems were protected;

10 (c) Whether 23andMe's conduct, including its failure to act, resulted in or
11 was the proximate cause of the breach of its systems, resulting in the
12 disclosure of Plaintiffs and Class Members' PGI;

13 (d) Whether 23andMe engaged in unfair, unlawful, or deceptive practices
14 by failing to safeguard Plaintiffs and Class Members' PGI;

15 (e) Whether 23andMe obtained written authorization from Plaintiffs and
16 the Class before disclosing their PGI;

17 (f) Whether, with respect to the State Genetic Privacy Statute Subclass,
18 Defendant's conduct violates the Illinois Genetic Privacy Act, Alaska
19 Genetic Privacy Act, and Oregon Genetic Privacy Statutes;

20 (g) Whether Plaintiff Melvin and the State Genetic Privacy Statute Subclass
21 are entitled to actual and/or statutory damages as a result of 23andMe's
22 wrongful conduct; and

23 (h) Whether Plaintiffs and Class Members are entitled to injunctive and
24 declaratory relief.

25 102. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and
26 all Class Members sustained damages arising out of and caused by 23andMe's common course
27 of conduct in violation of law, as alleged herein.

28

1 103. Adequacy of Representation: Plaintiffs are adequate representatives of the
2 Classes in that Plaintiffs have the same interest in the litigation of this case as the Class
3 Members, are committed to the vigorous prosecution of this case, and have retained competent
4 counsel who are experienced in conducting litigation of this nature. Plaintiffs are not subject to
5 any individual defenses unique from those conceivably applicable to other Class Members or
6 the Classes in their entirety. Plaintiffs anticipate no difficulties managing this litigation.

7 104. Predominance and Superiority: The Classes can be properly maintained because
8 the above common questions of law and fact predominate over any questions affecting
9 individual Class Members. A class action is also superior to other available methods for the fair
10 and efficient adjudication of this litigation because individual litigation of each Class
11 Member's claim is impracticable. Even if each Class Member could afford individual litigation,
12 the court system could not. It would be unduly burdensome if thousands of individual cases
13 proceed. Individual litigation also presents the potential for inconsistent or contradictory
14 judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of
15 recovery among those with equally meritorious claims. Individual litigation would increase the
16 expense and delay to all parties and the courts because it requires individual resolution of
17 common legal and factual questions. By contrast, the class-action device presents far fewer
18 management difficulties and provides the benefit of a single adjudication, economies of scale,
19 and comprehensive supervision by a single court.

20 105. Declaratory and Injunctive Relief: The prosecution of separate actions by
21 individual Class Members would create a risk of inconsistent or varying adjudications with
22 respect to individual Class Members that would establish incompatible standards of conduct for
23 Defendant. Such individual actions would create a risk of adjudications that would be
24 dispositive of the interests of other Class Members and impair their own interests. Defendant
25 has acted and/or refused to act on grounds generally applicable to the Classes, making final
26 injunctive relief or corresponding declaratory relief appropriate.

FIRST CAUSE OF ACTION

Negligence

(On Behalf of Plaintiffs, the Nationwide Class, and Vulnerable Persons Subclass)

106. Plaintiffs incorporate the foregoing allegations as if fully set forth herein. Plaintiffs bring this claim on behalf of themselves, the Nationwide Class, and the Vulnerable Persons Subclass.

107. Defendant requires its customers, including Plaintiffs and the Class Members, to submit confidential PGI and personally identifiable information as a condition of receiving services, and, in return, 23andMe had a duty to safeguard their information.

108. Defendant had a duty to exercise reasonable care in protecting such information from being compromised or disclosed to unauthorized parties, including by:

(a) Designing, maintaining, and testing security protocols to ensure PGI in its possession was adequately secured and protected against common and foreseeable cyber threats;

(b) Using reasonable and adequate security procedures and systems that were/are compliant with industry-standard and best practices to timely act on warnings about data breaches; and

(c) Promptly notifying Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PGI.

109. Defendant had full knowledge of the sensitivity of the PGI it stored and the types of harm that Plaintiffs and Class Members could and would suffer if their PGI was wrongfully disclosed. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures.

110. Defendant has admitted that Plaintiffs' and Class Members' PGI was wrongfully disclosed to unauthorized third persons as a result of the data breach.

111. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate data security practices to protect their PGI in ways including but not limited to:

(a) Failing to provide reasonable computer systems and data security

1 practices to safeguard the PGI of Plaintiffs and Class Members, including,
2 but not limited to, the failure to require two-step verification, a known
3 preventative against a credential-stuffing attack, the failure to utilize
4 adequate tools and monitoring systems to flag suspicious transactions and
5 data being exfiltrated in large volumes, and the failure to timely monitor
6 and/or act upon online discussions of a data breach;

7 (b) Failing to detect in a timely manner that Plaintiffs' and Class Members'
8 PGI and personally identifiable information had been compromised and
9 allowing unmonitored and unrestricted access to unsecured PGI;

10 (c) Failing to timely and accurately disclose that Plaintiffs' and Class
11 Members' PGI had been improperly acquired or accessed including
12 significant details about the disclosure such as the number of impacted users
13 and the importance of the threat to users' PGI; and

14 (d) Failing to timely institute security measures after the breach that could
15 have mitigated harm and further disclosure, including the disabling of the
16 DNA Relatives feature and immediately requiring two-step verification.

17 112. Defendant's willful failure to abide by these duties was wrongful, reckless, and
18 grossly negligent in light of the foreseeable risks and known threats.

19 113. If Plaintiffs and the Class Members had known that Defendant failed to comply
20 with its own security statements, industry best practices, and reasonable security standards,
21 they would not have purchased or chosen to entrust the Defendant with highly confidential
22 information such as their PGI or would have paid significantly less.

23 114. Further, as a proximate and foreseeable result of Defendant's conduct, Plaintiffs
24 and Class Members have suffered damages and are at imminent, and even permanent, risk of
25 additional harms and damages.

26 115. But for Defendant's failure to implement security measures to protect the PGI
27 and personally identifiable information of Plaintiffs and Class Members and its negligent
28 breach of duties owed to Plaintiff and Class Members, the PGI of Plaintiffs and the Class

1 would not have been compromised and/or subsequently misused by unauthorized third parties
2 thereby harming Plaintiffs and Class Members.

3 116. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class
4 Members have suffered and will suffer injury, including:

5 (a) overpayment of monies, in that Plaintiffs and the Class members would
6 have paid Defendant significantly less, or nothing at all, had they known
7 about Defendant's failure to comply with its own security statements,
8 industry best practices, and reasonable security standards;

9 (b) increased risk of identity theft, fraud, or misuse of their PGI;

10 (c) the loss of the opportunity to dictate how their PGI is used;

11 (d) the compromise, disclosure, and/or theft of their PGI;

12 (e) diminished value of their PGI; and

13 (f) the continued and permanent risk to their PGI.

14 117. Further, Plaintiff J.L. and the Vulnerable Persons Subclass have suffered
15 additional harm in that they are now subjected to the increased threat of harassment,
16 intimidation, vandalism, assault, and discrimination, including in the workplace.

17 118. Plaintiffs and Class Members are entitled to compensatory and consequential
18 damages suffered as a result of the breach, as well as injunctive relief requiring Defendant to:
19 (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual
20 audits of those systems and monitoring procedures; and (iii) provide notice to all impacted
21 customers of the actual scope and severity of the breach and inform them that their PGI has
22 been leaked on the dark web, and with respect to the Vulnerable Persons Subclass members,
23 inform them that they have been specifically targeted by the hacker.

24 **SECOND CAUSE OF ACTION**
25 **Threat Assessment and Monitoring**
(On Behalf of Plaintiff J.L. and the Vulnerable Persons Subclass)

26 119. Plaintiff J.L. incorporates the foregoing allegations as if fully set forth herein.
27 Plaintiff J.L. brings this claim on behalf of himself and the Vulnerable Persons Subclass.

28 120. As a leading company in the genetic testing industry, 23andMe is well aware of

1 the immense value of genetic data and recognizes that such information is a prime target for
2 cybercriminals. 23andMe also knows that people would not purchase its genetic testing kits or
3 provide their genetic information unless they were assured that the company has implemented
4 robust cybersecurity measures to protect their data against the persistent threat of hacking.

5 121. For that reason, as described above, 23andMe has made numerous and explicit
6 promises to assure its customers that their genetic information would be properly safeguarded
7 on its systems and protected using data protection measures that “exceed” industry standards.
8 Even its October 6 Announcement about the breach was designed to reassure customers that
9 their data was perfectly safe, reiterating that “At 23andMe, we take security seriously. We
10 exceed industry data protection standards and have achieved three different ISO certifications
11 to demonstrate the strength of our security program.”

