ROBERT C. SCHUBERT (rschubert@sjk.law) (SBN 62684)
WILLEM F. JONCKHEER (wjonckheer@sjk.law) (SBN 178748)
AMBER L. SCHUBERT (aschubert@sjk.law) (SBN 278696)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St, Ste 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

POLINA IOFFE, *Plaintiff*, v. 23ANDME, INC., *Defendant*.	No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Polina Ioffe ("Plaintiff"), on behalf of herself and all others similarly situated alleges the following complaint against Defendant 23andMe, Inc. ("23andMe" or "Defendant") upon personal knowledge as to her own acts, and based upon her investigation, her counsel's investigation, and information and belief as to all other matters.

INTRODUCTION

1. Defendant is a biotechnology company which specializes in consumer genetics and research. Defendant is well known for using "genotyping" to identify genetic markers associated with certain traits including, but not limited to, "important health conditions" and "ancestry." Defendant prides itself on pioneering "direct access to genetic information" and has stored genetic profiles for over 14 million customers.[1]

2. On October 6, 2023, Defendant 23andMe, Inc. announced that hackers had breached customer accounts on Defendant's website and accessed customer profile information without the account user's authorization.[2]

3. Compromised accounts not only revealed highly sensitive and personal genetic markers and profile information about the directly compromised account itself to the hackers, but they also obtained private and identifying information from other accounts which shared information through the "DNA Relatives feature."[3] Stolen PII from these victims includes but is not limited to the name of individual account holders, percentage of shared DNA, Ancestry reports, geographic location, family names, profile pictures, birthdays, family tries, and more.[4] Millions of customer profiles have been compromised as a result of the data breach including

[1] https://investors.23andme.com (Last accessed 11/28/2023)
[2] https://blog.23andme.com/articles/addressing-data-security-concerns?utm_medium=search_brand&utm_source=google&gad_source=1&gclid=Cj0KCQiApOyqBhDlARIsAGfnyMqtFWmhFZVc7wmOu0koVAhOCKvTeXua3T88t9lXnTtQG5oTYRVin5AaAkY0EALw_wcB&gclsrc=aw.ds (Last accessed 11/28/2023)
[3] https://blog.23andme.com/articles/addressing-data-security-concerns?utm_medium=search_brand&utm_source=google&gad_source=1&gclid=Cj0KCQiApOyqBhDlARIsAGfnyMoQ-RnBuXzQtop7pMYWaZr90Czn6TVmMJY2E5BuiYdUOSyx1HcGX-oaAgNwEALw_wcB&gclsrc=aw.ds(Last accessed 11/28/2023)
[4] https://customercare.23andme.com/hc/en-us/articles/115004659308 (Last accessed 11/28/2023)

information on at least one million customers with Ashkenazi Jewish heritage and hundreds of thousands of individuals with Chinese ancestry now for sale by criminal organizations on the dark web.[5]

4. 23andMe understands the extremely sensitive and private nature of their data. On their website they display large colorful banners advertising "Your privacy comes first." Defendant acknowledges that customers are entrusting it with "important personal information"[6] and advertise that they're "committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected."[7] 23andMe additionally cites its audits and assessments as an assurance that it will "never let our guard down."[8]

5. 23andMe intended, at least in part, to encourage paying customers to entrust 23andMe with valuable and innately personal information including, but not limited to, genetic materials and information on DNA profiles and genetic markers. Upon information and belief, 23andMe advertised purported "industry leading" certifications and privacy practices to persuade consumers to use Defendant's services and to provide Defendant with both monetary compensation and with genetic materials to assist with Defendant's research purposes.

6. Defendant owed Plaintiff and class members a non-delegable duty to take and maintain reasonable efforts to secure the "important personal information" on their website, including medical markers and ancestry data, from unauthorized access and disclosure.

7. 23andMe understood the high value of the information in their possession to third parties including criminal organizations. Specifically, 23andMe understood that its position as a prominent genetic testing company made it and its customers a prime target for hackers and other malicious groups.

8. 23andMe understood they were safeguarding highly valuable and extraordinarily private genetic profile information including data concerning medical issues and family ancestry.

---

[5] https://portal.ct.gov/AG/Press-Releases/2023-Press-Releases/Attorney-General-Tong-Issues-Inquiry-Letter-to-23andMe-Following-Data-Breach (last accessed 11/28/2023)
[6] https://www.23andme.com/privacy/ (last accessed 11/28/2023)
[7] *Id.*
[8] *Id.*

9. 23andMe understood that with respect to the "Relations" function in particular, a breach of a single individual could compromise the integrity of many customers who shared relations with the compromised account.

10. 23andMe knew that customers might often share passwords between different websites and the poor security practices of a single customer could potentially compromise the integrity of PII belonging to many customers.

11. In an announcement on October 6, 2023, 23andMe released the following statement concerning a major data breach of PII from customer accounts and profiles:

> "We recently learned that certain 23andMe customer profile information that they opted into sharing through our DNA Relatives feature, was compiled from individual 23andMe.com accounts without the account users' authorization.
>
> After learning of suspicious activity, we immediately began an investigation. While we are continuing to investigate this matter, we believe threat actors were able to access certain accounts in instances where users recycled login credentials – that is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked,
>
> We believe the threat actor may have then, in violation of our Terms of Service, accessed 23andMe.com accounts without authorization and obtained information from certain accounts, including information about users' DNA Relatives profiles, to the extent a user opted into that service."

12. 23andMe attempts to shift the blame to their customers for the data breach by blaming customers for "recycling login credentials" and "Opt[ing] into sharing through our DNA Relatives feature" rather than identifying any deficiencies within their own security protocols.

13. This notice from 23andMe is deficient because, in addition to placing sole blame on customers and third-party bad actors, 23andMe failed to disclose when they first discovered the breach, the approximate size of the breach, the number of customers affected, whether the breach was ongoing, and how long they were aware of this security vulnerability. This information is critical to individuals who have suffered from a data breach, especially given the scale and depth of the information compromised here. Plaintiff Ioffe was not informed by 23andMe that her account was one of those whose private information was breached until October

24, more than 2 weeks after the initial data breach was reported. On information and belief, Plaintiff expects other like members of the impacted class did not receive notifications for weeks after the initial reported breach.

