ROB BONTA
Attorney General of California
NICKLAS A. AKERS
Senior Assistant Attorney General
STACEY D. SCHESSER (SBN 245735)
BERNARD A. ESKANDARI (SBN 244395)
Supervising Deputy Attorneys General
YEN P. NGUYEN (SBN 239095)
DANIEL M.B. NADAL (SBN 299661)
IAN C.J. HOGG (SBN 313924)
Deputy Attorneys General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
Telephone: (415) 510-3497
E-mail: TiTi.Nguyen@doj.ca.gov

Attorneys for The People of the State of California

[EXEMPT FROM FILING FEES GOVERNMENT CODE § 6103]

SUPERIOR COURT OF THE STATE OF CALIFORNIA

CITY AND COUNTY OF SAN FRANCISCO

THE PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, **v.** **CHROME HOLDING CO. (F/K/A 23ANDME HOLDING CO.), a Delaware corporation; CHROMECO, INC. (F/K/A 23ANDME, INC.), a Delaware corporation; and DOES 1 through 50, INCLUSIVE,** Defendants.	**CGC-26-636891** Case No. **COMPLAINT FOR INJUNCTION, CIVIL PENALTIES, AND OTHER EQUITABLE RELIEF** (CIV. CODE, §§ 56.18 *et seq.*, 1798.100 *et seq.*; BUS. & PROF. CODE, §§ 17200 *et seq.*, 17500 *et seq.*) [VERIFIED ANSWER REQUIRED PURSUANT TO CODE OF CIVIL PROCEDURE § 446]

Plaintiff, the People of the State of California ("Plaintiff" or the "People"), by and through Rob Bonta, Attorney General of the State of California, brings this action for violations of California's consumer and privacy laws and alleges the following on information and belief:

INTRODUCTION

1. For years, 23andMe,[1] a direct-to-consumer genetic testing company, misled consumers and failed to take obvious steps necessary to safeguard its customers' sensitive personal information and genetic data related to their health, genetic predispositions and risk factors, biological relatives, ancestry, and ethnicity. In 2023, an unauthorized threat actor exploited several vulnerabilities created by 23andMe's security failures in order to access and steal the personal information and genetic data of nearly 7 million 23andMe customers. 23andMe's security measures were so lax that the threat actor was able to operate undetected within 23andMe's systems for over five months, and remarkably, 23andMe only began investigating after the threat actor offered the stolen user data for sale on the dark web and reached out to 23andMe to demand a ransom. While 23andMe publicly touted its commitment to data privacy and transparency, in truth it failed to take reasonable measures to protect its customers' most sensitive data, ignored known vulnerabilities in its systems, and failed to properly investigate or respond to numerous warnings that its systems had been compromised, resulting in the unauthorized access to and disclosure of millions of customers' data. It also misled its customers and the public regarding the adequacy of its data safeguards and crucial aspects of the resulting data breach.

2. Genetic data is amongst the most sensitive and unique categories of personal information that an individual possesses. Genetic data includes not only an individual's raw genetic code, genes, chromosomes, and any data from the analysis of an individual's biological sample, but also any information that can be extrapolated, derived, or inferred from those things,

[1] 23andMe began operations in 2006 under the corporate name 23andMe, Inc. 23andMe, Inc. re-organized as a wholly owned subsidiary of the Delaware corporation, 23andMe Holding Co., in 2021. In 2025, 23andMe Holding Co. and 23andMe, Inc. changed their legal names to Chrome Holding Co. and ChromeCo, Inc., respectively. For purposes of this Complaint, Chrome Holding Co., ChromeCo, Inc., any predecessor entities, and their agents, executives, and employees are collectively referred to as "23andMe."

such as information relating to ancestry, ethnicity, biological family relationships, and medical information revealing health predispositions and risk factors. Genetic data is immutable, specific to an individual, reveals sensitive information about the individual's relatives, and is capable of revealing sensitive health and medical information. Once exposed, genetic data cannot be clawed back or truly deidentified, and the potential for misuse is indescribable. As the California legislature has recognized, it is critical that privacy and consumer protection laws, and the entities and individuals subject to them, recognize the unique sensitivity of genetic data and treat it accordingly.

3. At all times relevant, 23andMe was one of the largest businesses that provided direct-to-consumer genetic testing kits to the public. As part of this business, 23andMe collected and maintained a vast amount of sensitive personal information and genetic data about consumers. 23andMe customers sent their saliva sample to 23andMe, which had the DNA from these samples extracted, analyzed, and stored. 23andMe then stored the consumer's raw DNA sequence and used it to provide them with reports about their ancestry, ethnicity, and genetic health predispositions. 23andMe also offered a series of opt-in features. For example, it allowed users to access information concerning their relationship to other users, including both close and distant biological relatives, with whom they shared DNA, and it allowed those users to connect and communicate with each other. It also included automated tools for constructing family trees. At the time of the 2023 data breach, 23andMe had about 15 million customers nationwide, a substantial portion of whom resided in California.

4. As an entity that marketed its business to and maintained the personal information and genetic data of California consumers, 23andMe was required to comply with several state privacy laws, including the Genetic Information Privacy Act (GIPA), the Reasonable Data Security Law, and the California Consumer Privacy Act (CCPA). These statutes mandate a heightened legal obligation to protect genetic data—including information on health, ancestry, ethnicity, and biological family relationships derived from DNA testing—as well as other personal information from unauthorized access, destruction, use, modification, or disclosure and to adhere to reasonable security procedures and practices.

5. In early October 2023, 23andMe announced that it had a massive breach involving millions of consumers' genetic data and personal information, including that of nearly 1 million Californians. 23andMe's investigation found that from April through October 2023, a threat actor accessed about 14,000 customers' 23andMe.com accounts and leveraged those accounts to obtain data regarding nearly 7 million 23andMe customers. The threat actor employed "credential stuffing"—a well-known type of cyberattack that businesses, particularly those that collect and maintain sensitive personal information and genetic data, should be familiar with and guard against. Credential stuffing exploits consumers' tendency to use weak or common passwords or to re-use credentials across accounts at multiple companies, by using the same username and password that they use with one company to log into their account with another company. Here, by using stolen user account credentials that were exposed in prior data breaches—including the widely publicized breach of MyHeritage, one of 23andMe's former partners—the threat actor was able to gain unauthorized access to about 14,000 23andMe accounts. The threat actor had access to and stole the full, uninterpreted DNA of some customers, as well as self-reported health data and health data derived from the consumers' DNA. The threat actor then exploited a critical coding error in 23andMe's "DNA Relatives" feature—an opt-in feature that allowed DNA-related 23andMe customers to see which other participating users they were biologically related to—to steal additional data about nearly 7 million consumers, including information regarding ethnicity and how—both qualitatively and quantitatively—the customers were genetically related.