12 122. But for 23andMe’s promises and assurance, Plaintiff J.L. and the Vulnerable
13 Persons Subclass would not have purchased its genetic testing kits and would not have
14 provided it with their genetic information.

15 123. As described above, the breach revealed for the first time that 23andMe did not
16 implement basic, industry-standard data security measures, let alone security measures that
17 “exceed” industry standards. As a result, 23andMe’s Jewish and Chinese customers were
18 specifically targeted by a hacker that posted their genetic information—along with their full
19 names, home addresses, photographs, and birth dates—on the dark web hacker forum, Breach
20 Forums. The data generated immediate interest by users around the world, and was
21 downloaded and shared an untold number of times.

22 124. There can be no question as to whether the data was, in fact, downloaded by
23 other Breach Forum users. As shown in Figures 3 and 4, above, Golem included a message
24 beneath each of the Jewish and Chinese list download links that stated, “After 10 downloads
25 the link is automatically deleted. Those who download the file can share the link by uploading
26 it again.” The links were deleted within an hour, meaning that the Jewish and Chinese lists
27 were quickly downloaded 10 times by other Breach Forum users. The download links were
28 then reposted on Breach Forums (and very likely elsewhere on the dark web) an untold number

1 of times thereafter.

2 125. The breach and subsequent disclosure of the Jewish and Chinese lists on the dark
3 web have exposed Plaintiff J.L. and the Vulnerable Persons Subclass to ongoing and severe
4 threats to their personal safety.

5 126. The individuals that downloaded the stolen Jewish and Chinese lists on the dark
6 web can exploit them for a variety of nefarious and dangerous purposes, including to single out
7 individuals or groups for hate crimes or other forms of harassment, intimidation, violence, and
8 discrimination, both online and in real life.

9 127. The current geopolitical and social climate amplifies the risks to 23andMe's
10 Jewish and Chinese customers. The recent Israel-Hamas war has heightened global tensions
11 and anti-Semitic sentiment, and increased the vulnerability of Jewish communities to targeted
12 violence and discrimination. Likewise, the Chinese government's sophisticated surveillance
13 and intimidation apparatus presents a significant threat to Chinese customers on the list, who
14 may face persecution or coercion in China and abroad. In this environment, the exposure of the
15 Jewish and Chinese lists dramatically escalates the danger of being identified and located by
16 those with hostile intentions. The geopolitical and social climate is only getting worse and
17 underscores the urgent need to provide vigilant monitoring and protective measures for
18 Plaintiff J.L. and the Vulnerable Persons Subclass.

19 128. Given the magnitude of these threats, the creation of a Threat Assessment and
20 Monitoring Fund ("TAM Fund") is necessary to ensure the ongoing safety and well-being of
21 Plaintiff J.L. and the Vulnerable Persons Subclass by providing the necessary funds to pay for
22 technical and professional services, including:

23 (a) Dark Web Surveillance. Employ advanced cybersecurity services to
24 conduct deep and dark web scans for any sharing of Vulnerable Persons
25 Subclass members' personal and genetic information. This includes the use
26 of specialized software to infiltrate and monitor darknet markets and forums
27 where such information may be exchanged.

28 (b) Threat Intelligence and Protection Operations. Partner with personal

1 protection firm(s) and cybersecurity to collect, analyze, and operationalize
2 in real-time threat intelligence related to the leaked data, enabling proactive
3 identification of potential threats before they materialize and taking
4 immediate action on threats of physical or other harm including by
5 coordinating with relevant law enforcement authorities and dispatching
6 personal protection personnel.

7 (c) Digital Footprint Analysis. Implement digital footprint analysis tools to
8 track the digital shadows of the Vulnerable Persons Subclass members'
9 personal information, alerting them to any unauthorized appearances on the
10 internet.

11 (d) Security Advisory Services. Provide access to security consultants who
12 can advise the Vulnerable Persons Subclass members on physical
13 safeguards and operational security, protecting their digital identity, and
14 responding to threats.

15 (e) Legal and Remediation Services. Fund professional services, including
16 legal counsel, to advise on and take action against illicit use of the data,
17 including through peace and/or restraining orders, cease and desist actions,
18 and takedown demands.

19 (f) Public Records Sweeping. Utilize services that scan public records and
20 request removal of any sensitive personal information linked to class
21 members that should not be publicly available.

