Cari Campen Laufenberg (*pro hac vice*)
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel: (206) 623-1900
claufenberg@kellerrohrback.com

Gayle M. Blatt (SBN 122048)
CASEY GERRY SCHENK FRANCAVILLA
BLATT & PENFIELD LLP
110 Laurel Street
San Diego, CA 92101
Tel: (619) 238-1811
gmb@cglaw.com

Norman E. Siegel (*pro hac vice*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road
Suite 200
Kansas City, MO 64112
Tel: 816 714-7100
siegel@stuevesiegel.com

Co-Lead Counsel

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

IN RE: 23ANDME, INC. CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates to: ALL ACTIONS	MDL No. 3098 Master Case No. 3:24-md-03098-EMC **JUDGE EDWARD M. CHEN**

CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

I. INTRODUCTION

1. Plaintiffs, individually and on behalf of all others similarly situated, bring this action against Defendant 23andMe, Inc. ("23andMe" or "Defendant") as victims of a targeted cyberattack on 23andMe that was announced on October 6, 2023. Plaintiffs' and Class Members' most sensitive personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information")—including but not limited to name, sex, date of birth, genetic information, predicted relationships with genetic matches, ancestry reports, ancestors' birth locations and family names, family tree information, profile pictures, and geographic location—was compromised and exfiltrated in the data breach announced by 23andMe on October 6, 2023 (the "Data Breach").[1] Plaintiffs bring this action against Defendant 23andMe for its failure to properly secure and safeguard the Private Information of themselves and all those similarly situated, seeking monetary damages, restitution, and/or injunctive relief.

2. 23andMe collects and maintains the genetic information of its customers—one of, if not the most, personal and highly sensitive forms of personally identifiable information and protected health information in existence. 23andMe profits from the highly sensitive Private Information that it collects and maintains, including through providing direct-to-consumer genetic testing services. 23andMe recognizes that it has an enormous responsibility to protect this highly sensitive Private Information, and it assures consumers through its Privacy and Data Protection statement that 23andMe "exceed[s] industry data protection standards and ha[s] achieved three different ISO certifications to demonstrate the strength of [its] security program."[2] Likewise, its Privacy and Data Protection statement acknowledges that its consumers "entrust us with important Private Information," that "since day one, protecting your privacy has been our number one priority," and that 23andMe is "committed

[1] 23andMe, Inc., *Addressing Data Security Concerns*, 23andMe Blog (Dec. 5, 2023), https://web.archive.org/web/20231206145806/https://blog.23andme.com/articles/addressing-data-security-concerns; *see also* Lily Hay Newman, *23andMe User Data Stolen in Targeted Attack on Ashkenazi Jews*, Wired (Oct. 6, 2023), https://www.wired.com/story/23andme-credential-stuffing-data-stolen.

[2] 23andMe, Inc., *Addressing Data Security Concerns*, 23andMe Blog (Oct. 6, 2023), https://web.archive.org/web/20231007110808/https://blog.23andme.com/articles/addressing-data-security-concerns.

to providing you with a safe place where you can learn about your DNA knowing your privacy is protected."[3] However, 23andMe completely failed to meet these promises and responsibilities to protect the Private Information of millions of its customers.

3. Instead, 23andMe suffered a massive Data Breach in which the most highly sensitive Private Information of approximately seven million of its customers was compromised. Cybercriminals specifically targeted Plaintiffs' and Class Members' genetic and ancestral information and posted it for sale on the dark web.

4. Among those specifically targeted for sale on the dark web are the 23andMe customers of Chinese and Ashkenazi Jewish descent, who face particularly acute dangers on account of being targeted because of antisemitism and anti-Asian ideologies.

5. The following allegations are made upon information and belief derived from, among other things, investigation of counsel, public sources, and the facts and circumstances as currently known. Because only 23andMe (as well as the cybercriminals who perpetrated the Data Breach) have knowledge of the totality of the information compromised, Plaintiffs reserve the right to supplement these allegations with additional facts and injuries as they are discovered.

II. JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Defendant is a citizen of states different from that of at least one Class Member. This Court also has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

7. This Court has personal jurisdiction over 23andMe because 23andMe is headquartered in California, within this District; 23andMe has its principal place of business in Santa Clara County, California, within this District; and 23andMe is authorized to and regularly conducts business in the State of California, including by selling, marketing, and advertising its products and services to Class

[3] 23andMe, Inc., *Your privacy comes first*, https://www.23andme.com/privacy/ (last visited June 20, 2024).

Members located in the State of California and within this District. 23andMe therefore has sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary.

8. Venue is proper in this District pursuant to 28 U.S.C. § 1407 and the April 11, 2024, Transfer Order of the Judicial Panel on Multidistrict Litigation in MDL 3098 or, in the alternative, pursuant to 28 U.S.C. § 1391(a) through (d) because 23andMe's principal place of business is located in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District.

III. DEFENDANT

9. Defendant 23andMe, Inc. is a business incorporated under the laws of the state of Delaware with its principal place of business in California, at 223 North Mathilda Avenue in Sunnyvale, California 94086. 23andMe is a genetic testing company that designs its products in California, and its marketing efforts emanate from California.

10. As of March 31, 2023, 23andMe cumulatively possesses and stores the Private Information of over 14.1 million people in its databases.[4] This Private Information includes genetic information provided by individuals since 2006 in connection with the company's "Personal Genome Service" business, which purports to provide consumers "with a broad suite of genetic reports, including information on customers' genetic ancestral origins, personal genetic health risks, and chances of passing on certain rare carrier conditions to their children, as well as reports on how genetics can impact responses to medication."[5]

IV. PLAINTIFFS

11. Plaintiffs are individuals who had their Private Information exfiltrated and compromised in the Data Breach. Plaintiffs bring this action on behalf of themselves and all those similarly situated both across the United States and within their State of residence.

12. Plaintiffs place significant value in the security of their Private Information. Plaintiffs entrusted their Private Information to 23andMe with the understanding that 23andMe would keep their Private Information secure and employ reasonable and adequate security measures to ensure that it

[4] 23andMe Holding Co., Annual Report (Form 10-K) (May 25, 2023) ("FY 2022 10-K") at 69.
[5] *Id.* at 92.

would not be compromised. Had Plaintiffs known of 23andMe's lax security practices with respect to Private Information, they would not have entrusted their Private Information to 23andMe.

ALASKA

Susan Kennedy

13. Plaintiff Susan Kennedy is a resident of the State of Alaska and is a customer of 23andMe.

14. Plaintiff Kennedy purchased a 23andMe DNA kit in or around 2014 and provided a sample of her genetic material to 23andMe for testing.

15. Plaintiff Kennedy opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

16. Plaintiff Kennedy was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Kennedy's Private Information was maintained by 23andMe.

17. Plaintiff Kennedy was notified by 23andMe on or about October 11, 2023 that her Private Information was compromised in the Data Breach.

18. As a result of the data breach, Plaintiff Kennedy invested significant time and resources to address the incident. Specifically, she verified the legitimacy of the breach, monitored her 23andMe and other accounts for fraudulent activity, enabled multi-factor authentication on these accounts, changed her passwords, and researched the disclosed information to understand its potential misuse.

19. After the Data Breach, Plaintiff Kennedy experienced a significant increase in spam and phishing calls, texts, and emails.

20. Plaintiff Kennedy places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Kennedy entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Kennedy would not have entrusted her Private Information to 23andMe had she

known of 23andMe's lax data security policies.

21. Plaintiff Kennedy is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Kennedy has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life.

22. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Kennedy has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

23. As a result of the Data Breach, Plaintiff Kennedy is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Kennedy therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

24. Plaintiff Kennedy has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

Samantha Van Vleet

25. Plaintiff Samantha Van Vleet is a resident of the State of Alaska and is a customer of 23andMe.

26. Plaintiff Van Vleet purchased a 23andMe DNA kit in or around 2015 and provided a sample of her genetic material to 23andMe for testing.

27. Plaintiff Van Vleet opted out of the arbitration provisions of 23andMe's Terms and

Conditions using 23andMe's opt out procedure.

28. Plaintiff Van Vleet was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Van Vleet's Private Information was maintained by 23andMe.

29. Plaintiff Van Vleet was notified by 23andMe on or about October 23, 2023 that her Private Information was compromised in the Data Breach.

30. As a result of the data breach, Plaintiff Van Vleet invested significant time and resources addressing the incident. Specifically, she verified the breach's legitimacy, monitored her 23andMe and other accounts for fraudulent activity, enabled multi-factor authentication on these accounts, changed her passwords, researched the nature of the disclosed information and its potential misuse, and informed her family members about the breach.

31. After the Data Breach, Plaintiff Van Vleet experienced a significant increase in spam and phishing calls, texts, and emails.

32. Plaintiff Van Vleet places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Van Vleet entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Van Vleet would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

33. Plaintiff Van Vleet is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Van Vleet has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential

and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life.

34. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Van Vleet has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

35. As a result of the Data Breach, Plaintiff Van Vleet is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Van Vleet therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

36. Plaintiff Van Vleet has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

CALIFORNIA

Lenora Claire

37. Plaintiff Lenora Claire is a resident of the State of California and is a customer of 23andMe.

38. Plaintiff Claire purchased a 23andMe DNA kit in or around late 2013 and provided a sample of her genetic material to 23andMe for testing.

39. Plaintiff Claire was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Claire's Private Information was maintained by 23andMe.

40. Plaintiff Claire was notified by 23andMe in or around late 2023 that her Private Information was compromised in the Data Breach.

41. As a result of the Data Breach, Plaintiff Claire spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Claire spent time: (1) verifying the legitimacy of

the Data Breach; (2) monitoring her 23andMe and other accounts for fraudulent activity; (3) changing 23andMe and other account passwords; (4) researching what information was disclosed in this Data Breach and how it could be used against her; and (5) speaking with family members to inform them of the Data Breach.

42. After the Data Breach, Plaintiff Claire experienced attempted identity theft when, in December 2023, someone attempted to rent an apartment in another country using her name and a credit reporting bureau found a hard inquiry on her credit that she had not requested. As a result, she put a credit freeze on her account.

43. Plaintiff Claire places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Claire entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Claire would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

44. Plaintiff Claire is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Claire has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff Claire is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

45. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Claire has already suffered

injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

46. As a result of the Data Breach, Plaintiff Claire is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Claire therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

47. Plaintiff Claire has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

Daniel Pinho

48. Plaintiff Daniel Pinho is a resident of the State of California and is a customer of 23andMe.

49. Plaintiff Pinho purchased a 23andMe DNA kit in or around April 2020 and provided a sample of his genetic material to 23andMe for testing.

50. Plaintiff Pinho was required to provide his Private Information, including his name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Pinho's Private Information was maintained by 23andMe.

51. Plaintiff Pinho was notified by 23andMe on or about October 9, 2023 that his Private Information was compromised in the Data Breach.

52. As a result of the Data Breach, Plaintiff Pinho spent considerable time and money researching and responding to the Data Breach. In particular, Plaintiff Pinho spent time verifying the legitimacy of the Data Breach. He spent time monitoring his 23andMe and other accounts for fraudulent activity. He spent time looking at his credit reports from the three credit bureaus. He spent time enabling multi-factor authentication on 23andMe and spent time and money researching and purchasing identity theft protection services. Plaintiff Pinho purchased a monthly subscription of identity theft protection following the Data Breach. He spent time changing 23andMe and other account passwords as well as

enabling Google sign in. He spent time researching what information was disclosed in this Data Breach and how it could be used against him and spent time speaking with family members to inform them of the Data Breach.

53. After the Data Breach, Plaintiff Pinho began receiving a significant increase in spam and phishing emails.

54. Plaintiff Pinho places significant value in the security of his Private Information and has taken reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Pinho entrusted his Private Information to 23andMe and relied on 23andMe to keep his Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Pinho would not have entrusted his Private Information to 23andMe had he known of 23andMe's lax data security policies.

55. Plaintiff Pinho is very concerned about how the theft of his highly sensitive Private Information may impact him, including with respect to the security of his other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Pinho has also suffered fear, anxiety, and emotional distress as a result of the release of his Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing his Private Information, as well as on account of knowing that his highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against him for the rest of his. Additionally, Plaintiff Pinho is of a targeted ethnicity and is concerned he may be targeted by bad actors because his genetic data revealed his ethnicity.

56. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Pinho has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having his Private Information compromised in the Data Breach.

57. As a result of the Data Breach, Plaintiff Pinho is at a present risk and will continue to

be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Pinho therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

58. Plaintiff Pinho has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

Melissa Ryan

59. Plaintiff Melissa Ryan is a resident of the State of California and is a customer of 23andMe.

60. Plaintiff Ryan purchased a 23andMe DNA kit in or around 2014 and provided a sample of her genetic material to 23andMe for testing.

61. Plaintiff Ryan was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Ryan's Private Information was maintained by 23andMe.

62. Plaintiff Ryan was notified by 23andMe in or around October 2023 that her Private Information was compromised in the Data Breach.

63. As a result of the Data Breach, Plaintiff Ryan spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Ryan spent time monitoring her 23andMe and other accounts for fraudulent activity and checking credit reports, and spent time further inquiring about the scope of the Data Breach.

64. After the Data Breach, Plaintiff Ryan experienced actual and attempted identity theft and fraud, including a compromised bank account.

65. Plaintiff Ryan places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Ryan entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and

adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Ryan would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

66. Plaintiff Ryan is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Ryan has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life.

67. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Ryan has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

68. As a result of the Data Breach, Plaintiff Ryan is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Ryan therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

69. Plaintiff Ryan has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

David Tso

70. Plaintiff David Tso is a resident of the State of California and a customer of 23andMe.

71. Plaintiff Tso purchased a 23andMe DNA kit in or around October 2018 and provided a sample of his genetic material to 23andMe for testing. In addition, since his daughter was a minor at

the time, Mr. Tso had to register her account under his profile because she was not permitted to have an individual account. As of today, Mr. Tso's daughter is still a minor.

72. Plaintiff Tso was required to provide his and his minor child's Private Information, including their names, genders, dates of birth, birthplaces, geographic locations, and genetic materials, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Tso's and his minor child's Private Information were both maintained by 23andMe.

73. Plaintiff Tso was first notified by 23andMe about the Data Breach on or about October 10, 2023. A follow-up email from 23andMe on October 13, 2023, confirmed that his DNA Relatives profile was compromised in the Data Breach, which contains his and his minor child's Private Information.

74. As a result of the Data Breach, Plaintiff Tso spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Tso spent time verifying the legitimacy of the Data Breach, blocking spam calls and texts, changing passwords across his accounts, speaking with family members to inform them of the Data Breach, and monitoring his identity protection service and financial accounts for any signs of fraudulent activity.

75. After the Data Breach, Plaintiff Tso experienced a significant increase in spam, such as phishing calls, texts, and emails. Specifically, he received calls from strangers who spoke Mandarin Chinese to him without knowing him personally, indicating those strangers had a presumption that Plaintiff Tso was Chinese. Additionally, Plaintiff Tso received multiple alerts from Google, warning him that his passwords had been compromised due to a data breach.

76. Plaintiff Tso places significant value in the security of his and his family's Private Information and has taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff Tso entrusted his and his minor child's Private Information to 23andMe and relied on 23andMe to keep their Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Tso would not have entrusted their Private Information to 23andMe had he known of 23andMe's lax data security policies.

77. Plaintiff Tso is very concerned about how the theft of his and his minor child's highly

sensitive Private Information may impact them, including with respect to the security of Mr. Tso's other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Tso has also suffered fear, anxiety, and emotional distress as a result of the release of his and his minor child's Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing their Private Information, as well as on account of knowing that their highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against him for the rest of his life. Additionally, Plaintiff Tso and his minor child are of a targeted ethnicity and are concerned they may be targeted by bad actors because their genetic data revealed their ethnicity.

78. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Tso has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having their Private Information compromised in the Data Breach.

79. As a result of the Data Breach, Plaintiff Tso is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Tso, therefore, anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

80. Plaintiff Tso has a continuing interest in ensuring that his and his minor child's Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

CONNECTICUT

Bonnie Eden

81. Plaintiff Bonnie Eden is a resident of the State of Connecticut and is a customer of 23andMe.

82. Plaintiff Eden purchased a 23andMe DNA kit in or around March 2017 and provided a

sample of her genetic material to 23andMe for testing.

83. Plaintiff Eden was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Eden's Private Information was maintained by 23andMe.

84. Plaintiff Eden was notified by 23andMe in October of 2023 that her Private Information was compromised in the Data Breach.

85. As a result of the Data Breach, Plaintiff Eden spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Eden spent time verifying the legitimacy of the Data Breach; monitoring her 23andMe and other accounts for fraudulent activity; and researching what information was disclosed in this Data Breach and how it could be used against her.

86. After the Data Breach, Plaintiff Eden experienced a significant increase in phishing emails and phishing phone calls. Plaintiff Eden has received multiple notices that her information is on the dark web.

87. Plaintiff Eden places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Eden entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Eden would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

88. Plaintiff Eden is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Eden has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and

can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff Eden is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

89. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Eden has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

90. As a result of the Data Breach, Plaintiff Eden is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Eden therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

91. Plaintiff Eden has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

DELAWARE

Emily Beale

92. Plaintiff Emily Beale is a current resident of the State of Texas and is a customer of 23andMe. At the time of the Breach, Plaintiff Beale was a resident of the State of Delaware.

93. Plaintiff Beale received a 23andMe DNA kit in or around November 2021 as a gift and provided a sample of her genetic material to 23andMe for testing.

94. Plaintiff Beale was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Beale's Private Information was maintained by 23andMe.

95. Plaintiff Beale was notified by 23andMe on or about October 23, 2023 that her Private Information was compromised in the Data Breach.

96. As a result of the Data Breach, Plaintiff Beale spent considerable time and money researching and responding to the Data Breach. In particular, Plaintiff Beale spent time verifying the legitimacy of the Data Breach, spent time monitoring her 23andMe and other accounts for fraudulent activity, spent time and money purchasing identity theft protection services and dark web monitoring services, and spent time changing passwords on her 23andMe and other personal and financial accounts.

97. After the Data Breach, Plaintiff Beale experienced a significant increase in spam and phishing calls, texts, and emails.

98. Plaintiff Beale places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Beale entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Beale would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

99. Plaintiff Beale is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Beale has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life.

100. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Beale has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

101. As a result of the Data Breach, Plaintiff Beale is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Beale therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

102. Plaintiff Beale has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected, and safeguarded from future breaches.

FLORIDA

Harold Velez

103. Plaintiff Harold Velez is a resident of the State of Florida and is a customer of 23andMe.

104. Plaintiff Velez received a 23andMe DNA kit in or around December 2020 as a gift and provided a sample of his genetic material to 23andMe for testing.

105. Plaintiff Velez was required to provide his Private Information, including his name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Velez's Private Information was maintained by 23andMe.

106. Plaintiff Velez was notified by 23andMe on or about October 13, 2023 that his Private Information was compromised in the Data Breach.

107. As a result of the Data Breach, Plaintiff Velez spent considerable time and/or money researching and responding to the Data Breach. In particular, Plaintiff Velez spent time verifying the legitimacy of the Data Breach and researching its implications, and spent time speaking with family members to inform them of the Data Breach.

108. Plaintiff Velez places significant value in the security of his Private Information and has taken reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Velez entrusted his Private Information to 23andMe and relied on 23andMe to keep his Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this

information. Plaintiff Velez would not have entrusted his Private Information to 23andMe had he known of 23andMe's lax data security policies.

109. Plaintiff Velez is very concerned about how the theft of his highly sensitive Private Information may impact him, including with respect to the security of his other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Velez has also suffered fear, anxiety, and emotional distress as a result of the release of his Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing his Private Information, as well as on account of knowing that his highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against him for the rest of his life. Additionally, Plaintiff Velez is of a targeted ethnicity and is concerned he may be targeted by bad actors because his genetic data revealed his ethnicity.

110. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Velez has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having his Private Information compromised in the Data Breach.

111. As a result of the Data Breach, Plaintiff Velez is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Velez therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

112. Plaintiff Velez has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

GEORGIA

Jaime Kelly

113. Plaintiff Jaime Kelly is a resident of the State of Georgia and is a customer of 23andMe.

114. Plaintiff Kelly purchased a 23andMe DNA kit in approximately 2006 or 2007 and provided a sample of her genetic material to 23andMe for testing.

115. Plaintiff Kelly opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

116. Plaintiff Kelly was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Kelly's Private Information was maintained by 23andMe.

117. Plaintiff Kelly was notified by 23andMe on or about October 11, 2023 that her Private Information was compromised in the Data Breach.

118. As a result of the Data Breach, Plaintiff Kelly spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Kelly spent time verifying the legitimacy of the Data Breach, spent time monitoring her 23andMe and other accounts for fraudulent activity, spent time enabling multi-factor authentication for 23andMe, spent time changing her 23andMe account password, spent time researching what information was disclosed in this Data Breach and how it could be used against her, and spent time speaking with family members to inform them of the Data Breach.

119. After the Data Breach, Plaintiff Kelly experienced an increase in spam and phishing calls, texts, and emails. She also experienced one or more attempts to access accounts using her name.

120. Plaintiff Kelly places significant value in the security of her Private Information and has taken steps to maintain the confidentiality of her Private Information. Plaintiff entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Kelly would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

121. Plaintiff Kelly is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related

to the Private Information exposed in the Data Breach. Plaintiff Kelly has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life.

122. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Kelly has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

123. As a result of the Data Breach, Plaintiff Kelly is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Kelly therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

124. Plaintiff Kelly has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

R.T.

125. Plaintiff R.T. is a resident of the State of Georgia and is a customer of 23andMe.

126. Plaintiff R.T. purchased a 23andMe DNA kit in or around December 2022 and provided a sample of her genetic material to 23andMe for testing.

127. Plaintiff R.T. opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

128. Plaintiff R.T. was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff R.T.'s Private Information was maintained by 23andMe.

129. Plaintiff R.T. was notified by 23andMe on or about October 13, 2023, that her Private Information was compromised in the Data Breach.

130. As a result of the Data Breach, Plaintiff R.T. spent considerable time and money researching and responding to the Data Breach. In particular, Plaintiff R.T. spent time: verifying the legitimacy of the Data Breach; monitoring her 23andMe and other accounts for fraudulent activity; enabling multi-factor authentication on 23andMe and other accounts; changing 23andMe and other account passwords; researching what information was disclosed in this Data Breach and how it could be used against her; and speaking with family members to inform them of the Data Breach. Plaintiff R.T. also spent time and money researching and adding outdoor security lighting at her place of residence.

131. After the Data Breach, Plaintiff R.T. experienced attempted identity theft and fraud, which included receiving a significant increase in spam and phishing calls and emails.

132. Plaintiff R.T. places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff R.T. entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff R.T. would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

133. Plaintiff R.T. is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff R.T. has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally,

Plaintiff R.T. is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

134. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff R.T. has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

135. As a result of the Data Breach, Plaintiff R.T. is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff R.T. therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

136. Plaintiff R.T. has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

ILLINOIS

Michele Bacus

137. Plaintiff Michele Bacus is a resident of the State of Illinois and is a customer of 23andMe.

138. Plaintiff Bacus received her 23andMe DNA kit from Defendant in or around 2017 as consideration for participating in a study. Plaintiff Bacus provided a sample of her genetic material to 23andMe for testing.

139. Plaintiff Bacus opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

140. Plaintiff Bacus was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Bacus's Private Information was maintained by 23andMe.

141. Plaintiff Bacus was notified by 23andMe on or about October 11, 2023 and then again

on or about October 23, 2023 that her Private Information was compromised in the Data Breach.

142. As a result of the Data Breach, Plaintiff Bacus expended significant time and resources addressing its impact. Specifically, she devoted considerable effort to verifying the breach's legitimacy, monitoring her 23andMe and other accounts for fraudulent activity, and enabling multi-factor authentication on her 23andMe account. She also invested time in researching identity theft protection services, changing passwords for 23andMe and other accounts, investigating the nature and potential misuse of the disclosed information, and informing her family members about the breach.

143. After the Data Breach, Plaintiff Bacus experienced actual identity theft and fraud. She also encountered a significant increase in spam and phishing calls, texts, and emails, and received one or more notifications that her information was found on the dark web.

144. Plaintiff Bacus places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Bacus entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Bacus would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

145. Plaintiff Bacus is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Bacus has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her lives.

146. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Bacus has already suffered

injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

147. As a result of the Data Breach, Plaintiff Bacus is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Bacus therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

148. Plaintiff Bacus has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

Alexandra Hoffman

149. Plaintiff Alexandra Hoffman is a resident of the State of Illinois and is a customer of 23andMe.

150. Plaintiff Hoffman purchased a 23andMe DNA kit on or about September 8, 2022 and provided a sample of her genetic material to 23andMe for testing.

151. Plaintiff Hoffman opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

152. Plaintiff Hoffman was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Hoffman's Private Information was maintained by 23andMe.

153. Plaintiff Hoffman was notified by 23andMe on or about October 9, 2023 that her Private Information was compromised in the Data Breach.

154. As a result of the Data Breach, Plaintiff Hoffman spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Hoffman spent time verifying the legitimacy of the Data Breach, spent time monitoring her 23andMe and other accounts for fraudulent activity, spent time researching identity theft protection services, spent time changing 23andMe and other account passwords, spent time placing credit freezes with the three major credit reporting bureaus,

spent time researching what information was disclosed in this Data Breach and how it could be used against her, spent time removing her Private Information from public websites, and spent time speaking with family members to inform them of the Data Breach.

155. After the Data Breach, Plaintiff Hoffman experienced attempted identity theft and fraud, which included receiving a significant increase in spam and phishing calls, texts, and emails using her Private Information, as well as attempted fraud activity on one of her accounts.

156. Plaintiff Hoffman places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Hoffman entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Hoffman would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

157. Plaintiff Hoffman is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Hoffman has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff Hoffman is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

158. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Hoffman has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

159. As a result of the Data Breach, Plaintiff Hoffman is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Hoffman therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

160. Plaintiff Hoffman has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

Eileen Mullen

161. Plaintiff Eileen Mullen is a resident of the State of Illinois and is a customer of 23andMe.

162. Plaintiff Mullen purchased a 23andMe DNA kit in or around 2017 and provided a sample of her genetic material to 23andMe for testing.