6. On October 1, 2023, 23andMe customer data appeared for sale on the dark web, with the poster specifically touting that a tranche of about 1.1 million consumers' data belonged to Asian-Pacific Islander and Ashkenazi Jewish users. Information related to the dark web posting was also flagged in the public 23andMe subreddit page on Reddit, a public, forum-based, social media website.[2]

7. 23andMe acknowledged the data breach on October 6, 2023, when it issued a press release informing the public of "suspicious activity" in certain 23andMe customer accounts and

[2] A subreddit is a smaller, sub-community or forum within Reddit that is dedicated to specific topics, each of which is created and moderated by Reddit users.

those who had opted into the "DNA Relatives" feature. However, even after finally notifying the public of the data breach, 23andMe continued to mislead consumers about both the severity of the breach and 23andMe's role in precipitating it.

8. Although 23andMe claimed that it first discovered the data breach on October 1, 2023, that is untrue. In fact, 23andMe was aware of but did not adequately investigate suspicious login activity in its systems months earlier, and prematurely closed its investigation into an August 2023 Reddit post claiming that 23andMe customer data was being offered for sale on the dark web. Specifically, on July 6, 2023, 23andMe noticed a suspicious spike in user login attempts that involved over 1 million successful user logins to the same customer account throughout a single day[3] and an actor making 1,300 login requests per minute from a single IP address. These kinds of highly suspicious login patterns are often a critical red flag that a malicious actor is attempting to gain unauthorized access into a secure system. Yet 23andMe failed to take action to protect its users and their data. And on August 11, 2023, a threat actor advertised a set of 23andMe customer data for sale on the dark web, which was flagged in a public Reddit post on the 23andMe subreddit. 23andMe's data security team became aware of and briefly investigated the August 2023 Reddit post but quickly closed the investigation. Despite these multiple warnings that its systems had been compromised, 23andMe did not take any remedial action, implement any new security measures, such as a mandatory password reset, or notify consumers of the breach at that time.

9. 23andMe's post-breach public statements also deceived the public regarding the severity of the breach and 23andMe's knowledge of it. Specifically, 23andMe's October 6, 2023 press release misled the public about 23andMe's responsibility for the breach by asserting that 23andMe had not experienced a data security incident within its systems, downplayed the sensitivity of the stolen data by claiming that the information stolen from the "DNA Relatives" feature was essentially public, and attempted to shift blame for the breach to its customers. Rather than acknowledging that it failed to take multiple basic steps to guard against credential

[3] This number is over five times larger than the average number of daily logins (approximately 151,000) that 23andMe experienced over the preceding four years.

stuffing, including searching for and preventing the re-use of stolen user credentials, 23andMe instead sought to deflect by unfairly accusing its own customers of being responsible for the breach.

10. Behind the scenes, 23andMe's actions told a much different story. Unbeknownst to consumers, while 23andMe was downplaying the severity of the breach and belatedly implementing the appropriate safeguards and remedial measures, 23andMe communicated with the threat actor and ultimately paid a ransom in exchange for, among other things, the threat actor removing damaging information regarding the breach that had been posted online and providing information about several 23andMe security vulnerabilities.

11. Despite 23andMe's attempts to shift the focus and blame for the 2023 data breach to its customers, it was 23andMe's responsibility to protect California residents' genetic data and personal information. 23andMe failed to implement basic, reasonable safeguards to do so.

12. 23andMe knew that the security of genetic data and personal information was very important to its customers and thus assured them through multiple statements that their data was safe with 23andMe. For example, on its website, 23andMe told users and the public, "we meet the highest industry standards for data security," and that 23andMe was "doing everything in our power to keep your personal data safe." However, 23andMe's failures to implement reasonable and well-known safeguards to protect genetic data and personal information were contrary to 23andMe's many public promises and statements about the reasonableness and adequacy of its data security.

13. 23andMe's failure to secure consumer genetic data and personal information, and its misleading statements, violated multiple California laws. Accordingly, the Attorney General of the State of California brings this law enforcement action to enforce the State's police and regulatory powers, including those under GIPA (Civ. Code section 56.18 *et seq.*) and the CCPA (Civ. Code section 1798.100 *et seq.*), as well as the Unfair Competition Law (UCL, Bus. & Prof. Code section 17200) and False Advertising Law (FAL, Bus. & Prof. Code section 17500) against 23andMe.

PLAINTIFF

14. Plaintiff is the People of the State of California. Plaintiff brings this action by and through Rob Bonta, Attorney General. The Attorney General is authorized by Civil Code section 56.182 to bring actions to enforce the Genetic Information Privacy Act (GIPA), Civil Code section 1798.199.90 to bring actions to enforce the California Consumer Privacy Act (CCPA), Business and Professions Code sections 17535 and 17536 to bring actions to enforce the False Advertising Law (FAL), and Business and Professions Code sections 17204 and 17206 to bring actions to enforce the Unfair Competition Law (UCL).

DEFENDANTS

15. Defendant Chrome Holding Co. (f/k/a 23andMe Holding Co.), is a Delaware corporation with its principal place of business in San Francisco, California and a service address at 490 Post Street, Suite 500 PMB 2065, San Francisco, CA 94102.

16. Defendant ChromeCo, Inc. (f/k/a 23andMe, Inc.), is a Delaware corporation with its principal place of business in San Francisco, California. ChromeCo, Inc. is the accounting predecessor and a wholly owned subsidiary of Chrome Holding Co.

17. Plaintiff is not aware of the true names and capacities of defendants sued herein as DOES 1 through 50, inclusive, and, therefore, sues these defendants by such fictitious names. Each fictitiously named defendant is responsible in some manner for the violations of law alleged. Plaintiff will amend this Complaint to add the true names of the fictitiously named defendants once they are discovered. Whenever reference is made in this Complaint to "Defendants" and "23andMe," such references shall include DOES 1 through 50.