22 (g) Incident Response Team. Establish a rapid response team that can be
23 deployed to assist Vulnerable Persons Subclass members in the event of an
24 immediate threat, providing physical protection and technical and legal
25 assistance.

26 129. These measures are designed to provide comprehensive protection and support
27 to the Vulnerable Persons Subclass, monitor for and mitigate the ongoing risks they face, and
28 restore confidence in their personal security and privacy following the breach.

1 130. Accordingly, Plaintiff J.L. respectfully seeks an order from the Court requiring
 2 23andMe to establish a TAM Fund for the benefit of the Vulnerable Persons Subclass that is
 3 sufficiently funded to provide the services described above for a period of twenty (20) years
 4 from the establishment date, which is a reasonable period of time given the enduring nature of
 5 the threats described herein.

6 **THIRD CAUSE OF ACTION**
 7 **Violation of Cal. Bus. & Prof. Code § 17200, *et seq.***
 8 **(On Behalf of Plaintiffs, the Nationwide Class, and the Vulnerable Persons Subclass)**

9 131. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.
 Plaintiffs bring this claim on behalf of themselves, the Nationwide Class, and the Vulnerable
 10 Persons Subclass.

11 132. The California Unfair Competition Law, Cal. Bus. & Prof Code § 17200 *et seq.*
 12 (“UCL”), prohibits any “unlawful,” “fraudulent,” or “unfair” business act or practice and any
 13 false or misleading advertising, as defined by the UCL and relevant case law.

14 133. Defendant 23andMe, Inc. and Plaintiffs are “persons” under Cal. Bus. & Prof.
 15 Code § 17201.

16 134. By reason of Defendant’s failure to take reasonable precautions to protect the
 17 PGI of Plaintiffs and the Class Members, the resulting data breach, and the unauthorized
 18 disclosure of Plaintiffs’ and Class Members’ PGI, Defendant engaged in unlawful, unfair, and
 19 fraudulent practices within the meaning of the UCL.

20 135. Defendant engaged in “unlawful” acts and practices with respect to its services
 21 by failing to establish proper security practices and procedures described herein; by soliciting
 22 and collecting Plaintiffs and Class Members’ PGI with knowledge that the information would
 23 not be adequately protected; and by storing Plaintiffs’ and Class Members’ PGI in an unsecure
 24 electronic environment in violation of FTC guidance and industry norms, which require
 25 Defendant to use reasonable methods of safeguarding the PGI of Plaintiffs and Class Members.

26 136. Defendant’s business practices as alleged herein are “unfair” because they
 27 offend established public policy and are immoral, unethical, oppressive, unscrupulous, and
 28 substantially injurious to consumers in that the PGI and personally identifiable information of

1 Plaintiffs and Class Members has been compromised for unauthorized parties to see, use, and
2 otherwise exploit. These actions include, but are not limited to:

3 (a) Defendant failed to implement and maintain reasonable data security
4 measures to protect the Plaintiffs' and Class Members' PGI;

5 (b) Defendant failed to identify foreseeable security risks, remediate
6 identified risks, and adequately improve its data security in light of the
7 highly sensitive nature of the data it maintained;

8 (c) To the extent Defendant may have identified a threat from duplicated
9 account credentials, or external discussions of a breach, it did not implement
10 timely and reasonable security measures; and

11 (d) Defendant's grievous conduct is unfair when weighed against the harm
12 to the Plaintiffs and Class Members whose PGI have been compromised.

13 137. Defendant's failure to implement and maintain reasonable data security
14 measures was contrary to state law—including specifically the California Genetic Privacy Act,
15 Cal. Civ. Code § 56.18 *et seq.*— and public policy that seeks to protect consumers' personally
16 identifiable information and ensure that entities entrusted with PGI adopt appropriate security
17 measures.

18 138. Pursuant to Cal. Civ. Code § 56.181(d)(1), a direct-to-consumer genetic testing
19 company, such as 23andMe, is required to "implement and maintain reasonable security
20 procedures and practices to protect a consumer's genetic data against unauthorized access,
21 destruction, use, modification, or disclosure."

22 139. Failure to comply with Cal. Civ. Code § 56.18 *et seq.* constitutes an unlawful
23 practice under the UCL.

24 140. Defendant's failure to implement and maintain reasonable data security
25 measures led to substantial consumer injuries as described herein, which are not outweighed by
26 countervailing benefits to consumers or competition.