163. Plaintiff Mullen was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Mullen's Private Information was maintained by 23andMe.

164. Plaintiff Mullen was notified by 23andMe on or about October 11, 2023, that her Private Information was compromised in the Data Breach.

165. As a result of the Data Breach, Plaintiff Mullen spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Mullen spent time monitoring her 23andMe and other accounts for fraudulent activity, enabling multi-factor authentication on 23andMe and other accounts, and changing 23andMe and other account passwords.

166. After the Data Breach, Plaintiff Mullen experienced attempted identity theft and fraud, which included receiving a significant increase in spam and phishing calls, texts, and emails and receiving several notifications that her information was found on the dark web.

167. Plaintiff Mullen places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Mullen entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information

confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Mullen would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

168. Plaintiff Mullen is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Mullen has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff Mullen is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

169. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Mullen has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

170. As a result of the Data Breach, Plaintiff Mullen is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Mullen therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

171. Plaintiff Mullen has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

MASSACHUSETTS

Anna DaVeiga

172. Plaintiff Anna DaVeiga is a resident of the State of Massachusetts and is a customer of 23andMe.

173. Plaintiff DaVeiga received a 23andMe DNA kit in or around December 2019 as a gift and provided a sample of her genetic material to 23andMe for testing.

174. Plaintiff DaVeiga was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff DaVeiga's Private Information was maintained by 23andMe.

175. Plaintiff DaVeiga was notified by 23andMe on or about October 13, 2023 that her Private Information was compromised in the Data Breach.

176. As a result of the Data Breach, Plaintiff DaVeiga spent considerable time and money researching and responding to the Data Breach. In particular, Plaintiff DaVeiga spent time verifying the legitimacy of the Data Breach and monitoring her 23andMe and other accounts for fraudulent activity. Plaintiff DaVeiga also spent time and money researching and registering for identity theft protection services and dark web monitoring services through her credit card company and credit union and spent time changing 23andMe and other financial account passwords.

177. After the Data Breach, Plaintiff DaVeiga experienced a significant increase in spam, phishing calls and emails.

178. Plaintiff DaVeiga places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff DaVeiga entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff DaVeiga would not have entrusted her Private Information to 23andMe had she known of 23andMe's inadequate data security policies.

179. Plaintiff DaVeiga is very concerned about how the theft of her highly sensitive Private

Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff DaVeiga has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff DaVeiga is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

180. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff DaVeiga has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

181. As a result of the Data Breach, Plaintiff DaVeiga is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff DaVeiga therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

182. Plaintiff DaVeiga has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected, and safeguarded from future breaches.

Neil Haven

183. Plaintiff Neil Haven is a resident of the State of Massachusetts and is a customer of 23andMe.

184. In or around August 2014, Plaintiff Haven received his 23andMe DNA kit from Defendant as consideration for participating in a study. Plaintiff Haven provided a sample of his genetic material to 23andMe for testing.

185. Plaintiff Haven opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

186. Plaintiff Haven was required to provide his Private Information, including his name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Haven's Private Information was maintained by 23andMe.

187. Plaintiff Haven was first notified by 23andMe on or about October 11, 2023 that his Private Information was compromised in the Data Breach.

188. As a result of the Data Breach, Plaintiff Haven spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Haven spent time verifying the legitimacy of the Data Breach, spent time monitoring his 23andMe and other accounts for fraudulent activity, spent time enabling multi-factor authentication on 23andMe, spent time changing his 23andMe account password, and spent time researching what information was disclosed in this Data Breach and how it could be used against him.

189. After the Data Breach, Plaintiff Haven experienced an increase in spam and phishing calls, texts, and emails.

190. Plaintiff Haven places significant value in the security of his Private Information and has taken steps to maintain the confidentiality of his Private Information. Plaintiff entrusted his Private Information to 23andMe and relied on 23andMe to keep his Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Haven would not have entrusted his Private Information to 23andMe had he known of 23andMe's lax data security policies.

191. Plaintiff Haven is very concerned about how the theft of his highly sensitive Private Information may impact him, including with respect to the security of his other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Haven has also suffered fear, anxiety, and emotional distress as a result of the release of his Private Information, including anxiety, concern,

and unease about unauthorized parties viewing, sharing, and misusing his Private Information, as well as on account of knowing that his highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against him for the rest of his life.

192. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Haven has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having his Private Information compromised in the Data Breach.

193. As a result of the Data Breach, Plaintiff Haven is at present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Haven therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

194. Plaintiff Haven has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

MARYLAND

Claire Paddy

195. Plaintiff Claire Paddy is a resident of the State of Maryland and is a customer of 23andMe.

196. Plaintiff Paddy purchased a 23andMe DNA kit in early 2018 and provided a sample of her genetic material to 23andMe for testing.

197. Plaintiff Paddy opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

198. Plaintiff Paddy was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Paddy's Private Information was maintained by 23andMe.

199. Plaintiff Paddy was first notified by 23andMe on or about October 11, 2023 that her Private Information was compromised in the Data Breach.

200. As a result of the Data Breach, Plaintiff Paddy spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Paddy spent time verifying the legitimacy of the Data Breach, spent time monitoring her 23andMe and other accounts for fraudulent activity, spent time enabling multi-factor authentication on 23andMe, spent time changing 23andMe account password, spent time researching what information was disclosed in this Data Breach and how it could be used against her, and spent time speaking with family members to inform them of the Data Breach.

201. After the Data Breach, Plaintiff Paddy experienced an increase in spam and phishing calls, texts, and emails.

202. Plaintiff Paddy places significant value in the security of her Private Information and has taken steps to maintain the confidentiality of her Private Information. Plaintiff entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Paddy would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

203. Plaintiff Paddy is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Paddy has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff Paddy is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

204. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Paddy has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

205. As a result of the Data Breach, Plaintiff Paddy is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Paddy therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

206. Plaintiff Paddy has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

MISSOURI

J.S.

207. Plaintiff J.S. is a resident of the State of Missouri and is a customer of 23andMe.

208. Plaintiff J.S. purchased a 23andMe DNA kit in or around 2020 and provided a sample of his genetic material to 23andMe for testing.

209. Plaintiff J.S. was required to provide his Private Information, including his name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff J.S.'s Private Information was maintained by 23andMe.

210. Plaintiff J.S. learned about the Data Breach from a news article that he read in or around October 2023.

211. As a result of the Data Breach, Plaintiff J.S. spent considerable time researching and responding to the Data Breach. In particular, Plaintiff J.S. spent time verifying the legitimacy of the Data Breach; spent time monitoring his 23andMe and other accounts for fraudulent activity; spent time changing 23andMe and other account passwords; spent time researching what information was disclosed in this Data Breach and how it could be used against him; and spent time speaking with

family members to inform them of the Data Breach.

212. After the Data Breach, Plaintiff J.S. experienced attempted identity theft and fraud, which included receiving a significant increase in spam and phishing calls, texts, and emails. He also received one or more notifications that his information was found on the dark web.

213. Plaintiff J.S. places significant value in the security of his Private Information and has taken reasonable steps to maintain the confidentiality of his Private Information. Plaintiff J.S. entrusted his Private Information to 23andMe and relied on 23andMe to keep his Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff J.S. would not have entrusted his Private Information to 23andMe had he known of 23andMe's lax data security policies.

214. Plaintiff J.S. is very concerned about how the theft of his highly sensitive Private Information may impact him, including with respect to the security of his other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff J.S. has also suffered fear, anxiety, and emotional distress as a result of the release of his Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing his Private Information, as well as on account of knowing that his highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against him for the rest of his life. Additionally, Plaintiff J.S. is of a targeted ethnicity and is concerned he may be targeted by bad actors because his genetic data revealed his ethnicity.

215. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff J.S. has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having his Private Information compromised in the Data Breach.

216. As a result of the Data Breach, Plaintiff J.S. is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information

disclosed in the Data Breach for years to come. Plaintiff J.S. therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

217. Plaintiff J.S. has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

NORTH CAROLINA

Pamela Zager-Maya

218. Plaintiff Pamela Zager-Maya is a resident of the State of North Carolina and is a customer of 23andMe.

219. Plaintiff Zager-Maya purchased a 23andMe DNA kit in or around 2018 and provided a sample of her genetic material to 23andMe for testing.

220. Plaintiff Zager-Maya opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

221. Plaintiff Zager-Maya was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Zager-Maya's Private Information was maintained by 23andMe.

222. Plaintiff Zager-Maya was notified by 23andMe on or about October 12, 2023 that her Private Information was compromised in the Data Breach.

223. As a result of the Data Breach, Plaintiff Zager-Maya spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Zager-Maya spent time verifying the legitimacy of the Data Breach; spent time monitoring her 23andMe and other accounts for fraudulent activity; spent time enabling multi-factor authentication on 23andMe; spent time researching what information was disclosed in this Data Breach and how it could be used against her; and spent time speaking with family members to inform them of the Data Breach.

224. After the Data Breach, Plaintiff Zager-Maya experienced attempted identity theft and fraud, including receiving multiple requests for unauthorized authentication to her email account; and

receiving a significant increase in spam and phishing calls, texts, and emails.

225. Plaintiff Zager-Maya places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Zager-Maya entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Zager-Maya would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

226. Plaintiff Zager-Maya is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Zager-Maya has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff Zager-Maya is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

227. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Zager-Maya has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

228. As a result of the Data Breach, Plaintiff Zager-Maya is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Zager-Maya therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

229. Plaintiff Zager-Maya has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

NEW JERSEY

M.L.

230. Plaintiff M.L. is a resident of the State of New Jersey and is a customer of 23andMe.

231. Plaintiff M.L. purchased a 23andMe DNA kit in or around 2019-2020 and provided a sample of her genetic material to 23andMe for testing.

232. Plaintiff M.L. opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

233. Plaintiff M.L. was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff M.L.'s Private Information was maintained by 23andMe.

234. Plaintiff M.L. was notified by 23andMe in or around October 2023 that her Private Information was compromised in the Data Breach.

235. As a result of the Data Breach, Plaintiff M.L. spent considerable time and money researching and responding to the Data Breach. In particular, Plaintiff M.L. spent time verifying the legitimacy of the Data Breach; spent time monitoring her 23andMe and other accounts for fraudulent activity; spent time cancelling her 23andMe account and changing other account passwords; spent time researching what information was disclosed in this Data Breach and how it could be used against her; spent time speaking with family members to inform them of the Data Breach; and spent time and money retaining and speaking with a therapist to discuss her fear and anxiety around the potential ramifications of this data breach.

236. After the Data Breach, Plaintiff M.L. experienced attempted identity theft and fraud, including receiving a significant increase in spam.

237. Plaintiff M.L. places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff M.L.

entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff M.L. would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

238. Plaintiff M.L. is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff M.L. has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff M.L. is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

239. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff M.L. has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

240. As a result of the Data Breach, Plaintiff M.L. is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff M.L. therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

241. Plaintiff M.L. has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

Rachel DeCarlo

242. Plaintiff Rachel DeCarlo is a resident of the State of New Jersey and is a customer of 23andMe.

243. Plaintiff DeCarlo purchased a 23andMe DNA kit in or around December 2016 and provided a sample of her genetic material to 23andMe for testing.

244. Plaintiff DeCarlo opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

245. Plaintiff DeCarlo was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff DeCarlo's Private Information was maintained by 23andMe.

246. Plaintiff DeCarlo was notified by 23andMe on or about October 11, 2023 that her Private Information was compromised in the Data Breach.

247. As a result of the Data Breach, Plaintiff DeCarlo spent considerable time researching and responding to the Data Breach. In particular, Plaintiff DeCarlo spent time verifying the legitimacy of the Data Breach. She spent time monitoring her 23andMe and other accounts for fraudulent activity which she continues to do on a regular basis. She spent time enabling multi-factor authentication on 23andMe and changing 23andMe and other account passwords. She spent time researching what information was disclosed in this Data Breach and how it could be used against her, as well as spending time speaking with family members to inform them of the Data Breach. In addition, Plaintiff DeCarlo spent time and money installing security cameras on the outside of her house following the Data Breach. Plaintiff DeCarlo also paid for a yearly subscription to view the camera footage in real time and spends time viewing the footage.

248. After the Data Breach, Plaintiff DeCarlo experienced a significant increase in phishing phone calls.

249. Plaintiff DeCarlo places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff DeCarlo entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information

confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff DeCarlo would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

250. Plaintiff DeCarlo is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff DeCarlo has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff DeCarlo is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

251. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff DeCarlo has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

252. As a result of the Data Breach, Plaintiff DeCarlo is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff DeCarlo therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

253. Plaintiff DeCarlo has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

A.B.

254. Plaintiff A.B. is a resident of the State of Pennsylvania and is a customer of 23andMe. At the time of the Breach, Plaintiff A.B. was a resident of the State of New Jersey.

255. Plaintiff A.B. received a 23andMe DNA kit in or around 2020 as a gift and provided a sample of her genetic material to 23andMe for testing.

256. Plaintiff A.B. opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

257. Plaintiff A.B. was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff A.B.'s Private Information was maintained by 23andMe.

258. Plaintiff A.B. initially learned about Data Breach from a news article around October 2023 and was subsequently notified by 23andMe in October of 2023 that her Private Information was compromised in the Data Breach.

259. As a result of the Data Breach, Plaintiff A.B. spent considerable time and money researching and responding to the Data Breach. In particular, Plaintiff A.B. spent time verifying the legitimacy of the Data Breach. She spent time monitoring her 23andMe and other accounts for fraudulent activity as well as spending time enabling multi-factor authentication on 23andMe. Plaintiff A.B. spent time researching identity theft protection services and dark web monitoring services and purchased DeleteMe for a yearly subscription. In addition, Plaintiff A.B. spent time changing 23andMe and other account passwords as well as spending time researching what information was disclosed in this Data Breach and how it could be used against her as well as speaking with family members to inform them of the Data Breach.

260. After the Data Breach, Plaintiff A.B. experienced a significant increase in spam and phishing emails. Plaintiff A.B. has received multiple notices that her information is on the dark web.

261. Plaintiff A.B. places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff A.B. entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information

confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff A.B. would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

262. Plaintiff A.B. is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff A.B. has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff A.B. is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

263. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff A.B. has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

264. As a result of the Data Breach, Plaintiff A.B. is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff A.B. therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

265. Plaintiff A.B. has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

NEW YORK

L.G.

266. Plaintiff L.G. is a resident of the State of New York and is a customer of 23andMe.

267. Plaintiff L.G. purchased a 23andMe DNA kit in or around October 2020 and provided a sample of her genetic material to 23andMe for testing.

268. Plaintiff L.G. opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

269. Plaintiff L.G. was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff L.G.'s Private Information was maintained by 23andMe.

270. Plaintiff L.G. was notified by 23andMe on or about October 13, 2023, that her Private Information was compromised in the Data Breach.

271. As a result of the Data Breach, Plaintiff L.G. spent considerable time and money researching and responding to the Data Breach. In particular, Plaintiff L.G. spent time verifying the legitimacy of the Data Breach; spent time monitoring her 23andMe and other accounts for fraudulent activity; spent time and money researching and purchasing identity theft protection services; spent time changing 23andMe and other account passwords; spent time researching what information was disclosed in this Data Breach and how it could be used against her; and spent time speaking with family members to inform them of the Data Breach.

272. Plaintiff L.G. places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff L.G. entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff L.G. would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

273. Plaintiff L.G. is very concerned about how the theft of her highly sensitive Private

Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff L.G. has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff L.G. is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

274. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff L.G. has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

275. As a result of the Data Breach, Plaintiff L.G. is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff L.G. therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

276. Plaintiff L.G. has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

Tracy Scott

277. Plaintiff Tracy Scott is a resident of the State of New York and is a customer of 23andMe.

278. Plaintiff Scott purchased a 23andMe DNA kit in or around December 2015 and provided a sample of her genetic material to 23andMe for testing.

279. Plaintiff Scott was required to provide her Private Information, including her name,

gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Scott's Private Information was maintained by 23andMe.

280. Plaintiff Scott was notified by 23andMe on or about October 23, 2023 that her Private Information was compromised in the Data Breach.

281. As a result of the Data Breach, Plaintiff Scott spent considerable time and money researching and responding to the Data Breach. In particular, Plaintiff Scott spent time verifying the legitimacy of the Data Breach, spent time monitoring her 23andMe account, spent time monitoring her life insurance account, spent time monitoring her financials accounts for fraudulent activity, purchasing identity theft protection services and dark web monitoring services, spent time changing 23andMe and other account passwords, spent time researching what information was disclosed in this Data Breach and how it could be used against her, and spent time speaking with family members to inform them of the Data Breach.

282. After the Data Breach, Plaintiff Scott experienced a significant increase in spam and phishing calls, texts, and emails.

283. Plaintiff Scott places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Scott entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Scott would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

284. Plaintiff Scott is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Scott has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well

as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff Scott is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

285. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Scott has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

286. As a result of the Data Breach, Plaintiff Scott is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Scott therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

287. Plaintiff Scott has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected, and safeguarded from future breaches.

OREGON

Cody Vogel

288. Plaintiff Vogel is a resident of the State of Oregon and is a customer of 23andMe.

289. Plaintiff received a 23andMe DNA kit in or around December 2017, as a gift and provided a sample of his genetic material to 23andMe for testing.

290. Plaintiff Vogel opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

291. Plaintiff Vogel was required to provide his Private Information, including his name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Vogel's Private Information was maintained by 23andMe.

292. Plaintiff Vogel was notified by 23andMe in or around October 2023, that his Private Information was compromised in the Data Breach.

293. As a result of the Data Breach, Plaintiff Vogel spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Vogel spent time monitoring his 23andMe and other accounts for fraudulent activity, enabling multi-factor authentication on 23andMe and other accounts, and changing 23andMe and other account passwords.

294. After the Data Breach, Plaintiff Vogel experienced attempted identity theft and fraud, including receiving a significant increase in spam and phishing calls, texts, and emails.

295. Plaintiff Vogel places significant value in the security of his Private Information and has taken reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Vogel entrusted his Private Information to 23andMe and relied on 23andMe to keep his Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Vogel would not have entrusted his Private Information to 23andMe had he known of 23andMe's lax data security policies.

296. Plaintiff Vogel is very concerned about how the theft of his highly sensitive Private Information may impact him, including with respect to the security of his other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Vogel has also suffered fear, anxiety, and emotional distress as a result of the release of his Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing his Private Information, as well as on account of knowing that his highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against him for the rest of his life.

297. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Vogel has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having his Private Information compromised in the Data Breach.

298. As a result of the Data Breach, Plaintiff Vogel is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Vogel therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

299. Plaintiff Vogel has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

Daniel Anderson

300. Plaintiff Daniel Anderson is a resident of the State of Oregon and is a customer of 23andMe.

301. Plaintiff Anderson received a 23andMe DNA kit as a gift in or around December 2018 and provided a sample of his genetic material to 23andMe for testing.

302. Plaintiff Anderson was required to provide his Private Information, including his name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Anderson's Private Information was maintained by 23andMe.

303. Plaintiff Anderson was first notified by 23andMe about the Data Breach on or about October 10, 2023. A follow-up email from 23andMe on or about October 24, 2023, confirmed that his Private Information was compromised in the Data Breach.

304. As a result of the Data Breach, Plaintiff Anderson spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Anderson spent time verifying the legitimacy of the Data Breach, changing passwords across his accounts, and monitoring his identity protection service and financial accounts for any signs of fraudulent activity.

305. After the Data Breach, Plaintiff Anderson experienced a significant increase in spam, such as phishing calls, texts, and emails. In addition, a stranger contacted him through the 23andMe platform, inquiring about his relations to others on the platform.

306. Plaintiff Anderson places significant value in the security of his Private Information and

has taken reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Anderson entrusted his Private Information to 23andMe and relied on 23andMe to keep his Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Anderson would not have entrusted his Private Information to 23andMe had he known of 23andMe's lax data security policies.

307. Plaintiff Anderson is very concerned about how the theft of his highly sensitive Private Information may impact him, including with respect to the security of his other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Anderson has also suffered fear, anxiety, and emotional distress as a result of the release of his Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing his Private Information, as well as on account of knowing that his highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against him for the rest of his life.

308. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Anderson has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having his Private Information compromised in the Data Breach.

309. As a result of the Data Breach, Plaintiff Anderson is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Anderson therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

310. Plaintiff Anderson has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

PENNSYLVANIA

Adriane Famer

311. Plaintiff Adriane Farmer is a resident of the State of Pennsylvania and is a customer of 23andMe.

312. Plaintiff Farmer purchased a 23andMe DNA kit in or around August 2021 and provided a sample of her genetic material to 23andMe for testing.

313. Plaintiff Farmer was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Farmer's Private Information was maintained by 23andMe.

314. Plaintiff Farmer was notified by 23andMe on or about October 13, 2023, that her Private Information was compromised in the Data Breach.

315. As a result of the Data Breach, Plaintiff Farmer spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Farmer spent time changing passwords, verifying the legitimacy of the Data Breach, and reviewing credit reports, financial account statements, and medical records for any indications of actual or attempted identity theft or fraud. She also switched her VPN provider and invested in additional security measures including antivirus software, Dark Web monitoring, and credit monitoring services.

316. After the Data Breach, Plaintiff Farmer experienced attempted identity theft and hacks to her email account, which included a significant increase in spam, phishing calls, texts, and emails. In order to stop the influx of spam, Plaintiff Farmer had to shut down her old email address. She also received notifications that her information was found on the dark web, and there were several unauthorized attempts to log into her email account that she used for the 23andMe website.

317. Plaintiff Farmer places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Farmer entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this

information. Plaintiff Farmer would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

318. Plaintiff Farmer is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Farmer has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff Farmer is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

319. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Farmer has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

320. As a result of the Data Breach, Plaintiff Farmer is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Farmer, therefore, anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

321. Plaintiff Farmer has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

TENNESSEE

Kristina Chew

322. Plaintiff Kristina Chew is a resident of the State of Tennessee and is a customer of

23andMe.

323. Plaintiff Chew purchased a 23andMe DNA kit in or around 2019 and provided a sample of her genetic material to 23andMe for testing.

324. Plaintiff Chew opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

325. Plaintiff Chew was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Chew's Private Information was maintained by 23andMe.

326. Plaintiff Chew was notified by 23andMe on or about October 11, 2023 that her Private Information was compromised in the Data Breach.

327. As a result of the Data Breach, Plaintiff Chew devoted significant time and resources to addressing its impact. Specifically, she spent time verifying the legitimacy of the Data Breach, monitoring her 23andMe and other accounts for fraudulent activity, enabling multi-factor authentication, changing passwords, and researching the exposed information and potential misuse.

328. After the Data Breach, Plaintiff Chew experienced a significant increase in spam and phishing calls, texts, and emails.

329. Plaintiff Chew places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Chew entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Chew would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

330. Plaintiff Chew is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Chew has also suffered fear, anxiety,

and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life.

331. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Chew has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

332. As a result of the Data Breach, Plaintiff Chew is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Chew therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

333. Plaintiff Chew has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

Britany Deloach

334. Plaintiff Britany Deloach is a resident of the State of Tennessee and is a customer of 23andMe.

335. Plaintiff Deloach purchased a 23andMe DNA kit in or around 2018 and provided a sample of her genetic material to 23andMe for testing.

336. Plaintiff Deloach opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

337. Plaintiff Deloach was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Deloach's Private Information was maintained by 23andMe.

338. Plaintiff Deloach was notified by 23andMe on or about October 11, 2023 that her Private Information was compromised in the Data Breach.

339. As a result of the data breach, Plaintiff Deloach invested significant time and resources addressing the incident. Specifically, she verified the breach's legitimacy, monitored her 23andMe and other accounts for fraudulent activity, enabled multi-factor authentication on these accounts, changed her passwords, researched the disclosed information to understand its potential misuse, and informed her family members about the breach.

340. After the data breach, Plaintiff Deloach experienced instances of actual fraud, including fraudulent activity on one of her accounts. She also experienced attempted identity theft and fraud, including a significant increase in spam and phishing calls, texts, and emails.

341. Plaintiff Deloach places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Deloach entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Deloach would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

342. Plaintiff Deloach is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Deloach has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life.

343. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Deloach has already suffered

injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

344. As a result of the Data Breach, Plaintiff Deloach is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Deloach therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

345. Plaintiff Deloach has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

TEXAS

Benjamin Woessner

346. Plaintiff Benjamin Woessner is a resident of the State of Texas and is a customer of 23andMe.

347. Plaintiff Woessner purchased a 23andMe DNA kit on or about December 11, 2012 and provided a sample of his genetic material to 23andMe for testing.

348. Plaintiff Woessner has opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedures.

349. Plaintiff Woessner was required to provide his Private Information, including his name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Woessner's Private Information was maintained by 23andMe.

350. Plaintiff Woessner was notified by 23andMe in or around October 2023 that his Private Information was compromised in the Data Breach.

351. As a result of the Data Breach, Plaintiff Woessner spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Woessner spent time verifying the legitimacy of the Data Breach, monitoring his 23andMe and other accounts for fraudulent activity, changing 23andMe and other account passwords, and researching what information was disclosed in this Data

Breach and how it could be used against him. Plaintiff Woessner also spent time speaking with family members to inform them of the Data Breach.

352. After the Data Breach, Plaintiff Woessner received notification that his Private information was found on the dark web.

353. Plaintiff Woessner places significant value in the security of his Private Information and has taken reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Woessner entrusted his Private Information to 23andMe and relied on 23andMe to keep his Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Woessner would not have entrusted his Private Information to 23andMe had he known of 23andMe's lax data security policies.

354. Plaintiff Woessner is very concerned about how the theft of his highly sensitive Private Information may impact him, including with respect to the security of his other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Woessner has also suffered fear, anxiety, and emotional distress as a result of the release of his Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing his Private Information, as well as on account of knowing that his highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against him for the rest of his life. Additionally, Plaintiff Woessner is of a targeted ethnicity and is concerned he may be targeted by bad actors because his genetic data revealed his ethnicity.

355. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Woessner has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having his Private Information compromised in the Data Breach.