18. The defendants identified in Paragraphs 15 through 17 are hereafter referred to collectively in this Complaint as "23andMe" or "Defendants."

19. At all relevant times, each Defendant acted individually and jointly with every other named Defendant in committing all acts alleged in this Complaint.

20. At all relevant times, each Defendant acted: (a) as a principal; (b) under express or implied agency; or (c) with actual or ostensible authority to perform the acts alleged in this Complaint on behalf of every other named Defendant.

21. At all relevant times, some or all Defendants acted as the agent of the others, and all Defendants acted within the scope of their agency if acting as an agent of another.

22. At all relevant times, each Defendant knew or realized, or should have known or realized, that the other Defendants were engaging in or planned to engage in the violations of law alleged in this Complaint. Knowing or realizing that the other Defendants were engaging in such unlawful conduct, each Defendant nevertheless facilitated the commission of those unlawful acts. Each Defendant intended to and did encourage, facilitate, or assist in the commission of the unlawful acts, and thereby aided and abetted the other Defendants in the unlawful conduct.

23. Defendants have engaged in a conspiracy, common enterprise, and common course of conduct, the purpose of which was to engage in the violations of law alleged in this Complaint.

24. Whenever reference is made in this Complaint to any act of any Defendant or Defendants, the allegation shall mean that the Defendant or Defendants did the acts alleged in this Complaint either personally or through the Defendant's or Defendants' officers, directors, employees, agents, or representatives acting within the actual or ostensible scope of their authority.

25. 23andMe was founded and, at all times relevant, maintained its principal place of business in California. As a result, 23andMe's conduct emanated from California, impacting consumers both within and outside of the state.

26. Each Defendant is a "person" as defined in Business and Professions Code section 17201.

JURISDICTION AND VENUE

27. This Court has original jurisdiction over this action pursuant to California Constitution article VI, section 10.

28. This Court has jurisdiction over Defendants because at all times relevant 23andMe was registered with the Secretary of State to conduct business in the State of California, maintained 23andMe's principal place of business in California, and because Defendants, by conducting business in California, including by marketing their products and services throughout

California and selling their products and services in California, intentionally availed themselves of the California market so as to render the exercise of jurisdiction over Defendants by the California courts consistent with traditional notions of fair play and substantial justice.

29. Defendants have transacted business within the State of California, including the City and County of San Francisco, at all times relevant to this Complaint.

30. The violations of law alleged in this Complaint occurred in the City and County of San Francsico and elsewhere in the State of California.

31. Venue is proper in this Court pursuant to Code of Civil Procedure section 395.5, because 23andMe's principal place of business is situated in the City and County of San Francisco.

32. Venue is also proper in this Court pursuant to Code of Civil Procedure section 393, subdivision (a), because violations of law that occurred in the City and County of San Francisco are a "part of the cause" upon which the People seek the recovery of penalties imposed by statute.

TOLLING

33. Pursuant to valid agreements between the People and Defendants, the parties have tolled all time limits and time-related defenses, either in law or in equity, including but not limited to any statutes of limitations, the statute of repose, and the doctrine of laches, relating to the claims that the People might bring against Defendants arising out of or relating to the security incident disclosed by 23andMe on or around October 6, 2023. The initial tolling agreement became effective on June 1, 2024, and tolled all such claims not then expired until June 1, 2025. These claims were further tolled by 11 U.S.C. section 108, starting on March 23, 2025, when 23andMe filed voluntary petitions for relief under chapter 11 of the Bankruptcy Code.[4]

[4] Those bankruptcy filings do not operate to stay this enforcement action, which is brought by a governmental unit to enforce its police and regulatory power. *See, e.g.*, *In re Universal Life Church, Inc.* (9th Cir. 1997) 128 F.3d 1294, 1298 ["'[W]here a governmental unit is suing a debtor to prevent or stop violation of fraud, . . . consumer protection, safety, or similar police or regulatory laws . . . the action or proceeding is not stayed under the [bankruptcy] automatic stay.'"] (quoting Sen.Rep. No. 95-989, 2d Sess., p. 52 (1977)].

FACTUAL ALLEGATIONS

A. 23andMe Promised to Use the Highest Level of Security to Protect Consumers' Sensitive Personal Information and Genetic Data That It Collects, Uses, and Maintains

34. 23andMe was founded in 2006, and at all times relevant was a "direct-to-consumer genetic testing company," that collected saliva samples and possessed the genetic data of over 15 million customers, a substantial portion of which belong to California consumers. 23andMe also provided web-based tools that included analyzing ancestry composition, maternal and paternal genetic groups, and health predispositions, and web-based features including those that allowed 23andMe users to access information concerning their relationship to other users, including both close and distant biological relatives, with whom they shared DNA, and it allowed those users to connect and communicate with each other, as well as create family trees.

35. To use 23andMe's services, consumers were required to provide their sensitive personal information to 23andMe. This included consumers' raw genetic data, which is among the most sensitive and unique forms of personal information an individual possesses, including because it is immutable, specific to an individual, revealing of sensitive information about kin, kinship, ancestry, and ethnicity, of ever-increasing informational value, and capable of revealing sensitive health information.

36. 23andMe was aware of the importance of data privacy to its customers and the need to keep their sensitive genetic information secure, telling consumers on its corporate website: "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."

37. 23andMe also publicly touted its privacy protections and data security measures on its corporate website, assuring consumers that "[w]e meet the highest industry standards for data security," and that 23andMe was "doing everything in our power to keep your personal data safe."

B. The 23andMe Data Breach Affecting Nearly 7 Million 23andMe Customers' Personal Information and Genetic Data

38. Starting in late April 2023, a threat actor was able to breach 23andMe's systems by using compromised credentials to compile customer data from individual 23andMe accounts without authorization. The actor used a technique known as "credential stuffing," a type of cyberattack in which the actor gains unauthorized access to an account by exploiting consumers' tendency to use weak or common passwords, or to re-use login credentials across accounts at multiple companies. The threat of credential stuffing is old and well-known, and businesses can and should know how to guard against it. Indeed, in the years leading up to the data breach, various government agencies and industry groups published best practices designed to help companies secure their systems from credential stuffing and similar attacks. 23andMe failed to implement many of them.

