EDELSBERG LAW, P.A.
Scott Edelsberg, Esq. (CA Bar No. 330990)
1925 Century Park E #1700
Los Angeles, CA 90067
Telephone: 305-975-3320
scott@edelsberglaw.com

Counsel for Plaintiffs and Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

MONICA SANTANA and PAULA KLEYNBURD, on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

23ANDME, INC.,

Defendant.

Case No.

CLASS ACTION

COMPLAINT FOR NEGLIGENCE, BREACH OF IMPLIED CONTRACT, INVASION OF PRIVACY AND UNJUST ENRICHMENT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Monica Santana and Paula Kleynburd (collectively "Plaintiffs"), on behalf of themselves and all others similarly situated, alleges the following Class Action Complaint (the "Action") against Defendant 23andMe, Inc. ("23andMe" or "Defendant") upon personal knowledge as to themselves and their own actions, and upon information and belief, including the investigation of counsel as follows:

I. SUMMARY

1. Defendant is a biotechnology company that looks at specific locations in an individual's genome that are known to differ between people for the purpose of creating personalized genetic reports on everything from ancestry composition to traits to genetic health risks.[1] Defendant has more than 14 million customers worldwide.[2]

2. Plaintiffs brings this Action on behalf of themselves and all other similarly situated victims as a result of a recent cyberattack and data breach involving the personally identifiable information of customers of Defendant ("Customers").

3. On or about October 6, 2023, Defendant announced, via their website, that "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.[3]

4. As a direct result of Defendant's failure to secure and safeguard the sensitive information of over one people that entrusted them to do so, the following types of personally identifiable information are now in the hands of criminal hackers: Names, sex, date of birth, genetic

[1] https://www.23andme.com/# (last visited Oct. 6, 2023).
[2] https://medical.23andme.com/#:~:text=23andMe%20has%20more%20than%2014,own%20homes%2C%20without%20medical%20requisition. (last visited Oct. 6, 2023).
[3] https://blog.23andme.com/articles/addressing-data-security-concerns (last visited Oct. 8, 2023).

ancestry results, profile photos, and geographical location ("PHI, and collectively with PII, "Private Information").

5. 23andMe owed a non-delegable duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Private Information against unauthorized access and disclosure.

6. In the announcement posted to 23andMe's website ("Press Release"), 23andMe explains:

> "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 treat 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."

7. 23andMe attempts to redirect the blame on to the criminal actors that gained access to Defendant's customer accounts, in violation of their Terms of Service, while avoiding mention that their safeguards were inadequate. further admits in the

8. The Notice is deficient for several reasons: (1) 23andME fails to state if they were able to contain or end the cybersecurity threat, leaving victims to fear whether the PII that 23andMe continues to maintain is secure; and (2) 23andMe fails to state how the breach itself occurred. This information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity and wide array of information compromised in this specific breach.

9. As a result of the Data Breach, Plaintiffs and Class Members suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of, and diminution in, value of their PII.

10. In addition, Plaintiffs' and Class Members' sensitive PII —which was entrusted to Defendant — was compromised and unlawfully accessed due to the Data Breach. This information, while compromised and taken by unauthorized third parties, also remains in Defendant's possession. Without additional safeguards and independent review and oversight, it remains vulnerable to future cyberattacks and theft.

11. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect victims' PII.

12. Plaintiffs brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party.

13. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant's computer network in a condition vulnerable to cyberattacks.

14. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendant and entities like it, and Defendant was thus on notice that failing to take steps necessary to secure the PII against those risks left that property in a dangerous condition and vulnerable to theft. Defendant was further on

notice of the severe consequences that would result to Plaintiffs and Class Members from its failure to safeguard their PII.

15. Defendant disregarded the rights of Plaintiffs and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard member PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiffs and Class Members prompt notice of the Data Breach.

16. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the PII. Had Defendant properly monitored its computer network and systems, it would have discovered the intrusion sooner, as opposed to letting cyberthieves roam freely in Defendant's IT network for and unknown period of time.

17. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

18. In fact, several new outlets have even reported that Plaintiffs' and the Class Members' data is already for sale on the black market:

> "The stolen user data seems to be part of a targeted attack focused on Ashkenazi Jews. The hacker responsible for posting the sample data on BreachForum claimed it contained a staggering one million data points exclusively pertaining to this group. Additionally, data of hundreds of thousands with Chinese heritage has been disclosed.
>
> The hacker is currently peddling 23andMe data profiles on the underground market, pricing them between $1 to $10. Noteworthy figures like Mark Zuckerberg, Elon Musk, and Sergey Brin are among the individuals whose

> profiles have been compromised. These profiles encompass basic information such as names, genders, birth years, and some additional genetic data."[4]

19. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

20. Plaintiffs and Class Members will incur out of pocket costs for undertaking protective measures to deter and detect identity theft.

21. Plaintiffs seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

22. Plaintiffs seeks remedies including, but not limited to, actual damages, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

23. Plaintiffs also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the putative Class.

II. JURISDICTION AND VENUE

24. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interests and costs, there are more than 100 members of the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity, namely, Plaintiff Monica Santana is a Florida resident and Plaintiff Paula Kleynburd is a New York resident whereas Defendant's principal place of business is within this District.

25. This Court has personal jurisdiction over Defendant because Defendant is headquartered and does substantial business from and within in this District.

[4] https://www.pelhamplus.com/us-news/stolen-user-data-from-23andme-users-emerges-on-breachforum/ (last accessed October 8, 2023).

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

III. PARTIES

27. Plaintiff Monica Santana is an individual citizen of Florida and has been a customer of 23andMe since June of 2022.

28. Plaintiff Paula Kleynburd is an individual citizen of New York and has been a customer of 23andMe since March of 2020.

29. Defendant 23andMe, Inc. provides biotechnology company that looks at specific locations in an individual's genome that are known to differ between people for the purpose of creating personalized genetic reports on everything from ancestry composition to traits to genetic health risks.

IV. FACTUAL ALLEGATIONS

Defendant's Business

30. According to Defendant's website:

> 23andMe has more than 14 million customers worldwide. Our Health + Ancestry and Membership services allows individuals to acquire this information from the privacy of their own homes, without medical requisition.[5]

31. Defendant collects PII from their customers in the course of doing business. This PII includes the PII which was compromised in the Data Breach alleged herein.

32. Prior to receiving services from Defendant, Plaintiffs and Class Members were required to and did in fact turn over their PII.

[5] https://medical.23andme.com (last visited Oct. 6, 2023).

33. Upon information and belief, Defendant promises to maintain the confidentiality of Plaintiffs' and Class Members' PII to ensure compliance with federal and state laws and regulations, and not to use or disclose Plaintiffs' and Class Members' PII for non-essential purposes.

34. Indeed, Defendant's Privacy Policy states, "[w]e encrypt all sensitive information and conduct regular assessments to identify security vulnerabilities and threats."[6]

35. As a condition of receiving Defendant's services, Defendant requires that Plaintiffs and Class Members entrust it with highly sensitive PII.

36. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

37. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members would not have entrusted Defendant with their Private Information had they known that Defendant would fail to implement industry standard protections for that sensitive information.

38. Plaintiffs and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Attack and Data Breach

39. Defendant informed Plaintiffs and the Class Members via the Press Release that:

> "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.

[6] https://www.23andme.com/privacy/ (last visited Oct. 7, 2023).

> 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 treat 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."

40. The PII that was compromised includes but is not limited to Customers' names, sex, date of birth, genetic ancestry results, profile photos, geographical location and other information and other data provided to 23andMe.

41. In its Data Breach Press Release, 23andMe also encourages the victims confirm they have strong passwords and ensure the use of multi-factor authentication (MFA). Through these statements, Defendant is acknowledging that Plaintiffs and Class Members are subject to an imminent threat of fraud and identity theft.

42. Due to Defendant's inadequate security measures, Plaintiffs and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

43. Upon information and belief, the PII was not encrypted prior to the data breach.

44. Upon information and belief, the cyberattack was targeted at Defendant as a company that collects and maintains valuable personal and data from its many Customers, including Plaintiffs and Class Members.

45. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiffs and Class Members.

46. Defendant had obligations to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

47. Plaintiffs and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach Was Foreseeable and the Defendant Was Aware of Its Risk

48. It is well known that PII, particularly Social Security numbers and Customer names, are invaluable commodities and a frequent target of hackers.

49. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[7]

50. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

51. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

[7] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/

52. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and thwart such an attack.

53. Despite the prevalence of public announcements of data breach and data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

Defendant Had a Duty to Plaintiffs and Class Members to Secure PII

54. At all relevant times, Defendant had a duty to Plaintiffs and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to *promptly* notify Plaintiffs and Class Members when Defendant became aware that their PII may have been compromised.

55. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and the Plaintiffs and the Class Members, on the other hand. The special relationship arose because Plaintiffs and the Members of the Class relied on Defendant to secure their PII when they entrusted Defendant with the information required to obtain Defendant's services.

56. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect Customers' PII. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

57. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

58. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[9]

59. The ramifications of Defendant's failure to keep its Customers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of PII

[8] 17 C.F.R. § 248.201 (2013).
[9] *Id.*

60. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[11]

61. As a growing number of federal courts have begun to recognize the loss of value of PII as a viable damages theory, the sale of PII from data breaches, as in the Data Breach alleged herein, is particularly harmful to data breach victims – especially when it takes place on the dark web.

62. The dark net is an unindexed layer of the internet that requires special software or authentication to access.[12] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is

[10] *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 Aug. 4, 2023).
[11] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed December 10, 2021).
[12] *What Is the Dark Web?,* Experian, *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/

ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[13] This prevents dark web marketplaces from being easily identifiable to authorities or those not in the know.

63. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[14] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth and medical information.[15] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others." [16]

64. Plaintiffs and Class Members' PII is a valuable commodity, a market exists for Plaintiffs and Class Members' PII (which is why the Data Breach was perpetrated in the first place), and Plaintiffs and Class Members' PII is being likely being sold by hackers on the dark web (as that is the *modus operandi* of data thieves) – as a result, Plaintiffs and Class Members have lost the value of their PII, which is sufficient to plausibly allege injury arising from a data breach.

65. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[17] In fact, the data marketplace is so

[13] *Id.*
[14] *What is the Dark Web?* – Microsoft 365, *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web
[15] *Id.*; *What Is the Dark Web?,* Experian, *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/
[16] *What is the Dark Web?* – Microsoft 365, *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web
[17] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[18][19] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[20]

66. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[21] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[22]

67. Cyber criminals seek out PHI at greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient records exposed.[23] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[24]

68. PII and PHI are valuable property rights.[25] Their value as a commodity is measurable.[26] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory

---

[18] https://datacoup.com/
[19] https://worlddataexchange.com/about
[20] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed Aug. 4, 2023).
[21] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data*") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").
[22] *Id*.
[23] *See* PROTENUS, *2023 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last visited Oct. 2, 2023).
[24] *Id*.
[25] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.
[26] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

frameworks."[27] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[28] It is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

69. According to a report released by the Federal Bureau of Investigation's (FBI) Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[29]

70. Criminals can use stolen PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[30] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[31]

71. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and

[27] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.
[28] *See* IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.
[29] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[30] *What Happens to Stolen Healthcare Data*, *supra* note 20.
[31] *Id.*

accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[32]

72. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Defendant Fails to Comply with FTC Guidelines

73. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

74. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[33]

75. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[34]

---

[32] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable /23015560?seq=1.

[33] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 2, 2023).

[34] *Id.*

76. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on 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.

77. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

78. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

79. Defendant failed to properly implement basic data security practices.

80. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

81. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its customers, Defendant was also aware of the

significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendant Fails to Comply with Industry Standards

82. Several best practices have been identified that, at a minimum, should be implemented by entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

83. Other best cybersecurity practices that are standard in the industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protecting physical security systems; protecting against any possible communication system; and training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failing to train staff.

84. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

85. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and upon information and belief, Defendant failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Theft of Private Information Has Grave and Lasting Consequences for Victims

86. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[35]

87. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[36] Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[37]

88. With access to an individual's Private Information, criminals can do more than just empty a victim's bank account—they can also commit all manners of fraud, including: obtaining

[35] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Oct. 2, 2023).

[36] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[37] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security number to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.[38]

89. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[39]

90. Theft of Private Information is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[40] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[41] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use Private Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [42] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[43]

Theft of Private Information Has Grave and Lasting Consequences for Victims

[38] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Oct. 2, 2023).
[39] *See* Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited Oct. 2, 2023).
[40] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[41] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk…*, *supra* note 23.
[42] *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 Oct. 2, 2023).
[43] *Id*.

91. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services neither sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime. For example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; and victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[44]

92. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[45]

93. It is within this context that Plaintiffs and Class members must now live with the knowledge that their Private Information is forever in cyberspace and was taken by and in the

[44] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* note 39.
[45] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

possession of people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Common Injuries and Damages

94. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class members has materialized and is present and continuing, and Plaintiffs and Class members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' Private Information.

The Data Breach Increases Victims' Risk Of Identity Theft

95. Plaintiffs and Class members are at a heightened risk of identity theft for their lifetimes.

96. The unencrypted Private Information of Class members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class members.

97. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

98. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

99. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or Phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victims.

100. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[46]

[46] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-

101. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

102. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

103. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the Data Breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiffs and the other Class members.

104. Thus, even if certain information (such as driver's license numbers) was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package.

105. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

106. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the

](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on Oct. 2, 2023).

dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

107. Plaintiffs and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach as well as monitoring their accounts for any indication of fraudulent activity, which may take years to detect.

108. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[47]

109. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[48]

Future Cost Of Credit And Identity Theft Monitoring Is Reasonable And Necessary

110. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, upon

[47] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[48] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Oct. 2, 2023).

information and belief, entire batches of stolen information have been placed on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

111. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

112. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[49] The information disclosed in this Data Breach is impossible to "close" and impossible, to change (such as genetic markers).

113. Consequently, Plaintiffs and Class members are at a present and continuous risk of fraud and identity theft for the remainder of their lives.

114. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class member. This is a reasonable and necessary cost to monitor to protect Class members from the risk of identity theft that arose from the Data Breach. This is a future cost that

[49] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

Plaintiffs and Class members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss Of The Benefit Of The Bargain

115. Furthermore, Defendant's poor data security deprived Plaintiffs and Class members of the benefit of their bargain. When agreeing to pay Defendant for products and/or services, reasonable consumers, including Plaintiffs and Class members, understood and expected that they were, in part, paying for the service that provided the necessary data security to protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Monica Santana's Experience

116. Plaintiff Santana is a customer of Defendant. Defendant provided Plaintiff with insight into diseases and familial matches as a result of an analysis of Plaintiffs' genome.

117. As a condition to utilize Defendant's services, Plaintiff was required to provide and did provider her PII to Defendant as a condition of receiving services with Defendant. Plaintiff was further required to provide a DNA sample for analysis.

118. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

119. At the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

120. Subsequent to the Data Breach, Plaintiff has suffered numerous, substantial injuries including, but not limited to: (i) lost or diminished value of her Private Information; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) invasion of privacy; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

121. Plaintiff also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy and PHI, being in the hands of criminals.

122. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

123. As a result of the Data Breach, Plaintiffs anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

124. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

125. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Paula Kleynburd's Experience

126. Plaintiff Kleynburd is a customer of Defendant. Defendant provided Plaintiff with insight into diseases and familial matches as a result of an analysis of Plaintiff's genome.

127. As a condition to utilize Defendant's services, Plaintiff was required to provide and did provider her PII to Defendant as a condition of receiving services with Defendant. Plaintiff was further required to provide a DNA sample for analysis.

128. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

129. At the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

130. Subsequent to the Data Breach, Plaintiff has suffered numerous, substantial injuries including, but not limited to: (i) lost or diminished value of her Private Information; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) invasion of privacy; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

131. Plaintiff also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy and PHI, being in the hands of criminals.

132. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

133. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

134. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

135. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ACTION ALLEGATIONS

136. Plaintiffs bring this suit on behalf of themselves and a class of similarly situated individuals under Federal Rule of Civil Procedure 23, which is preliminarily defined as:

> All persons whose PII or PHI was compromised in the Data Breach by unauthorized persons. (the "Class").

137. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

138. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, it is likely that hundreds, if not thousands, of individuals had their PII compromised in this Data Breach, given the Defendant operates in over 100 markets in the United States. The identities of

Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

139. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

i. Whether 23andMe failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

ii. Whether 23andMe had a duty not to disclose the Private information of Plaintiffs and Class members to unauthorized third parties;

iii. Whether 23andMe failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' Private Information;

iv. Whether 23andMe breached a fiduciary duty to Plaintiffs and Class Members when it failed to protect their Private Information;

v. Whether 23andMe was unjustly enriched when it did not provide adequate data security in return for the benefit Plaintiffs and Class members provided;

vi. Whether 23andMe breached its duties to protect Plaintiffs' and Class members' Private Information; and

vii. Whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.

140. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class member, was compromised in the Data Breach.

141. Adequacy of Representation. Plaintiffs will fairly and adequately represent and

protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

142. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

143. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

144. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

145. Likewise, particular issues under Federal Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which

would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

i. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

ii. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

iii. Whether Defendant's failure to institute adequate protective security measures amounted to negligence; and

iv. Whether Defendant failed to take commercially reasonable steps to safeguard PII,

146. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and all Class Members)

147. Plaintiffs hereby repeats and realleges all preceding paragraphs contained herein.

148. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' PII for pecuniary gain, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

149. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' PII.

150. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed. The harm that Plaintiffs and Class Members experienced was within the zone of foreseeable harm known to Defendant.

151. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between each Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII, a mandatory step in receiving services from Defendant. While this special relationship exists independent from any contract, it is recognized by Defendant's privacy practices, as well as applicable laws and regulations. Specifically, Defendant actively solicited and gathered PII as part of their businesses and were solely responsible for and in the position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a resulting data breach.

152. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs and the Class, to maintain adequate data security.

153. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices and the frequency of data breaches in general.

154. Defendant also had a common law duty to prevent foreseeable harm to others. Plaintiffs and the Class were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems. It was

foreseeable that Plaintiffs and Class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

155. Defendant's conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendant's wrongful conduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decision not to comply with industry standards for the safekeeping of Plaintiffs' and the Class's PII, including basic encryption techniques available to Defendant.

156. Plaintiffs and the Class had and have no ability to protect their PII that was in, and remains in, Defendant's possession.

157. Defendant was in a position to effectively protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

158. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

159. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' PII within Defendant's possession.

160. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' PII.

161. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

162. Defendant's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' PII to be compromised.

163. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), Defendant had a separate and independent duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII.

164. The FTCA is intended, in part, to protect individuals whose PII is maintained by another and who are unable to safeguard their information as they cannot exercise control or direction over the data security practices.

165. Plaintiffs and the members of the Class are within the class of persons that the FTCA was intended to protect as their PII was collected and maintained by Defendant and they were unable to exercise control over Defendant's data security practices.

166. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against.

167. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the members of the Class.

168. Defendant breached its duties to Plaintiffs and the members of the Class under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

169. Had Plaintiffs and the members of the Class known that Defendant would not adequately protect their Private Information, Plaintiffs and the members of the Class would not have entrusted Defendant with their Private Information.

170. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

171. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and the members of the Class, they would not have been injured.

172. The injury and harm suffered by Plaintiffs and the members of the Class was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiffs and the members of the Class to experience the foreseeable harms associated with the exposure of their Private Information.

173. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and

future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the current and former employees' PII in their continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class Members.

174. As a direct and proximate result of Defendants' negligence and negligence per se, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

175. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

176. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs and the Class are now at an increased risk of identity theft or fraud.

177. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and all Class Members)

178. Plaintiffs hereby repeats and realleges all preceding paragraphs contained herein.

179. Plaintiffs and the Class entrusted their PII to Defendant as a condition of receiving Defendant's services. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

180. At the time Defendant acquired the PII of Plaintiffs and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

181. Implicit in the agreements between Plaintiffs and Class Members and Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

182. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

183. Defendant breached the implied contracts they made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information

of Plaintiffs and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

184. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

185. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT III
INVASION OF PRIVACY – INTRUSION UPON SECLUSION

186. Plaintiffs hereby repeats and realleges all preceding paragraphs contained herein.

187. Plaintiffs and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access, as occurred with the Data Breach.

188. Plaintiffs and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

189. Defendant intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their PII to a third party. Defendant's acts and omissions giving rise to the Data Breach were intentional in that the decisions to implement lax security and failure to timely notice Plaintiffs and the Class were undertaking willfully and intentionally.

190. By failing to keep Plaintiffs' and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

191. This invasion of privacy resulted from Defendant's intentional failure to properly secure and maintain Plaintiffs' and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded and private data.

192. Plaintiffs' and Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' and Class Members' PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

193. The disclosure of Plaintiffs' and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

194. Defendant's willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiffs' and Class Members' sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

195. The unauthorized access, exfiltration, and disclosure of Plaintiffs' and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

196. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT IV
UNJUST ENRICHMENT

197. Plaintiffs hereby repeats and realleges all preceding paragraphs contained herein.

198. This Count is brought in the alternative to Count II, Breach of Implied Contract.

199. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. In so conferring this benefit, Plaintiffs and Class Members understood that part of the benefit Defendant derived from the PII would be applied to data security efforts to safeguard the PII.

200. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII.

201. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense

of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

202. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

203. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

204. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

205. Plaintiffs and Class Members have no adequate remedy at law.

206. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to

prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

207. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

208. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

COUNT V
DECLARATORY JUDGMENT
(On behalf of Plaintiffs and all Class Members)

209. Plaintiffs hereby repeats and realleges all preceding paragraphs contained herein.

210. Defendant owes duties of care to Plaintiffs and Class Members that require Defendant to adequately secure their PII.

211. Defendant still possess Plaintiffs' and Class Members' PII.

212. Plaintiffs and Class Members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

213. Plaintiffs, therefore, seeks a declaration that (1) Defendant's existing security measures do not comply with its duties of care to provide reasonable security procedure and practices appropriate to the nature of the information to protect customers' PII, and (2) to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to

promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiffs and Class Members for a period of ten years; and

h. Meaningfully educating Plaintiffs and Class Members about the threats they face as a result of the loss of their PII and PHI to third parties, as well as the steps they must take to protect themselves.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class defined herein, prays for judgment as against Defendant as follows:

a.) For an Order certifying this action as a Class action and appointing Plaintiffs and her counsel to represent the Class;

b.) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c.) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Breach;

d.) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e.) Ordering Defendant to pay for lifetime credit monitoring services for Plaintiffs and the Class;

f.) For an award of actual damages, compensatory damages, statutory damages and statutory penalties, in an amount to be determined, as allowable by law;

g.) For an award of punitive damages, as allowable by law;

h.) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i.) Pre- and post-judgment interest on any amounts awarded and,

j.) All such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs hereby demands a trial by jury.

DOCUMENT PRESERVATION DEMAND

Plaintiffs demands that Defendant take affirmative steps to preserve all records, lists, electronic databases, or other itemization of telephone numbers associated with the communications or transmittal of the calls as alleged herein.

DATED: October 9, 2023

Respectfully submitted,

By: *Scott Edelsberg*
Scott Edelsberg (CA Bar No. 330990)
EDELSBERG LAW, P.A.
1925 Century Park E #1700
Los Angeles, CA 90067
Telephone: 305-975-3320
scott@edelsberglaw.com

Andrew J. Shamis *
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 400
Miami, FL 33132
Telephone: 305-479-2299
ashamis@shamisgentile.com

Attorneys for Plaintiffs and the Putative Classes
** Pro Hac Vice Forthcoming*