356. As a result of the Data Breach, Plaintiff Woessner is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private

Information disclosed in the Data Breach for years to come. Plaintiff Woessner therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

357. Plaintiff Woessner has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

VIRGINIA

Thomas Vickery

358. Plaintiff Thomas Vickery is a resident of the State of Virginia and is a customer of 23andMe.

359. Plaintiff Vickery received a 23andMe DNA kit on or about July 15, 2023 as a gift and provided a sample of his genetic material to 23andMe for testing.

360. Plaintiff Vickery was required to provide his Private Information, including his name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Vickery's Private Information was maintained by 23andMe.

361. Plaintiff Vickery was notified by 23andMe on or about October 10, 2023 that his Private Information was compromised in the Data Breach.

362. As a result of the Data Breach, Plaintiff Vickery spent considerable time and money researching and responding to the Data Breach. In particular, Plaintiff Vickery spent time verifying the legitimacy of the Data Breach; spent time monitoring his 23andMe and other accounts for fraudulent activity; spent time enabling multi-factor authentication on 23andMe and other accounts; spent time and money researching and purchasing identity theft protection services; spent time changing 23andMe and other account passwords; spent time placing credit freezes with the three major credit reporting bureaus; researching what information was disclosed in this Data Breach and how it could be used against him; and spent time speaking with family members to inform them of the Data Breach.

363. After the Data Breach, Plaintiff Vickery experienced attempted identity theft and fraud, including one or more attempts to open unauthorized accounts using his Private Information.

364. Plaintiff Vickery places significant value in the security of his Private Information and has taken reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Vickery entrusted his Private Information to 23andMe and relied on 23andMe to keep his Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Vickery would not have entrusted his Private Information to 23andMe had he known of 23andMe's lax data security policies.

365. Plaintiff Vickery is very concerned about how the theft of his highly sensitive Private Information may impact him, including with respect to the security of his other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Vickery has also suffered fear, anxiety, and emotional distress as a result of the release of his Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing his Private Information, as well as on account of knowing that his highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against him for the rest of his life.

366. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Vickery has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having his Private Information compromised in the Data Breach.

367. As a result of the Data Breach, Plaintiff Vickery is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Vickery therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

368. Plaintiff Vickery has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

WASHINGTON

Tracie Payne Mitchell

369. Plaintiff Tracie Payne Mitchell is a resident of the State of Washington and is a customer of 23andMe.

370. Plaintiff Payne Mitchell received a 23andMe DNA kit on or about March 3, 2021 as a gift and provided a sample of her genetic material to 23andMe for testing.

371. Plaintiff Payne Mitchell was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Payne Mitchell's Private Information was maintained by 23andMe.

372. Plaintiff Payne Mitchell was notified by 23andMe on or about December 29, 2023 that her Private Information was compromised in the Data Breach.

373. As a result of the Data Breach, Plaintiff Payne Mitchell spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Payne Mitchell spent time verifying the legitimacy of the Data Breach, spent time monitoring her 23andMe and other accounts for fraudulent activity, and spent time contacting her bank to ensure her accounts were secure and placing credit freezes with the three major credit reporting bureaus.

374. After the Data Breach, Plaintiff Payne Mitchell experienced a significant increase in spam and phishing calls, texts, and emails. Also following the Data Breach, Plaintiff Payne Mitchell learned from a credit monitoring service supplied to her by one of her credit card companies that her Private Information was available on the dark web.

375. Plaintiff Payne Mitchell places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Payne Mitchell entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Payne Mitchell would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

376. Plaintiff Payne Mitchell is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Payne Mitchell has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff Payne Mitchell is of a targeted ethnicity and is concerned she may be targeted by bad actors because of her ethnicity.

377. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Payne Mitchell has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

378. As a result of the Data Breach, Plaintiff Payne Mitchell is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Payne Mitchell therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

379. Plaintiff Payne Mitchell has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

Camie Picha

380. Plaintiff Camie Picha is a resident of the State of Michigan and is a customer of 23andMe. At the time of the Breach, Plaintiff Picha was a resident of the State of Washington.

381. Plaintiff Picha purchased a 23andMe DNA kit in or around June 2022 and provided a sample of her genetic material to 23andMe for testing.

382. Plaintiff Picha opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

383. Plaintiff Picha was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain 23andMe's services. At the time of the Data Breach, Plaintiff Picha's Private Information was maintained by 23andMe.

384. Plaintiff Picha was notified by 23andMe on or about October 23, 2023 that her Private Information was compromised in the Data Breach.

385. As a result of the Data Breach, Plaintiff Picha spent considerable time and money researching and responding to the Data Breach. In particular, Plaintiff Picha spent time verifying the legitimacy of the Data Breach; spent time monitoring her 23andMe and other accounts for fraudulent activity; spent time and money researching and purchasing identity theft protection services; spent time changing 23andMe and other account passwords; spent time placing credit freezes with the three major credit reporting bureaus; and spent time researching what information was disclosed in this Data Breach and how it could be used against her.

386. After the Data Breach, Plaintiff Picha experienced attempted identity theft and fraud, including receiving a significant increase in spam and phishing calls, texts, and emails, as well as receiving notice that her information was found on the dark web.

387. Plaintiff Picha places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Picha entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Picha would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

388. Plaintiff Picha is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related

to the Private Information exposed in the Data Breach. Plaintiff Picha has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life.

389. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties and sale on the dark web, Plaintiff Picha has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

390. As a result of the Data Breach, Plaintiff Picha is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Picha therefore anticipates spending considerable time and money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

391. Plaintiff Picha has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

WISCONSIN

Kathleen Loftus

392. Plaintiff Kathleen Loftus is a resident of the State of Wisconsin and is a customer of 23andMe.

393. Plaintiff Loftus purchased a 23andMe DNA kit in or around December 2017 and provided a sample of her genetic material to 23andMe for testing.

394. Plaintiff Loftus opted out of the arbitration provisions of 23andMe's Terms and Conditions using 23andMe's opt out procedure.

395. Plaintiff Loftus was required to provide her Private Information, including her name, gender, date of birth, geographic location, and genetic material, to 23andMe in order to obtain

23andMe's services. At the time of the Data Breach, Plaintiff Loftus's Private Information was maintained by 23andMe.

396. Plaintiff Loftus was notified by 23andMe on or about October 13, 2023 that her Private Information was compromised in the Data Breach.

397. Plaintiff Loftus spent considerable time researching and responding to the Data Breach. In particular, Plaintiff Loftus spent time verifying the legitimacy of the Data Breach; spent time researching what information was disclosed in this Data Breach and how it could be used against her; spent time enabling multi-factor authentication; spent time speaking with family members to inform them of the Data Breach.

398. Plaintiff Loftus places significant value in the security of her Private Information and has taken reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Loftus entrusted her Private Information to 23andMe and relied on 23andMe to keep her Private Information confidential and secure, to use this information for business purposes only, to employ reasonable and adequate security measures to protect this information, and to make only authorized disclosures of this information. Plaintiff Loftus would not have entrusted her Private Information to 23andMe had she known of 23andMe's lax data security policies.

399. Plaintiff Loftus is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to the security of her other accounts, personal healthcare information, and the associated risks of identity theft, healthcare fraud, or other fraud related to the Private Information exposed in the Data Breach. Plaintiff Loftus has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life. Additionally, Plaintiff Loftus is of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity.

400. Given the highly-sensitive nature of the information stolen, and its subsequent

dissemination to unauthorized parties and sale on the dark web, Plaintiff Loftus has already suffered injury and remains at a substantial and imminent risk of future harm as a result of having her Private Information compromised in the Data Breach.

401. As a result of the Data Breach, Plaintiff Loftus is at a present risk and will continue to be at increased risk of identity theft and fraud, and other risks of harm unique to the Private Information disclosed in the Data Breach for years to come. Plaintiff Loftus therefore anticipates spending considerable time and/or money on an ongoing basis to attempt to mitigate and address harms caused by the Data Breach.

402. Plaintiff Loftus has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in 23andMe's possession, is protected and safeguarded from future breaches.

V. STATEMENT OF FACTS

A. 23andMe Collects, Stores, and Profits from Its Customers' Private Information and Promises to Keep It Secure.

403. 23andMe is a consumer genetics and research company, founded in 2006, that describes its mission as helping people access, understand, and benefit from the human genome. According to the "Corporate Profile" on its website, 23andMe "want[s] to disrupt the healthcare experience by building a personalized health and wellness experience that caters uniquely to the individual by harnessing the power of their DNA" and touts itself as having "pioneered direct access to genetic information" and being "the only company with multiple FDA clearances for genetic health reports."[6]

404. As stated in its last annual report filed with the U.S. Securities and Exchange Commission, as of March 31, 2023, 23andMe has approximately 14.1 million customers who have supplied their Private Information to the company.[7]

405. This Private Information includes PHI, which is considered "the most confidential and

[6] 23andMe, Inc., *Investor Relations*, https://investors.23andme.com (last visited June 20, 2024); *see also* 23andMe, Inc. Press Release, *23andMe Receives FDA Clearance for Direct-to-Consumer Genetic Test on a Hereditary Prostate Cancer Marker* (Jan. 10, 2022), https://investors.23andme.com/news-releases/news-release-details/23andme-receives-fda-clearance-direct-consumer-genetic-test.

[7] FY 2022 10-K at 69, *supra* note 4.

valuable type of PII . . . irrevocable once breached."[8] In this regard, an individual's unique and immutable genetic information is the most confidential and valuable form of PHI.

406. Similarly, this Private Information includes genetic information provided by individuals since 2006 in connection with the company's "Personal Genome Service" business, which aims to provide consumers "with a broad suite of genetic reports, including information on customers' genetic ancestral origins, personal genetic health risks, and chances of passing on certain rare carrier conditions to their children, as well as reports on how genetics can impact responses to medication."[9]

407. In order for 23andMe to offer its services to customers including Plaintiffs and Class Members, Plaintiffs and Class Members were required to transfer possession of their Private Information—including their personal genetic material—to 23andMe. 23andMe thereby acquires and electronically stores Private Information provided by its customers, and 23andMe was therefore required to ensure that Plaintiffs' and Class Members' Private Information was not disclosed or disseminated to unauthorized third parties.

408. Through the taking possession and use of Plaintiffs' and Class Members' Private Information—including their unique genetic information—23andMe assumed duties owed to Plaintiffs and Class Members to secure, maintain, protect, and safeguard that highly sensitive Private Information against unauthorized access and disclosure through reasonable and adequate security measures. 23andMe knew that it was responsible for safeguarding Plaintiffs' and Class Members' Private Information from unauthorized access and misuse.

409. 23andMe has publicly touted its data security and cybersecurity abilities, including

---

[8] Junyuan Ke et al., *My Data or My Health? Examining Patients' Response to a Healthcare Data Breach*, SSRN, 7 (Feb. 10, 2022), https://ssrn.com/abstract=4029103. (Under the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. §§ 1320d, et seq., PHI is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. *See also* 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered PHI under HIPAA, as are genetic data, national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information.) *See also Summary of the HIPAA Privacy Rule*, U.S. Dep't of Health & Human Servs. (2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[9] FY 2022 10-K at 92, *supra* note 4.

stating that the company "is committed to providing you with a safe and secure place where you can learn about your DNA knowing your privacy is protected" and that it "take[s] security seriously."[10]

410. 23andMe assures customers that "[y]our privacy comes first,"[11] stating: "When you explore your DNA with 23andMe, you entrust us with important personal information. That's why, since day one, protecting your privacy has been our number one priority. We're committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected."[12]

411. 23andMe's customers are also told that their genetic data will not be shared with third parties "without your explicit consent"; that "[y]our data is fiercely protected by security practices that are regularly reviewed and updated"; and the company is "doing everything in our power to keep your personal data safe."[13]

412. 23andMe was aware of methods that would provide necessary security that would safeguard its customers' highly sensitive data from unauthorized access and disclosure, including but not limited to requiring users to change their passwords frequently, requiring the use of "strong" passwords, and mandating the use of multi-factor authentication ("MFA") that would require its customers to provide more verification than just a single password to access their accounts. Indeed, 23andMe acknowledges that, while MFA "provides an extra layer of security and can prevent bad actors from accessing an account through recycled passwords," it only "offered and encouraged" use of MFA starting in 2019.[14]

413. 23andMe claims that it "is committed to providing you with a safe and secure place where you can learn about your DNA knowing your privacy is protected" and that it "take[s] security seriously."[15] Moreover, the company claims that:

> We exceed industry data protection standards and have achieved three different ISO certifications to demonstrate the strength of our security program. We actively and routinely monitor and audit our systems to ensure that your data is protected. When we receive information through those processes or from other sources claiming customer

[10] 23andMe Blog, *supra* note 2.
[11] 23andMe, Inc., *Your privacy comes first*, supra note 3.
[12] *Id.*
[13] *Id.*
[14] 23andMe Blog, *supra* note 2.
[15] *Id.*

> data has been accessed by unauthorized individuals, we immediately investigate to validate whether this information is accurate.[16]

414. Likewise, 23andMe promises that "Privacy is in our DNA," and Jacquie Haggarty, 23andMe's Vice President, General Counsel, and Privacy Officer, represents that: "We believe it's our responsibility to provide a safe place for people to explore their DNA," on account of which 23andMe's "commitment to privacy is built on a foundation of transparency and choice—our customers know that they are always in control of their data."[17]

415. 23andMe similarly recognizes that "[w]hen you explore your DNA with 23andMe, you entrust us with important personal information," and "since day one, protecting your privacy has been our number one priority."[18] 23andMe further reassures its customers that "[y]ou are in control of your data," and "you decide how your information is used and with whom it is shared."[19]

416. Plaintiffs and Class Members entrusted their Private Information to 23andMe, its officials, and agents. Plaintiffs and Class Members relied on 23andMe to keep their Private Information secure and safeguarded against unauthorized access and disclosure to unauthorized persons. 23andMe owed a duty to Plaintiffs and Class Members to secure their Private Information, and 23andMe breached that duty, as Plaintiffs' and Class Members' Private Information was compromised, unlawfully accessed, and exfiltrated due to the Data Breach.

B. Despite its Promises, 23andMe Failed to Protect Plaintiffs' Private Information.

417. Despite its promises, 23andMe and its employees failed to properly monitor the computer networks and systems in which the Private Information of Plaintiffs and Class Members was maintained, and failed to detect and prevent the Data Breach. Had 23andMe properly monitored its systems and employed appropriate security measures commensurate with the sensitivity of the Private Information, it would have either discovered the intrusion sooner or been able to prevent it entirely.

418. According to news reports, on or about August 11, 2023, "a hacker on a known

---

[16] *Id.*

[17] 23andMe, Inc., *What you should know about privacy at 23andMe*, https://web.archive.org/web/20240110065513/https://www.23andme.com/legal/privacy (last visited June 20, 2024).

[18] 23andMe, Inc., *Your privacy comes first*, *supra* note 3.

[19] *Id.*

cybercrime forum called Hydra advertised a set of 23andMe user data."[20] The hacker claimed "to have 300 terabytes of stolen 23andMe user data" that it would sell for $50 million, and offered to sell "a subset of data" for between $1,000 and $10,000.[21] The hacker also purportedly indicated that they had contacted 23andMe, "'but instead of taking the matter seriously, [the Company] asked irrelevant questions.'"[22] At least one person saw the hacker's August 11, 2023 post in the Hydra forum and sought to alert 23andMe users on an unofficial 23andMe user forum on Reddit that same day.[23]

419. For nearly two months, 23andMe did nothing in response to the August 11, 2023 Hydra and Reddit posts, leaving Plaintiffs and Class Members uninformed about the Data Breach, while their Private Information was offered for sale to criminals on the dark web, and unauthorized parties accessed and viewed Plaintiffs' and Class Members' unencrypted, unredacted Private Information, including their highly sensitive genetic data.

420. In early October 2023, 23andMe user data misappropriated in the Data Breach appeared for sale on another hacking forum called BreachForums, including data that was claimed to come from "one million 23andMe users of Jewish Ashkenazi descent and 100,000 23andMe Chinese users."[24] Subsequently, "the actor began selling what it claims are 23andMe profiles for between $1 and $10 per account, depending on the scale of the purchase."[25]

421. A researcher examining the leaked database found that much of the compromised data appeared to be authentic.[26] The researcher spoke on condition of anonymity because he found the information of his wife and several of her family members in the leaked data set. He also found other acquaintances and verified that their compromised information was accurate. The researcher

---

[20] Lorenzo Franceschi-Bicchierai et al., *Hackers advertised 23andMe stolen data two months ago*, TechCrunch (Oct. 10. 2023), https://techcrunch.com/2023/10/10/hackers-advertised-23andme-stolen-data-two-months-ago.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] Lily Hay Newman, *23andMe User Data Stolen in Targeted Attack on Ashkenazi Jews*, Wired (Oct. 6, 2023, 5:53 PM), https://www.wired.com/story/23andme-credential-stuffing-data-stolen/.

[26] Jonathan Greig, *23andMe scraping incident leaked data on 1.3 million users of Ashkenazi and Chinese descent*, The Record (Oct. 6, 2023), https://therecord.media/scraping-incident-genetic-testing-site.

downloaded two files from the BreachForums post. One file had information for one million 23andMe users of Ashkenazi heritage, and the other file included the data of more than 300,000 users of Chinese heritage. The data included "profile and account ID numbers, names, gender, birth year, maternal and paternal genetic markets, [and] ancestral heritage results[.]"[27]

422. 23andMe did not acknowledge or address the Data Breach until October 6, 2023, when it announced, via a blog post on its website (the "October 6 Blog Post"), that the company had "recently learned that certain 23andMe customer profile information . . . was compiled from individual 23andMe.com accounts without the account users' authorization" as a result of "threat actors" being able to "access certain accounts."[28] The October 6 Blog Post attempted to shift responsibility to 23andMe users, expressing Defendant's "belie[f]" that the Data Breach was the result of "threat actors [who] 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."[29] The October 6 Blog Post explained that the "threat actor" had accessed "users' DNA Relatives profiles."[30] The "DNA Relatives" feature "consist[s] of information that a customer chooses to make available to their genetic relatives when they opt in to participate in 23andMe's DNA Relatives," including "information such as display name, predicted relationships, and percentage of DNA shared with matches," among other information.[31]

423. 23andMe's October 6 Blog Post did not provide any details on how many people were affected by the Data Breach and failed to mention that hackers already had been selling the exfiltrated 23andMe user data on the dark web for nearly two months.

424. While the October 6 Blog Post did not expressly indicate the scope of the Data Breach in terms of the numbers of users affected or recite the categories of Private Information that were exposed, compromised, and stolen by unauthorized third parties, the categories of information in the DNA Relatives feature referenced by Defendant include:

---

[27] *Id.*
[28] 23andMe Blog, *supra* note 2.
[29] *Id.*
[30] *Id.*
[31] 23andMe Blog, *supra* note 1.

i. Names;

ii. Sex;

iii. Dates of Birth;

iv. Genetic Information that includes (but is not limited to);

a. Maternal and Paternal Haplogroup results;

b. Neanderthal Ancestry results;

v. Predicted relationships with genetic matches;

vi. Ancestry reports;

vii. Ancestors' birth locations and family names;

viii. Family tree information;

ix. Profile pictures; and

x. Geographic location.[32]

425. Notably, this initial notice was silent as to the hackers' motivations and the fact that they had targeted profiles of customers of Chinese and Ashkenazi Jewish ancestry, preventing Class Members from taking immediate action. In fact, as 23andMe knew or should have known, the cybercriminals had already posted an initial data sample of such information on the platform BreachForums.

426. The October 6 Blog Post and subsequent updates thereto also do not include information about the cause of the Data Breach, the vulnerabilities exploited, and any remedial measures 23andMe has taken to ensure that such a breach does not occur again.

427. 23andMe updated its October 6 Blog Post on October 9, 2023 to report, among other things, that it had recently engaged a third-party forensic expert and was "working with federal law enforcement."[33]

428. On about October 10, 2023, 23andMe first sent out an email notice (the "October 10 Notice") to some customers whose Private Information had been hacked. In the October 10 Notice,

[32] 23andMe, Inc., Customer Care, *DNA Relatives Privacy & Display Settings*, https://customercare.23andme.com/hc/en-us/articles/212170838 (last visited June 20, 2024).

[33] 23andMe Blog, *supra* note 2.

23andMe admitted that "certain profile information—which a customer creates and chooses to share with their genetic relatives in the DNA Relatives feature—was accessed from individual 23andMe.com accounts." The October 10 Notice further states that this access was done "without the account users' authorization." 23andMe further explained that it was engaged in an ongoing investigation and that it believed that the threat actors had used passwords that had been subject to earlier hacks of other platforms.

429. Similar to its online notice, the October 10 Notice said nothing about the facts that the Data Breach was apparently politically and/or racially motivated, that individuals of Ashkenazi Jewish and Chinese descent had been targeted, and that their information was already being sold on the dark web.

430. Also on October 10, 2023, 23andMe filed a Form 8-K with the Securities and Exchange Commission regarding the Data Breach.[34] The disclosure did not provide details of the Data Breach. 23andMe wrote that "certain profile information" was accessed, and that "certain accounts" were compromised. 23andMe noted that it "undertook immediate action in accordance with its incident response plan, including taking affirmative security measures to mitigate any potential impact of the incident, working to validate whether data that was accessed was legitimate data from the website, and determining the full scope of data accessed by unauthorized individuals."[35] The disclosures underscored that 23andMe's investigation was ongoing, and that 23andMe was working to confirm the scope of compromised data, the nature of the Private Information in question, and any related legal obligations.

431. 23andMe disseminated another notice a few days later, on or about October 13, 2023 (the "October 13 Notice"). The October 13 Notice disclosed to customers that their profile information had been part of the Data Breach, including and most importantly the analysis of their ancestry and ancestry report and matching DNA segments, their relatives' DNA and the percentage of DNA shared with their matches, their name and state of residence, their DNA Relatives display names, their birth

[34] 23andMe Holding Co., Current Report (Form 8-K) (Oct. 10, 2023), https://investors.23andme.com/node/8961/html.

[35] *Id.*

year, and how recently they had logged in.

432. On October 20, 2023, 23andMe announced that it had temporarily disabled certain features on the DNA Relatives tool.[36] This post, as well as the two previous updates, again failed to provide basic details concerning the Data Breach, including whether the breach was a system-wide breach, how many people were affected by the Data Breach, and whether certain populations, ethnic groups, or other identifiable categories of individuals were targeted in the cyberattack. 23andMe encouraged users to take precautions, including resetting their passwords and using multi-factor authentication, but by that time hackers had already exfiltrated Plaintiffs' and Class Members' Private Information.

433. Over two weeks later, on November 6, 2023, nearly seven months after its system was infiltrated, 23andMe updated its October 6 Blog Post to report that "[s]tarting today, we are requiring all customers to utilize email 2-step verification (2SV) as an added layer of protection for their account."[37]

434. Following that post, on December 1, 2023, 23andMe filed an Amendment to its October 10th SEC Form 8-K filing. The amendment identified the October 10th SEC filing as the incident that prompted 23andMe's investigation and incident response. The amendment flagged that "[b]ased on its investigation, 23andMe has determined that the threat actor was able to access a very small percentage (0.1%) of user accounts," or around 14,000 accounts.[38] The information accessed by the hackers for those accounts "varied by user account, and generally included ancestry information, and, for a subset of those accounts, health-related information based upon the user's genetics."[39] 23andMe also noted that "the threat actor also accessed a significant number of files containing profile information about other users' ancestry" but did not disclose a number.[40]

---

[36] 23andMe, Inc., *Addressing Data Security Concerns*, 23andMe Blog (Nov. 6, 2023), https://web.archive.org/web/20231107080148/https://blog.23andme.com/articles/addressing-data-security-concerns.

[37] *Id.*

[38] 23andMe Holding Co., Current Report (Form 8-K/A) (Dec. 1, 2023), https://investors.23andme.com/node/9131/html.

[39] *Id.*

[40] *Id.*

435. And on December 1, 2023, 23andMe updated its October 6 Blog Post to report that "23andMe has completed its investigation, assisted by third-party forensic experts," and is "in the process of notifying affected customers, as required by law."[41]

436. As before, 23andMe concealed the BreachForums leak and again failed to notify customers with Chinese or Ashkenazi Jewish ancestry that they were specifically targeted by cybercriminals.

437. Yet the next day, in an email sent to TechCrunch late on Saturday, December 2, 23andMe spokesperson Katie Watson "confirmed that hackers accessed the personal information" of 6.9 million individuals.[42] This included about 5.5 million people who opted-in to 23andMe's DNA Relatives feature, which allows customers to automatically share some of their data with others. The stolen data included the person's name, birth year, relationship labels, the percentage of DNA shared with relatives, ancestry reports and self-reported location. That number also included another group of about 1.4 million people who opted-in to DNA Relatives and "had their Family Tree profile information accessed," which includes display names, relationship labels, birth year, self-reported location and whether the user decided to share their information, the spokesperson said.[43]

438. Finally, on December 5, 2023, 23andMe again updated its October 6 Blog Post, stating that "[a]s our investigation comes to a close, we wanted to share the details of what took place and our findings," including the following information:

> The threat actor used the compromised accounts to access information shared with these accounts. Specifically, DNA Relatives profiles connected to these compromised accounts, which consist of information that a customer chooses to make available to their genetic relatives when they opt in to participate in 23andMe's DNA Relatives feature. A DNA Relatives profile includes information such as display name, predicted relationships, and percentage of DNA shared with matches. . . .
>
> Additionally, through the compromised accounts, the threat actor accessed a feature called Family Tree, which includes a limited subset of DNA Relatives profile

[41] 23andMe Blog, *supra* note 2.

[42] Lorenzo Franceschi-Bicchierai, *23andMe confirms hackers stole ancestry data on 6.9 million users*, TechCrunch (Dec. 4, 2023 9:56 AM PST), https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users.

[43] *Id.*

information. The Family Tree feature does not include ancestry information such as the percentage of DNA shared with genetic matches or ancestry reports.

Additional Details

- The threat actor was able to access less than 0.1%, or roughly 14,000 user accounts, of the existing 14 million 23andMe customers through credential stuffing.
- The threat actor used the compromised credential stuffed accounts to access the information included in a significant number of DNA Relatives profiles (approximately 5.5 million) and Family Tree feature profiles (approximately 1.4 million), each of which were connected to the compromised accounts.[44]

439. 23andMe's December 5, 2023 public announcement fell woefully short of providing sufficient information about the Data Breach and again failed to warn victims that their Private Information had already been leaked on BreachForums. By failing to disclose this critical information, 23andMe continued to misrepresent the scope and severity of the Data Breach to its customers.