39. During the data breach, the threat actor was able to access roughly 14,000 23andMe user accounts by using stolen account credentials that were exposed in prior data breaches. The threat actor then used the compromised accounts and other vulnerabilities within 23andMe's systems to access and steal "DNA Relatives" and "Family Tree" profiles of other users, resulting in the compromise of at least 6.9 million profiles, nearly half of 23andMe's customer base. The majority of the 23andMe user credentials that the threat actor exploited to breach 23andMe's systems were previously exposed nearly five years earlier during a highly publicized data breach of MyHeritage, one of 23andMe's former partners.

40. The data stolen from each individual varied depending on whether they were directly compromised through the credential-stuffing attack or were impacted through the "DNA Relatives" or "Family Tree" features. For the approximately 14,000 consumers whose accounts were directly compromised by credential stuffing, the information that the threat actor was able to access or steal included: uninterpreted raw genotype data; health reports derived from the processing of customers' genetic information, including health-predisposition reports, wellness reports, and carrier status reports; and self-reported health condition information. Using a combination of the credential-stuffed accounts and a coding error in the "DNA Relatives" feature,

the threat actor was also able to access and extract personal information and genetic data about a further 5.5 million 23andMe customers. For those consumers, the unauthorized disclosure of data included: user display names, profile pictures, and birth years; the date of last login; relationship labels; predicted relationships with other users (e.g., "cousin" or "parent"); the percentage of DNA shared with other users; ancestry reports; reports on the DNA and chromosomal information they shared with other users; self-reported location data (city/zip code); ancestor birth locations and family names; and weblinks to family trees. For the additional 1.4 million 23andMe customers whose data the threat actor accessed via the Family Tree feature, the unauthorized disclosure included: display names and birth years, relationship labels; the percentage of DNA shared with other users; and self-reported location data.

41. About 855,541 of the affected consumers reside in California.

42. As a result of this incident, sensitive data stolen from 23andMe customers was posted for sale on the dark web, including targeted sales of the data of about 1.1 million individuals with Ashkenazi Jewish heritage, as well as hundreds of thousands of individuals with Chinese ancestry.

43. While 23andMe publicly disclosed this incident on October 6, 2023, the company later admitted that the threat actor first breached its system months earlier, in late April 2023 or early May 2023, and that 23andMe failed to detect the threat actor for approximately five months, despite multiple warnings.

44. The first post advertising stolen 23andMe data was published on the dark web on August 11, 2023. On the same date, a public post on the 23andMe-specific forum, or subreddit, on Reddit, a forum-based social media site, stated that the data of over 10 million 23andMe customers, including "Raw DNA Data," was being sold online.

45. In early October 2023, sensitive data from 23andMe customers was again offered for sale on the dark web, with the poster purportedly selling 23andMe profiles for between $1 and $10 per account. Information related to the sale of 23andMe data on the dark web was also posted on the 23andMe subreddit page on October 1, 2023.

46. The threat actor posted 23andMe user data on BreachForums, a dark web cyber-

crime discussion board, on at least three occasions: the tranche discussed in the October 1, 2023 Reddit post; October 17, 2023; and October 18, 2023. 23andMe verified that these three postings included 23andMe customers' personal information and genetic data.

47. On October 6, 2023, 23andMe published a post on its corporate web blog informing consumers of "suspicious activity" in certain 23andMe customer accounts. In the blog post, 23andMe claimed that it did "not have any indication at this time that there has been a data security incident within our systems," and did not announce any measures 23andMe had taken to ensure or enhance the security of the personal information of its customers.

48. 23andMe claims that it first learned of the data breach on October 1, 2023, when a third party posted a sample of the stolen data on the 23andMe subreddit.

49. However, 23andMe has admitted that its data security team was in fact aware of the August 2023 Reddit post discussing a possible breach and the exfiltration and offer for sale of 23andMe user data two months earlier. And on July 6, 2023, 23andMe's engineering team became aware of a suspicious spike in user login attempts, during which time 23andMe's access logs showed over five times the normal daily number of user log-ins, with a single actor making 1,300 login requests per minute from a single IP address. Although this is a classic red flag that a malicious actor may be attempting to infiltrate your system, 23andMe did not appropriately respond.

50. 23andMe did not disclose that at the same time it was assuring consumers that it did not have "any indication at this time that there has been a data security incident within our systems," it was simultaneously negotiating the payment of a ransom with the threat actor in an attempt to contain the fallout from the breach.

51. Throughout October 2023, 23andMe communicated with the threat actor and ultimately paid their monetary demand. On October 7 and 8, 2023, the threat actor sent messages to three people: Anne Wojcicki, the co-founder and, at the time, CEO of 23andMe; a 23andMe employee; and a spouse of a 23andMe employee. From October 8, 2023, through October 25, 2023, 23andMe negotiated with the threat actor, discussing a range of possible payments in order for the threat actor to take certain actions related to the breach. 23andMe ultimately paid the

threat actor $400,000 in cryptocurrency in exchange for the threat actor: reporting the vulnerabilities that they exploited during the breach; reporting two additional vulnerabilities they found but did not exploit; destroying the user data they possessed; deleting damaging posts they made online about the breach; and providing a cover story that mitigated the severity of the breach. The threat actor agreed to delete both the user data that was made available on the dark web, as well as additional 23andMe user information that the threat actor had stolen but not publicized, after receiving 23andMe's payment. It is unknown whether the threat actor in fact deleted any of the sensitive personal or genetic data that 23andMe's security failings enabled them to steal.

52. When 23andMe finally did take steps to implement some of the basic security safeguards that they should have had in the first place, their actions were far too little and too late to protect their customer's personal information and genetic data. For example, despite knowing that 23andMe accounts hold highly sensitive data, including consumers' genetic data and health information, 23andMe did not require multi-factor authentication, a common additional layer of security that requires a user to use two or more verification methods, such as both a phone number and an email address, to login to their account, to secure customer accounts until November 6, 2023. And although 23andMe was aware of suspicious activity within its systems months earlier, 23andMe did not initiate a global password reset until October 10, 2023, by which time the threat actor had already been able to access and steal 23andMe's customer's data for over five months.

C. 23andMe Failed to Implement Reasonable Safeguards to Protect Consumers' Personal Information and Genetic Data

53. 23andMe was aware of but failed to implement security processes and procedures that were appropriate to the highly sensitive nature of the personal information and genetic data that 23andMe collected and maintained regarding its customers that were necessary to protect this information from unauthorized access, destruction, use, modification, or disclosure.