14. This delay in notification to specific victims of the breach is unacceptable and directly harms victims of the breach, including Plaintiff, by creating uncertainty about whether they have actually been harmed and the need to engage in various services and efforts in the wake of the data breach including but not limited to examining whether PII has been sold on the dark web, taking measures to protect against identity theft crimes, expenses and/or time spent on credit monitoring and identity theft insurance, time spent examining bank statements, time and effort spent initiating fraud alerts, and other consequential harm.

15. This harm is particularly acute for many victims, including Plaintiff Ioffe, because they have histories of trauma and abuse based on ethnicity. Plaintiff Ioffe, for example, immigrated to the United States because she was abused by teachers as a child in a foreign country because of her Jewish heritage and faith. She, like many others, used 23andMe to connect with relatives in the belief that 23andMe was secure and her personal information would be protected. Plaintiff Ioffe, like many others, now lives in fear that she may once again be targeted based on her ethnicity and genetic heritage. This fear is even keen given current world events including the war in Israel and significant increases in anti-Semitic attacks on people like Plaintiff. That people with ethnic histories of trauma would suffer from a data breach is entirely foreseeable, yet 23andMe took entirely insufficient security measures considering the risk of this significant harm. As discussed above, the data for at least one million Ashkenazi Jews, like Plaintiff Ioffe, has been breached.

16. 23andMe also unreasonably delayed implementing reasonable security measures following the breach. Although 23andMe reported the breach on October 6, they did not begin limiting access within the heavily compromised Relations feature until October 20, 2023.[9] Indeed, given 23andMe stated in their October 6th notice that the breach occurred in the Relatives feature,

[9] https://blog.23andme.com/articles/addressing-data-security-concerns (last accessed 11/22/23)

the delay in restricting features for two weeks was an entirely insufficient response to the breach. Additionally, 23andMe did not begin requiring 2-step verification for account holders until November 6, 2023, despite knowing that compromised accounts were the likely source of the breach and despite having 2-step verification as an available technology on their platform since at least 2019. 23andMe has still failed to provide sufficient information on what information was seized by hackers or to provide any compensation or protection to customers who were victimized in the breach, such as by offering credit monitoring or identity protection services.

17. Despite 23andMe's promise to "Never let [its] guard down]"[10] 23andMe understood their platform faced significant potential security risks, that they failed to effectively mitigate. Specifically, Defendants understood: (1) that its position as a prominent genetic testing company made it and its customers a prime target for hackers and other malicious groups; (2) that they were safeguarding highly valuable and extraordinarily private genetic profile information including medical issues and history; (3) that hackers will routinely acquire passwords from other data breaches and attempt to use them on other accounts; (4) that many people, including many 23andMe customers, will recycle login credentials even though this is not best practice; and (5) that a single account that was breached due to recycled credentials could potentially expose the sensitive information for many customers due to the nature of the Relatives feature.

18. Nevertheless, despite knowing that a single compromised account could result in the theft of highly sensitive PII and genetic information from many customers, 23andme did not limit features within the DNA relatives tool to protect customers until October 20, 2023 – two months after sources first began discussing the breach online was reported.[11] Additionally, Defendant did not require Multi-factor authentication (MFA) until November 6th, an additional month after they initially reported the breach.[12]

[10] https://www.23andme.com/privacy/ (last accessed 11/27/23)
[11] https://blog.23andme.com/articles/addressing-data-security-concerns?utm_medium=search_brand&utm_source=google&gad_source=1&gclid=Cj0KCQiApOyqBhDlARIsAGfnyMqtFWmhFZVc7wmOu0koVAhOCKvTeXua3T88t9lXnTtQG5oTYRVin5AaAkY0EALw_wcB&gclsrc=aw.ds (Last accessed 11/28/2023)
[12] *Id.*

19. Plaintiff, individually and on behalf of all others similarly situated, alleges claims under the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200, *et seq.*), the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq*.), the California Consumer Records Act (Cal. Civ. Code § 1798.80, *et seq*.), the California Consumers Legal Remedies Act (Cal. Civ. Code § 1750, *et seq*.), the California Confidentiality of Medical Information Act (Cal. Civ. Code § 56.06, *et seq*.), breach of implied contract, and for negligence. Plaintiff, individually and on behalf of all others similarly situated, asks the Court to compel Defendant to adopt reasonable information security practices to secure the sensitive medical and PII that Defendant collects and stores in its databases and to grant such other relief as the Court deems just and proper.

PARTIES

Plaintiff

20. Plaintiff Polina Ioffe, a resident and citizen of Massachusetts, has been a 23andMe customer for many years up to its initial launch. She was informed she was a victim of the data breach on October 24, 2023. She also has Ashkenazi Jewish ancestry and this ethnicity has been expressly targeted by the data breach.

Defendant

21. Defendant 23andMe, Inc. is a Delaware corporation headquartered at 223 North Mathilda Avenue, Sunnyvale, California. 23andMe, Inc. is a publicly traded biotechnology technology in the business of creating personalized genetic reports for the general public for a wide range of genetic markers including ancestry and health risks, and which is engaged in DNA research and development.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction and diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The putative class contains millions of members, many

of whom have citizenship diverse from 23andMe. The value of the stolen data is extremely high given the irreplaceable and personal nature of DNA and the risk of harm to Plaintiff is high.

23. Intradistrict Assignment: Pursuant to Civil L.R. 3-2(c) and 3-5(b), assignment to the San Jose Division of the Northern District of California is proper because a substantial part of the events or omissions which give rise to the claim occurred in this Division or a substantial part of the property subject to the action is situated in this Division. Defendant is engaged in the extensive promotion, marketing, distribution, and sales of the products at issue in this Division.

24. This Court has jurisdiction over 23andMe, Inc. because its principal place of business is in the Northern District of California, it operates in this District, and the computer systems implicated in the 23andMe Data Breach are likely based in this District. Its business operations are in this District, and 23andMe intentionally avails itself of the markets within this District such that the exercise of jurisdiction by this Court is just and proper.