440. Further, despite having actual knowledge that the hacker curated and leaked lists of customers of Chinese and Ashkenazi Jewish ancestry on the dark web, a 23andMe spokesperson told the *New York Times* on December 4, 2023, that "we have not learned of any reports of inappropriate use of the data after the leak."[45]

441. Notably, on November 30, 2023, while it was still concealing material aspects of the Data Breach, 23andMe moved to try to undermine the rights of Plaintiffs and Class Members to protect themselves by changing its terms of service.[46] The updated terms of service provide a new method for arbitration that forecloses collective arbitrations and changes the rules surrounding arbitration, compelling customers to individually negotiate a dispute with 23andMe for 60 days before filing an

[44] *Id.*

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

[46] *See* Jacob Knutson, *23andMe changes terms of service amid legal fallout from data breach*, Axios (Dec. 6, 2023), https://www.axios.com/2023/12/07/23andme-terms-of-service-update-data-breach; Joey Solitro, *23andMe Sees Backlash for Updating Service Terms Before Massive Data Breach*, Kiplinger (Dec. 13, 2023), https://www.kiplinger.com/personal-finance/23andme-data-breach-affects-69-million-users.

arbitration claim.[47] But in emails notifying customers of the terms of service update, 23andMe failed to identify the changes made to the terms or service. Once customers received email notice, 23andMe had already posted the updated terms of service on their website. 23andMe's incomplete notice prevented customers from reasonably understanding and making informed decisions about which changes 23andMe had made and represented a bad faith attempt to undermine Class Members' claims before 23andMe had even disclosed the full extent of the Data Breach.

442. Further, in January 2024, 23andMe submitted to the California Attorney General sample breach notification letters, in which the company disclosed that its investigation suggested the Data Breach had in fact begun in April 2023, six months before 23andMe first acknowledged the Data Breach in an October 2023 blog post on its website.[48]

443. Although 23andMe's public statements lay the blame for the Data Breach on its customers, technology experts have indicated that the Data Breach was due to a loophole in the company's web design. As one commentator noted, a researcher revealed that 23andMe had a significant loophole in its website design, allowing anyone to view a user's profile by entering a profile ID into the URL.[49] The commentator stated, "This is a glaring oversight for a company dealing with such sensitive data."[50]

444. The Data Breach of genetic information about Class Members, including individuals of Ashkenazi Jewish and Chinese ancestry, is especially dangerous and compromises the security of Plaintiffs and Class Members. In this regard, the *Wall Street Journal* posted an editorial entitled, "The Global War on the Jews," noting that antisemitism is surging on a worldwide basis.[51] Similarly, anti-

---

[47] *Terms of Service*, 23andMe (Nov. 30, 2023), https://www.23andme.com/legal/terms-of-service/full-version.

[48] Cal. Dep't. of Just., *Submitted Breach Notification Sample*, Off. of the Att'y Gen., https://oag.ca.gov/ecrime/databreach/reports/sb24-579679 (last visited June 20, 2024); Lorenzo Franceschi-Bicchierai, *23andMe admits it didn't detect cyberattacks for months*, TechCrunch (Jan. 25, 2024), https://techcrunch.com/2024/01/25/23andme-admits-it-didnt-detect-cyberattacks-for-months.

[49] Tom Donovan, *23andMe Data Breach,* The Final Hop (Oct. 6, 2023), https://www.thefinalhop.com/23andMe-data-breach.

[50] *Id.*

[51] *The Global War on the Jews*, Wall St. J. (Oct. 30, 2023), https://www.wsj.com/articles/israel-hamas-jews-pogroms-russia-u-s-europe-germany-anti-semitism.

Asian rhetoric and violence is on the rise both in the United States and internationally.[52]

C. 23andMe Compounded its Failure by Providing Inadequate Notice.

445. 23andMe's notice to Plaintiffs and Class Members was untimely and woefully deficient, failing to provide basic details concerning the Data Breach, including but not limited to how unauthorized third parties were able to access Private Information, what Private Information was in fact compromised, and how many people were affected by the Data Breach.

446. It is well-documented that:

> [t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[53]

447. This best practice likewise applies to 23andMe and the unauthorized access to Plaintiffs' and Class Members' accounts.

448. Indeed, once a data breach has occurred,

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers . . . If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves.[54]

---

[52] *Edwin Rios*, Hate incidents against Asian Americans continue to surge, study finds, The Guardian (July 21, 2022), https://www.theguardian.com/us-news/2022/jul/21/asian-americans-hate-incidents-study (noting that "[b]etween March 2020 and March 2022, more than 11,400 hate incidents against Asian Americans have been reported across the united States"); Suyin Haynes, *'This Isn't Just a Problem for North America.' The Atlanta Shooting Highlights the Painful Reality of Rising Anti-Asian Violence Around the World*, Time (Mar. 22, 2021), https://time.com/5947862/anti-asian-attacks-rising-worldwide (explaining that the increase in anti-Asian hate crimes in the United States, spurred by the coronavirus pandemic in 2020, "is one facet of a global increase in anti-Asian attacks").

[53] Javelin Strategy & Research, *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire (Feb. 1, 2017), https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million.

[54] Allen St. John, *The Data Breach Next Door*, Consumer Reps. (Jan. 31, 2019), https://www.consumerreports.org/data-theft/the-data-breach-next-door/.

449. Although their Private Information was improperly exposed on or before August 11, 2023, Plaintiffs and Class Members were not notified until October 6, 2023. 23andMe's delay deprived Plaintiffs and Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

450. As a result of 23andMe's delay in detecting and notifying individuals of the Data Breach, the risk of fraud for Plaintiffs and Class Members has been heightened, a warning State Attorneys General have alluded to when questioning 23andMe about its "unreasonable delay" in notifying affected consumers about the Data Breach.[55]

451. Moreover, 23andMe's efforts to notify Plaintiffs and Class Members fell critically short of providing key information about the Data Breach, consisting of brief messages with little substantive information that failed to sufficiently warn victims to take action to protect themselves from identity theft and fraud.

452. 23andMe's deficient notices compounded the harm suffered by Plaintiffs and Class Members, by failing to timely provide Data Breach victims with the very details necessary to protect themselves.

D. The Data Breach Was a Foreseeable Risk of Which 23andMe Was on Notice.

453. It is well known that PII and PHI are valuable commodities frequently and intentionally targeted by cybercriminals and hackers. Companies that collect such information, including 23andMe, are well aware of the risk of being targeted by hackers and cybercriminals.

454. In 2021, for instance, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[56]

455. Genetic and ancestry information is also extremely valuable, especially as hackers can sell that material to insurance companies, sell it on the dark web, or in this case use it to threaten

[55] Letter from William Tong, Att'y Gen. of Conn. to Jacquie Cooke, Gen. Couns. and Priv. Officer for 23andMe, re: Data Breach (Oct. 30, 2023) (available at https://portal.ct.gov/-/media/AG/Press_Releases/2023/10-30-2023-William-Tong--23andMe-Inc-Inquiry-Letter-final-002.pdf).

[56] 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.

members of particular racial or religious groups based on information from their genetic testing.[57]

456. Several genetic testing entities have been the subject of well publicized hacks or data breaches, of which 23andMe was or should have been aware, particularly given its representation that "[t]o prevent unauthorized access or disclosure, to maintain data accuracy, and to ensure the appropriate use of information, 23andMe uses a range of physical, technical, and administrative measures to safeguard your Personal Information."[58]

457. For example, several months ago, 1Health.io, another genetics testing company, was fined $75,000 by the Federal Trade Commission ("FTC") for failing to secure sensitive data. In 2021, the Ohio and Pennsylvania States Attorney General fined DNA Diagnostic Center, a DNA testing entity, $400,000 for a data breach that affected 2.1 million customers.[59] And in 2018, hackers breached the accounts of 92 million customers of MyHeritage, although the hackers never accessed actual genetic data.[60]

458. Thus, the risk of the Data Breach was eminently foreseeable to 23andMe. In its March 31, 2022 Form 10-K statement, 23andMe specifically acknowledged and warned of the risk posed by a data breach that could compromise the Private Information of its customers:

> Increased global IT security threats and more sophisticated and targeted computer crime pose a risk to the security of our systems and networks and the confidentiality, availability, and integrity of our data. There have been several recent, highly publicized cases in which organizations of various types and sizes have reported the unauthorized disclosure of customer or other confidential information, as well as cyberattacks involving the dissemination, theft, and destruction of corporate information, intellectual property, cash, or other valuable assets. There have also been several highly publicized cases in which hackers have requested "ransom" payments in exchange for not disclosing customer or other confidential information or for not disabling the target company's computer or other systems. A security breach or privacy violation that leads

[57] Angela Chen, *Why a DNA data breach is much worse than a credit card leak*, Ctr. for Genetics and Soc'y (June 6, 2018), https://www.geneticsandsociety.org/article/why-dna-data-breach-much-worse-credit-card-leak.

[58] 23andMe, Inc., *How is my personal information protected?*, https://customercare.23andme.com/hc/en-us/articles/202907840-How-Is-My-Personal-Information-Protected (last visited June 24, 2024).

[59] Apurva Venkat, DNA Diagnostic Center fined $400,000 for 2021 data breach, CSO (Feb. 21, 2023), https://www.csoonline.com/article/574597/dna-diagnostic-center-fined-400-000-for-2021-data-breach.html.

[60] Chen, *supra* note 57.

> to disclosure or unauthorized use or modification of, or that prevents access to or otherwise impacts the confidentiality, security, or integrity of, sensitive, confidential, or proprietary information we or our third-party service providers maintain or otherwise process, could compel us to comply with breach notification laws, and cause us to incur significant costs for remediation, fines, penalties, notification to individuals and governmental authorities, implementation of measures intended to repair or replace systems or technology, and to prevent future occurrences, potential increases in insurance premiums, and forensic security audits or investigations. Additionally, a security compromise of our information systems or of those of businesses with whom we interact that results in confidential information being accessed by unauthorized or improper persons could harm our reputation and expose us to customer and patient attrition, and claims brought by our customers, patients, or others for breaching contractual confidentiality and security provisions or data protection laws. Monetary damages imposed on us could be significant and not covered by our liability insurance.[61]

459. Despite its knowledge of the substantial risks and consequences of inadequate security, 23andMe failed to fortify its security measures and, as a result, the data of 23andMe customers, including those of Ashkenazi Jewish and Chinese ancestry, has appeared for sale on the dark web.

460. For instance, an NBC Report on October 7, 2023, stated that NBC News had a list of 999,999 people who allegedly used 23andMe, which was posted for sale on the dark web. The database, which showed up on the dark web, included the first and last names of Jewish customers, their sex, and 23andMe's evaluation of where their ancestors came from. It was entitled, "Ashkenazi DNA Data of Celebrities," although most of the people in the database were not famous and, according to NBC News, appears to have only included people with Ashkenazi heritage.[62] The compromised data of people with Ashkenazi Jewish and Chinese heritage included "profile and account ID numbers, names, gender, birth year, maternal and paternal genetic markers, [and] ancestral heritage results."[63]

E. 23andMe Is Under Investigation.

461. Given the apparent political, anti-Semitic, and anti-Chinese nature of the Data Breach, 23andMe is now under Congressional and state investigation.

462. On October 20, 2023, Senator Bill Cassidy, the Ranking Member of the Senate

[61] 23andMe Holding Co., Annual Report (Form 10-K), at 67 (Mar. 31, 2022), https://investors.23andme.com/static-files/536ba9a7-8a85-4b73-8b09-8215451089a0.
[62] Kevin Collier, *23andMe user data targeting Ashkenazi Jews leaked online*, NBC News (Oct. 7, 2023), https://www.nbcnews.com/news/us-news/23andme-user-data-targeting-ashkenazi-jews-leaked-online-rcna119324.
[63] Greig, *supra* note 26.

Committee on Health, Education, Labor and Pensions, sent a letter to Ann Wojcicki, 23andMe's Chief Executive Officer (the "October 20 Letter") noting his concern regarding the Data Breach and requesting the production of certain information pertaining to it.[64]

463. In the October 20 Letter, Senator Cassidy stated that he was particularly concerned with the "unauthorized disclosure of 1.3 million customers' information being posted on the dark web, including one million customers identified as people of Ashkenazi Jewish descent and 300 thousand [sic] customers identified as people of Chinese heritage."[65]

464. Senator Cassidy further stated that the disclosed data included name, sex, birth year, location, photos, health information and genetic ancestry results, and that this information was shared online as a database entitled, "Ashkenazi DNA Data of Celebrities."[66] He noted the danger in which that disclosure placed those Ashkenazi Jews whose information had been disclosed, citing to one poster who claimed, "Crazy, this could be used by Nazis," which is particularly concerning given the "increasing rates of global antisemitism and anti-Asian hate, which can be leveraged to draw higher prices for the information and increase the threat from potential evildoers." He noted that the records were selling for between $1 and $10 each.[67]

465. The October 20 Letter further explained that the Data Breach could have implications far beyond that incident and gave the company until November 3, 2023 to answer a number of pertinent questions, including how only several thousand compromised user accounts could provide hackers with information for millions of personal accounts, and what the company was doing to compensate affected users.

466. On or about October 30, 2023, the Connecticut Attorney General, William Tong, sent Jacquie Cooke, 23andMe's General Counsel and Privacy Officer, a similar letter entitled, "Data

---

[64] Ranking Member Cassidy Raises Concerns over 23andMe Data Leaks, Potential Targeting of Minority Groups, U.S. Senate Comm. on Health, Educ. Lab. & Pensions (Oct. 20, 2023), https://www.help.senate.gov/ranking/newsroom/press/ranking-member-cassidy-raises-concerns-over-23andMe-data-leaks-potential-targeting-of-minority-groups.

[65] *Id.*

[66] *Id.*

[67] *Id.*

Breach" (the "October 30 Letter") pertaining to how the Data Breach affected Connecticut residents.[68]

467. In the October 30 Letter, Attorney General Tong also noted his concern that a hack targeting Jewish and Asian customers was particularly dangerous given the rising antisemitic and anti-Asian rhetoric and violence in recent years. Attorney General Tong further stated that 23andMe was required to but had failed to comply with Connecticut's notice requirements and may well have violated the Connecticut Data Privacy Act.[69]

468. Attorney General Tong similarly posed a number of pointed questions to 23andMe, including whether the company intended to comply with Connecticut's notice requirement and what kind of safeguards it had in place to prevent "credential stuffing," requesting responses by November 13, 2023.

469. Likewise, Arizona Attorney General Kris Mayes sent a January 2024 letter to Ms. Cooke, expressing her concerns for the safety of 23andMe's Jewish and Chinese customers.[70] Attorney General Mayes noted that "the recent increase in all hate crimes across the country, especially antisemitic and anti-Asian hate crimes, means that this is a particularly dangerous time for the targeted sale of information of individuals identifying and belonging to specific racial or ethnic groups—information that 23andMe profits from analyzing."[71]

470. Similarly, in a January 11, 2024 letter to the FBI, U.S. Congressman Josh Gottheimer, a member of the House Permanent Select Committee on Intelligence, expressed "concern[] that the leaked data could empower Hamas, their supporters, and various international extremist groups to target the American Jewish population and their families" and expressed an urgent need "to protect the information, locations, and lives of the American Jewish population."[72]

471. On June 10, 2024, British and Canadian authorities announced a joint investigation into

---

[68] Letter from William Tong, *supra* note 55.

[69] *Id.*

[70] Letter from Kris Mayes, Ariz. Att'y Gen., to Jacquie Cook, 23andMe Gen. Couns. And Priv. Officer (Jan. 4, 2024) (available at https://www.azag.gov/sites/default/files/2024-01/AG%20Mayes_23andMe%201.8.24.pdf).

[71] *Id.*

[72] Release, Josh Gottheimer, *Gottheimer Calls For FBI Investigation into 23andMe Data Breach* (Jan. 11, 2024) (available at https://gottheimer.house.gov/posts/release-gottheimer-calls-for-fbi-investigation-into-23andme-data-breach).

the Data Breach.[73] This investigation shall examine the scope of information compromised and harms to those impacted, whether 23andMe had adequate safeguards to protect its customers' highly sensitive information, and whether 23andMe provided an adequate notification of the Data Breach.[74] Philippe Dufresne, Privacy Commissioner of Canada, stated: "In the wrong hands, an individual's genetic information could be misused for surveillance or discrimination."[75] John Edwards, UK Information Commissioner, said that because "[t]his data breach had an international impact," "[p]eople need to trust that any organization handling their most sensitive personal information has the appropriate security and safeguards in place."[76]

F. 23andMe Failed to Comply with Regulatory Guidance and Industry-Standard Cybersecurity Practices.

472. 23andMe's Data Breach is attributable to its failure to comply with state and federal laws and requirements as well as industry standards governing the protection of PII and PHI.

473. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license, or maintain PII to implement and maintain "reasonable security procedures and practices" and to protect PII from unauthorized access. California is one such state, which requires that "[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, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b).

474. 23andMe also failed to comply with Federal Trade Commission ("FTC") guidance on protecting PII and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has

[73] *See* ICO to investigate 23andMe data breach with Canadian counterpart, Info. Comm'r's Off. (June 10, 2024), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/06/ico-to-investigate-23andme-data-breach-with-canadian-counterpart.
[74] *Id.*
[75] *Id.*
[76] *Id.*

made clear that protecting sensitive customer data should factor into virtually all business decisions.

475. The FTC recommends, among other things:

- limiting access to customer information to those who have a legitimate business need for it;
- encrypting customer information on system and in transit;
- implementing multi-factor authentication for anyone accessing customer information;
- implementing procedures and controls to monitor when authorized users are accessing customer information;
- maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information; and
- implementing procedures and controls to detect unauthorized access to customer information, including monitoring activity logs for signs of unauthorized access to customer information.[77]

476. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[78]

477. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[79] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. 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

[77] *See* Fed. Trade Comm'n, *FTC Safeguards Rule: What Your Business Needs to Know* (May 2022), https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know.

[78] Fed. Trade Comm'n, *Start With Security: A Guide for Business*, at 2 (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[79] Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

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.

478. The FTC further recommends that businesses apply security measures that have proven successful in the particular industry and verify that third parties with access to sensitive information use reasonable security measures.

479. 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 FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

480. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

481. 23andMe was aware of its obligations to protect its customers' Private Information and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers' Private Information from unauthorized access. 23andMe was also aware of the significant repercussions if it failed to do so because 23andMe collected Private Information from millions of consumers and it knew that this Private Information, if hacked, would result in injury to consumers, including Plaintiffs and Class Members.

482. Based upon the known details of how the Data Breach occurred, 23andMe also failed to fully comply with industry-standard cybersecurity practices, including, but not limited to rate limiting, user-activity monitoring, and data-loss prevention.

483. HIPAA requires covered entities to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C

484. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

485. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected

Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

486. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information[.]" 45 C.F.R. § 164.302.

487. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

488. HIPAA's Security Rule requires covered entities to do the following:

A. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

B. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

C. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

D. Ensure compliance by its workforce.

489. HIPAA also requires covered entities to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information[.]" 45 C.F.R. § 164.306(e). Additionally, covered entities must "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights[.]" 45 C.F.R. § 164.312(a)(1).

490. HIPAA and HITECH also obligate covered entities to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); see also 42 U.S.C. § 17902.

491. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires covered

entities to provide notice of a data breach to each affected individual "without unreasonable delay and in no case later than 60 days following the discovery of a breach."[80]

492. HIPAA likewise requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

493. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

494. HIPAA also requires the Office of Civil Rights ("OCR") within the Department of Health and Human Services ("HHS") to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule."[81] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI."[82]

G. The Effect of the Data Breach on Plaintiffs and Class Members.

495. 23andMe's failure to keep Plaintiffs' and Class Members' Private Information secure has severe ramifications. Given the sensitive nature of the Private Information stolen in the Data Breach—including name, sex, date of birth, genetic information, predicted relationships with genetic matches, ancestry reports, ancestors' birth locations and family names, family tree information, profile pictures, and geographic location—cybercriminals can commit identity theft, financial fraud, and other

[80] Breach Notification Rule, U.S. Dep't of Health & Hum. Servs. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.
[81] Security Rule Guidance Material, U.S. Dep't of Health & Human Servs. (Feb. 16, 2024), http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[82] Guidance on Risk Analysis, U.S. Dep't of Health & Hum. Servs. (July 22, 2019), https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs have suffered injury and face an imminent and substantial risk of further injury, including actual or attempted identity theft, fraud, or related cybercrimes due to the Data Breach.

496. Armed with the Private Information accessed in the Data Breach, data thieves can use that data to commit a variety of crimes, including using Class Members' genetic and ethnic information to commit identity theft and fraud using their compromised Private Information. Moreover, data thieves or malicious actors who may have purchased or otherwise illegally obtained Private Information may use that data to target Plaintiffs and Class Members with violence or threats of harm based on animus toward members of particular ethnic groups. Indeed, the fact that initial leaks of Private Information stolen in the Data Breach and "advertised [for sale] on BreachForums allegedly contain one million 23andMe users of Jewish Ashkenazi descent and 100,000 23andMe Chinese users"[83] has prompted at least one State Attorney General to observe that "the increased frequency of antisemitic and anti-Asian rhetoric and violence in recent years means that this may be a particularly dangerous time for such targeted information to be released to the public."[84] For example, on October 17, 2023, a cybercriminal returned to BreachForums to state that he had acquired data about "wealthy families serving Zionism" that he was offering for sale in the aftermath of the deadly October 2023 explosion at Al-Ahli Arab Hospital in Gaza City.[85]

497. Further, malicious actors often wait months or years to use the PII and/or PHI obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also reuse stolen PII and/or PHI, meaning individuals can be the victim of several instances of identity theft, fraud, or other cybercrimes stemming from a single data breach.

498. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have

[83] Lorenzo Franceschi-Bicchierai et al., *supra* note 20.
[84] William Tong Letter, *supra* note 68.
[85] Rebecca Carballo et al., *23andMe Breach Targeted Jewish and Chinese Customers, Lawsuit Says*, N.Y. Times (Jan. 26, 2024), https://www.nytimes.com/2024/01/26/business/23andme-hack-data.html.

been sold or posted on the Web, fraudulent use of that information may continue for years."[86] Moreover, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. Plaintiffs will therefore need to spend time and money to continuously monitor their accounts for years to ensure their Private Information obtained in the Data Breach is not used to harm them. Plaintiffs and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach. In other words, Plaintiffs have been harmed by the value of identity protection services or other security products they must purchase in the future to ameliorate the risk of harm they now face due to the Data Breach.

499. As such, these harms are ongoing, and Plaintiffs and Class Members will suffer from future damages associated with the unauthorized use and misuse of their Private Information, as data thieves and malicious actors who purchase the stolen Private Information will continue to use the information to the detriment of Plaintiffs and Class Members for many years to come, placing Plaintiffs and Class Members at heightened and imminent risk of harms including identity theft, fraud, blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, and other related harms.

500. As a direct result of the Data Breach, Plaintiffs and Class Members have suffered actual and attempted identity theft and fraud, and they will continue to be exposed to a heightened and imminent risk of identity theft, fraud, and other harms, potentially for the rest of their lives. Plaintiffs and Class Members must now and in the future closely monitor their medical, insurance, and financial accounts to guard against identity theft and fraud and take other measures to protect themselves against the heightened and imminent risk of other harms that they face because of the Data Breach.

501. For this reason, Class Members may incur out-of-pocket costs for purchasing protective measures to deter and detect identity theft and fraud as well as purchasing other protective measures to mitigate against the misuse of their genetic information and other Private Information and the heightened and imminent risk of other harms that they face because of the Data Breach, including

[86] U.S. Gov't Accountability Off., *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

blackmail, harassment, intimidation, vandalism, assault, extortion, and hate crimes.

502. As a direct and proximate result of the Data Breach and subsequent exposure of their Private Information, Plaintiffs and Class Members have suffered, and will continue to suffer, damages and economic losses in the form of lost time needed to take appropriate measures to avoid and address the misuse of their Private Information, potential unauthorized and fraudulent charges, coping with spam phone calls, letters, text messages, and emails, and addressing the heightened and imminent risk of other harms that they face as a result of the Data Breach and the unauthorized disclosure and misuse of their Private Information.

503. Plaintiffs and Class Members have also realized harm in the lost or reduced value of their Private Information. Plaintiffs' Private Information is not only valuable to 23andMe, but Plaintiffs also place high value on their Private Information based on their understanding that their Private Information is a financial asset to companies that collect it.[87]

504. One measure of harm to the Plaintiffs and Class Members whose Private Information was accessed without authorization is the market value the hackers ascribed to Class Members' Private Information when it was posted for sale on the dark web. This market value for access to PII and/or PHI can be determined by reference to both legitimate and illegitimate markets for such information.

505. Plaintiffs and Class Members have been further harmed and damaged in the amount of monetary profit 23andMe has made from them and from their Private Information, profits which 23andMe unjustly retains.

506. Moreover, Plaintiffs and Class Members value the privacy of this information and expect 23andMe to allocate sufficient resources to ensure it is adequately protected. Plaintiffs and other customers would not have conducted business with 23andMe, provided their Private Information to 23andMe, nor paid the same prices for 23andMe's goods and services had they known 23andMe did not implement reasonable security measures to protect their Private Information. Customers reasonably

[87] *See, e.g.*, Ponemon Institute, LLC, *Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers*, at 14 (Mar. 2015) (explaining that 53% of respondents "believe personal data is a financial asset similar to traded goods, currencies or commodities" and valuing, as but one example, their Social Security number at $55.70), https://docplayer.net/836701-Privacy-and-security-in-a-connected-life-a-study-of-us-european-and-japanese-consumers.html.

expect that the payments they made to 23andMe incorporate the costs to implement reasonable security measures to protect their Private Information. As a result, Plaintiffs and Class Members did not receive the benefit of their bargain with 23andMe because they paid a value for services they expected but did not receive.