27 141. Defendant's business practices as alleged herein are "fraudulent" because:

28 (a) Defendant represented to consumers that the PGI they provided to

1 Defendant would remain private and secure, when in fact it has not been
2 maintained in a private and secure manner and Defendant failed take proper
3 measures to identify, investigate, and remediate a data breach;

4 (b) Defendant could and should have made a proper disclosure related to
5 the DNA Relations feature directly to consumers to inform them of the
6 potential for significant unauthorized disclosures through the feature;

7 (c) Defendant knew or should have known that its data security practices
8 were deficient because, among other things, Defendant was aware of the
9 sensitive nature of the information it held; and

10 (d) Defendant made express representations that its data security practices
11 were sufficient to protect consumers' PGI including but not limited to, that
12 they "exceed industry data protection standards," they "regularly conduct
13 audits and assessment of [their] systems," and that "personally identifiable
14 information . . . is stored in a separate database." These representations were
15 false and misleading.

16 142. Plaintiffs and Class Members suffered injuries in the form of overpayment of
17 monies, in that they would have paid Defendant significantly less, or nothing at all, had they
18 known about Defendant's failure to comply with state law, its own security statements,
19 industry best practices, and reasonable security standards.

20 143. Plaintiffs and Class Members also suffered (and continue to suffer) injury and
21 lost money or property as a direct and proximate result of Defendant's above-described
22 wrongful actions, inaction, and omissions, including, *inter alia*, the disclosure of their PGI and
23 lack of notice of that disclosure.

24 144. But for Defendant's misrepresentations and omissions, Plaintiffs and Class
25 Members would not have provided their PGI to Defendant or would have insisted that their
26 data be more securely protected.

27 145. As a direct and proximate result of Defendant's unlawful practices and acts,
28 Plaintiffs and Class Members were injured and lost money or property, including but not

1 limited to the price received by Defendant for the services, the loss of Plaintiffs' and Class
2 Members' legally protected interest in the confidentiality and privacy of their PGI, nominal
3 damages, and additional losses as described herein.

4 146. Defendant knew or should have known that Defendant's computer systems and
5 data security practices were inadequate to safeguard Plaintiffs' and Class Members' PGI and
6 that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the
7 above-named unlawful practices and acts was negligent, knowing, and willful, and/or wanton
8 and reckless with respect to the rights of Plaintiffs and Class Members.

9 147. Plaintiffs and Class Members lack an adequate remedy at law because the
10 injuries here include an imminent risk of identity theft and fraud that can never be fully
11 remedied through damages, as well as long term incalculable risk associated with medical fraud
12 and release of genetic profiles.

13 148. Further, Plaintiff J.L. and the Vulnerable Persons Subclass have suffered
14 additional harm in that they are now subjected to the increased threat of harassment, vandalism,
15 assault, and discrimination, including in the workplace.

16 149. Plaintiffs, on behalf of themselves, the Nationwide Class, and the Vulnerable
17 Persons Subclass, seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not
18 limited to, restitution to Plaintiffs and Class Members of money or property that Defendant
19 may have acquired by means of Defendant's unlawful and unfair business practices, including
20 the purchase price of the testing kits, disgorgement of all profits accruing to Defendant because
21 of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and
22 costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

23 150. Plaintiffs also seek injunctive relief requiring Defendant to: (i) strengthen its
24 data security systems and monitoring procedures; (ii) submit to future annual audits of those
25 systems and monitoring procedures; and (iii) provide notice to all impacted customers of the
26 actual scope and severity of the breach and inform them that their PGI has been leaked on the
27 dark web, and with respect to the Vulnerable Persons Subclass members, inform them that they
28 have been specifically targeted by the hacker.

FOURTH CAUSE OF ACTION

**Violation of the Illinois, Alaska, and Oregon Privacy Statutes
(On Behalf of Plaintiff Melvin and the State Genetic Privacy Statute Subclass)**

151. Plaintiff Melvin incorporates the foregoing allegations as if fully set forth herein. Plaintiff Melvin brings this claim on behalf of himself and the State Genetic Privacy Statute Subclass, as the genetic privacy statutes in Illinois, Alaska, and Oregon are substantially similar in that all three (i) contain private rights of action, (ii) broadly cover genetic information and information derived from genetic information, and (iii) provide for statutory damages.