25. Venue is proper under 28 U.S.C. § 1391(b)(1) because 23andMe is headquartered and does substantial business in this district. Venue is also proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to this action occurred in this District. 23andMe is based in this District, maintains customer PII in the District, and has caused harm to Plaintiff and to Class Members residing in this District.

SUBSTANTIVE ALLEGATIONS

I. The Data Breach

26. At least as early as August 11, 2023, Defendant either became aware, or should have become aware, of the risk of a serious data breach.

27. On October 10, 2023, just four days after Defendant disclosed the breach, the website TechCrunch published an article reporting evidence of a breach being public knowledge at least as early as August 11th, excerpt below.

> On August 11, a hacker on a known cybercrime forum called Hydra advertised a set of 23andMe user data that matches some of the data leaked last week on another hacking forum called BreachForums.
>
> The hacker claimed in the earlier post on Hydra to have 300 terabytes of stolen 23andMe user data, and said they had contacted 23andMe, "but instead of taking

> the matter seriously, they asked irrelevant questions." The hacker asked for $50 million for the data, and claimed they would only sell it once, but also offered to sell only a subset of data for between $1,000 and $10,000.
>
> But at least one person saw the Hydra post and publicized it on the open internet long before the news of the leak was reported last week. On the same day as the Hydra forum post, a Reddit user wrote on the 23andMe unofficial subreddit, alerting other users of the alleged breach.
>
> In the Hydra post, the hacker shared the alleged genetic data of a senior Silicon Valley executive, which contained the same user profile and genetic data found in one of the datasets advertised last week on BreachForums, though the two datasets are structured differently. The datasets advertised on BreachForums allegedly contain one million 23andMe users of Jewish Ashkenazi descent and 100,000 23andMe Chinese users.[13]

28. The article reports that hackers purportedly contacted 23andMe prior to August 11 in an attempt to ransom massive quantities of customer data. Even if this contact did not take place, at a minimum 23andMe should have been made aware of a potential breach due to the circulation of sensitive data and a post about the breach appearing on the subreddit.

29. 23andMe touts their active monitoring and security programs. Specifically, they often advertised on their purported industry leading privacy and security practices including active monitoring, audits, and encryption. Indeed, even after the data breach, Defendant continued to state in an email to effected customers on October 24, 2023, "We actively and routinely monitor and audit our systems to ensure that your data is protected. When we receive information through these processes or from other sources claiming customer data has been accessed by unauthorized individuals, we immediately investigate to validate whether this information is accurate."[14]

30. As reported, 23andMe should have been aware of the breach far earlier than they publicly admitted. At a minimum, they should have at least become aware of the potential for a breach when chatter around the breach arose on the 23andMe subreddit. Either 23andMe lapsed in their monitoring and security protocols, or they were aware of the breach in a timely manner and completely failed to adequately remedy the harm, or even to timely alert consumers to the threat.

---

[13] https://techcrunch.com/2023/10/10/hackers-advertised-23andme-stolen-data-two-months-ago/ (last accessed 11/22/2023)

[14] See Exhibit B

31. On October 6, 2023, nearly two months after the reports of user data for sale, 23andMe issued a notice to customers on their blog advising there had been a data breach. However, the notice was far too little and far too late. Even as late as November 22, 2023, 23andMe has still yet to recommend customers take any actions besides rotating passwords and enabling Multi-Factor-Authentication, despite the risk their customers now face with respect to identity and medical related crimes.

32. The scope of the Data Breach is likely massive. Public reporting states hundreds of thousands of consumers with Chinese ancestry and over a million customers with Ashkenazi Jewish ancestry have been victims of the breach, along with likely millions of others.

II. 23andMe's Privacy Representations

33. 23andMe acknowledges its legal and contractual obligations to protect its clients' sensitive PII. According to the Company's U.S. Privacy Policy, 23andMe claims "At 23and Me, Privacy is in our DNA."[15] It also acknowledges that "When you explore your "[w]e maintain physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control."[16]

34. 23andMe further acknowledges that it uses its customers' data in part for its own profit-generating purposes, including to "develop, operate, improve, maintain, and safeguard our services, including developing new product tools and features," to conduct "Personalize, contextualize and market our Services to you," and to "Provide cross-context behavioral and targeted advertising."[17]

III. 23andMe Failed to Comply with Reasonable Cybersecurity Standards

35. At all times relevant to this Complaint, 23andMe knew or should have known the significance and necessity of safeguarding its customers' PII and the foreseeable consequences of a data breach. 23andMe knew or should have known that because it collected and maintained the PII for a significant number of customers, a significant number of customers would be harmed

[15] https://www.23andme.com/legal/privacy/full-version/ (Last accessed 11/27/2023)
[16] *Id.*
[17] *Id.*

by a breach of its systems. 23andMe further knew due to the nature of its genetic research of the deeply personal, sensitive, and immutable nature of the data it collected and for a breach to potentially impact not just individual accounts, but entire families and communities.

36. Because PII is so sensitive and cyberattacks have become a rising threat, the FTC has issued numerous guides for businesses holding sensitive PII and emphasized the importance of adequate data security practices. The FTC also stresses that appropriately safeguarding PII held by businesses should be factored into all business-related decision making.

37. An FTC Publication titled "Protecting Personal Information: A Guide for Business" lays out fundamental data security principles and standard practices that businesses should implement to protect PII.[18] The guidelines highlight that businesses should (a) protect the personal customer information they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems.

38. The FTC also recommends businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity, monitor for large amounts of data being transmitted from their systems, and have a response plan prepared in the event of a breach.

39. The FTC also recommends that businesses limit access to sensitive PII, require complex passwords to be used on the networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures—a step that would have been particularly prudent in light of the methods used by the perpetrators in this case.

40. Businesses that do not comply with the basic protection of sensitive PII are facing enforcement actions brought by the FTC. Failure to employ reasonable and appropriate measures

[18] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last accessed 11/22/2023)

to protect against unauthorized access to confidential consumer data is an unfair act or practice prohibited pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

41. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

42. 23andMe knew or should have known of its obligation to implement appropriate measures to protect its customers' PII but failed to comply with the FTC's basic guidelines and other industry best practices, including the minimum standards set by the National Institute of Standards and Technology Cybersecurity Framework Version 1.1.[19]

43. Defendant's failure to employ reasonable measures to adequately safeguard against unauthorized access to PII constitutes an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, as well as by state statutory analogs.