1. 23andMe failed to implement reasonable security procedures to prevent and detect the well-known risk of credential stuffing

54. Credential stuffing is a relatively unsophisticated form of cyberattack in which threat actors use lists of previously compromised user credentials to gain access to another company's systems. Here, the threat actor was able to breach 23andMe's system by using thousands of usernames and passwords of 23andMe customers that were exposed in earlier data breaches, including the widely publicized 2017 data breach of MyHeritage, a former business partner of 23andMe.

55. For years, the threat of credential stuffing has been well known, and various government agencies have provided businesses with specific guidance on how to prevent such attacks to effectively safeguard networks and sensitive data.

56. In February 2016, the Attorney General published the *California Data Breach Report*, which stated: "The 20 controls in the Center for Internet Security's Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes lack of reasonable security." At the time, Account Monitoring and Control were among the controls in the Center for Internet Security's Critical Security Controls. By 2016, the Critical Security Controls recommended multi-factor authentication for all user accounts that have access to sensitive data or systems.

57. In the *California Data Breach Report*, the Attorney General further acknowledged that individuals often do not use unique passwords for their accounts and do not use strong passwords. Accordingly, the Attorney General recommended that "[m]ulti-factor authentication should also be more widely available for consumer-facing online accounts that contain sensitive personal information."

58. In 2017, the Federal Trade Commission published data security guidance which cautioned:

> Consumers and employees often reuse usernames and passwords across different online accounts, making those credentials extremely valuable to remote attackers.

> Credentials are sold on the dark web and used to perpetrate credential stuffing attacks – a kind of attack in which hackers automatically, and on a large scale, input stolen usernames and passwords into popular internet sites to determine if any of them work. Some attackers time their log-in attempts to get around restrictions on unsuccessful log-ins. To combat credential stuffing attacks and other online assaults, companies should combine multiple authentication techniques for accounts with access to sensitive data.

59. By 2020, the Center for Internet Security recognized that "credential stuffing" had a "very high" frequency and that "62% of users admit reuse." In addition to multi-factor authentication, the Center for Internet Security recommended, among other things:

- **Password Banning (Deny Lists)** – **"Check for known bad passwords.** [¶] Organizations should ban the use of common bad passwords. . . . [¶] When processing requests to create or change a password, the new password should be checked against a list that contains values known to be commonly-used, expected, or compromised. For example, the list should include but is not limited to: Passwords obtained from previous breaches . . ."
- **Limiting Failed Login Attempts (Lockout)** – "To limit password guessing, temporarily lock the account after a predefined number of failed login attempts. . . . A temporary (15 minute) account lockout after 5 consecutive failed login attempts has proven to be an effective solution against online password guessing and brute force attempts . . . Another technique that is gaining popularity is *throttling*, which progressively increases the delay before the next login attempt can occur."
- **Monitoring Failed Login Attempts** – "The goal of strong passwords is to prevent unauthorized users (attackers in particular) from gaining access to systems or accounts. There, *logging* is a key component to investigate attempts at gaining access to a user account, whether this be a regular user or an administrator account. To achieve this, at a minimum, failed login attempts must be monitored and key personnel alerted to the events."

60. Likewise, in January 2022, the New York Attorney General's Office released a

business guide for credential stuffing attacks that detailed how businesses could protect themselves and consumers ("NYAG Business Guide"). The recommended safeguards to *prevent* credential stuffing included:

- **Bot Detection** – "Effective bot detection systems can distinguish between human and bot traffic even when the bot traffic has been disguised — for example, by rotating through multiple IP addresses or device identifiers."
- **Multi-Factor Authentication** – "Most attackers that have access to a stolen password will not have access to other credential types."
- **Web Application Firewalls** – "Most businesses should use a Web Application Firewall (WAF) as a first line of defense against malicious traffic. WAFs can include a variety of features capable of mitigating basic web application attacks[,]" including rate limiting, HTTP request analysis, and IP address blacklisting.
- **Preventing Reuse of Compromised Passwords** – "Businesses can stop attackers from accessing at least some customer accounts by preventing customers from reusing passwords that have previously been compromised. This functionality typically relies on third-party vendors that compile credentials from known data breaches. When a customer selects a password, it is compared to the passwords in the library of stolen data; if the password matches, the customer is asked to choose another password."

61. In addition to safeguards to prevent credential stuffing, the NYAG Business Guide recommended customer activity monitoring as the most effective safeguard to *detect* that a credential stuffing incident is occurring. In particular: "Most credential stuffing attacks can be identified through the footprints they leave on customer traffic. Attacks often appear as spikes in traffic volume or failed login attempts. Even sophisticated credential stuffing attacks have attack signatures that can be identified through analysis of customer activity. Most businesses should therefore have processes in place to systematically monitor customer traffic."

62. With respect to use of compromised credentials, since 2017, the National Institute of Standards and Technology has recommended that user-provided passwords be checked against

existing data breaches. NIST warns: "Users' password choices are very predictable, so attackers are likely to guess passwords that have been successful in the past. These include dictionary words and passwords from previous breaches, such as . . . 'Password1!' . . . For this reason, it is recommended that passwords chosen by users be compared against a 'black list' of unacceptable passwords. This list should include passwords from previous breach corpuses . . . ."

63. The risk of a credential stuffing attack was both reasonably foreseeable and particularly acute for 23andMe, because MyHeritage, a separate consumer genealogy website with which 23andMe had previously partnered, had suffered a well-publicized data breach several years earlier.

64. Consumers pursuing genetic genealogy projects, for example to answer questions about their biological parentage, will often establish accounts with multiple genetic testing sites to maximize their chances of finding matches that might aid their searches. Moreover, in 2014, 23andMe and MyHeritage announced a partnership that included a free trial of the MyHeritage service for 23andMe customers as well as a product integration that allowed 23andMe customers to connect their 23andMe accounts to MyHeritage.

65. Because of the nature of genetic genealogy research, and since 23andMe and MyHeritage users were at one time encouraged to connect their accounts on the two websites, it was reasonably foreseeable that customers would use the same login credentials for both accounts.

66. In 2017, MyHeritage experienced a massive, well-publicized data breach that exposed the credentials of over 92 million MyHeritage users. At least one senior member of 23andMe's cyber security team was aware of the MyHeritage data breach as early as 2018.