152. In enacting the Genetic Information Privacy Act (“GIPA”), the Illinois Legislature recognized that “[t]he public health will be served by facilitating voluntary and confidential nondiscriminatory use of genetic testing information.” 410 ILCS 513/5(3); *see also* Alaska Stat. § 18.13.010, *et seq.*; Or. Rev. Stat. § 192.533.

153. GIPA mandates that no person may disclose the identity of any person upon whom a genetic test is performed or the results of a genetic test in a manner that permits identification of the subject of the test. *See* 410 ILCS 513/30(a); Alaska Stat. § 18.13.010; Or. Rev. Stat. §§ 192.537, 192.539.

154. Defendant is a corporation and, thus, a “person” under 410 ILCS 513/10; *see also* Alaska Stat. § 18.13.020; Or. Rev. Stat. § 192.531.

155. Plaintiff Melvin and the State Genetic Privacy Statute Subclass members provided their genetic information to Defendant and therefore provided Defendant with “genetic test[s]” and/or the “information derived from genetic testing” within the meaning of the GIPA. *See also* Alaska Stat. § 18.13.100; Or. Rev. Stat. § 192.531.

156. As explained above, Defendant disclosed Plaintiff Melvin’s and the State Genetic Privacy Statute Subclass members’ genetic testing and information derived from genetic testing by failing to enact or enforce adequate data security measures and policies, resulting in the data breach. *See* 410 ILCS 513/30; Alaska Stat. § 18.13.010; Or. Rev. Stat. § 192.537.

157. Defendant disclosed Plaintiff Melvin’s and the State Genetic Privacy Statute Subclass members identifying information to unknown third parties by allowing them to access

1 their genetic information and genetic tests, in addition to personally identifying information.

2 158. GIPA plainly prohibits such disclosures because they contain, among other
3 things, the results of Plaintiff Melvin’s and the State Genetic Privacy Statute Subclass’ genetic
4 tests, including in a manner that permits identification of the subject of the test. *See* 410 ILCS
5 513/15 and 30; Alaska Stat. § 18.13.010; Or. Rev. Stat. §§ 192.537, 192.539.

6 159. Defendant did not obtain any authorization—including written authorization—
7 from Plaintiff Melvin or the State Genetic Privacy Statute Subclass members before disclosing
8 their genetic test results and information derived from genetic testing, as mandated by 410
9 ILCS 513/30(a)(2); Alaska Stat. § 18.13.010; Or. Rev. Stat. §§ 192.537, 192.539.

10 160. By disclosing the results of their genetic tests and information sufficient to
11 identify Plaintiff Melvin and the State Genetic Privacy Statute Subclass members as described
12 herein, Defendant violated Plaintiff Melvin’s and the State Genetic Privacy Statute Subclass’s
13 statutorily protected rights to privacy in their genetic information under their respective state’s
14 genetic privacy statutes.

15 161. On behalf of himself and the State Genetic Privacy Statute Subclass, Plaintiff
16 Melvin seeks: (1) injunctive and equitable relief as is necessary to protect the interests of
17 himself and the State Genetic Privacy Statute Subclass members by requiring Defendant
18 comply with the state genetic privacy statutes at issue; (2) liquidated damages or actual
19 damages, whichever is greater, as provided by the state genetic privacy statutes at issue; and (3)
20 costs and reasonable attorneys’ fees pursuant to the state genetic privacy statutes at issue. 410
21 ILCS 513/40(a)(3); Alaska Stat. § 18.13.020; Or. Rev. Stat. § 192.541.

22 **FIFTH CAUSE OF ACTION**
23 **Declaratory Judgment**
(On Behalf of Plaintiffs and the Nationwide Class)

24 162. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.
25 Plaintiffs brings this claim on behalf of themselves and the Nationwide Class.

26 163. Under the Declaratory Judgment Act, “any court of the United States, upon the
27 filing of an appropriate pleading, may declare the rights and other legal relations of any
28 interested party seeking such declaration, whether or not further relief is or could be sought.”

1 28 U.S.C. § 2201(a). This count is brought under the federal Declaratory Judgment Act, 28
2 U.S.C. §§ 2201, *et seq.*, which authorizes the Court to enter a judgment declaring the rights and
3 legal relations of the parties and grant further necessary relief. The Court has broad authority to
4 restrain acts, such as here, that are tortious and violate the state statutes described herein.