44. 23andMe failed to use reasonable care in maintaining the privacy and security of Plaintiff' and Class Members' PII. If 23andMe had implemented adequate security measures, cybercriminals could never have accessed the PII of Plaintiff and Class Members, and the Data Breach would have either been prevented in its entirety or have been much smaller in scope. For example, if 23andMe has implemented adequate monitoring systems, they could have detected patterns of activity in compromised accounts that were indicative of a potential breach earlier and acted to greatly limit the number of accounts impacted. Defendants could have also required multi-factor-authentication for all accounts logging into shared pools of sensitive information, such as under the Relatives feature, so a single compromised account would be much less likely to result in a mass breach. Finally, once 23andMe became aware of the breach, they could have acted far faster and more aggressively in responding to the breach and in assisting victims in redressing harms.

45. Personally Identifiable Information is of high value to criminals. Sensitive information can often be sold on the dark web, with personal information being sold at a price

[19] https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf. (last accessed 11/27/2023)

ranging from $40 to $200 and bank details with a price from $50 to $200.[20] The Data Breach exposed PII that is both valuable and highly coveted on underground markets because it can be used to commit identity theft and financial fraud. Identity thieves use such PII to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use this PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities." Additionally, identity thieves often wait significant amounts of time—months or even years—to use the PII obtained in data breaches because victims often become less vigilant in monitoring their accounts as time passes, therefore making the PII easier to use without detection. These identity thieves will also re-use stolen PII, resulting in victims of one data breach suffering the effects of several cybercrimes from one instance of unauthorized access to their PII.

46. Moreover, 23andMe is in the business of collecting and analyzing the most sensitive and irreplicable information about individuals, their genetic code. Government reports have also indicated that the data breach has resulted in the targeted exfiltration and sale on the black market of at least one million data profiles pertaining to individuals with Ashkenazi Jewish heritage, including Plaintiff Ioffe. Indeed, many 23andMe customers, including Plaintiff Ioffe, now live in fear because of traumatic histories of being targeted and attacked based on ethnicity. This is a particularly dangerous time for such information to be released considering the rise in antisemitic threats and the war in Israel. The combination of genetic heritage data and personal information could allow bad actors to target 23andMe customers based on ethnic or religious backgrounds putting them at serious risk of harassment, stalking, or even acts of violence.

47. Victims of data breaches are much more likely to become victims of identity fraud than those who have not. Data Breach victims who do experience identity theft often spend

[20] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed November 22, 2023).

hundreds of hours fixing the damage caused by identity thieves.[21] Additionally, the U.S. Department of Justice's Bureau of Justice Statistics has reported that, even if data thieves have not caused financial harm, data breach victims "reported spending an average of about 7 hours clearing up the issues."[22]

48. The information compromised in the Data Breach—including genetic code information which is the "most sensitive and irreplaceable information about individuals"[23]—is much more valuable than the loss of credit card information in a retailer data breach. There, victims can simply close their credit and debit card accounts and potentially even rely on automatic fraud protection offered by their banks. Here, however, the information compromised is much more difficult, if not impossible, for consumers to re-secure after being stolen because it goes to the core of their identity. Additionally, the genetic profiling of hundreds of thousands or even millions of 23andMe customers raises additional risks related to the potential for hate crimes or even threats to physical security.

49. Data breaches involving medical records are not only incredibly costly, they can "also [be] more difficult to detect, taking almost twice as long as normal identity theft."[24] The FTC warns that a thief may use private medical information to, among other things, "see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care"[25] and that this may have far reaching consequences for a victim's ability to access medical care and use insurance benefits.

50. In the wake of the data breach, 23andMe has implemented new policies including requiring password changes, requiring multi-factor authentication, and disabling some of the most problematic elements of the Relationships feature. However, this is the equivalent to closing the

[21] https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf. (last accessed 11/22/2023)
[22] https://bjs.ojp.gov/content/pub/pdf/vit14.pdf. (last accessed 11/22/2023)
[23] https://portal.ct.gov/-/media/AG/Press_Releases/2023/10-30-2023-William-Tong--23andMe-Inc-Inquiry-Letter-final-002.pdf (last accessed 11/22/2023)
[24] *See What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Nov. 22, 2023).
[25] *Id*

barn door after the horse has already bolted. As of November 22, 2023, 23andMe has yet to provide customers with any assurance about how they will redress damages suffered from the security breach. 23andMe has not offered any kind of free identity protection services, or compensation for victims who used its service, and its email advising about "What to do" to victims only mentions enabling MFA and using unique passwords and is utterly inadequate. Plaintiff and Class Members maintain an interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

51. Security Standards for businesses storing PII commonly include, but are not limited to:

a. Maintaining a secure firewall

b. Monitoring for suspicious or unusual traffic on the website

c. Looking for trends in user activity including for unknown or suspicious users

d. Looking at server requests for PII

e. Looking for server requests from VPNs and Tor exit notes

f. Requiring Multi-factor authentication before permitting new IP addresses to access user accounts and PII

g. Structuring a system including design and control to limit user access as necessary including a users access to the account data and PII of other users.

IV. Plaintiff' Experiences

52. To become members of Defendant's Service, Plaintiff provided sensitive PII 23andMe including individual genetic samples. Released data includes, among other things, names, sex, date of birth, geographical location, and genetic ancestry results.

53. Plaintiff has taken reasonable steps to maintain the confidentiality of their PII. She relied upon 23andMe's representations, experience, and sophistication to keep their information secure and confidential.

54. As a result of the Data Breach, Plaintiff was forced to take measures to mitigate the harm, including spending time monitoring their credit and financial accounts, researching the

Data Breach, and researching and taking steps to prevent and mitigate the likelihood of identity theft, among other harms.