507. Instead of affirmatively protecting its customers and taking responsibility for its website's flawed design and poor security, 23andMe has repeatedly shirked responsibility and blamed customers for their alleged negligence, claiming that over half its users were exposed to a threat actor from purported breaches to only 0.1% of 23andMe's accounts. Instead, despite knowledge that at least some of the data had been advertised for sale, 23andMe told the New York Times that it had "not learned of any reports of inappropriate use of the data after the leak."[88] By maintaining insecure data practices and then failing to inform their customers about the scope and danger of the leak, and further failing to provide their customers with any remedy, 23andMe has repeatedly shirked its duty to its customers and exposed them to heightened risk for harassment, financial fraud, and identity theft for years to come.

508. As part and parcel of 23andMe's disregard for its customers, before sending notices in December about the Data Breach to the seven million customers affected, 23andMe first changed its terms of service to add arbitration requirements to prevent customers from pursuing claims against the company. On November 30, 2023, mere days before its December 1st SEC filing and its December 5th notice to affected customers, 23andMe updated its terms of service.[89] These changes represent an effort to make it increasingly difficult for the victims of the Data Breach to bring collective arbitrations by mandating an initial 60-day dispute resolution period and compelling customers to attempt to resolve any disputes with 23andMe individually before filing an arbitration claim.

509. Given 23andMe's failure to protect Plaintiffs' and Class Members' Private Information, Plaintiffs have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects them from suffering

[88] Carballo, *supra* note 43.

[89] Lorenzo Franceschi-Bicchierai, *23andMe changes to terms of service are 'cynical' and 'self-serving,' lawyers say*, TechCrunch (Dec. 11, 2023), https://techcrunch.com/2023/12/11/23andme-changes-to-terms-of-service-are-cynical-and-self-serving-lawyers-say.

further harm, as their Private Information remains in 23andMe's possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on a large class of persons.

510. In sum, Plaintiffs and Class Members were injured as follows: (i) theft of their Private Information and the resulting loss of privacy rights in that information; (ii) improper disclosure of their Private Information; (iii) loss of value of their Private Information; (iv) the lost value of access to Plaintiffs' and Class Members' Private Information permitted by 23andMe; (v) the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; (vi) 23andMe's retention of profits attributable to Plaintiffs' and Class Members' Private Information that 23andMe failed to adequately protect; (vii) the certain, imminent, and ongoing threat of identity theft, fraud, blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, and other related harms, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to 23andMe for services purchased, as Plaintiffs reasonably believed a portion of the sale price would fund reasonable security measures that would protect their PII, which was not the case; and (x) nominal damages.

VI. CLASS ACTION ALLEGATIONS

NATIONWIDE CLASSES

511. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following two nationwide classes (the "Nationwide Classes"):

> Nationwide Class: All natural persons residing in the United States whose Private Information was exfiltrated in the Data Breach.
>
> Nationwide Ethnically Targeted Persons Class: All natural persons of Chinese or Ashkenazi Jewish descent residing in the United States whose Private Information was exfiltrated in the Data Breach.[90]

512. The Nationwide Classes assert claims against 23andMe for negligence (Count 1),

[90] Plaintiffs reserve the right to expand this definition to include any additional ethnic, racial, or otherwise vulnerable populations that were specifically targeted through the Data Breach.

negligence per se (Count 2), breach of confidence (Count 3), invasion of privacy (Count 4), breach of express contract (Count 5), breach of implied contract (Count 6), breach of the implied covenant of good faith and fair dealing (Count 7), breach of fiduciary duty (Count 8), conversion (Count 9), unjust enrichment (Count 10), violation of California's Unfair Competition Law (Count 11), and declaratory judgment (Count 12).

STATEWIDE SUBCLASSES

513. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts 13 through 40), on behalf of two separate statewide Subclasses for each State (the "Statewide Subclasses"), defined as follows:

> Statewide Subclass: All natural persons residing in [name of state or territory] whose Private Information was exfiltrated in the Data Breach.
>
> Statewide Ethnically Targeted Persons Subclass: All natural persons of Chinese or Ashkenazi Jewish descent residing in [name of state or territory] whose Private Information was exfiltrated in the Data Breach.[91]

514. Excluded from the Nationwide Classes and each Subclass are 23andMe, any entity in which 23andMe has a controlling interest, and 23andMe's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Classes and each Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

515. Plaintiffs reserve the right to amend the Class definitions if further investigation and discovery indicate that the Class definitions should be narrowed, expanded, or otherwise modified.

516. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Nationwide Class and each Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, 23andMe has acknowledged that the Private Information of millions of

[91] As above, Plaintiffs reserve the right to expand this definition to include any additional ethnic, racial, or otherwise vulnerable populations that were specifically targeted through the Data Breach.

individuals has been compromised. Those individuals' names and addresses are available from 23andMe's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least millions of individuals in the Nationwide Class and at least thousands of individuals in each Subclass, making joinder of all Class Members impracticable.

517. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** As to the Nationwide Class and each Subclass, this action involves common questions of law and fact, which predominate over any questions affecting individual Class Members. These common questions include:

a. Whether 23andMe had a duty to protect Class Members' Private Information;

b. Whether 23andMe failed to take reasonable and prudent security measures to ensure the Private Information it maintains was adequately protected from unauthorized disclosure;

c. Whether 23andMe failed to take available steps to prevent and stop the Data Breach from happening;

d. Whether 23andMe knew or should have known that the Private Information it maintains was vulnerable to compromise;

e. Whether 23andMe was negligent in failing to implement reasonable and adequate security procedures and practices;

f. Whether 23andMe's security measures to protect the Private Information it maintains were reasonable in light of known legal requirements and industry standards;

g. Whether 23andMe's conduct constituted unfair or deceptive trade practices;

h. Whether 23andMe violated state or federal law when it failed to implement reasonable security procedures and practices;

i. Which security procedures and notification procedures 23andMe should be required to implement;

j. Whether 23andMe has a contractual obligation to provide for the security of customer Private Information;

k. Whether 23andMe has complied with any contractual obligations to protect customer Private Information;

l. What security measures, if any, must be implemented by 23andMe to comply with its contractual obligations;

m. Whether 23andMe violated state consumer protection laws in connection with the actions described herein;

n. Whether 23andMe failed to notify Plaintiffs and Class Members as soon as practicable and without delay after the Data Breach was discovered;

o. Whether 23andMe's conduct resulted in or was the proximate cause of the loss of the Private Information of Plaintiffs and Class Members;

p. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of 23andMe's failure to reasonably protect their Private Information;

q. Whether 23andMe should retain the money paid by Plaintiffs and Class Members to protect their Private Information, and the profits 23andMe generated through Plaintiffs' and Class Members' Private Information;

r. Whether and how 23andMe should retain Plaintiffs' and Class Members' valuable Private Information; and,

s. Whether Plaintiffs and Class Members are entitled to damages or injunctive relief.

518. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to each Class and Subclass, Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subjected to the same allegedly unlawful conduct and harmed in the same way. Plaintiffs' Private Information was in 23andMe's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to those of other Class Members, and Plaintiffs seek relief consistent with the relief of the Class.

519. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

520. **Predominance & Superiority: Federal Rule of Civil Procedure 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the

management of this class action. Common issues in this litigation also predominate over individual issues because the issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against 23andMe, and thus, individual litigation to redress 23andMe's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

521. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for 23andMe.

522. **Ascertainability.** The Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. The Class and Subclasses consist of individuals who provided their Private Information to 23andMe, and Class Membership can be determined using 23andMe's records.

523. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). 23andMe, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect Class Members' data. Plaintiffs seek prospective injunctive relief as a wholly separate remedy from any monetary relief.

524. Likewise, particular issues under 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.

VII. CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT ONE — NEGLIGENCE

On Behalf of Plaintiffs and the Nationwide Classes, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

525. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

526. 23andMe required Plaintiffs and Class Members to submit sensitive Private Information in order to obtain its services.

527. 23andMe owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Private Information in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing 23andMe's security systems to ensure that Plaintiffs' and Class Members' Private Information in 23andMe's possession was adequately secured and protected; (b) implementing processes that would detect unauthorized access to the Private Information it maintains in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding unauthorized access to the Private Information it maintains; and (d) maintaining data security measures consistent with industry standards.

528. 23andMe's duty to use reasonable care arose from several sources, including but not limited to those described herein.

529. 23andMe had common law duties to prevent foreseeable harm to Plaintiffs and the Class Members. These duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiffs and Class Members would be harmed by 23andMe's failure to protect their Private Information because hackers routinely attempt to steal such information and use it for nefarious purposes, 23andMe knew that it was more likely than not Plaintiffs and other Class Members would be harmed if it allowed such a breach.

530. 23andMe's duty to use reasonable security measures also arose as a result of the special

relationship that existed between 23andMe, on the one hand, and Plaintiffs and Class Members, on the other hand. The special relationship arose because Plaintiffs and Class Members entrusted 23andMe with their highly sensitive Private Information as part of the purchase of the services 23andMe offers. 23andMe alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

531. 23andMe's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair practice of failing to use reasonable measures to protect Private Information by companies such as 23andMe. Various FTC publications and data security breach orders further form the basis of 23andMe's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

532. 23andMe's duty also arose from 23andMe's superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the 23andMe Data Breach.

533. 23andMe admits that it has a responsibility to protect the Private Information with which it is entrusted.

534. 23andMe knew or should have known that its data storage architecture was vulnerable to unauthorized access and targeting by cybercriminals for the purpose of stealing and misusing confidential Private Information.

535. 23andMe also had a duty to safeguard the Private Information of Plaintiffs and Class Members and to promptly notify them of a breach because of state laws and statutes that require 23andMe to reasonably safeguard sensitive Private Information, as detailed herein.

536. Timely, adequate notification was required, appropriate and necessary so that, among other things, Plaintiffs and Class Members could take appropriate measures to freeze or lock their credit profiles, avoid or mitigate identity theft or fraud, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by 23andMe's misconduct.

537. 23andMe breached the duties it owed to Plaintiffs and Class Members described above

and thus was negligent. 23andMe breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Private Information of Plaintiffs and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the Private Information at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiffs' and the Class Members' Private Information in 23andMe's possession had been or was reasonably believed to have been, stolen or compromised.

538. But for 23andMe's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

539. 23andMe's failure to take proper security measures to protect the sensitive Private Information of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiffs' and Class Members' Private Information.

540. Plaintiffs and Class Members were foreseeable victims of 23andMe's inadequate data security practices, and it was also foreseeable that 23andMe's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members as described in this Complaint.

541. As a direct and proximate result of 23andMe's negligence, Plaintiffs 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on dark web, identity defense, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; expenses and time spent initiating fraud alerts; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the

amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's 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 TWO — NEGLIGENCE PER SE

On Behalf of Plaintiffs and the Nationwide Classes, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

542. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

543. Section 5 of the FTC Act, 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 companies such as 23andMe of failing to use reasonable measures to protect Private Information.

544. The FTC publications and orders also form the basis of 23andMe's duty.

545. 23andMe violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. 23andMe's conduct was particularly unreasonable given the nature and amount of Private Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving the highly sensitive Private Information it maintains, including specifically the damages that would result to Plaintiffs and Class Members.

546. In addition, under state data security statutes, 23andMe had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Private Information.

547. 23andMe's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

548. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

549. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, 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 Class.

550. 23andMe breached its duties to Plaintiffs and Class Members under the FTC Act and state data security statutes by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiffs' and Class Members' Private Information.

551. Plaintiffs and Class Members were foreseeable victims of 23andMe's violations of the FTC Act and state data security statutes. 23andMe knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiffs' and Class Members' Private Information would cause damage to Plaintiffs and Class Members.

552. But for 23andMe's violation of the applicable laws and regulations, Plaintiffs' and Class Members' Private Information would not have been accessed by unauthorized parties.

553. As a direct and proximate result of 23andMe's negligence per se, Plaintiffs 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; expenses and time spent initiating fraud alerts; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's 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 THREE — BREACH OF CONFIDENCE

On Behalf of Plaintiffs and the Nationwide Classes, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

554. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

555. Plaintiffs and Class Members maintained a confidential relationship with 23andMe whereby 23andMe undertook a duty not to disclose the Private Information provided by Plaintiffs and Class Members to 23andMe to unauthorized third parties. Such Private Information was confidential and novel, highly personal and sensitive, and not generally known.

556. 23andMe knew Plaintiffs' and Class Members' Private Information was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the Private Information they collected, stored, and maintained.

557. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' Private Information in violation of this understanding. The unauthorized disclosure occurred because 23andMe failed to implement and maintain reasonable safeguards to protect the Private Information in its possession and failed to comply with industry-standard data security practices.

558. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to unauthorized third parties.

559. But for 23andMe's disclosure of Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. 23andMe's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Private Information, as well as the resulting damages.

560. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of 23andMe's unauthorized disclosure of Plaintiffs' and Class Members' Private Information.

561. As a direct and proximate result of 23andMe's breach of confidence, Plaintiffs 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; expenses and time spent initiating fraud alerts; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's 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 FOUR — INVASION OF PRIVACY

On Behalf of Plaintiffs and the Nationwide Classes, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

562. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

563. Plaintiffs and Class Members had a legitimate expectation of privacy in their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

564. 23andMe owed a duty to Plaintiffs and Class Members, to keep their Private Information confidential.

565. 23andMe failed to protect, and allowed unknown and unauthorized third parties to access, the Private Information of Plaintiffs and Class Members.

566. The Private Information that was publicized during the Data Breach was highly

sensitive, private, and confidential.

567. 23andMe acted with reckless disregard for the privacy of Plaintiffs and Class Members rising to the level of: (a) an intentional intrusion by Defendant; (b) into a matter that Plaintiffs and Class Members have a right to keep private (i.e., their Private Information); and (c) which is highly offensive to a reasonable person.

568. 23andMe acted knowingly when it permitted the Data Breach to occur; it had actual knowledge that its information security practices were inadequate and insufficient.

569. 23andMe was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' data and Private Information.

570. 23andMe acted with such reckless disregard as to the safety of Plaintiffs' and Class Members' Private Information to rise to the level of intentionally allowing the intrusion upon Plaintiffs' and Class Members' seclusion.

571. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and Class Members would be highly offensive to a reasonable person.

572. Plaintiffs and Class Members have been damaged by the invasion of their privacy in an amount to be determined at trial.

COUNT FIVE — BREACH OF EXPRESS CONTRACT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

573. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

574. Plaintiffs and Class Members entered into contracts with 23andMe. Through their course of conduct, 23andMe was to adequately safeguard Plaintiffs' and Class Members' Private Information, genetic information (including information derived from genetic testing), and other highly sensitive and confidential information in exchange for Plaintiffs' and Class Members' paid use of 23andMe's services and products.

575. 23andMe required Plaintiffs and Class Members to provide their Private Information as a condition of using 23andMe's service and products. In fact, 23andMe solicited and invited Plaintiffs and Class Members to do so.

576. By submitting their DNA tests to 23andMe, Plaintiffs and Class Members accepted 23andMe's offer, and there was a meeting of the minds.

577. Plaintiffs and Class Members fully performed their obligations under the contracts with 23andMe by creating accounts, paying for 23andMe's services and products, and submitting their DNA tests to 23andMe.

578. 23andMe breached its agreement with Plaintiffs and Class Members by failing to protect their Private Information. Specifically, 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, in violation of the agreement.

579. As a direct and proximate result of 23andMe's breach of contract, Plaintiffs 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; expenses and time spent initiating fraud alerts; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; disgorgement of profits; nominal and general damages; and other economic and non-economic harm.

COUNT SIX — BREACH OF IMPLIED CONTRACT

On Behalf of Plaintiffs and the Nationwide Classes, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

580. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

581. Plaintiffs and Class Members entered into an implied contract with 23andMe when they obtained services from 23andMe, or otherwise provided Private Information to 23andMe.

582. As part of these transactions, 23andMe agreed to safeguard and protect the Private Information of Plaintiffs and Class Members and to timely and accurately notify them if their Private Information was breached or compromised.

583. Plaintiffs 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 legal requirements and industry standards. Plaintiffs 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 Private Information they provided to fund adequate and reasonable data security practices.

584. Plaintiffs and Class Members would not have provided and entrusted their Private Information to 23andMe or would have paid less for 23andMe products or services in the absence of the implied contract or implied terms between them and 23andMe. The safeguarding of the Private Information of Plaintiffs and Class Members was critical to realize the intent of the parties.

585. Plaintiffs and Class Members fully performed their obligations under the implied contracts with 23andMe.

586. 23andMe breached its implied contracts with Plaintiffs and Class Members to protect their Private Information 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.

587. As a direct and proximate result of 23andMe's breach of implied contract, Plaintiffs 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; expenses and time spent initiating fraud alerts; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; disgorgement of profits; nominal and general damages; and other economic and non-economic harm.

COUNT SEVEN — BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

On Behalf of Plaintiffs and the Nationwide Classes, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

588. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

589. As noted above, Plaintiffs and Class Members entered into contracts with 23andMe.

590. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations—both explicit and fairly implied—and would not impair the rights of the other parties to receive their rights, benefits, and reasonable expectations under the contracts. These included the covenants that 23andMe would act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' Private Information and to comply with industry standards and federal and state laws and regulations for the security of this information.

591. 23andMe promised and was obligated to protect the confidentiality of Plaintiffs' and Class Members' Private Information from disclosure to unauthorized third parties. 23andMe breached the covenant of good faith and fair dealing by failing to take adequate measures to protect the

confidentiality of Plaintiffs' and Class Members' Private Information, which resulted in the Data Breach. 23andMe unreasonably interfered with the contract benefits owed to Plaintiffs and Class Members by failing to implement reasonable and adequate security measures consistent with industry standards to protect and limit access to the Plaintiffs and the Class Members' Private Information in 23andMe's possession.

592. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to 23andMe, including paying 23andMe for services or products and providing them the confidential Private Information required by the contracts.

593. As a result of 23andMe's breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class Members did not receive the full benefit of their bargain—services with reasonable data privacy—and instead received services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiffs and Class Members have suffered actual damages in an amount equal to the difference in the value between services with reasonable data privacy that Plaintiffs and Class Members paid for, and the services they received without reasonable data privacy.

594. As a result of 23andMe's breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered actual damages resulting from the theft of their Private Information and remain at imminent risk of suffering additional damages in the future.

595. As a result of 23andMe's breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered actual damages resulting from their attempt to ameliorate the effect of the Data Breach, including, but not limited to, taking steps to protect themselves from the loss of their Private Information.

596. As a direct and proximate result of 23andMe's breach of the implied covenant of good faith and fair dealing, Plaintiffs 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 Private

Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; expenses and time spent initiating fraud alerts; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; disgorgement of profits; nominal and general damages; and other economic and non-economic harm.

597. As a direct and proximate cause of 23andMe's conduct, Plaintiffs and Class Members have suffered injury in fact and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining 23andMe from its conduct. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law.

COUNT EIGHT — BREACH OF FIDUCIARY DUTY

On Behalf of Plaintiffs and the Nationwide Classes, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

598. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

599. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information—including highly sensitive personal genetic information—that was conveyed to and collected, stored, and maintained by 23andMe and that was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach.

600. 23andMe, in taking possession of this highly sensitive information, formed a special relationship with its customers, including Plaintiffs and Class Members.

601. Plaintiffs and Class Members put their trust and confidence in 23andMe's judgment, honesty, and integrity in protecting their Private Information and the various accounts that could be accessed through use (or misuse) of that Private Information.

602. 23andMe knew that Plaintiffs and Class Members were relying on 23andMe to safeguard and accepted that trust and confidence when they accepted Private Information from Plaintiffs and Class Members.

603. As a result of that special relationship, 23andMe was provided with and stored Plaintiffs' and Class Members' private and valuable information, which 23andMe was required by law and industry standards to maintain in confidence.

604. In light of the special relationship between 23andMe and Plaintiffs and Class Members, whereby 23andMe became a guardian of Plaintiffs' and Class Members' Private Information, Defendant undertook a fiduciary duty to act primarily for the benefit of its customers, including Plaintiffs and Class Members, by safeguarding their Private Information.

605. 23andMe had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of this relationship, in particular, to keep secure and maintain the confidentiality of Plaintiffs' and Class Members' Private Information.

606. 23andMe owed a duty to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in 23andMe's possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

607. Plaintiffs and Class Members have a privacy interest in their personal, health, genetic, and proprietary matters, and 23andMe had a duty not to disclose or allow unauthorized access to such confidential information.

608. Plaintiffs' and Class Members' Private Information is not generally known to the public and is confidential by nature. Moreover, Plaintiffs and Class Members did not consent to nor authorize Defendant to release or disclose their Private Information to unknown criminal actors.

609. 23andMe breached its fiduciary duty to Plaintiffs and Class Members when Plaintiffs' and Class Members' Private Information was disclosed to unknown criminal hackers by way of 23andMe's own acts and omissions, as alleged herein.

610. 23andMe knowingly breached its fiduciary duties by failing to safeguard Plaintiffs' and Class Members' Private Information, including by, among other things:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of the Private Information;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control those risks;

c. failing to design and implement information safeguards to control those risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the Data Breach at the time it began or within a reasonable time thereafter and give timely and adequate notice to Plaintiffs and Class Members thereof;

g. failing to follow its own security practices published to its customers;

h. failing to disclose that the hackers had targeted and posted Private Information of customers of Chinese and Ashkenazi Jewish descent;

i. storing Private Information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and

j. making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class Members' Private Information to a criminal third party.

611. But for 23andMe's wrongful breach of its fiduciary duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' privacy would not have been compromised and their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

612. As a direct and proximate result of 23andMe's breach of its fiduciary duties, Plaintiffs 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 Private Information; illegal sale of the

compromised Private Information on the black market; the resulting emotional distress; 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 credit reports and accounts and taking other such protective actions; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; disgorgement of profits; nominal and general damages; and other economic and non-economic harm.

613. As a direct and proximate result of 23andMe's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT NINE — CONVERSION

On Behalf of Plaintiffs and the Nationwide Classes, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

614. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

615. Plaintiffs and Class Members were the owners and possessors of their Private Information.

616. Internet users have a property interest in their Private Information and data.

617. The economic value of this property interest in Private Information is well understood as a robust market for such data drives the entire technology economy. As experts have noted, the world's most valuable resource is "no longer oil, but data," and has been for years now.[92]

618. As the result of 23andMe's wrongful conduct, 23andMe has interfered with Plaintiffs' and Class Members' rights to possess and control such property, to which they had a superior right of

[92] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

possession and control at the time of conversion.

619. As a direct and proximate result of 23andMe's conduct, Plaintiffs and Class Members suffered injury, damage, loss or harm.

620. In failing to adequately safeguard Plaintiffs' Private Information, 23andMe has acted with malice, oppression and in conscious disregard of the Plaintiffs' and Class Members' rights.

621. Plaintiffs and the Class Members did not consent to 23andMe's mishandling and loss of their Private Information.

622. Plaintiffs seek injunctive relief, restitution, and all other damages available under this cause of action.

COUNT TEN — UNJUST ENRICHMENT

On Behalf of Plaintiffs and the Nationwide Classes, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

623. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

624. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conferred upon, collected by, and maintained by 23andMe and that was ultimately stolen in the 23andMe Data Breach.

625. 23andMe was benefitted by the conferral upon it of the Private Information pertaining to Plaintiffs and Class Members and by its ability to retain, use, and profit from that information. 23andMe understood that it was in fact so benefitted.

626. 23andMe also understood and appreciated that the Private Information pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon 23andMe maintaining the privacy and confidentiality of that Private Information.

627. But for 23andMe's willingness and commitment to maintain its privacy and confidentiality, that Private Information would not have been transferred to and entrusted with 23andMe.

628. Because of its use of Plaintiffs' and Class Members' Private Information, 23andMe sold more services than it otherwise would have. 23andMe was unjustly enriched by profiting from the

additional services it was able to market, sell, and create to the detriment of Plaintiffs and Class Members.

629. 23andMe also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

630. 23andMe also benefited through its unjust conduct in the form of the profits it gained through the use of Plaintiffs' and Class Members' Private Information.

631. It is inequitable for 23andMe to retain these benefits.

632. As a result of 23andMe's wrongful conduct as alleged in this Complaint (including among things its failure to employ adequate data security measures, its continued maintenance and use of the Private Information belonging to Plaintiffs and Class Members without having adequate data security measures, and its other conduct facilitating the unauthorized disclosure of that Private Information), 23andMe has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

633. 23andMe's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive Private Information, while at the same time failing to maintain that information secure from unauthorized access by hackers and identity thieves.

634. It is inequitable, unfair, and unjust for 23andMe to retain these wrongfully obtained benefits. 23andMe's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

635. The benefit conferred upon, received, and enjoyed by 23andMe was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for 23andMe to retain the benefit.

636. 23andMe's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their Private Information and has caused the Plaintiffs and Class Members other damages as described herein.

637. Plaintiffs and the Class Members have no adequate remedy at law.

638. 23andMe is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on 23andMe as a result of its wrongful conduct, including specifically: the value to 23andMe of the Private Information that was stolen in the Data Breach; the profits 23andMe received and is receiving from the use of that information; the amounts that 23andMe overcharged Plaintiffs and Class Members for use of 23andMe's products and services; and the amounts that 23andMe should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

COUNT ELEVEN — CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200, *ET SEQ.*

On Behalf of Plaintiffs and the Nationwide Classes, or Alternatively, on behalf of California Plaintiffs and the California Subclasses

639. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

640. The California Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200, *et seq.* ("UCL"), prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

641. By reason of 23andMe's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs and Class Members' Private Information, 23andMe engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

642. 23andMe has violated Cal. Bus. and Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code § 17200 with respect to the services provided to the Nationwide Classes.

643. 23andMe's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that the Private Information of Plaintiffs and Class Members has been compromised for unauthorized parties to see, use, and otherwise exploit.

644. 23andMe's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information also constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code 17200, *et seq.*, in that 23andMe's conduct was substantially injurious to Plaintiffs and Class Members, offensive to public policy, immoral, unethical, oppressive and unscrupulous, and the gravity of 23andMe's conduct outweighs any alleged benefits attributable to such conduct.

645. 23andMe engaged in unlawful acts and practices with respect to the services by establishing the substandard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class Members' Private Information with knowledge that the information would not be adequately protected; and by violating the California Consumer Privacy Act, Cal. Civ. Code § 17598, *et seq.*

646. 23andMe's practices were also unlawful and in violation of Cal. Civ. Code § 1798 *et seq.* and 23andMe's own privacy policy because 23andMe failed to take reasonable measures to protect Plaintiffs' and Class Members' Private Information and failed to take remedial measures such as notifying its users when it first discovered that their Private Information may have been compromised.