5 164. An actual controversy has arisen in the wake of the data breach.¹⁹ Defendant has
6 attempted to block Plaintiffs' access to justice and redress through surprise and unfair
7 arbitration provisions that it added to its Terms of Service ("TOS") on November 30, 2023.
8 Defendant delayed sending notice to impacted customers for two months so that it could first
9 update its TOS to insulate itself from the fallout.

10 165. Defendant continues to possess the genetic information of Plaintiffs and Class
11 Members who remain subject to the TOS.

12 166. Defendant's material changes to the arbitration provisions in its TOS are
13 designed to intentionally constrain Plaintiffs' and the Class's legal rights. Defendant inserted
14 new language, TOS § 5(a) which prohibits Plaintiffs from initiating any arbitration or court
15 proceeding for at least sixty days after delivery of a "valid" notice of dispute. The provision
16 includes "condition precedent[s]" prohibiting Plaintiffs from initiating a lawsuit or arbitration
17 unless notices include specific information outlined by Defendant and mandates a conference
18 during the "Initial Dispute Resolution Period." This requires that Plaintiffs "personally appear
19 at the conference," and "participate" regardless of whether they are represented by counsel.

20 167. Such language imposes new and significant hurdles for Plaintiffs to exercise
21 their legal rights and to seek redress for the unauthorized disclosures of their highly sensitive
22 genetic information.

23 168. Defendant's new November 2023 arbitration language also materially changes
24 the TOS to unfairly impact Plaintiffs' choice of counsel by imposing a two-tiered set of
25 arbitration procedures for Plaintiffs. Pursuant to TOS § 5(c), arbitrations are administered by

26 _____
27 ¹⁹ Though 23andMe's counsel has indicated that the company does not intend to enforce the
28 arbitration clause, he has yet to respond to the undersigned's request for a formal stipulation to
that effect. To the extent a formal stipulation is provided, Plaintiffs will voluntarily dismiss this
claim.

1 JAMS, unless they are subject to an exemption for “Mass Arbitration” defined as “25 more
2 demands for arbitration . . . relating to the same or similar subject matter and sharing common
3 issues of law or fact, and counsel for the parties submitting the demands are the same or
4 coordinated.” TOS § 5(c)(v). Unlike singular arbitrations, Mass Arbitrations are administered
5 by NAM and are subject to the appointment and sole discretion of a “Procedural Arbitrator”
6 with broad authority to “rule on proposals by the parties for the efficient and cost-effective
7 management of the Mass Arbitration to the extent the parties cannot agree.” TOS § 5(c)(v)(1).
8 Such authority is not clearly defined in either Defendant’s arbitration clause nor the relevant
9 NAM rules and should be considered vague and standardless.

10 169. These terms will have an immediate impact on Defendant’s customers’ ability to
11 obtain representation as plaintiffs’ counsel will be deterred from representing more than the
12 twenty-five-client threshold while the Defendant retains all advantages of a repeat-player—
13 including the retention of the same law firm—in any dispute.

14 170. The surprise amendments to the TOS also deny Plaintiffs arbitrator selection
15 rights articulated by California state law. *See* Cal. Civ. Proc. Code §§ 1281.9, 1281.91(b).
16 NAM rules incorporated by the Defendant’s language, allow for NAM to decide in Mass
17 Arbitration, among other things, whether a challenged arbitrator is removed, the admissibility
18 and the merits of a challenge, and for the appointment of the same arbitrator to multiple
19 matters. *See* NAM Rule 23; NAM Mass Filing Rule 8. Such provisions run counter to statutory
20 and unwaivable arbitrator selection rights under state law.

21 171. Defendant’s amended arbitration clause further imposes a one-year contractual
22 limitations period under TOS § 5(f) stating, “you agree that regardless of any statute or law to
23 the contrary, any claim or cause of action arising out of or related to use of the Services or the
24 Terms must be filed within one (1) year after such claim or cause of action arose or be forever
25 barred.” This provision unfairly imposes a period of limitations that is shorter than otherwise
26 available under state law, including claims for negligence and unfair business practices
27 pursuant to Cal. Bus. & Prof. Code § 17208.

28 172. Actual harm has arisen in the wake of the data breach and the unlawful

1 disclosure of Plaintiffs' genetic information. Since the data breach, Defendant has failed to
2 provide sufficient details related to its scope and severity and to inform customers as to
3 whether vulnerabilities in its systems, protocols, and practices have been remedied to prevent
4 further exposure. As such, Defendant seeks to limit Plaintiffs' and Class Members' access to
5 justice while they remain at imminent risk of continued exposure of their genetic information.