55. **Plaintiff Ioffe** has been a 23andMe client since in or around when 23andMe first launched. On October 24, 2023, 23andMe notified Plaintiff Ioffe that she was a victim of the Data Breach. After learning about the Data Breach, Plaintiff Ioffe has taken steps to monitor and secure her identity, including contacting her bank and changing bank and email passwords.

56. As a result of the Data Breach, Plaintiff and Class Members have suffered actual injuries including: (a) paying money to 23andMe for services, which Plaintiff would not have done had 23andMe disclosed that it lacked data security practices adequate to safeguard Plaintiff' PII from theft; (b) damages to and diminution in the value of Plaintiff's PII—property that Plaintiff entrusted to 23andMe as a condition of receiving its services; (c) loss and invasion of Plaintiff' privacy; and (d) injuries arising from the increased risk of fraud and identity theft, including the cost of taking reasonable identity theft protection measures, which will continue for years.

CLASS ACTION ALLEGATIONS

57. Plaintiff brings this action as a class action pursuant to Rules 23(a) and 23(b)(1)-(3) of the Federal Rules of Civil Procedure, on behalf of herself and a **Nationwide** Class, defined as follows:

> All persons in the United States whose personal information was compromised in the Data Breach announced by 23andMe, Inc. in October 2023.

58. Excluded from the Nationwide Class are governmental entities, Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

59. This action is brought and may be properly maintained as a class action pursuant to Rule 23. This action satisfies the requirements of Rule 23, including numerosity, commonality, typicality, adequacy, predominance, and superiority.

60. **Numerosity.** The Nationwide Class are so numerous that the individual joinder of all members is impracticable. While the Nationwide Class exact number are currently unknown and can only be ascertained through appropriate discovery, Plaintiff, on information and belief, allege that the Nationwide Class include anywhere from several hundred thousand to several million members.

61. **Commonality.** Common legal and factual questions exist that predominate over any questions affecting only individual Nationwide Class Members. These common questions, which do not vary among Nationwide Class Members and which may be determined without reference to any Nationwide Class Member's individual circumstances, include, but are not limited to:

a. Whether Defendant knew or should have known that its systems were vulnerable to unauthorized access;

b. Whether Defendant failed to take adequate and reasonable measures to ensure its data systems were protected;

c. Whether Defendant failed to take available steps to prevent and stop the breach from happening;

d. Whether Defendant unreasonably delayed in notifying Plaintiff once the breach had occurred;

e. Whether Defendant unreasonably delayed in implementing reasonable security measures including disabling aspects of the Ancestry feature and requiring MFA for all users.

f. Whether Defendant owed a legal duty to Plaintiff and Class Members to protect their PII;

g. Whether Defendant breached any duty to protect the personal information of Plaintiff and Class Members by failing to exercise due care in protecting their PII;

h. Whether Plaintiff and Class Members are entitled to actual, statutory, or other forms of damages and other monetary relief; and,

i. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief or restitution.

62. **Typicality.** Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

63. **Adequacy of Representation.** Plaintiff are adequate Nationwide Class representatives because they are Nationwide Class Members, and their interests do not conflict with the Nationwide Class interests. Plaintiff retained counsel who are competent and experienced in class action and data breach litigation. Plaintiff and their counsel intend to prosecute this action vigorously for the Nationwide Class' benefit and will fairly and adequately protect their interests.

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

65. **Declaratory and Injunctive Relief.** The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with

respect to individual Class Members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their interests. Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

CLAIMS FOR RELIEF

Count 1
Negligence
On behalf of Plaintiff and the Nationwide Class

1. Plaintiff incorporates by reference and reallege each and every allegation above as though fully set forth herein.

2. Plaintiff was required to provide uniquely personal and permanent PII, a sample of genetic material for analysis and profiling, as a condition of using the 23andMe service.

3. Plaintiff and Class Members entrusted their PII to 23andMe with the understanding that 23andMe would safeguard their PII.

4. In its written privacy policies, 23andMe states "We're committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected." And expressly promised Plaintiff and Class Members that "We give you full control to decide how your information is used and with whom it is shared." However, it appears millions of users (including Plaintiff) had sensitive data "shared" with hackers without the user's knowledge or consent. In addition, 23andMe promised to "exceed industry data protection standards" and make "privacy [their] number one priority." However, 23andMe did not take reasonable and appropriate safeguards to protect Plaintiff and Class Members' PII.

5. 23andMe had full knowledge of the sensitivity of the PII that it stored and the types of harm that Plaintiff and Class Members could and would suffer if that PII were wrongfully disclosed.

6. 23andMe violated its duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and

testing 23andMe's information security controls sufficiently rigorously to ensure that PII in its possession was adequately secured by, for example, encrypting sensitive personal information, installing effective intrusion detection systems and monitoring mechanisms, using access controls to limit access to sensitive data, limiting access to the PII of multiple "relatives" when a single account using the "Relatives" feature was breached, failing to require MFA as a precondition for using the "Relatives" feature, failing to notify customers of the breach in a timely manner, and failing to remedy the continuing harm by unreasonably delaying additional security features (including disabling aspects of the Relatives feature and requiring MFA) until weeks after the initial disclosure of a breach.

7. 23andMe's duty of care arose from, among other things,

a. 23andMe's exclusive ability (and Class Members' inability) to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur;

b. Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures;

c. 23andMe's common law duties to adopt reasonable data security measures to protect customer PII and to act as a reasonable and prudent person under the same or similar circumstances would act; and

d. State statutes requiring reasonable data security measures, including the California Genetic Information Privacy Act Cal. Civ. Section 56.181(d), which requires "direct-to-consumer genetic testing companies" to "implement and maintain reasonable security procedures and practices to protect a consumer's genetic data against unauthorized access, destruction, use, modification, or disclosure."[26]

[26] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=1.&title=&part=2.6.&chapter=2.6.&article= (Last accessed 11/27/23)

8. 23andMe's violation of the FTC Act and state Genetic Information Privacy statutes constitutes negligence per se for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the types of harm that resulted from the Data Breach.

9. 23andMe is an internationally known multi-million-dollar publicly traded company which reported FY2023 revenue at 299 million dollars[27] that had the financial and personnel resources necessary to prevent the Data Breach. 23andMe nevertheless failed to adopt reasonable data security measures, in breach of the duties it owed to Plaintiff and Class Members.