67. The compromised MyHeritage credentials were posted for sale on the dark web in the years leading up to the 23andMe data breach.

68. In their communications with 23andMe, the threat actor told 23andMe that they were able to breach 23andMe's systems by using compromised MyHeritage credentials to perform a brute force credential-stuffing attack on 23andMe user accounts. The threat actor admonished 23andMe for not having taken measures against this, as 23andMe shared a large

number of common customers with MyHeritage.

69. Indeed, during the internal investigation of the 2023 data breach, 23andMe finally checked its customers' credentials against credentials from known prior breaches. 23andMe found that of the 14,000 23andMe accounts accessed by the threat actor, over 50% percent had been exposed years earlier in the 2017 MyHeritage breach and almost 100% had been in at least one other prior breach.

70. Prior to the 23andMe data breach, 23andMe did not check customer credentials against credentials from known prior breaches, including the MyHeritage breach. 23andMe also did not require customers to reset their passwords or use multi-factor authentication following the MyHeritage breach. Had 23andMe done so and required customers with compromised credentials to reset their passwords, the 23andMe data breach would not have occurred.

71. Further, at the time of the 2023 breach, 23andMe did not require multi-factor authentication to secure customer accounts even though 23andMe was aware of multi-factor authentication and it is a well-recognized and simple access control. Had 23andMe required all customers to use multi-factor authentication before the breach, the credential stuffing attack would have been mitigated, as most threat actors that gain access to stolen passwords do not have access to multiple user credential types.

72. 23andMe also missed several opportunities to detect the credential stuffing attack or otherwise discover the threat actor before October 2023.

73. Notably, the threat actor carried out credential-stuffing attempts from May 1 through 16, 2023, and from September 12 through 18, 2023, which created noticeable—and unusual—differences from the typical daily log-in patterns recorded and logged by 23andMe. A responsible company, particularly one that maintained sensitive personal information and genetic data about its customers, would monitor for and investigate suspicious login patterns, for example large jumps in overall login attempts and unusual spikes in the percentage of unsuccessful logins. Yet, although both happened here, 23andMe neither noticed nor raised alerts regarding this unusual log-in activity.

74. In August 2023, 23andMe was contacted by an individual who claimed to have

breached 23andMe's security and to have stolen data—including ancestry composition, health data, and raw DNA data—from 23andMe's systems relating to 10 million 23andMe customers. 23andMe linked this individual to an August 11, 2023 Reddit post that claimed the stolen data was available for sale on the dark web. However, 23andMe did not investigate what was in fact available on the dark web, nor did it attempt to obtain or assess samples of the stolen customer data. Instead, 23andMe relied solely on two examples provided by the unknown individual. The example data that the individual provided related to Anne Wojcicki and Google co-founder Sergey Brin, both of whom had previously chosen to make their information public. 23andMe did not attempt to discover whether the allegedly stolen data included data of customers whose information was not public. Instead, 23andMe concluded that, based on the two examples provided, the information could have been obtained legitimately through the regular use of 23andMe.com and the "DNA Relatives" feature, and closed its investigation after 4 days. Incredibly, 23andMe's investigation did not discover the credential-stuffing threat actor who had been operating undetected within 23andMe's supposedly secure systems for over three months.

75. Instead of taking responsibility for its own security failures, 23andMe simply blamed its customers for the data breach, accusing customers in breach notification letters of "negligently recycl[ing] and fail[ing] to update their passwords following . . . past security incidents."

76. 23andMe's failure to prevent or even detect the data breach for five months, failure to screen customer passwords for known breached passwords, including those exposed in the breach of a former partner, failure to initiate a global password reset until October 10, 2023, and failure to require multi-factor authentication to secure customer accounts until *after* the 2023 breach show that 23andMe failed to implement reasonable security procedures to protect highly sensitive customer data.

2. 23andMe failed to implement reasonable security procedures and practices to guard against the exploitation of a coding error in the "DNA Relatives" feature

77. In addition to failing to take steps that could have prevented the 2023 credential

stuffing attack, 23andMe also failed to detect and prevent the threat actor from exploiting an internal coding error in the "DNA Relatives" feature, which the threat actor used to expedite and expand the scope of their unauthorized access to and exfiltration of sensitive customer data.

78. A typical 23andMe customer who had opted-into the "DNA Relatives" feature would see a list of other 23andMe customers who had also opted-into the "DNA Relatives" feature who were genetically related to that customer. The 23andMe customer was required to click on each "DNA Relative" who matched with them in order to see the information that relative had chosen to share, including how that "DNA Relative" was related to them (i.e., the percentage match and centiMorgans of overlap between the two individuals, combined with a rough graphical illustration of which portions of which chromosomes were matching). A 23andMe customer could also search their "DNA Relatives" list for those who were related to them based on name, relation, location, or other information. When a 23andMe customer made such a query, the 23andMe database would then search the 23andMe customer's "DNA Relatives" and return matches, which would then be displayed to the 23andMe customer who submitted the query.

79. The "DNA Relatives" feature and its search function were meant to be limited such that an opted-in 23andMe customer was only able to view and search for those 23andMe customers who had both opted-in to the "DNA Relatives" feature and appeared on the querying 23andMe customer's "DNA Relatives" list. However, there was a coding error in the "DNA Relatives" feature that allowed a user to submit a doctored query to the 23andMe database that would search for and return results on ***any*** 23andMe customer who had opted-into "DNA Relatives" feature, even if that customer was not on the querying user's "DNA Relatives" list.

80. 23andMe did not detect or correct this coding error, which the threat actor was able to exploit in order to expand the number of 23andMe customer accounts whose data the threat actor was able to steal. As a result, after gaining access to 23andMe's systems, the threat actor was able to submit doctored queries—which the 23andMe database should have, but failed to flag and reject as containing improper and unvalidated search parameters—to gain access to information on any 23andMe user who had opted-in to the "DNA Relatives" feature. Thus, the

threat actor was able to use any compromised 23andMe account to search at will for any 23andMe customer who had opted-into the "DNA Relatives" feature, instead of being required to laboriously click through each and every "DNA Relative" who happened to be genetically linked to one of the compromised accounts (assuming that the compromised account in question had also opted-in to the "DNA Relatives" feature), before repeating the same process in another 23andMe customer's account. Had 23andMe implemented appropriate safeguards to prevent tampering with database queries, the threat actor would not have been able to steal personal information and genetic data regarding nearly as many 23andMe customers as they did during their five months in 23andMe's system. Appropriate monitoring and safeguards would also have increased the likelihood that 23andMe could have detected and caught the threat actor sooner.