6 173. Pursuant to its authority under the Declaratory Judgment Act, this Court should
7 enter a judgment, declaring, among other things, that:

8 (a) 23andMe continues to owe a legal duty and contractual obligations to
9 Plaintiffs and Class Members; and

10 (b) The provisions in 23andMe's modified arbitration agreement, including
11 the mandates for individual participation in dispute resolution proceedings,
12 vague and standardless Mass Arbitration procedures, denials of arbitration
13 selection rights protected by state law, and unreasonably time-constrained
14 limitations periods are unconscionable, invalid, and unenforceable.

15 **PRAYER FOR RELIEF**

16 **WHEREFORE**, Plaintiffs Melvin and J.L., individually and on behalf of the
17 Nationwide Class, the Vulnerable Persons Subclass, and the State Genetic Privacy Statute
18 Subclass, respectfully request that this Court enter an Order:

19 (a) Certifying the Classes as defined above, appointing Plaintiffs Melvin
20 and J.L. as the representatives of the Classes, and appointing their counsel
21 as Class Counsel;

22 (b) Awarding injunctive relief requiring Defendant to take appropriate
23 measures to strengthen the data security systems that maintain PGI and to
24 prohibit Defendant from continuing to engage in the unlawful acts,
25 omissions and practices described herein;

26 (c) Requiring Defendant to pay all costs associated with class notice and
27 administration of class-wide relief;

28 (d) Awarding to Plaintiffs and all Class Members actual, compensatory,

1 consequential, incidental, nominal, and statutory damages, punitive
2 damages, restitution and disgorgement in an amount to be determined at
3 trial;

4 (e) Awarding injunctive relief requiring Defendant to: (i) strengthen its data
5 security systems and monitoring procedures; (ii) submit to future annual
6 audits of those systems and monitoring procedures; and (iii) provide notice
7 to all impacted customers of the actual scope and severity of the breach, and
8 informing them that their PGI has been leaked on the dark web, and with
9 respect to the Vulnerable Persons Subclass members, informing them that
10 they have been specifically targeted by the hacker;

11 (f) Establishing a TAM Fund for the benefit of the Vulnerable Persons
12 Subclass that is sufficiently funded to provide the services described above
13 for a period of twenty (20) years from the establishment date;

14 (g) Declaring on behalf of the State Genetic Privacy Statute Subclass that
15 Defendant's conduct described herein violates the genetic privacy statutes
16 identified herein;

17 (h) Declaring that Defendant's November 30, 2023 modifications to the
18 TOS are void and unenforceable;

19 (i) Awarding the State Genetic Privacy Statute Subclass statutory damages
20 as provided by each statute;

21 (j) Requiring Defendant to pay pre-judgment and post-judgment interest,
22 as provided by law;

23 (k) Enjoining Defendant from further deceptive and unfair practices and
24 making untrue statements with respect to the data breach and stolen PGI;

25 (l) Awarding equitable relief requiring restitution and disgorgement of the
26 revenues wrongfully retained as a result of Defendant's wrongful conduct;

27 (m) Awarding reasonable attorneys' fees and costs; and

28 (n) Awarding such further relief that the Court deems reasonable and just.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

JURY DEMAND

Plaintiffs request a trial by jury of all claims that can be so tried.

Respectfully Submitted,

DAVID MELVIN and J.L., individually and on behalf of all others similarly situated,

Dated: January 26, 2024

By: /s/ Rafey S. Balabanian
One of Plaintiffs' Attorneys

Rafey S. Balabanian (SBN 315962)
rbalabanian@edelson.com
EDELSON PC
150 California Street, 18th Floor
San Francisco, California 94111
Tel: 415.212.9300
Fax: 415.373.9435

Jay Edelson (*pro hac vice* forthcoming)
jedelson@edelson.com
J. Eli Wade-Scott (*pro hac vice* forthcoming)
ewadescott@edelson.com
Michael Ovca (*pro hac vice* forthcoming)
movca@edelson.com
Emily Penkowski Perez (*pro hac vice* forthcoming)
epenkowski@edelson.com
Hannah P. Hilligoss (*pro hac vice* forthcoming)
hhilligoss@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

Counsel for Plaintiffs and the Putative Classes