10. Plaintiff and Class Members were the foreseeable victims of 23andMe's inadequate data security. 23andMe knew that a breach of its systems could and would cause harm to Plaintiff and Class Members.

11. 23andMe's conduct created a foreseeable risk of harm to Plaintiff and Class Members. 23andMe's conduct included its failure to adequately restrict access to its Ancestor's feature that held consumers' PII.

12. 23andMe knew or should have known of the inherent risks in collecting and storing massive amounts of PII, the importance of providing adequate data security over that PII, and the frequent cyberattacks within medical and genetic research industry.

13. 23andMe through its actions and inactions, breached its duty owed to Plaintiff and Class Members by failing to exercise reasonable care in safeguarding their PII while it was in 23andMe's possession and control. 23andMe breached its duty by, among other things, its failure to adopt reasonable data security practices and its failure to anticipate credential spoofing (a commonly used technique) of a handful of accounts could compromise the PII of many customers using the Ancestors feature, and in failing to monitor the use of the Ancestors feature for data scraping and suspicious activities sufficiently and in failing to mandate more stringent security measures (including MFA) before permitting customers to access the PII of relatives.

[27] https://investors.23andme.com/news-releases/news-release-details/23andme-reports-fy2023-fourth-quarter-and-full-year-financial (Last accessed 11/28/23)

14. 23andMe inadequately safeguarded consumers' PII in deviation of standard industry rules, regulations, and best practices at the time of the Data Breach.

15. But for 23andMe's breach of its duty to adequately protect Class Members' PII, Class Members' PII would not have been stolen.

16. There is a temporal and close causal connection between 23andMe's failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiff and Class Members.

17. As a result of 23andMe's negligence, Plaintiff and Class Members suffered and will continue to suffer the various types of damages alleged herein.

18. Plaintiff and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate identity protection services. Plaintiff and Class Members are also entitled to the injunctive relief sought herein.

Count 2
Breach of Implied Contract
On behalf of plaintiff and the Nationwide Class

1. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

2. Plaintiff and Class Members entered into an implied contract with 23andMe when they entrusted Defendant with their PII.

3. As part of these transactions, 23andMe agreed to safeguard and protect the PII of Plaintiff and Class Members and to timely and accurately notify them if their PII was breached or compromised.

4. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that 23andMe's data security practices and policies were reasonable and consistent with, or indeed were in excess of (based on representations by 23andMe) the legal requirements and industry standards. Plaintiff and Class Members believed that 23andMe would use part of the

monies paid to 23andMe under the implied contracts or the monies obtained from the benefits derived from the PII they provided to fund proper and reasonable data security practices.

5. Plaintiff and Class Members would not have provided and entrusted their PII to 23andMe or would have paid less for 23andMe's products or services in the absence of the implied contract or implied terms between them and 23andMe. The safeguarding of the PII of Plaintiff and Class Members was critical to realize the intent of the parties.

6. Plaintiff and Class members fully performed their obligations under the implied contracts with 23andMe.

7. 23andMe breached its implied contracts with Plaintiff and Class Members to protect their PII when it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties.

8. As a direct and proximate result of 23andMe's breach of implied contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the 23andMe Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

Count 3
Violation of California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200
On behalf of Plaintiff and the Nationwide Class.

9. Plaintiff incorporates by reference and reallege each and every allegation above as though fully set forth herein.

10. 23andMe, Inc. and Plaintiff are "persons" as defined by the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17201.

11. The UCL states that "unfair competition shall mean and include any [1] unlawful, unfair or fraudulent business act or practice and [2] unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

12. By failing to take reasonable precautions to protect the PII of Plaintiff and the class members, 23andMe has engaged in "unlawful," "unfair," and "fraudulent" business practices in violation of the UCL.

13. First, 23andMe engaged in "unlawful" acts or practices because it violated multiple laws, including but not limited to the California Consumer Records Act, Cal. Civ. Code § 1798.81.5 (requiring reasonable data security measures); the FTC Act, 15 U.S.C. § 45; and the common law, all as alleged herein.

14. Second, 23andMe engaged in "unfair" acts or practices, including the following:

a. 23andMe failed to implement and maintain reasonable data security measures to protect the Class Members' PII. 23andMe failed to identify foreseeable security risks, remediate identified risks, and adequately improve its data security in light of the highly sensitive nature of the data which it maintained and the known risk of cyber intrusions to companies storing sensitive medical and other personal information. Additionally, to the extent which Defendant may have identified a threat from duplicated account credentials, they did not implement timely reasonable security measures including mandatory MFA. Defendant's conduct, with little if any social utility, is unfair when weighed against the harm to the Class Members whose PII has been compromised.

b. 23andMe's failure to implement and maintain reasonable data security measures was also contrary to legislatively declared public policy that seeks to protect consumers' personal information and ensure that entities entrusted with PII adopt appropriate security measures. These policies are reflected in various laws, including but not limited to the FTC Act, 15 U.S.C. § 45; and the California Consumer Records Act, Cal. Civ. Code § 1798.81.5 (requiring reasonable data security measures).

c. 23andMe's failure to implement and maintain reasonable data security measures also led to substantial consumer injuries described herein, which are not outweighed by countervailing benefits to consumers or to competition.

15. Third, 23andMe engaged in "fraudulent" acts or practices, including but not limited to the following:

a. 23andMe omitted and concealed the fact that it did not employ reasonable safeguards to protect consumers' PII. 23andMe could and should have made a proper disclosure during the account creation process for the Relations feature directly to consumers, or by any other means reasonably calculated to inform consumers of the inadequate data security. 23andMe knew or should have known that its data security practices were deficient. This is true because, among other things, 23andMe was aware that the extremely sensitive nature of the information they held and the immutable and personal nature of DNA making this information particularly attractive to criminals, would make them a likely target of sophisticated cyberattacks. 23andMe knew or should have known that its data security was insufficient to guard against those attacks and in particular was insufficient to protect one compromised account from stealing mass data using the Relations feature.

b. 23andMe also made express representations that its data security practices were sufficient to protect consumers' PII. 23andMe required consumers to

> provide DNA samples for analysis, the results of which contain highly sensitive and deeply personal information. 23andMe knows the importance of this data and made express representations about their security including that "Security and privacy are the highest priorities at 23andMe," that 23andMe "exceed[s] industry data protection standards,"[28] and that "We regularly conduct audits and assessments of our systems, ensuring we will never let our guard down."[29] In doing so, 23andMe made implied or implicit representations that its data security practices were sufficient to protect consumers. Those representations were false and misleading.