81. It is a basic principle of data security that databases—and especially databases containing sensitive personal information—and the code effectuating database queries should be protected against tampering. This includes properly reviewing the relevant code for errors, as well as checking for and preventing the use of improper or unvalidated parameters in search queries, so that unauthorized users cannot access or query the database, nor can anyone (authorized or unauthorized) make unauthorized types of queries that return data that the querying user is not authorized to see.

82. During ransom negotiations with 23andMe in October 2023, the threat actor revealed that they exploited the coding error in the "DNA Relatives" feature during the data breach. However, even though 23andMe was aware of this vulnerability, 23andMe's disclosures to consumers regarding the threat actor's use of the "DNA Relatives" feature to steal personal information and genetic data failed to mention the role that 23andMe's coding error and security failure played in facilitating and expanding the scope of the breach.

3. 23andMe failed to consider the high-level of sensitivity of consumers' genetic data when drafting and implementing security procedures and practices

83. When drafting and implementing data security procedures and practices, it is axiomatic that the type of data involved, its nature, and its level of sensitivity must be taken into consideration in order to ensure the appropriate safeguards are in place. Personal information that

is highly sensitive requires a higher level of protection. Without doubt, genetic data by its very nature requires one of the highest levels of protection. California law—GIPA, the Reasonable Data Security Law, and the CCPA—recognizes the unique privacy risks posed by genetic data and accordingly mandates a heightened legal obligation to protect genetic data and personal information from unauthorized access, destruction, use, modification, or disclosure and to adhere to reasonable security procedures and practices.

84. Despite consumers' genetic data being the primary reason for 23andMe's existence and despite 23andMe's collection, storage, and analysis of millions of consumers' biological samples and genetic data, 23andMe's security practices and procedures failed to properly account—or to account at all—for genetic data, its nature, and its high-level of sensitivity.

85. As an example, 23andMe's Information Security Policy generally discusses protecting business information, but does not discuss anything specific to genetic data or acknowledge the unique privacy risks facing a genetic testing and ancestry research company, let alone, how to address them. Similarly, 23andMe's Network Security Policy is a standard network security policy and does not address anything specific to genetic or ancestry information or any unique network security that would be required for a genetic testing and ancestry research company. Even 23andMe's Data Classification, which was in place at the time of the data breach and was supposed to provide guidance to 23andMe staff on its three-tier data classification system, fails to address genetic or ancestry information and further fails to inform staff which classification such data falls under. None of the three classifications specify whether they include genetic or ancestry information. To the extent 23andMe intended to treat genetic or ancestry information as falling under the most sensitive tier—"Sensitive Confidential Information"—then 23andMe failed to adhere to its policies related to such information, as the Data Classification Policy required multi-factor authentication for access to such information. In contradiction to its own policy, 23andMe did not require multi-factor authentication for customers to access this information until after the data breach, in November 2023.

86. 23andMe's cavalier attitude towards the privacy of its customers' genetic data and

ancestry information is perhaps best exemplified by the sworn testimony of 23andMe's former CEO, Anne Wojcicki, who testified during 23andMe's recent bankruptcy proceedings, "I think my email and my bank accounts are potentially more sensitive than my genetic information."

87. While 23andMe and its former CEO may not view genetic information as particularly sensitive, the California legislature has reached the opposite conclusion. Under California law and basic data security principles, 23andMe should have but failed to account for the unique nature of genetic data and its high level of sensitivity when drafting and implementing its data security procedures and practices.

D. 23andMe Misled Consumers About Its Security Measures, the Severity of the 2023 Data Breach, and the "DNA Relatives" Feature

88. 23andMe's public statements assured consumers that the company took data privacy seriously and employed the highest level of security to protect customer's personal information. Both before and after the 2023 data breach, 23andMe promoted its security practices as meeting the highest industry standards and claimed that its systems were safe and secure. Such promises are important to many consumers, particularly those deciding whether and to whom to entrust their most sensitive personal information: their genetic data. But in reality, 23andMe's data security practices fell well below industry standards, and the company failed to implement numerous well-known security procedures to protect consumer data.

89. 23andMe's deceptive conduct included: (1) misleading consumers about the level of security the company used to protect their personal information and genetic data; (2) misleading the public regarding the 2023 data breach in an effort to hide both the breach's severity and 23andMe's responsibility for it; and (3) misleading the public regarding the "DNA Relatives" feature.

90. As described below, 23andMe's statements were likely to deceive consumers about the level of security that was actually used to protect their sensitive personal information and genetic data, about 23andMe's security failures that led to and exacerbated the 2023 data breach, and about the "DNA Relatives" feature.

1. 23andMe's pre-breach deception

91. 23andMe advertised its offerings on its corporate website, which included numerous misleading representations about 23andMe's security procedures designed to induce consumers to entrust their most sensitive data to the company. These statements repeatedly mischaracterized 23andMe's data privacy practices as meeting the highest standards, while deceiving consumers about the level of protection and security their data actually received.

92. Before the data breach, the Privacy page of 23andMe's corporate website informed consumers that 23andMe "meet[s] the highest industry standards for data security." 23andMe's privacy page also stated:

> Your data is fiercely protected by security practices that are regularly reviewed and updated. Your genetic information deserves the highest level of security, because without security, you can't have privacy. 23andMe employs software, hardware, and physical security measures to protect your data. And while no security standard or system is bulletproof, we're doing everything in our power to keep your personal data safe.

93. Contrary to these representations, 23andMe did not "meet the highest industry standards for data security," did not employ "the highest level of security," and was not "doing everything in [its] power to keep [customers'] personal data safe." Among other things, 23andMe failed to require the use of multi-factor authentication, screen customer passwords for known breached passwords, or to adequately protect against users submitting doctored, unauthorized queries to its databases, even though these measures have long been among the list of basic data security best practices. 23andMe also failed to initiate a global password reset until October 10, 2023, over five years after the well-known breach of a former partner, MyHeritage, which exposed over 92 million user credentials.