647. In addition, 23andMe engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82 and Cal. Health & Safety Code §1280.15(b)(2).

648. 23andMe's business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the Private Information they provided to 23andMe will remain private and secure, when in fact it has not been maintained in a private and secure manner, and that 23andMe would take proper measures to investigate and remediate a data breach, when 23andMe did not do so.

649. Plaintiffs and Class Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of 23andMe's above-described wrongful actions, inaction, and omissions including, inter alia, the unauthorized release and disclosure of their Private Information and lack of notice.

650. But for 23andMe's misrepresentations and omissions, Plaintiffs and Class Members

would not have provided their Private Information to 23andMe or would have insisted that their Private Information be more securely protected.

651. Plaintiffs do not have an adequate remedy at law.

652. As a direct and proximate result of 23andMe's unlawful practices and acts, Plaintiffs and Class Members were injured and lost money or property, including but not limited to the price received by 23andMe for the services, the loss of Plaintiffs' and Class Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described herein.

653. 23andMe knew or should have known that 23andMe's computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' Private Information and that the risk of a data breach or theft was highly likely. 23andMe's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

654. Plaintiffs, on behalf of the Class, seek relief under Cal. Bus. & Prof. Code § 17200, et seq., including, but not limited to, restitution to Plaintiffs and Class Members of money or property that 23andMe may have acquired by means of 23andMe's unlawful and unfair business practices, restitutionary disgorgement of all profits accruing to 23andMe because of 23andMe's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT TWELVE — DECLARATORY JUDGMENT

On Behalf of Plaintiffs and the Nationwide Classes, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

655. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

656. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

657. An actual controversy has arisen in the wake of the 23andMe Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether 23andMe is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future given the publicity around the Data Breach and the nature and quantity of the Private Information stored by 23andMe.

658. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

A. 23andMe continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

B. 23andMe continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

659. The Court also should issue corresponding prospective injunctive relief requiring 23andMe to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information. The Court should enter an injunction requiring, among other things, the following:

A. 23andMe engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

B. 23andMe engage third-party security auditors and internal personnel to run automated security monitoring;

C. 23andMe audit, test, and train security personnel regarding any new or modified procedures;

D. 23andMe segment customer data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

E. 23andMe conduct regular database scans and security checks;

F. 23andMe routinely and continually conduct 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; and

G. 23andMe meaningfully educate customers about the threats they face as a result of the loss of their personal information to third parties, as well as the steps current and former customers should take to protect themselves.

660. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at 23andMe. The risk of another such breach is real, immediate, and substantial. If another breach at 23andMe occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

661. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to 23andMe if an injunction is issued. Among other things, if another data breach occurs at 23andMe, Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to 23andMe of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and 23andMe has a preexisting legal obligation to employ such measures.

662. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at 23andMe, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers if their confidential information were to be further compromised.

VIII. CLAIMS ON BEHALF OF THE STATE SUBCLASSES

CLAIM ON BEHALF OF THE ALASKA SUBCLASS

COUNT THIRTEEN — ALASKA GENETIC PRIVACY ACT, ALASKA STAT. § 18.13.010, *ET SEQ.*

663. The Alaska Plaintiffs identified above, Susan Kennedy and Samantha Van Vleet ("Plaintiffs," for purposes of this Count), individually and on behalf of the Alaska Subclass, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Alaska and on behalf of all other Alaska residents whose Private

Information was compromised as a result of the Data Breach.

664. The Alaska Genetic Privacy Act ("AGPA") mandates that no person may "disclose the results of a DNA analysis unless the person has first obtained the informed and written consent of the person" for the disclosure. Alaska Stat. § 18.13.010(1). "DNA analysis" is defined as "DNA or genetic typing and testing to determine the presence or absence of genetic characteristics in an individual, including tests of nucleic acids or chromosomes in order to diagnose or identify a genetic characteristic." Alaska Stat. § 18.13.100(2).

665. Through 23andMe's processing of its genetic testing kits purchased by Plaintiffs and Alaska Subclass Members, 23andMe performed "DNA analysis" under Alaska Stat. § 18.13.100(2).

666. As set forth above, 23andMe disclosed Plaintiffs' and the results of Alaska Class Members' DNA analyses by failing to enact or enforce adequate data security measures and policies, resulting in the Data Breach. *See* Alaska Stat. § 18.13.010.

667. 23andMe disclosed Plaintiffs' and Alaska Subclass Members' DNA or genetic typing and testing to unknown third parties by allowing them to access their genetic information and genetic testing stored on 23andMe's platform, in addition to other Private Information.

668. The AGPA plainly prohibits such disclosures because they contain, among other things, the results of Plaintiffs' and Alaska Subclass Members' DNA analyses. *See* Alaska Stat. § 18.13.010; Or. Rev. Stat. §§ 192.537, 192.539.

669. 23andMe did not obtain any authorization—including written authorization—from Plaintiffs or Alaska Subclass Members before disclosing their genetic test results, as mandated by Alaska Stat. § 18.13.010.

670. By disclosing the results of their genetic tests, 23andMe violated Plaintiffs' and Alaska Subclass Members' statutorily protected right to privacy in their genetic information under the AGPA.

671. Because of the AGPA violations described above, Plaintiffs and Alaska Subclass Members seeks: (1) injunctive and equitable relief as is necessary to protect their interests by requiring 23andMe to comply with the AGPA; (2) liquidated damages or actual damages, whichever is greater, as provided by the AGPA; and (3) costs and reasonable attorneys' fees pursuant to the AGPA. *See* Alaska Stat. § 18.13.020.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT FOURTEEN — CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE § 56, *ET SEQ.*

672. The California Plaintiffs identified above, Lenora Claire, Daniel Pinho, and Melissa Ryan ("Plaintiffs," for purposes of all Counts brought on behalf of the California Subclasses), individually and on behalf of the California Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other California residents whose Private Information was compromised as a result of the Data Breach.

673. At all relevant times, 23andMe was a health care provider because it had the "purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage the individual's information, or for the diagnosis and treatment of the individual[.]" Cal. Civ. Code § 56.06(a).

674. 23andMe is a provider of healthcare within the meaning of Cal. Civ. Code § 56.06(a) and maintains medical information as defined by Cal. Civ. Code § 56.05.

675. Plaintiffs and Class Members are patients of 23andMe, as defined in Cal. Civ. Code § 56.05(k). Plaintiffs and Class Members provided their personal medical information to 23andMe.

676. At all relevant times, 23andMe collected, stored, managed, and transmitted Plaintiffs' and Class Members' personal medical information.

677. Section 56.10(a) of the Cal. Civ. Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

678. As a result of the Data Breach, 23andMe has misused, disclosed, and/or allowed third parties to access and view Plaintiffs' and Class Members' personal medical information without their written authorization compliant with the provisions of Cal. Civ. Code § 56, *et seq.*

679. The hacker or hackers who committed the Data Breach obtained Plaintiffs' and Class

Members' personal medical information, viewed it, and now have it available to them to sell to other bad actors or otherwise misuse.

680. As a further result of the Data Breach, the confidential nature of Plaintiffs' medical information was breached because of 23andMe's negligence. Specifically, Defendant knowingly allowed and affirmatively acted in a manner that actually allowed unauthorized parties to access and view Plaintiffs' and Class Members' Private Information, which was viewed and used when the unauthorized parties engaged in the above-described fraudulent activity.

681. 23andMe's misuse and/or disclosure of medical information regarding Plaintiffs and Class Members constitutes a violation of Cal. Civ. Code §§ 56.10, 56.11, 56.13, and 56.26.

682. Additionally, because 23andMe collects and analyzes genetic information about Plaintiffs and that information appears to have been disclosed or stolen in the Data Breach due to 23andMe's negligence, 23andMe is liable for the statutory penalties under Cal. Civ. Code §§ 56.17(b) and 56.17(d).

683. As a direct and proximate result of 23andMe's wrongful actions, inaction, omissions, and want of ordinary care, Plaintiffs' and Class Members' personal medical information was disclosed without written authorization.

684. By disclosing Plaintiffs' and Class Members' Private Information without their written authorization, 23andMe violated Cal. Civ. Code § 56, *et seq.*, and their legal duty to protect the confidentiality of such information.

685. 23andMe also violated Cal. Civ. Code §§ 56.06 and 56.101, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

686. As a direct and proximate result of 23andMe's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs' and Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiffs' and Class Members' written authorization.

687. As a direct and proximate result of 23andMe's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach

and its violation of Cal. Civ. Code § 56, *et seq.*, Plaintiffs and Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Plaintiff and Class Member, (iii) punitive damages of up to $3,000 per Plaintiff and Class Member, and (iv) attorneys' fees, litigation expenses and court costs under Cal. Civ. Code § 56.35.

COUNT FIFTEEN — CALIFORNIA CONSUMER PRIVACY ACT, CAL. CIV. CODE § 1798, *ET SEQ.*

688. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other California residents whose Private Information was compromised as a result of the Data Breach.

689. The California Consumer Privacy Act ("CCPA"), portions of which were operative beginning January 1, 2020, was enacted by the California Legislature "to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80)." Cal. Civ. Code § 1798.175. The CCPA applies to "the collection and sale of all personal information collected by a business from consumers." *Id.*

690. "Businesses," defined to include a "corporation" that "collects consumers' personal information" that "does business in the State of California" and has annual gross revenues in excess of $25 million, are required to comply with the CCPA. Cal. Civ. Code §1798.140(d). 23andMe is a "business" under the CCPA.

691. The CCPA protects "consumers." "Consumer" is defined as "a natural person who is a California resident[.]" Cal. Civ. Code § 1798.140(i). Plaintiffs and California Subclass Members are "consumers" within the meaning of the CCPA.

692. The protections of the CCPA extend to "personal information" of consumers. "Personal information" is defined by the CCPA to include "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with

a particular consumer or household." Cal. Civ. Code § 1798.140(v)(1). The Private Information of Plaintiffs and California Subclass Members that was compromised in 23andMe's data breach included "personal information" within the meaning of the CCPA.

693. The CCPA provides consumers with the right to institute a civil action where the consumers' "nonencrypted and nonredacted personal information" was the subject of "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[.]" Cal. Civ. Code § 1798.150(a)(1).

694. Plaintiffs and California Subclass Members provided to 23andMe their nonencrypted and nonredacted personal information as defined in § 1798.81.5 in the form of their Private Information.

695. 23andMe, as a "business" covered by the CCPA, owed a duty to Plaintiffs and California Subclass Members to implement and maintain reasonable security procedures and practices to protect the Private Information of Plaintiffs and California Subclass Members.

696. 23andMe breached this duty. The fact that Plaintiffs' and the California Subclass Members' Private Information was accessed without authorization establishes that 23andMe did not take adequate data security measures to store and protect its customers' Private Information. 23andMe failed to take adequate security measures to protect Plaintiffs' and the California Subclass Members' Private Information.

697. As a direct and proximate result of 23andMe's acts and omissions, Plaintiffs and California Subclass Members were subjected to unauthorized access and exfiltration, theft, or disclosure as a result of 23andMe's violation of the duty.

698. On behalf of the California Subclasses, Plaintiffs seek injunctive relief in the form of an order (a) enjoining 23andMe from continuing to violate the CCPA; and (b) requiring 23andMe to employ adequate security practices consistent with law and industry standards to protect California Class Members' Private Information.

699. Plaintiffs and California Subclass Members are at high risk of suffering, or have already suffered, injuries that cannot be remedied monetarily, such as reductions to their credit scores and

identity theft. As such, the remedies at law available to Plaintiffs and California Subclass Members are wholly inadequate by themselves.

700. The full extent of the existing and potential harm caused by 23andMe's failure to protect its customers' Private Information cannot be remedied by monetary damages alone because monetary compensation does nothing to prevent the reoccurrence of another data breach in the future.

701. Plaintiffs and California Subclass Members seek injunctive relief, actual pecuniary damages suffered as a result of 23andMe's violations described herein, and any other relief the Court deems proper pursuant to this section, such as attorneys' fees.

702. On October 11, 2023, Plaintiff Daniel Pinho sent written notice identifying 23andMe's violation of Cal. Civ. Code § 1798.150(a) and demanding that the Data Breach be cured. On June 25, 2024, Plaintiffs Lenora Claire and Melissa Ryan similarly sent written notice identifying 23andMe's violation of Cal. Civ. Code § 1798.150(a) and demanding that the Data Breach be cured. Accordingly, Plaintiffs seek all relief available under the CCPA, including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

COUNT SIXTEEN — CALIFORNIA CUSTOMER RECORDS ACT, CAL. CIV. CODE § 1798.80, *ET SEQ.*

703. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other California residents whose Private Information was compromised as a result of the Data Breach.

704. The California Customer Records Act requires that any 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, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5.

705. 23andMe is subject to the California Customer Records Act because it owns, maintains,

and licenses personal information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiffs and the Class.

706. 23andMe violated Cal. Civ. Code § 1798.81.5 by failing to adopt and utilize reasonable measures to protect Plaintiffs' personal information.

707. As a direct and proximate result of 23andMe's violations of Cal. Civ. Code § 1798.81.5, the Data Breach described above occurred.

708. Plaintiffs suffered damages and injury including, but not limited to, time and expenses related to monitoring their financial accounts for fraudulent activity, attorneys' fees and expenses in bringing suit to seek redress against 23andMe, an increased, imminent risk of fraud and identity theft, and loss of value of his personally identifying information.

709. Plaintiffs seek relief under Cal. Civ. Code § 1798.84 including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

COUNT SEVENTEEN — INVASION OF PRIVACY, CAL. CONST. ART. 1 § 1

710. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other California residents whose Private Information was compromised as a result of the Data Breach.

711. California established the right to privacy in Article I, Section 1 of the California Constitution.

712. Plaintiffs and the Class had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

713. 23andMe owed a duty to its current and former customers, including Plaintiffs and the Class, to keep their Private Information contained as a part thereof, confidential.

714. 23andMe failed to protect and released to unknown and unauthorized third parties the Private Information of Plaintiffs and the Class.

715. 23andMe allowed unauthorized and unknown third parties access to and examination of the Private Information of Plaintiffs and the Class, by way of 23andMe's failure to protect the Private Information.

716. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and the Class is highly offensive to a reasonable person.

717. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class disclosed their Private Information to 23andMe as part of obtaining genetic testing and analysis services at 23andMe, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

718. The Data Breach at the hands of 23andMe constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

719. 23andMe acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that its information security practices were inadequate and insufficient.

720. Because 23andMe acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class.

721. As a proximate result of the above acts and omissions of 23andMe, the Private Information of Plaintiffs and the Class was disclosed to third parties without authorization, causing Plaintiffs and the Class to suffer damages.

722. Unless and until enjoined, and restrained by order of this Court, 23andMe's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class in that the Private Information maintained by 23andMe can be viewed, distributed, and used by unauthorized persons for years to come.

723. Plaintiffs, on behalf of the Class, seek injunctive relief requiring 23andMe to (i)

strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) to provide adequate dark web monitoring and other threat reduction measures as needed to all Class Members.

724. Plaintiffs and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

COUNT EIGHTEEN — CALIFORNIA CONSUMER LEGAL REMEDIES ACT, CAL. CIV. CODE § 1750, *ET SEQ.*

725. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other California residents whose Private Information was compromised as a result of the Data Breach.

726. 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.

727. 23andMe is a "person" as defined by Cal. Civ. Code §§ 1761(c) and 1770, and has provided "services" as defined by Cal. Civ. Code §§ 1761(b) and 1770.

728. Plaintiffs and the California Subclass Members are "consumers" as defined by Cal. Civ. Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Cal. Civ. Code §§ 1761(e) and 1770.

729. 23andme's acts and omissions, as alleged herein, constitute unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA.

730. 23andme undertook its conduct in a manner that it knew was likely to deceive consumers.

731. 23andme violated the CLRA by "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have[.]" Cal. Civ. Code § 1770(a)(5). 23andme did so, as alleged herein, by representing that its systems were secure and

that it maintained cutting-edge, industry-standard data encryption and security. It also represented through its Privacy Policy that it had adopted and implemented appropriate measures to protect Plaintiffs' and California Subclass Members' Private Information.

732. 23andme also violated the CLRA by improperly handling, storing, and/or protecting either unencrypted or partially encrypted data.

733. As a result of engaging in such conduct, 23andMe has violated the CLRA.

734. As a direct and proximate result of 23andMe's CLRA violations, Plaintiffs and California Subclass Members suffered ascertainable losses including, but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their Private Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (d) 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; (e) the continued risk to their Private Information, which remains in 23andMe's possession and is subject to further unauthorized disclosures so long as 23andMe fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and California Subclass Members; and (g) the diminished value of 23andMe's services they received.

735. Plaintiffs and the California Subclasses seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, and attorneys' fees and costs under the CLRA.

736. On June 25, 2024, Plaintiffs sent written notice identifying 23andMe's violation of Cal. Civ. Code § 1782 and demanding that the Data Breach be cured.

CLAIM ON BEHALF OF THE DELAWARE SUBCLASS

COUNT NINETEEN — DELAWARE CONSUMER FRAUD ACT, 6 DEL. CODE § 2513, *ET SEQ.*

737. The Delaware Plaintiff identified above, Emily Beale ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Delaware and on behalf of all other Delaware residents whose Private Information was compromised as a result of the Data Breach.

738. 23andMe is a "person" within the meaning of 6 Del. Code § 2511(7).

739. 23andMe's genetic testing products and services are "merchandise" within the meaning of 6 Del. Code § 2511(6).

740. The Delaware Consumer Fraud Act ("Delaware CFA") prohibits the "act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, or the concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale, lease or advertisement of any merchandise, whether or not any person has in fact been misled, deceived or damaged thereby." 6 Del. Code § 2513(a).

741. The Delaware Subclass suffered ascertainable loss and actual damages as a direct and proximate result of 23andMe's misrepresentations and concealment of and failure to disclose material information. 23andMe had an ongoing duty to all their customers to refrain from unfair and deceptive practices under the Delaware CFA.

742. As a direct and proximate result of 23andMe's violations of the Delaware CFA, Plaintiff and Delaware Subclass 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting

emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

743. Plaintiff and Delaware Subclass Members seek damages under the Delaware CFA for injury resulting from the direct and natural consequences of Defendants' unlawful conduct. Plaintiff and Delaware Subclass Members also seek an order enjoining 23andMe's unfair, unlawful, and/or deceptive practices, declaratory relief, attorneys' fees, and any other just and proper relief available under the Delaware CFA.

744. 23andMe engaged in gross, oppressive or aggravated conduct justifying the imposition of punitive damages.

CLAIM ON BEHALF OF THE FLORIDA SUBCLASS

COUNT TWENTY — FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, FLA. STAT. § 501.201, *ET SEQ.*

745. The Florida Plaintiff identified above, Harold Velez ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Florida and on behalf of all other Florida residents whose Private Information was compromised as a result of the Data Breach.

746. This cause of action is brought under the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), which, pursuant to Fla. Stat. § 501.202, requires such claims be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

747. 23andMe offers, provisions, and sales or services at issue in this case are "consumer transaction[s]" within the scope of the FDUTPA. *See* Fla. Stat. §§ 501.201-213.

748. Plaintiff and Florida Subclass Members are "individual[s]," and are "consumer[s]" as defined by the FDUTPA. *See* Fla. Stat. § 501.203(7).

749. 23andMe offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. § 501.203.

750. Plaintiff and Florida Subclass Members paid for or otherwise availed themselves and received services from 23andMe, primarily for personal, family, or household purposes.

751. 23andMe engaged in the conduct alleged herein, entering into transactions intended to result, and which did result, in the provision of genetic testing and genealogical research services to or for Plaintiff and Florida Subclass Members.

752. 23andMe's acts, practices, and omissions were done in the course of 23andMe's business of offering and selling genetic testing and geological research services throughout Florida and the United States.

753. The unfair, unconscionable, and unlawful acts and practices of 23andMe alleged herein, and in particular the decisions regarding data security, emanated and arose—with respect to Florida Subclass Members, within the state of Florida, within the scope of the FDUTPA.

754. 23andMe engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. failing to implement and maintain reasonable and adequate computer systems and data security practices to safeguard customer Private Information;

b. omitting, suppressing, and concealing the material fact that its computer systems and data security practices were inadequate to safeguard customer Private Information from unauthorized access and theft;

c. failing to protect the privacy and confidentiality of Plaintiff's and Florida Subclass Members' Private Information; and

d. failing to disclose that the hackers had targeted and posted Private Information of customers of Chinese and Ashkenazi Jewish descent.

755. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including but not limited to the FTC Act, 15 U.S.C. § 45, and the FDUTPA, Fla. Stat. § 501.171(2).

756. 23andMe knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiff and Florida Subclass Members' Private Information and that the risk of a data breach or theft was high.

757. Plaintiff has standing to pursue this claim because as a direct and proximate result of 23andMe's violations of the FDUTPA, Plaintiff and Florida Subclass Members have been "aggrieved" by a violation of the FDUTPA and bring this action to obtain a declaratory judgment that 23andMe's acts or practices violate the FDUTPA. *See* Fla. Stat. § 501.211(a).

758. Plaintiff also has standing to pursue this claim because, as a direct result of 23andMe's knowing violation of the FDUTPA, Plaintiff and the Florida Subclasses are at a substantial and imminent risk of harm as a result of the Data Breach. 23andMe still possesses Plaintiff's and Florida Subclass Members' Private Information, and that Private Information has been both accessed and misused by unauthorized third parties, which is evidence of a substantial and imminent risk of harm to Plaintiff and all Florida Subclass Members, as well as a risk of theft of their Private Information.

759. Plaintiff and Florida Subclass Members are entitled to injunctive relief to protect them from the substantial and imminent risk of identity theft, including, but not limited to:

a. ordering that 23andMe engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

b. ordering that 23andMe engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that 23andMe audit, test, and train security personnel regarding any new or modified procedures;

d. ordering that 23andMe segment customer data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

e. ordering 23andMe to delete, destroy and purge the Private Information of Plaintiffs and Class Members who specifically request it, unless 23andMe can provide to the Court reasonable justification for the retention and use of such

information when weighed against the privacy interests of Plaintiffs and Class Members;

f. ordering that 23andMe conduct regular database scans and security checks;

g. ordering that 23andMe routinely and continually conduct 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;

h. ordering 23andMe to meaningfully educate customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the

i. steps present and former customers should take to protect themselves; and

j. ordering 23andMe to take reasonable steps to protect Plaintiffs and Florida Subclass Members against harm from misuse of their Private Information that was misappropriated in the Data Breach.

760. Plaintiff brings this action on behalf of themself and Florida Subclass Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Florida Subclass Members, and the public from 23andMe's unfair methods of competition and unfair, unconscionable, and unlawful practices. 23andMe's wrongful conduct as alleged in herein has had widespread impact on the public at large.

761. The above unfair, unconscionable, and unlawful practices and acts by 23andMe were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Florida Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

762. 23andMe's actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

763. Plaintiff and Florida Subclass Members seek relief under the FDUTPA, Fla. Stat. § 501.201, *et seq.*, including, but not limited to: damages; restitution; a declaratory judgment that 23andMe's actions and/or practices violate the FDUTPA; injunctive relief enjoining 23andMe, their employees, parents, subsidiaries, affiliates, executives, and agents from violating the FDUTPA; an order that 23andMe engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-

party security auditors; an order that 23andMe engage third-party security auditors and internal personnel to run automated security monitoring; an order that 23andMe audit, test, and train security personnel regarding any new or modified procedures; an order that 23andMe segment customer data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system; ordering that 23andMe conduct regular database scans and security checks; an order that 23andMe routinely and continually conduct 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; an order requiring 23andMe to meaningfully educate customers about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps current and former customers should take to protect themselves; an order requiring 23andMe to take reasonable steps to protect Plaintiff and Florida Subclass Members against harm from misuse of their Private Information that was misappropriated in the Data Breach; attorneys' fees and costs; and any other just and proper relief.

CLAIMS ON BEHALF OF THE GEORGIA SUBCLASS

COUNT TWENTY-ONE — GEORGIA FAIR BUSINESS PRACTICES ACT, GA. CODE ANN. § 10-1-399, *ET SEQ.*

764. The Georgia Plaintiffs identified above, R.T. and Jaime Kelly ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Georgia and on behalf of all other Georgia residents whose Private Information was compromised as a result of the Data Breach.

765. 23andMe, Plaintiff, and Georgia Subclass Members are "persons" within the meaning of the Georgia Fair Business Practices Act ("GFBPA"). Ga. Code Ann. § 10-1- 399(a).

766. 23andMe is engaged in, and its acts and omissions affect, trade and commerce under Ga. Code Ann. § 10-1-392(28). Further, 23andMe is engaged in "consumer acts or practices," which are defined as "acts or practices intended to encourage consumer transactions" under Ga. Code Ann. § 10-1-392(7).

767. 23andMe engaged in "[u]nfair or deceptive acts or practices in the conduct of consumer

transactions and consumer acts or practices in trade or commerce" in violation of Ga. Code Ann. § 10-1-393(a). Those acts and practices include those expressly declared unlawful by Ga. Code Ann. § 10-1-393(b), such as:

a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another; and

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

768. In addition, 23andMe engaged in the unfair and deceptive acts and practices described below that, while not expressly declared unlawful by Ga. Code Ann. § 10-1-393(b), are prohibited by Ga. Code Ann. § 10-1-393(a).

769. In the course of its business, 23andMe engaged in unfair acts and practices prohibited by Ga. Code Ann. § 10-1-393(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Georgia Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach; and

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Georgia Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

770. In the course of its business, 23andMe also engaged in deceptive acts and practices prohibited by Ga. Code Ann. § 10-1-393(a), including:

a. Misrepresenting that 23andMe would protect the privacy and confidentiality of Plaintiff's and Georgia Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

b. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Georgia Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Georgia Subclass Members' Private Information; and

d. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Georgia Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

771. The misrepresentations and omissions described in the preceding paragraph were material and made intentionally and knowingly with the intent that Plaintiff and Georgia Subclass Members rely upon them in connection with providing to 23andMe their extremely sensitive and valuable PII.

772. 23andMe knew of the inadequate security controls and vulnerabilities in its data security systems storing Plaintiff and the Georgia Subclass Members' sensitive and valuable Private Information but concealed these security failings.