16. Plaintiff and Class Members transacted with 23andMe in California by, among other things, sending physical DNA samples to 23andMe for analysis and in using and maintaining their accounts, including the ancestry profile. Plaintiff and Class Members were deceived when they joined and used the 23andMe's California based services and product despite deficient data security practices.

17. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members were injured, lost money or property, and suffered the various types of damages alleged herein.

18. The UCL states that an action may be brought by any person who has "suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Plaintiff and Class Members suffered injury in fact and lost money or property as a result of 23andMe's unfair competition including the loss of value of their breached PII. PII is valuable, which is demonstrated not only by the fact that 23andMe charges customers for the creation of this data and DNA profiles, but it encourages customers to use the data in value adding ways including through medical analysis among others.

19. Cal. Bus. & Prof. Code § 17203 states:

[28] https://www.23andme.com/privacy/ (last accessed 11/27/23)
[29] *Id*

> Any person who engages, has engaged, or proposes to engage in unfair competition may be enjoined in any court of competent jurisdiction. The court may make such orders or judgments […] as may be necessary to prevent the use or employment by any person of any practice which constitutes unfair competition, as defined in this chapter, or as may be necessary to restore to any person in interest any money or property, real or personal, which may have been acquired by means of such unfair competition.

20. Plaintiff and Class Members are entitled to the injunctive relief requested herein to address 23andMe's past and future acts of unfair competition.

21. Plaintiff and Class Members are entitled to restitution of money and property that was acquired by 23andMe by means of its unfair competition and restitutionary disgorgement of all profits accruing to 23andMe as a result of its unfair business practices.

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

23. Further, if an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury. The risk of another such breach is real, immediate, and substantial. It took Defendant a month to require MFA for account customers and detailed information on the cause and scope of the breaches has yet to be exposed. Plaintiff lacks an adequate remedy at law that will reasonably protect against the risk of such further breach.

24. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by the UCL, including reasonable attorneys' fees under Cal. Code of Civ. Procedure § 1021.5.

Count 4
Violation of California Consumer Privacy Act
Cal. Civ. Code § 1798.100, *et seq*.
On behalf of Plaintiff Nationwide Class

25. Plaintiff incorporate by reference and reallege each and every allegation above as though fully set forth herein.

26. Cal. Civ. Code § 1798.150(a)(1) provides that:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain

> reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action.

27. Plaintiff and the members of the national class are consumers as that term is defined in Cal. Civ. Code § 1798.140(i).

28. 23andMe is a business as that term is defined in Cal. Civ. Code § 1798.140(d). 23andMe is organized or operated for the profit or financial benefit of its owners. 23andMe collects consumers' personal information (including Plaintiff and the members of the national class) or such information is collected on behalf of 23andMe. 23andMe is headquartered and has its primary place of business in California.

29. The information compromised during the Data Breach constitutes "personal information" as that term is defined in Cal. Civ. Code § 1798.140(v)(1). Specifically, California extends this protection to "Biometric information"[30] and defines biometric information in the same code as "an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data to establish identity." The genetic information revealed by this data breach exactly meets the State's definition for protected biometric data. Additionally, there has been widespread reporting that breached data is being categorized and sold in part on the basis of ethnicity including individuals with Jewish and Asian ancestry. This meets the definition for "Characteristics of protected classifications under California or Federal Law" which the statute defines as protected personal information. The sensitive nature of this personal information could allow a criminal party to draw inferences from the collected information including reflections on the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

30. At a minimum, that information included names, sex, date of birth, geographical location, and genetic ancestry results.

[30] Cal. Civ. Code § 1798.140(v)(1)(E).

31. Under the CCPA, 23andMe had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information that it stored. Cal. Civ. Code § 1798.150(a)(1).

32. Plaintiff's and Class Members' nonencrypted and nonredacted personal information, as defined in Cal. Civ. Code § 1798.81.5(d)(1), was exfiltrated in the 23andMe Data Breach, including personal genetic and personally identifiable information.

33. 23andMe violated its duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing 23andMe's information security controls to ensure that PII in its possession was adequately secured by, for example, encrypting sensitive personal information, installing intrusion detection systems and monitoring mechanisms, using access controls to limit access to sensitive data from any compromised account, and requiring customers to agree to multi-factor authentication (MFA) before permitting them to access the sensitive information of other accounts through the "Relations" feature.

34. 23andMe knew or should have known that its computer systems and information security controls were inadequate to safeguard Plaintiff's and Class Members' PII and that unauthorized access and exfiltration, theft, or disclosures, was highly likely as a result. 23andMe's actions in engaging in the above-named unlawful practices and acts were negligent, knowing, willful, and/or wanton and reckless with respect to the rights of Plaintiff and California Class Members.

35. As a direct and proximate result of the foregoing, Plaintiff and Class Members have suffered injuries including but not limited to actual damages, and in being denied a statutory benefit conferred on them by the California legislature.

36. As a result of these violations, Plaintiff and the Class Members are entitled to actual pecuniary damages, injunctive or declaratory relief, and any other relief that the Court deems proper. Plaintiff reserves the right to amend this Complaint to seek statutory damages

under the CCPA on behalf of herself and the Class after providing 23andMe with the written notice required by Cal. Civ. Code § 1798.150(b).

Count 5
Violation of California Consumer Records Act
Cal. Civ. Code § 1798.80, *et seq*.
On behalf of Plaintiff and the Nationwide Class

37. Plaintiff incorporates by reference and reallege each and every allegation above as though fully set forth herein.

38. The California legislature enacted the California Customer Records Act ("CCRA") to "ensure that personal information about California residents is protected." Cal. Civ. Code § 1798.81.5.