773. 23andMe's deceptive acts and practices were likely to and did in fact deceive the public at large and reasonable consumers, including Plaintiff and Georgia Subclass Members, regarding the security and safety of the PII in its care.

774. 23andMe knew or should have known that by collecting, selling, and trafficking in Private Information, Plaintiff and Georgia Subclass Members would reasonably rely upon and assume 23andMe's data systems were secure unless 23andMe otherwise informed them.

775. Plaintiff and Georgia Subclass Members had no effective means on their own to discover the truth. 23andMe did not afford Plaintiff and Georgia Subclass Members any opportunity to inspect 23andMe's data security, learn that it was inadequate and non-compliant with legal requirements, or otherwise ascertain the truthfulness of 23andMe's representations and omissions regarding 23andMe's ability to protect data and comply with the law.

776. Plaintiff and Georgia Subclass Members relied to their detriment upon 23andMe's representations and omissions regarding data security, including 23andMe's failure to alert customers that its privacy and security protections were inadequate and insecure and thus were vulnerable to attack.

777. Had 23andMe disclosed to Plaintiff and Georgia Subclass Members that its data systems

were not secure and, thus, vulnerable to attack, 23andMe would have been forced to adopt reasonable data security measures and comply with the law. 23andMe was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and the Georgia Subclass. 23andMe accepted the responsibility of protecting the data, while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Georgia Subclass Members acted reasonably in relying on 23andMe's misrepresentations and omissions, the truth of which they could not have discovered.

778. 23andMe acted intentionally, knowingly, and maliciously to violate the GFBPA, and recklessly disregarded Plaintiff and Georgia Subclass Members' rights.

779. 23andMe's violations present a continuing risk to Plaintiff and Georgia Subclass Members, as well as to the general public.

780. 23andMe's unlawful acts and practices complained of herein affect the consumer marketplace and the public interest, including the millions of U.S. residents and many Georgia Subclass Members affected by the 23andMe Data Breach.

781. But for 23andMe's violations of the GFBPA described above, the 23andMe Data Breach would not have occurred.

782. The GFBPA permits any person who suffers injury or damages as a result of the violation of its provisions to bring an action against the person or persons engaged in such violations. Ga. Code Ann. § 10-1-399(a).

783. As a direct and proximate result of 23andMe's GFBPA violations, Plaintiff and Georgia Subclass 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports

and accounts and taking other such protective actions; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

784. Plaintiff brings this action on behalf of themselves and Georgia Subclass Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers and the public at large to make informed decisions related to the security of their sensitive Private Information, and to protect the public from 23andMe's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices.

785. Plaintiff and Georgia Subclass Members are entitled to a judgment against 23andMe for actual and consequential damages; general, nominal, exemplary, and trebled damages and attorneys' fees pursuant to the GFBPA; costs; and such other further relief as the Court deems just and proper.

COUNT TWENTY-TWO — GEORGIA UNIFORM DECEPTIVE PRACTICES ACT, GA. CODE. ANN. §§ 10-1-370, *ET SEQ.*

786. The Georgia Plaintiffs identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Georgia and on behalf of all other Georgia residents whose Private Information was compromised as a result of the Data Breach.

787. 23andMe, Plaintiff, and Georgia Subclass Members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("UDTPA").

788. 23andMe engaged in deceptive trade practices in the conduct of its business, in violation of Ga. Code Ann. § 10-1-372(a), 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 if they are of another; and

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

789. 23andMe's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Georgia Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Georgia Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Georgia Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Georgia Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Georgia Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Georgia Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

790. 23andMe's representations and omissions 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' Private Information.

791. 23andMe intended to mislead Plaintiff and Georgia Subclass Members and induce them to rely on its misrepresentations and omissions.

792. In the course of its business, 23andMe engaged in activities with a tendency or capacity

to deceive.

793. 23andMe acted intentionally, knowingly, and maliciously to violate the UDTPA, and recklessly disregarded Plaintiff and Georgia Subclass Members' rights.

794. Had 23andMe disclosed to Plaintiff and Georgia Subclass Members that its data systems were not secure and, thus, vulnerable to attack, 23andMe would have been forced to adopt reasonable data security measures and comply with the law. 23andMe was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and the Georgia Subclass. 23andMe accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Georgia Subclass Members acted reasonably in relying on 23andMe's misrepresentations and omissions, the truth of which they could not have discovered.

795. As a direct and proximate result of 23andMe's deceptive trade practices, Plaintiff and Georgia Subclass 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

796. Plaintiff and Georgia Subclass Members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under Ga. Code Ann. § 10-1-373.

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS

COUNT TWENTY-THREE — ILLINOIS CONSUMER FRAUD ACT, 815 ILL. COMP. STAT. § 505, *ET SEQ.*

797. The Illinois Plaintiffs identified above, Michele Bacus, Alexandra Hoffman, and Eileen Mullen ("Plaintiffs," for purposes of this Count), individually and on behalf of the Illinois Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Illinois and on behalf of all other Illinois residents whose Private Information was compromised as a result of the Data Breach.

798. The Illinois Consumer Fraud Act ("ICFA") is a regulatory and remedial statute intended to protect consumers, borrowers, and business persons against fraud, unfair methods of competition, and other unfair and deceptive business practices.

799. 23andMe is a "person" as defined by 815 Ill. Comp. Stat. § 505/1(c).

800. Plaintiffs and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. § 505/1(e).

801. 23andMe's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

802. Here, 23andMe's conduct is unfair under ICFA. First, 23andMe violated numerous regulations regarding HIPAA guidelines for safeguarding PHI and PII. In allowing the Data Breach to occur, 23andMe failed to: (a) ensure the confidentiality, integrity, and availability of all electronic protected health information the entity creates, receives, maintains, or transmits (45 C.F.R. § 164.306(a)(1)); (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information (45 C.F.R. § 164.306(a)(2)); (c) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required (45 C.F.R. § 164.306(a)(3)); (d) implement policies and procedures to prevent, detect, contain, and correct security violations (45 C.F.R. § 164.308(1)); (e) implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights (45 C.F.R. § 164.312(a)(1)); (f) have in place appropriate administrative, technical, and physical safeguards to protect the privacy of

protected health information (45 C.F.R. § 164.530(c)(1)); and (g) mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of protected health information (45 C.F.R. § 164.530(f)). Accordingly, 23andMe's inability to safeguard Plaintiffs' and Illinois Subclass Members' Private Information offends public policy.

803. Second, 23andMe's conduct against Plaintiffs and the Illinois Subclasses is oppressive in that even a request to delete data does not securely delete all data. Plaintiffs and the Illinois Subclasses were assured by 23andMe that their Private Information would be secured.

804. And third, 23andMe's failure to safeguard Plaintiffs' and Illinois Subclass Members' Private Information and leaving it exposed to cybercriminals and other unauthorized actors constitutes a substantial injury in that Plaintiffs and the Illinois Subclasses will not only have to spend the remainder of their lives at greater risk for identity theft and fraud (having to constantly monitor for the same), but also live with the knowledge that their most intimate genetic details are subject to public view.

805. Finally, 23andMe violated FTC guidelines as alleged herein. These failures constitute unfair acts or practices, subjecting them to an ICFA claim. 15 U.S.C. § 45.

806. In sum, 23andMe's numerous failures in safeguarding Plaintiffs' and Illinois Subclass Members' Private Information violates ICFA.

807. Pursuant to Section 5 of the FTC Act, failure to protect Private Information can constitute an unfair act or practice.

808. The state of Illinois has also addressed the protection of Private Information by enacting the Personal Information Protection Act ("PIPA"), 815 Ill. Comp. Stat. 530/1 *et seq.*

809. PIPA requires ". . . implement[ation] and maintain[enance of] reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure" of PHI by data collectors. 815 Ill. Comp. Stat. 530/45.

810. Failure to comply with PIPA constitutes an unlawful practice under ICFA. 815 Ill. Comp. Stat. § 530/20.

811. As a direct and proximate result of 23andMe's IFCA violations, Plaintiffs and Illinois Subclass Members suffered ascertainable losses including, but not limited to: (a) actual identity theft;

(b) the compromise, publication, and/or theft of their Private Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (d) 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; (e) the continued risk to their Private Information, which remains in 23andMe's possession and is subject to further unauthorized disclosures so long as 23andMe fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Illinois Subclass Members; and (g) the diminished value of 23andMe's services they received.

812. 23andMe's failure to safeguard Plaintiffs' and Illinois Subclass Members' Private Information in violation of HIPAA and the FTC Act, PIPA and common violations were the direct and proximate cause of damages incurred by Plaintiffs and the Illinois Subclasses.

813. Accordingly, Plaintiffs, on behalf of themselves and the other members of the Illinois Subclasses, seek compensatory damages for the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs as provided by 815 Ill. Comp. Stat. § 505/10(a) and, in the event that 23andMe's violations are found to be willful, punitive damages.

COUNT TWENTY-FOUR — ILLINOIS GENETIC INFORMATION PRIVACY ACT, 410 ILL. COMP. STAT. ANN. 513, *ET SEQ.*

814. The Illinois Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Illinois Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Illinois and on behalf of all other Illinois residents whose Private Information was compromised as a result of the Data Breach.

815. The Genetic Information Privacy Act ("GIPA"), 410 Ill. Comp. Stat. Ann. 513, *et seq.*, covers "[c]onfidentiality of genetic information" and provides in relevant part: "Except as otherwise provided in this Act, genetic testing and information derived from genetic testing is confidential and

privileged and may be released only to the individual tested and to persons specifically authorized, in writing in accordance with Section 30, by that individual to receive the information." 410 Ill. Comp. Stat. Ann. 513/15(a).

816. GIPA incorporates the definition of "genetic information" from 45 C.F.R. § 160.103, which defines the term as "information about" an individual's "genetic tests," "[t]he genetic tests of family members of the individual," "[t]he manifestation of a disease or disorder in family members of such individual," or "[a]ny request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual." 410 Ill. Comp. Stat. Ann. 513/10.

817. GIPA also incorporates the definition of "genetic test" from 45 C.F.R. § 160.103, which defines the term as "an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes." 410 Ill. Comp. Stat. Ann. 513/10.

818. The test performed by 23andMe qualifies as "genetic testing" under GIPA because it detects, *inter alia*, genotypes and mutations.

819. The information compromised in the breach of 23andMe's platform included genetic information, genetic testing, and information derived from such information. For example, the origin of Plaintiffs' ancestors, the list of other 23andMe users identified by 23andMe as Plaintiffs' DNA Relatives, and the information on the number of DNA segments Plaintiffs shared with those other users were all information about, and derived from, the 23andMe genetic test Plaintiffs purchased. Moreover, these results serve as a receipt of genetic services performed by 23andMe for Plaintiffs.

820. 23andMe negligently and recklessly released Plaintiffs and Illinois Subclass Members' genetic information and other confidential and highly sensitive Private Information by failing to adequately safeguard that information from malicious actors. Considering the number of data breaches and the sensitivity of the information it possessed, 23andMe was aware or should have been aware of the need to implement robust security measures to protect such information. It consciously refused to do so.

821. By negligently and recklessly releasing Plaintiffs' and Illinois Subclass Members' information (including genetic testing and information derived from genetic testing performed by

23andMe) to unauthorized parties, as alleged above, 23andMe violated GIPA.

822. Accordingly, Plaintiffs and Illinois Subclass Members are entitled to, and seek, damages of "$2,500 or actual damages, whichever is greater," for each negligent violation, or "$15,000 or actual damages, whichever is greater," for each intentional or reckless violation, as well as reasonable attorney's fees and costs. 410 Ill. Comp. Stat. Ann. 513/40.

823. Plaintiffs and Illinois Subclass Members are also authorized to obtain injunctive relief to prevent future violations. *Id.*

CLAIMS ON BEHALF OF THE MASSACHUSETTS SUBCLASS

COUNT TWENTY-FIVE — MASSACHUSETTS CONSUMER PROTECTION ACT, MASS. GEN. LAWS CH. 93A, *ET SEQ.*

824. The Massachusetts Plaintiffs identified above, Anna DaVeiga and Neil Haven ("Plaintiffs," for purposes of this Count), individually and on behalf of the Massachusetts Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Massachusetts and on behalf of all other Massachusetts residents whose Private Information was compromised as a result of the Data Breach.

825. Plaintiffs and Massachusetts Subclass Members are "persons" within the meaning of Mass. Gen. Laws Ch. 93A, §1(a).

826. At all relevant times, 23andMe has been engaged in "trade" and "commerce" within the meaning of Mass. Gen. Laws Ch. 93A, §1(b).

827. 23andMe engaged in the use or employment of unfair acts or practices prohibited by Chapter 93A §§2 and 9 by implementing and maintaining unreasonable data security measures that were inadequate to protect Private Information and prevent the Data Breach and by violating Mass. Gen. Laws Ch. 111, §70G(b).

828. 23andMe's affirmative acts in implementing and maintaining unreasonable data security measures were unfair within the meaning of Chapter 93A because such conduct violated the common law and undermined public policy that required 23andMe to protect Private Information as reflected in statutes such as Mass. Gen. Laws Ch. 111, §70G and the FTC Act, 15 U.S.C. §45(a)(1), which prohibit unfair trade practices.

829. 23andMe's affirmative acts in implementing and maintaining unreasonable data security measures were also unfair within the meaning of Chapter 93A because such conduct was immoral, unethical, oppressive, and unscrupulous; caused substantial injury to consumers; and provided no benefit to consumers.

830. Plaintiffs and Massachusetts Subclass Members reasonably expected 23andMe to implement and maintain reasonable data security measures that complied with industry standards and could prevent the Data Breach and protect Private Information.

831. Plaintiffs and Massachusetts Subclass Members had no knowledge and could not have reasonably known that 23andMe implemented and maintained unreasonable data security measures. Because 23andMe was solely responsible for implementing and maintaining reasonable data security measures to protect Private Information, neither Plaintiffs nor Massachusetts Subclass Members could have avoided the injuries they sustained.

832. There were reasonably available alternatives to further 23andMe's legitimate business interests, other than its conduct responsible for the Data Breach.

833. 23andMe willfully engaged in the unfair acts and practices described above and knew or should have known that those acts and practices were unfair in violation of Chapter 93A.

834. 23andMe's conduct has deprived Plaintiffs and Massachusetts Subclass Members their right to control the use and dissemination of their Private Information.

835. On June 25, 2024, Plaintiffs sent 23andMe presuit notice demand letters, pursuant to Mass. Gen. Laws Ch. 93A, §9.

836. As a direct and proximate result of 23andMe's unfair practices and violation of Chapter 93A, Plaintiffs and Massachusetts Subclass Members have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to damages and other relief as this Court considers necessary and proper.

CLAIMS ON BEHALF OF THE MARYLAND SUBCLASS

COUNT TWENTY-SIX — MARYLAND CONSUMER PROTECTION ACT, MARYLAND COMMERCIAL LAW CODE § 13-101, *ET SEQ.*

837. The Maryland Plaintiff identified above, Claire Paddy ("Plaintiff," for purposes of this

Count), individually and on behalf of the Maryland Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Maryland and on behalf of all other Maryland residents whose Private Information was compromised as a result of the Data Breach.

838. The Maryland Consumer Protection Act ("CPA") bars "unfair, abusive, or deceptive trade practices" in the sale or offer for sale of any consumer good or consumer services. Md. Com. Law Code § 13-303(1)-(2). The Act authorizes an action by "any person" "to recover for injury or loss sustained by him as the result of a practice prohibited by this title." *Id.* § 13-408(a).

839. Plaintiff and Maryland Subclass Members are "persons" and "consumers" as defined in the CPA. *Id.* § 13-101(c), (h).

840. 23andMe is a "person" as defined in the CPA. *Id.* § 13-101(c).

841. 23andMe's genetic testing products and services are "consumer goods" as defined in the CPA. *Id.* § 13-101(d)(1)-(2).

842. 23andMe engaged in unfair or deceptive trade practices in the sale of consumer goods, in violation . Md. Com. Law Code § 13-303(1)-(2), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Maryland Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Maryland Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Maryland Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Maryland Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Failing to timely and adequately notify Plaintiff and Maryland Subclass Members of the Data Breach;

g. Failing to disclose that the hackers had targeted and posted Private Information of customers of Chinese and Ashkenazi Jewish descent;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Maryland Subclass Members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Maryland Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

843. 23andMe's representations and omissions 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' Private Information.

844. 23andMe acted intentionally, knowingly, and maliciously to violate Maryland's CPA, and recklessly disregarded Plaintiff's and Maryland Subclass Members' rights.

845. As a result of their violations of Maryland's CPA, Plaintiffs and Maryland Subclass Members have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to damages and other relief as this Court considers necessary and proper.

CLAIMS ON BEHALF OF THE MISSOURI SUBCLASS

COUNT TWENTY-SEVEN — MISSOURI MERCHANDISE PRACTICES ACT, MO. REV. STAT. § 407.010, *ET SEQ.*

846. The Missouri Plaintiff identified above, J.S. ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Missouri and on behalf of all other Missouri residents whose Private Information was compromised as a result of the Data Breach.

847. 23andMe is a "person" as defined by Mo. Rev. Stat. § 407.010(5).

848. 23andMe advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat.

§ 407.010(4), (6) and (7).

849. Plaintiff and Missouri Subclass Members purchased or leased goods or services primarily for personal, family, or household purposes.

850. 23andMe engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Missouri Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Missouri Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Failing to disclose that the hackers had targeted and posted Private Information of customers of Chinese and Ashkenazi Jewish descent;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Missouri Class Members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Missouri Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Missouri Subclass Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Missouri Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

851. 23andMe's representations and omissions 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' Private Information.

852. 23andMe intended to mislead Plaintiff and Missouri Subclass Members and induce

them to rely on its misrepresentations and omissions.

853. 23andMe acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Plaintiff and Missouri Subclass Members' rights.

854. As a direct and proximate result of 23andMe's multiple, separate violations of Mo. Rev. Stat. § 407.010, Plaintiff and Missouri Subclass Members suffered ascertainable losses including, but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their Private Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (d) 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; (e) the continued risk to their Private Information, which remains in 23andMe's possession and is subject to further unauthorized disclosures so long as 23andMe fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Missouri Subclass Members; and (g) the diminished value of 23andMe's services they received.

855. Plaintiffs and Missouri Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT TWENTY-EIGHT — NEW JERSEY CONSUMER FRAUD ACT, N.J. STAT. ANN. § 56:8-1, *ET SEQ.*

856. The New Jersey Plaintiffs identified above, M.L., Rachel DeCarlo, and A.B. ("Plaintiffs," for purposes of this Count), individually and on behalf of the New Jersey Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of New Jersey and on behalf of all other New Jersey residents whose Private Information was compromised as a result of the Data Breach.

857. The New Jersey Consumer Fraud Act ("CFA") makes unlawful "[t]he act, use or employment by any person of any commercial practice that is unconscionable or abusive, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby[.]" N.J. Stat. Ann. § 56:8-2.

858. 23andMe, Plaintiffs, and New Jersey Subclass Members are "persons" within the meaning of N.J. Stat. Ann. § 56:8-1(d).

859. 23andMe engaged in "sales" of "merchandise" within the meaning of N.J. Stat. Ann. § 56-8-1(c), (e).

860. Plaintiffs and New Jersey Subclass Members are consumers who made payments to 23andMe for the furnishing of services that were primarily for personal, family, or household purposes.

861. New Jersey CFA claims for unconscionable commercial practice need not allege any fraudulent statement, representation, or omission by the defendant. The standard of conduct the term "unconscionable" entails is a lack of good faith, honesty in fact, and observance of fair dealing. Intent is not an element for allegations related to unconscionable commercial practices.

862. Here, 23andMe's conduct was unconscionable under the New Jersey CFA in its failure to maintain adequate data security and to safeguard the Private Information in its possession.

863. Specifically, 23andMe's handling and protection of Plaintiffs' and New Jersey Subclass Members' Private Information was unconscionable commercial practice for the following reasons, among others.

864. Plaintiffs and New Jersey Subclass Members had no choice as to whether to provide their Private Information to 23andMe, nor the categories of Private Information, in order to use 23andMe's services.

865. The terms and conditions under which Plaintiffs and New Jersey Subclass Members agreed to provide Private Information to 23andMe, and how 23andMe was to protect their Private Information were non-negotiable and were presented on a take-it-or-leave it basis to Plaintiffs and New

Jersey Subclass Members.

866. Plaintiffs and New Jersey Subclass Members were unable to discover the true state of 23andMe's data security measures and take measures on their own to protect their Private Information once it was in 23andMe's possession. Thus, Plaintiffs and New Jersey Subclass Members were completely dependent upon 23andMe to protect their Private Information once it was in 23andMe's possession.

867. Indeed, 23andMe lulled Plaintiffs and New Jersey Subclass Members into a false sense of security by representing that their Private Information would be well-taken-care-of. 23andMe specifically states in its Privacy Statement that:

> When you explore your DNA with 23andMe, you entrust us with important personal information. That's why, since day one, protecting your privacy has been our number one priority. We're committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected.[93]

868. With respect to protection of Private Information in general, 23andMe stated that:

> 23andMe takes seriously the trust you place in us. To prevent unauthorized access or disclosure, to maintain data accuracy, and to ensure the appropriate use of information, 23andMe uses a range of physical, technical, and administrative measures to safeguard your Personal Information, in accordance with current technological and industry standards. In particular, all connections to and from our website are encrypted using Secure Socket Layer (SSL) technology.[94]

869. 23andMe, operating in New Jersey, engaged in unconscionable trade acts or practices in the conduct of trade or commerce, in violation of N.J. Stat. Ann. § 56:8-2, including but not limited to the following:

a. failing to implement and maintain reasonable and adequate computer systems and data security practices to safeguard customer Private Information;

b. failing to disclose that the hackers had targeted and posted Private Information of customers of Chinese and Ashkenazi Jewish descent;

c. omitting, suppressing, and concealing the material fact that its computer systems and data security practices were inadequate to safeguard customer Private Information from unauthorized access and theft; and

---

[93] 23andMe, Inc., *Your privacy comes first*, supra, note 3.

[94] 23andMe, Inc., *How is my personal information protected?*, https://customercare.23andme.com/hc/en-us/articles/202907840-How-Is-My-Personal-Information-Protected (last visited June 24, 2024).

d. failing to protect the privacy and confidentiality of Plaintiffs' and New Jersey Subclass Members' Private Information.

870. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including by not limited to the FTC Act, 15 U.S.C. § 45, and the New Jersey CFA, N.J. Stat. Ann. § 56:8-163.

871. 23andMe's data protection practices are contrary to public policy in that they fail to comply with FTC rules and regulations relating to data security and other applicable standards as is set forth above.

872. 23andMe still possesses Plaintiffs' and New Jersey Subclass Members' Private Information, and that Private Information has been both accessed and misused by unauthorized third parties. Plaintiffs and New Jersey Subclass Members will have to spend the remainder of their lives at greater risk for harm, identity theft, and fraud (having to constantly monitor for the same).

873. The foregoing unconscionable commercial practices emanated from New Jersey and were directed at consumers/purchasers in New Jersey and in each state where Defendant did business.

874. As a direct and proximate result of 23andMe's multiple, separate violations of N.J. Stat. Ann. § 56:8-2, Plaintiffs and New Jersey Subclass 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products;

nominal and general damages; and other economic and non-economic harm.

875. Plaintiffs and New Jersey Subclass Members were injured because they: (a) would not have paid for 23andMe's services had they known the true nature and character of 23andMe's data security practices; (b) would not have entrusted their Private Information to 23andMe in the absence of promises that 23andMe would keep their information reasonably secure; and/or (c) would not have entrusted their Private Information to 23andMe in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

876. On behalf of themselves and other members of the Class, Plaintiffs are entitled to recover legal and/or equitable relief, including an order enjoining 23andMe's unlawful conduct, treble damages, costs, and reasonable attorneys' fees pursuant to N.J. Stat. Ann. § 56:8-19, and any other just and appropriate relief.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT TWENTY-NINE — NEW YORK GENERAL BUSINESS LAW, N.Y. GEN. BUS. LAW § 349, *ET SEQ.*

877. The New York Plaintiffs identified above, L.G. and Tracy Scott ("Plaintiffs," for purposes of this Count), individually and on behalf of the New York Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of New York and on behalf of all other New York residents whose Private Information was compromised as a result of the Data Breach.

878. 23andMe engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and New York Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New York Subclass Members' Private

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and New York Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New York Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New York Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

879. 23andMe's representations and omissions 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' Private Information.

880. 23andMe acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiffs and New York Subclass Members' rights.

881. As a direct and proximate result of 23andMe's deceptive and unlawful acts and practices, Plaintiffs and New York Subclass 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; lost work time; lost value of the Private Information; lost value of access to their Private Information

permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

882. 23andMe's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New York Subclass Members affected by the Data Breach.

883. The above deceptive and unlawful practices and acts by 23andMe caused substantial injury to Plaintiffs and New York Subclass Members that they could not reasonably avoid.

884. Plaintiffs and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS

COUNT THIRTY —NORTH CAROLINA IDENTITY THEFT PROTECTION ACT, N.C. GEN. STAT. § 75-60, *ET SEQ.*

885. The North Carolina Plaintiff identified above, Pamela Zager-Maya ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of North Carolina and on behalf of all other North Carolina residents whose Private Information was compromised as a result of the Data Breach.

886. 23andMe is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "Private Information"), as defined by N.C. Gen. Stat. § 75-61(1).

887. Plaintiff and North Carolina Subclass Members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

888. 23andMe is required to accurately notify Plaintiff and North Carolina Subclass Members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons) without unreasonable delay

under N.C. Gen. Stat. § 75-65.

889. Plaintiff's and North Carolina Subclass Members' Private Information includes PII as covered under N.C. Gen. Stat. § 75-61(10).

890. Because 23andMe discovered a security breach and had notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), 23andMe had an obligation to disclose the 23andMe Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

891. By failing to disclose the 23andMe Data Breach in a timely and accurate manner, 23andMe violated N.C. Gen. Stat. § 75-65.

892. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. § 75-1.1.

893. As a direct and proximate result of 23andMe's violations of N.C. Gen. Stat. § 75 65, Plaintiff and North Carolina Subclass Members have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to damages and other relief as this Court considers necessary and proper.

894. Plaintiff and North Carolina Subclass Members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorney's fees.

COUNT THIRTY-ONE — NORTH CAROLINA UNFAIR TRADE PRACTICES ACT, N.C. GEN. STAT. §§ 75-1.1, *ET SEQ.*

895. The North Carolina Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of North Carolina and on behalf of all other North Carolina residents whose Private Information was compromised as a result of the Data Breach.

896. 23andMe advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. § 75-1.1(b).

897. 23andMe engaged in unfair and deceptive acts and practices in or affecting commerce,

in violation of N.C. Gen. Stat. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and North Carolina Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and North Carolina Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and North Carolina Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and North Carolina Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and North Carolina Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and North Carolina Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

898. 23andMe's representations and omissions 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' Private Information.

899. 23andMe intended to mislead Plaintiff and North Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

900. Had 23andMe disclosed to Plaintiff and North Carolina Subclass Members that its data systems were not secure and, thus, vulnerable to attack, 23andMe would have been forced to adopt reasonable data security measures and comply with the law. 23andMe was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and the North

Carolina Subclass. 23andMe accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the North Carolina Subclass Members acted reasonably in relying on 23andMe's misrepresentations and omissions, the truth of which they could not have discovered.

901. 23andMe acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and North Carolina Subclass Members' rights.

902. As a direct and proximate result of 23andMe's unfair and deceptive acts and practices, Plaintiff and North Carolina Subclass 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

903. 23andMe's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. § 75-8.

904. Plaintiff and North Carolina Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE OREGON SUBCLASS

COUNT THIRTY-TWO — OREGON GENETIC PRIVACY LAW, OR. REV. STAT. § 192.531, *ET SEQ.*

905. The Oregon Plaintiffs identified above, Cody Vogel and Daniel Anderson ("Plaintiffs," for purposes of this Count), individually and on behalf of the Oregon Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Oregon and on behalf of all other Oregon residents whose Private Information was compromised as a result of the Data Breach.

906. "[A]n individual's genetic information and DNA sample are private and must be protected, and an individual has a right to the protection of that privacy." Or. Rev. Stat. § 192.537(1). "Any person authorized . . . by an individual . . . to obtain, retain or use an individual's genetic information or any DNA sample must maintain the confidentiality of the information or sample and protect the information or sample from unauthorized disclosure or misuse." *Id.*

907. The Oregon Genetic Privacy Law ("OGPL") forbids the disclosure of "the identity of an individual upon whom a genetic test has been performed or the identity of a blood relative of the individual, or to disclose genetic information about the individual or a blood relative of the individual in a manner that permits identification of the individual" except in certain enumerated circumstances. Or. Rev. Stat. § 192.539(1). This prohibition applies "to any redisclosure by any person after another person has disclosed genetic information or the identity of an individual upon whom a genetic test has been performed, or has disclosed genetic information or the identity of a blood relative of the individual." Or. Rev. Stat. § 192.539(2).

908. 23andMe's above-described conduct and misrepresentations of its security practices and procedures constitutes a "knowing violation based on a fraudulent misrepresentation" of Or. Rev. Stat. § 192.537 and § 192.539, for which Plaintiffs and Oregon Subclass Members are entitled to the greater of their actual damages or $15,000 in statutory damages for each violation of Or. Rev. Stat. § 192.537 and the greater of their actual damages or $150,000 in statutory damages for each violation of Or. Rev. Stat. § 192.539. Or. Rev. Stat. § 192.541(2)(d), (3)(d).

909. Alternatively, 23andMe's above-described conduct constitutes a "knowing or reckless

violation" of Or. Rev. Stat. § 192.537 and § 192.539, for which Plaintiffs and Oregon Subclass Members are entitled to the greater of their actual damages or $10,000 in statutory damages for each violation of Or. Rev. Stat. § 192.537 and the greater of their actual damages or $100,000 in statutory damages for each violation of Or. Rev. Stat. § 192.539. Or. Rev. Stat. § 192.541(2)(c), (3)(c).

910. Alternatively, 23andMe's above-described conduct constitutes a "negligent violation" of ORS § 192.537 and § 192.539, for which Plaintiffs and Oregon Subclass Members are entitled to the greater of their actual damages or $500 in statutory damages for each violation of Or. Rev. Stat. § 192.537 and the greater of their actual damages or $5,000 in statutory damages for each violation of Or. Rev. Stat. § 192.539. Or. Rev. Stat. § 192.541(2)(b), (3)(b).

911. Alternatively, should the Court find that 23andMe did not knowingly or negligently cause the Data Breach, the Data Breach remains "an inadvertent violation" of Or. Rev. Stat. § 192.537 and § 192.539, for which Plaintiffs and Oregon Subclass members are entitled to the greater of their actual damages or $100 in statutory damages for each violation of Or. Rev. Stat. § 192.537 and the greater of their actual damages or $1,000 in statutory damages for each violation of Or. Rev. Stat. § 192.539. Or. Rev. Stat. § 192.541(2)(a), (3)(a).

912. Plaintiffs seek actual or statutory damages, injunctive and declaratory relief, their costs and fees, and any other relief as deemed appropriate by the Court.

CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS

COUNT THIRTY-THREE — PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 PA. CONS. STAT. §§ 201-2 & 201-3, *ET SEQ.*

913. The Pennsylvania Plaintiff identified above, Adriane Farmer ("Plaintiff," for purposes of this Count), individually and on behalf of the Pennsylvania Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Pennsylvania and on behalf of all other Pennsylvania residents whose Private Information was compromised as a result of the Data Breach.

914. 23andMe is a "person," as meant by 73 Pa. Cons. Stat. § 201-2(2).

915. Plaintiff and Pennsylvania Subclass Members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or

household purposes.

916. 23andMe engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. § 201-3, including the following:

a. Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have (73 Pa. Cons. Stat. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Cons. Stat. § 201- 2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Cons. Stat. § 201-2(4)(ix)).

917. 23andMe's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Pennsylvania Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Pennsylvania Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Pennsylvania Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Pennsylvania Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Pennsylvania Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Pennsylvania Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

918. 23andMe's representations and omissions 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' Private Information.

919. 23andMe intended to mislead Plaintiff and Pennsylvania Subclass Members and induce them to rely on its misrepresentations and omissions.

920. Had 23andMe disclosed to Plaintiff and Pennsylvania Subclass Members that its data systems were not secure and, thus, vulnerable to attack, 23andMe would have been forced to adopt reasonable data security measures and comply with the law. 23andMe was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and the Pennsylvania Subclass. 23andMe accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Pennsylvania Subclass Members acted reasonably in relying on 23andMe's misrepresentations and omissions, the truth of which they could not have discovered.

921. 23andMe acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiffs and Pennsylvania Subclass Members' rights.

922. As a direct and proximate result of 23andMe's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass' reliance on them, Plaintiff and Pennsylvania Subclass 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted

by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

923. Plaintiff and Pennsylvania Subclass Members seek all monetary and non-monetary relief allowed by law, including, pursuant to 73 Pa. Cons. Stat. § 201-9.2, actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS

COUNT THIRTY-FOUR — TENNESSEE UNFAIR AND DECEPTIVE TRADE PRACTICES ACT, TENN. CODE ANN. § 47-18-2107

924. The Tennessee Plaintiffs identified above, Kristina Chew and Brittany Deloach ("Plaintiffs," for purposes of this Count), individually and on behalf of the Tennessee Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Tennessee and on behalf of all other Tennessee residents whose Private Information was compromised as a result of the Data Breach.

925. 23andMe engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, 23andMe obtained Plaintiffs and Tennessee Subclass Members' Private Information through advertising, soliciting, providing, offering, and/or distributing goods and services to Plaintiffs and Tennessee Subclass Members and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

926. As alleged herein this Complaint, 23andMe engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. Failure to implement adequate data security practices to safeguard Private Information;

b. Failure to audit, monitor, or verify the integrity of data security procedures implemented by third parties with whom 23andMe shared Private Information;

c. Failure to make only authorized disclosures of current and former customers' Private Information;

d. Failure to disclose that their data security practices were inadequate to safeguard Private Information from theft; and

e. Failure to timely and accurately disclose the Data Breach to Plaintiffs and Tennessee Subclass Members.

927. 23andMe's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, 23andMe engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to 23andMe's current and former customers. Plaintiffs and Tennessee Subclass Members relied on 23andMe to reasonably protect their Private Information and had no ability to influence 23andMe's data security practices or verify that such practices were appropriate to the nature and sensitivity of Private Information collected and shared.

928. In committing the acts alleged above, 23andMe engaged in unconscionable, deceptive, and unfair acts and practices by omitting, failing to disclose, or inadequately disclosing to 23andMe's current and former customers that they did not follow industry best practices for the collection, use, sharing, and storage of Private Information.

929. As a direct and proximate result of 23andMe's conduct, Plaintiffs and Tennessee Subclass Members have been harmed and have suffered damages including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in 23andMe's possession and is subject to further unauthorized disclosures so long as 23andMe fails to undertake appropriate and adequate measures to protect the Private Information.

930. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiffs and Tennessee Subclass Members have been damaged and are entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

931. Also, as a direct result of 23andMe's knowing violation of the Tennessee Unfair and Deceptive Trade Practices Act, Plaintiffs and Tennessee Subclass Members are entitled to injunctive

relief, including, but not limited to:

a. Ordering that 23andMe implement measures that ensure that the PII of 23andMe's current and former customers is appropriately encrypted and safeguarded when stored on 23andMe's network or systems;

b. Ordering that 23andMe delete, destroy and purge the Private Information of Plaintiffs and Class Members who specifically request it, unless 23andMe can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;;

c. Ordering that 23andMe routinely and continually conduct 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; and

d. Ordering 23andMe to meaningfully educate its current and former customers about the threats they face as a result of the accessibility of their Private Information to third parties, as well as the steps 23andMe's current and former customers must take to protect themselves.

CLAIMS ON BEHALF OF THE TEXAS SUBCLASS

COUNT THIRTY-FIVE — TEXAS DECEPTIVE TRADE PRACTICES–CONSUMER PROTECTION ACT, TEX. BUS. & COM. CODE ANN. §§ 17.41, *ET SEQ.*

932. The Texas Plaintiff identified above, Benjamin Woessner ("Plaintiff," for purposes of this Count), individually and on behalf of the Texas Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Texas and on behalf of all other Texas residents whose Private Information was compromised as a result of the Data Breach.

933. 23andMe is a "person," as defined by Tex. Bus. & Com. Code Ann. § 17.45(3).

934. Plaintiff and the Texas Subclass Members are "consumers," as defined by Tex. Bus. & Com. Code Ann. § 17.45(4).

935. 23andMe advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code Ann. § 17.45(6).

936. 23andMe engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code Ann. § 17.46(b), including:

a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another;

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

d. Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

937. 23andMe's false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Texas Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Texas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Texas Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Texas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Texas Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Texas Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

938. 23andMe intended to mislead Plaintiff and Texas Subclass Members and induce them to rely on its misrepresentations and omissions.

939. 23andMe's representations and omissions 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' Private Information.

940. Had 23andMe disclosed to Plaintiff and Texas Subclass Members that its data systems were not secure and, thus, vulnerable to attack, 23andMe would have been forced to adopt reasonable data security measures and comply with the law. 23andMe was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and the Texas Subclass. 23andMe accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Texas Subclass Members acted reasonably in relying on 23andMe's misrepresentations and omissions, the truth of which they could not have discovered.

941. 23andMe had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the Private Information in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Texas Subclass, and 23andMe because consumers are unable to fully protect their interests with regard to their data, and they placed trust and confidence in 23andMe. 23andMe's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Plaintiffs and the Texas Subclass that contradicted these representations.

942. 23andMe engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). 23andMe engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

943. Consumers, including Plaintiff and Texas Subclass Members, lacked knowledge about deficiencies in 23andMe's data security because this information was known exclusively by 23andMe.

Consumers also lacked the ability, experience, or capacity to secure the Private Information in 23andMe's possession or to fully protect their interests with regard to their data. Plaintiff and Texas Subclass Members lack expertise in information security matters and do not have access to 23andMe's systems in order to evaluate its security controls. 23andMe took advantage of its special skill and access to Private Information to hide its inability to protect the security and confidentiality of Plaintiff's and Texas Subclass Members' Private Information.

944. 23andMe intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from 23andMe's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from 23andMe's unconscionable business acts and practices, exposed Plaintiff and Texas Subclass Members to a wholly unwarranted risk to the safety of their Private Information and the security of their identity or credit and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiff and Texas Subclass Members cannot mitigate this unfairness because they cannot undo the Data Breach.

945. 23andMe acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass Members' rights.

946. As a direct and proximate result of 23andMe's unconscionable and deceptive acts or practices, Plaintiff and Texas Subclass 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 Private Information; illegal sale of the compromised Private Information on the black market; the resulting emotional distress; mitigation expenses and time spent on identity defense, dark web, and credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing credit reports and accounts and taking other such protective actions; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted

by 23andMe; the amount of the actuarial present value of ongoing high-quality identity defense, dark web, and credit monitoring services made necessary as mitigation measures because of 23andMe's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

947. 23andMe's violations present a continuing risk to Plaintiff and Texas Subclass Members as well as to the general public.

948. Plaintiff and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

CLAIMS ON BEHALF OF THE VIRGINIA SUBCLASS

COUNT THIRTY-SIX — VIRGINIA CONSUMER PROTECTION ACT, VA. CODE § 59.1-198 TO 59.1-207

949. The Virginia Plaintiff identified above, Thomas Vickery ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclasses, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Virginia and on behalf of all other Virginia residents whose Private Information was compromised as a result of the Data Breach.

950. The Virginia CPA prohibits certain "fraudulent acts or transactions by a supplier in connection with a consumer transaction." Va. Code § 59.1-200(A).

951. 23andMe is or was during all relevant times a "supplier" of "goods" and/or "services" in connection with "consumer transactions" as those terms are defined in § 59.1-198 of the Virginia Consumer Protection Act ("CPA").

952. 23andMe's fraudulent acts or practices, as alleged herein, fraudulent acts or practices, as alleged herein, were committed in connection with "consumer transactions," as defined by Va. Code Ann. § 59.1-198, because they occurred in connection with "[t]he advertisement, sale, lease, license or offering for sale, lease or license, of goods or services to be used primarily for personal, family or household purposes."

953. 23andMe violated the Virginia CPA, Va. Code § 59.1-200, by, at a minimum, committing the following fraudulent acts or practices:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Virginia Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Virginia Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Virginia Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Virginia Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Virginia Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Virginia Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

954. 23andMe intended to mislead Plaintiff and Virginia Subclass Members and induce them to rely on its misrepresentations and omissions.

955. 23andMe's representations and omissions 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' Private Information.

956. Had 23andMe disclosed to Plaintiff and Virginia Subclass Members that its data systems were not secure and, thus, vulnerable to attack, 23andMe would have been forced to adopt reasonable data security measures and comply with the law. 23andMe was trusted with sensitive and valuable

Private Information regarding millions of consumers, including Plaintiff and the Virginia Subclass. 23andMe accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Virginia Subclass Members acted reasonably in relying on 23andMe's misrepresentations and omissions, the truth of which they could not have discovered.

957. 23andMe acted intentionally, knowingly, and maliciously to violate Virginia's CPA, and recklessly disregarded Plaintiff and Virginia Subclass Members' rights.

958. As alleged herein, Plaintiff and Virginia Subclass Members have suffered losses as a result of 23andMe's violations of Virginia's CPA.

959. Accordingly, Plaintiff and Virginia Subclass Members seek damages (to include treble damages); injunctive relief; attorneys' fees and costs; civil penalties; and any other relief to which Plaintiffs and Virginia Subclass Members may be entitled.

CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS

COUNT THIRTY-SEVEN — WASHINGTON DATA BREACH NOTICE ACT, WASH. REV. CODE § 19.255.010, *ET SEQ.*

960. The Washington Plaintiffs identified above, Camie Picha and Tracie Payne Mitchell ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Washington and on behalf of all other Washington residents whose Private Information was compromised as a result of the Data Breach.

961. 23andMe is a business that owns or licenses computerized data that includes "personal information" as defined by Wash. Rev. Code § 19.255.010(1).

962. Plaintiff's and Washington Subclass Members' Private Information includes "personal information" as covered under Wash. Rev. Code § 19.255.010(5).

963. 23andMe is required to accurately notify Plaintiff and Washington Subclass Members following discovery or notification of the breach of its data security program if Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, in the most expedient time possible and without unreasonable delay under

Wash. Rev. Code § 19.255.010(1).

964. Because 23andMe discovered a breach of its security system in which Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, 23andMe had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010(1).

965. By failing to disclose the Data Breach to Plaintiffs and all Washington Subclass Members in a timely and accurate manner, 23andMe violated Wash. Rev. Code § 19.255.010(1).

966. As a direct and proximate result of 23andMe's violations of Wash. Rev. Code § 19.255.010(1), Plaintiff and Washington Subclass Members suffered damages, as described above.

967. Plaintiff and Washington Subclass Members seek relief under Wash. Rev. Code § 19.255.040, including actual damages and injunctive relief.

COUNT THIRTY-EIGHT — WASHINGTON CONSUMER PROTECTION ACT, WASH. REV. CODE § 19.86.020, *ET SEQ.*

968. The Washington Plaintiffs identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclasses, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of Washington and on behalf of all other Washington residents whose Private Information was compromised as a result of the Data Breach.

969. 23andMe is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

970. 23andMe advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010(2).

971. 23andMe engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Washington Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy

measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Washington Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Washington Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Washington Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Failing to timely and adequately notify Plaintiff and Washington Subclass Members of the Data Breach;

g. Failing to disclose that the hackers had targeted and posted Private Information of customers of Chinese and Ashkenazi Jewish descent;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Washington Subclass Members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Washington Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

972. 23andMe's representations and omissions 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' Private Information.

973. 23andMe's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Washington Subclass Members, that their Private Information was not exposed and misled Plaintiff and the Washington Subclass Members into believing they did not need to take actions to secure their identities.

974. 23andMe acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff's and Washington Subclass Members' rights.

975. 23andMe's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, including, but not limited to Wash. Rev. Code Ann. § 19.255.010, *et seq.* Alternatively, 23andMe's conduct is injurious to the public interest because it has injured Plaintiff and Washington Subclass Members, had the capacity to injure persons, and has the capacity to injure other persons. Further, its conduct affected the public interest, including the thousands of Washingtonians affected by the Data Breach.

976. As a direct and proximate result of 23andMe's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from 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; and loss of value of their Private Information.

977. Plaintiff and Washington Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WISCONSIN SUBCLASS

COUNT THIRTY-NINE — BREACH OF CONFIDENTIALITY OF HEALTH RECORDS, WIS. STAT. § 146.81, *ET SEQ.*

978. The Wisconsin Plaintiff identified above, Kathleen Loftus ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Wisconsin and on behalf of all other Wisconsin residents whose Private Information was compromised as a result of the Data Breach.

979. Under Wisconsin law, "[a]ll patient health care records shall remain confidential. Patient health care records may be released only to the persons designated in this section or to other persons with the informed consent of the patient or of a person authorized by the patient." Wis. Stat. § 146.82(1).

980. The compromised Private Information belonging to Plaintiffs and Wisconsin Subclass Members are "health care records" under Wis. Stat. § 146.81(4).

981. 23andMe violated Wis. Stat. §§ 146.81, et seq. when it compromised, allowed access to, released, and disclosed patient health care records and Private Information to third parties without the informed consent or authorization of Plaintiff and the Wisconsin Subclass Members. 23andMe did not and does not have express or implied consent to disclose, allow access to, or release Plaintiff's and the Wisconsin Subclass Members' Private Information. To the contrary, 23andMe expressly undertook a duty and obligation to Plaintiff and Wisconsin Subclass Members when it told them their Private Information would be private and secure.

982. 23andMe did not disclose to or warn Plaintiff and Wisconsin Subclass Members that their Private Information could be compromised, stolen, released, or disclosed to third parties without their consent because of 23andMe's computer systems and software being outdated, easy to hack, inadequate, and insecure. Plaintiff and Wisconsin Subclass Members did not know or expect, or have any reason to know or suspect, that 23andMe's computer systems and software were so outdated, easy to hack, inadequate, and insecure that it would expose their Private Information to unauthorized disclosure.

983. Plaintiff and the Wisconsin Subclasses request that the Court issue declaratory relief declaring 23andMe's practice of using insecure, outdated, and inadequate email and computer systems and software that are easy to hack for storage and communication of Private Information data between 23andMe and third parties unlawful. Plaintiff and the Wisconsin Subclasses further request the Court enter an injunction requiring 23andMe to cease the unlawful practices described herein, and enjoining 23andMe from disclosing or using Private Information without first adequately securing or encrypting it.

984. Plaintiff and the Wisconsin Subclasses request the Court order 23andMe to identify, seek, obtain, encrypt, and retain at the conclusion of this action all existing Private Information of Plaintiff and the Wisconsin Subclasses in their possession or the possession of third parties and provide it to Plaintiff and the Wisconsin Subclasses.

985. Plaintiff and Wisconsin Subclass Members request that the Court enter an injunction

ordering that 23andMe:

a. engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct tests, and audit 23andMe's safeguards and procedures on a periodic basis;

b. audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;

c. conduct regular checks and tests on its safeguards and procedures;

d. periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response;

e. meaningfully educate its former and current patients about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps 23andMe is taking to update its security technology to adequately secure and safeguard patient Private Information; and

f. identify to each Subclass Member in writing with reasonable specificity the Private Information of each such Subclass Member that was stolen in the Data Breach, including without limitation as required under Wis. Stat. § 134.98(3)(c).

986. Plaintiff and Wisconsin Subclass Members request the Court enter an order pursuant to Wis. Stat. § 146.84(1)(bm) awarding minimum statutory exemplary damages of $1,000 to Plaintiffs and the Wisconsin Subclass whose Private Information was compromised and stolen, as well as attorneys' fees and costs.

COUNT FORTY — WISCONSIN DECEPTIVE TRADE PRACTICES ACT, WIS. STAT. § 100.18, *ET SEQ.*

987. The Wisconsin Plaintiff identified above, Kathleen Loftus ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclasses, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. This claim is brought individually under the laws of Wisconsin and on behalf of all other Wisconsin residents whose Private Information was compromised as a result of the Data Breach.

988. 23andMe's conduct violates the Wisconsin Deceptive Trade Practices Act ("WDTPA"). Under the Act, no "firm, corporation or association . . . with intent to sell, distribute, increase the consumption of . . . any . . . merchandise . . . directly or indirectly, to the public for sale . . . shall make, publish, disseminate, circulate, or place before the public . . . in this state, in a . . . label . . . or in any

other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public . . . which . . . contains any assertion, representation or statement of fact which is untrue, deceptive or misleading." Wis. Stat. § 100.18(1). Plaintiffs and Wisconsin Subclass Members "suffer[ed] pecuniary loss because of a violation" of the WDTPA. Wis. Stat. § 100.18(11)(b)(2).

989. 23andMe deliberately engaged in deceptive and unlawful practices when it issued public announcements, statements, and representations, including in press releases and on 23andMe's website, in violation of Wisconsin law, by failing to include in its representations to Plaintiff and Wisconsin Subclass Members and the public the scope of the Data Breach, when 23andMe knew the scope because the breached records were already available on the dark web.

990. 23andMe deliberately engaged in deceptive and unlawful practices when it issued announcements, statements, and representations, including in press releases, on 23andMe's website, and in the direct notice to Plaintiff and the Wisconsin Subclasses, in violation of Wisconsin law by representing to Plaintiff, the Wisconsin Subclasses, and the public that 23andMe did not know what specific Private Information was stolen, when in fact, they did have said information and knowledge. The purpose of 23andMe's misrepresentations was to minimize the harm and injury-in-fact Plaintiff and the Wisconsin Subclasses face caused by the Data Breach, and therefore increase the sales and use of 23andMe's services.

991. Plaintiff and the Wisconsin Subclasses relied upon 23andMe's deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the Court deems proper. Wis. Stat. §§ 100.18(11)(b)(2) and 100.20(5).

IX. REQUEST FOR RELIEF

992. Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against 23andMe, as follows:

993. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead Interim Class Counsel as Class Counsel;

994. That the Court grant permanent injunctive relief to prohibit 23andMe from continuing to engage in the unlawful acts, omissions, and practices described herein, including:

a. Prohibiting 23andMe from engaging in the wrongful and unlawful acts described herein;

b. Requiring 23andMe to protect all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. Requiring 23andMe to delete, destroy and purge the Private Information of Plaintiffs and Class Members who specifically request it, unless 23andMe can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

d. Requiring 23andMe to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

e. Requiring 23andMe to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on 23andMe's systems on a periodic basis, and ordering 23andMe to promptly correct any problems or issues detected by such third-party security auditors;

f. Requiring 23andMe to engage independent third-party security auditors and internal personnel to run automated security monitoring;

g. Requiring 23andMe to audit, test, and train its security personnel regarding any new or modified procedures;

h. Requiring 23andMe to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

i. Requiring 23andMe to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

j. Requiring 23andMe to implement a system of testing to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with 23andMe's policies, programs and systems for protecting Private Information;

k. Requiring 23andMe to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor 23andMe's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

l. Requiring 23andMe to meaningfully educate all Class Members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

m. Requiring 23andMe to implement logging and monitoring programs sufficient to track traffic to and from 23andMe servers; and

n. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis 23andMe's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

995. That the Court award Plaintiffs and Class and Subclass Members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

996. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by 23andMe as a result of its unlawful acts, omissions, and practices;

997. That the Court award statutory damages, treble, and punitive or exemplary damages, to the extent permitted by law;

998. That Plaintiffs be granted the declaratory relief sought herein;

999. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

1000. That the Court award pre- and post-judgment interest at the maximum legal rate; and

1001. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

1002. Plaintiffs demand a jury trial on all claims so triable.

RESPECTFULLY SUBMITTED this 26th day of June, 2024.

/s/ Norman E. Siegel
Norman E. Siegel (*pro hac vice*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road
Suite 200
Kansas City, MO 64112
Tel: (816) 714-7100
siegel@stuevesiegel.com

Cari Campen Laufenberg (*pro hac vice*)
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel: (206) 623-1900
claufenberg@kellerrohrback.com

Gayle M. Blatt (SBN 122048)
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD LLP
110 Laurel Street
San Diego, CA 92101
Tel: (619) 238-1811
gmb@cglaw.com

Co-Lead Counsel