39. The CCRA states: "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access." Cal. Civ. Code § 1798.81.5(b).

40. The CCRA defines owns, licenses, and maintains as follows: "[T]he terms 'own' and 'license' include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term 'maintain' includes personal information that a business maintains but does not own or license.'" Cal. Civ. Code § 1798.81.5(a)(2). 23andMe owns, licenses, and/or maintains the PII that was involved in the Data Breach.

41. The CCRA defines personal information, in pertinent part, as follows:

> "Personal information" means either of the following: (A) An individual's first name or first initial and the individual's last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: …(iv) medical information. (v) health insurance information. (vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes. (vii) genetic data.

Cal. Civ. Code § 1798.81.5(d)(1). The PII stolen in the Data Breach includes personal information that meets this definition. In particular, Cal. Civ. Code § 1798.81.5(d)(1)(A)(vii) specifically

identifies "Genetic data" as personal information protected by the statute. The PII was unencrypted, as evidenced by the fact that a single compromised account could use the "Relations" feature to view sensitive information from many other accounts. According to reports, at least hundreds of terabytes of personal data was accessed by unauthorized criminals. 23andMe should have identified such unlawful behavior, locked down the website, and immediately notified impacted customers as was required under the laws of several states that require notification of unauthorized access to unencrypted and unredacted information.

42. 23andMe failed to maintain reasonable data security procedures appropriate to the PII. Accordingly, 23andMe violated Cal. Civ. Code § 1798.81.5(b).

43. Plaintiff and Class Members were injured by Defendant's violation of Cal. Civ. Code § 1798.81.5(b) and seek damages pursuant to Cal. Civ. Code § 1798.84(b). They seek all monetary and non-monetary relief allowed by the CCRA to compensate for their various types of damages alleged herein.

44. Plaintiff and the Class Members have suffered injuries including but not limited to actual damages, and in being denied a statutory benefit conferred on them by the California legislature.

Count 6
Violation of California Consumers Legal Remedies Act
Cal. Civ. Code § 1750, *et seq*.
On behalf of Plaintiff and the Nationwide Class

45. Plaintiff incorporates by reference and reallege each and every allegation above as though fully set forth herein.

46. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

47. 23andMe is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

48. Plaintiff and class members are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

49. The acts and practices of 23andMe were intended to and did result in the sales of products and services to Plaintiff and the Class Members in violation of Civil Code § 1770, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

50. The representations and omissions of 23andMe were material because they were likely to deceive reasonable consumers about the adequacy of 23andMe's data security and ability to protect the confidentiality of consumers' PII.

51. Had 23andMe disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, Plaintiff and Class Members would not have purchased its services or would have paid less to account for its inadequate data security. 23andMe was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff. 23andMe accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class Members acted reasonably in relying on 23andMe's misrepresentations and omissions, the truth of which they could not have discovered.

52. As a direct and proximate result of 23andMe's violations of California Civil Code § 1770, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft;

loss of value of their PII; overpayment for 23andMe's services; loss of the value of access to their PII; the value of identity protection services made necessary by the Breach, the increased risk of targeted attacks based on ethnicity, and the long term risks and costs associated with loss of sensitive medical data.

53. Plaintiff, on behalf of herself all class members, demands judgment against Defendant under the CLRA for injunctive relief.

54. Pursuant to Cal. Civ. Code § 1782(a), Plaintiff will serve Defendant with notice of its alleged violations of the CLRA by certified mail return receipt requested. If, within thirty days after the date of such notification, Defendant fails to provide appropriate relief for its violations of the CLRA, Plaintiff will amend this Complaint to seek monetary damages.

55. Notwithstanding any other statements in this Complaint, Plaintiff does not seek monetary damages in conjunction with her CLRA claim—and will not do so—until this thirty-day period has passed.

Count 7
Violation of California Confidentiality of Medical Information Act ("CMIA")
Civil Code Section 56.06
On behalf of Plaintiff and the National Class.

56. 23andMe is a provider of healthcare under Cal. Civ. Code Section 56.06, subdivisions (a) and (b), because 23andMe maintains medical information and offers software to consumers that is designed to maintain medical information for the purposes of allowing its users to manage their information or make the information available to a health care provider, or for the diagnosis, treatment, or management of a medical condition.

57. 23andMe is therefore subject to the requirements of the CMIA and obligated under Section 56.06 subdivision (e) to maintain the same standards of confidentiality required of a provider of health care with respect to medical information that it maintains on behalf of users.

58. The CMIA defines medical information as meaning any "individually identifiable information" in possession of or derived from "a provider of health care, health care service plan,

pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." The information 23andMe maintained and disclosed is medical information because relates to medical history including genetic profile, and was individually identifiable because it included information, including name and location, which "alone or in combination with other publicly available information reveals the identity of the individual."

59. 23andMe violated Cal. Civ. Code Section 53.06(e) because it did not maintain the confidentiality of members medical information. This identifiable information was shared with third parties including criminal third parties and hackers which are now selling the information on the dark web. This disclosure was not authorized by the individual.

60. This negligent disclosure is in violation of Cal. Civ. Code Section 53.06(e) Accordingly, Plaintiffs and Class members are entitled to: (1) nominal damages of $1,000 per violation; (2) actual damages, in an amount to be determined at trial; (3) statutory damages pursuant to Cal. Civ. Code Section 56.36(c); and reasonable attorneys' fees and other litigation costs reasonably incurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class set forth herein, respectfully request the following relief:

A. That the Court certify this action as a class action and appoint Plaintiff and her counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the PII of Plaintiff and the Class by implementing improved security controls;

C. That the Court award compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

D. That the Court award statutory or punitive damages as allowed by law in an amount to be determined at trial;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of Defendant's unlawful acts, omissions, and practices;

F. That the Court award to Plaintiff and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

G. That the Court award pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all claims so triable.

Dated: 11/30/2023

/s/ Amber L. Schubert

SCHUBERT JONCKHEER & KOLBE LLP
ROBERT C. SCHUBERT (rschubert@sjk.law)
AMBER L. SCHUBERT (aschubert@sjk.law)
2001 Union St, Ste 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161

Attorneys for Plaintiff and the Proposed Classes