94. 23andMe also misled consumers regarding who was able to access a customer's personal information and genetic data. Prior to the breach, 23andMe's corporate website assured customers that "[w]e implement physical, technical, and administrative measures aimed at preventing unauthorized access to or disclosure of your Personal Information." 23andMe similarly promised:

> [Y]our personally identifiable information (such as your name and email) is stored in a separate database from your genetic data so that **no one but you** (when you use your username and password) can connect the dots between the two. That means even if someone gained access to one of these databases, they could not connect your identity to your genetic data, or vice versa.

As the 2023 data breach showed, these statements were false. Among other things, 23andMe's failure to require the use of multi-factor authentication or to search for and bar the use of credentials exposed in prior data breaches meant that the threat actor was able to breach 23andMe's systems and to access both the personal and genetic information for each of the over 14,000 23andMe user accounts directly compromised by credential stuffing. Moreover, because 23andMe failed to identify and correct the coding error in the "DNA Relatives" feature, the threat actor was able to access personal and account names as well as shared genetic data for every 23andMe customer who opted into "DNA Relatives," regardless of whether they were related to one of the compromised accounts.

95. Before the data breach, 23andMe's Privacy Statement also promised: "We stay a step ahead of hackers" because "third-party security experts regularly conduct audits and assessments of our systems, ensuring we will never let our guard down." As the data breach showed, this too was false, as the threat actor was able to breach and then operate undetected within 23andMe's systems for over five months, while exfiltrating sensitive user data and offering it for sale on the dark web.

96. 23andMe's public statements regarding its data security measures were likely to mislead consumers into believing that 23andMe would adequately protect their sensitive personal information from unauthorized access. Consumers were assured that 23andMe took the protection of genetic data seriously, which was material to the consumers' decision to entrust the company with their genetic data. 23andMe's public representations on their website and privacy policies about data security were misleading and material to a reasonable consumer's decision to purchase their services.

97. At no point prior to the 2023 data breach did 23andMe's corporate website disclose that 23andMe did not check for or prevent customers from using credentials exposed in

prior data breaches, allowed users to submit doctored queries to access unauthorized user data, and violated its own internal Information Security Policy, which required the use of multi-factor authentication to access the most sensitive consumer information.

2. 23andMe misled consumers regarding its role in and the severity of the data breach

98. After the data breach became public, 23andMe continued to mislead consumers about its security procedures, the sensitivity of the stolen data, and the severity of the breach, inducing new consumers to entrust their most sensitive data to the company, and inducing existing 23andMe customers not to invoke their rights under GIPA and the CCPA to delete their accounts and any personal information collected and maintained by 23andMe. 23andMe assured consumers that the breach was minimal and did not involve any issues with or within 23andMe's systems. But in truth, 23andMe knew, but failed to disclose, that the breach exposed the existence of multiple vulnerabilities within 23andMe's systems, including vulnerabilities that the threat actor exploited to significantly expand the amount of user data they were able to steal, and involved more, and more sensitive, user data than 23andMe admitted to in public.

99. For example, in public blog posts made announcing the data breach and the company's investigation of it, 23andMe repeatedly told consumers "We do not have any indication at this time that there has been a data security incident within our systems." In truth, the threat actor informed 23andMe during ransom negotiations of multiple vulnerabilities within 23andMe's systems, including the coding error that the threat actor exploited to quickly search through and steal data from the full list of 23andMe customers who opted-in to the "DNA Relatives" feature. 23andMe also failed to disclose that threat actor chided 23andMe for their lax data security system, including 23andMe's failure to implement basic precautions, such as requiring the use of multi-factor authentication and searching for and barring the use of credentials exposed in prior breaches.

100. As it did before the breach, 23andMe's post-breach public statements continued to ensure consumers that 23andMe "take[s] security seriously," and "exceed[s] industry data protection standards." 23andMe also told consumers: "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 data has been accessed by unauthorized individuals, we immediately investigate to validate whether this information is accurate." But 23andMe's post-breach statements mischaracterized both the protections the company had in place as well as the quality of its investigation. Despite its promises, 23andMe and its employees failed to properly monitor the systems and databases in which the company stored the sensitive personal information and genetic data of its customers. In fact, 23andMe was aware of but did not adequately investigate suspicious log-in activity in its systems on multiple occasions, prematurely closed its investigation into an August 2023 Reddit post claiming that 23andMe user data was being offered for sale on the dark web, and failed to detect the threat actor for over five months, despite repeated warnings of unauthorized access to customer data.

101. 23andMe also misled the public regarding the scope and severity of the breach. For example, in one of its post-breach blog posts, 23andMe stated that the information accessed by the threat actor was limited to "DNA Relatives profiles connected to [the approximately 14,000] 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," and the Family Tree feature, which includes a limited subset of DNA Relatives profile information." In doing so, 23andMe created the misleading impression that the data the threat actor was able to steal and offer for sale on the dark web was of limited sensitivity and reflected information that was already partly shared with others. In truth, due to coding errors within 23andMe's systems, the threat actor was able to access and exfiltrate personal information, including snippets of genetic data, for every 23andMe customer who had opted-in to the "DNA Relatives" feature, regardless of whether they were connected to one of the 14,000 credential-stuffed accounts. The stolen information included personal and genetic data that 23andMe users had never agreed to share with the wider world or with other non-related 23andMe users. 23andMe's statement also failed to mention that, as the company was informed during ransom negotiations, the threat actor was able to access and exfiltrate additional 23andMe user data that was never publicized.

102. 23andMe's post-breach statements were misleading and omitted key information in an effort to downplay the severity of the breach and obscure significant failings by 23andMe's data security team. 23andMe continued to inform consumers that there was no data security incident within its systems, despite being informed by the threat actor during ransom negotiations of multiple exploitable vulnerabilities within 23andMe's systems, including vulnerabilities that were used to facilitate the attack. 23andMe touted its monitoring and investigative process while failing to mention that despite being aware of dark-web and Reddit posts on August 11, 2023 that claimed that the data of millions of 23andMe customers was for sale, 23andMe purportedly did not discover the data breach until October 1, 2023, when the threat actor posted a sample of the stolen data on the 23andMe subreddit. And 23andMe failed to mention that the threat actor had gained access to a broader set of user data that had not previously been publicized, including the raw genetic data of certain 23andMe customers.

3. 23andMe misled consumers about the limits of the "DNA Relatives" feature

103. 23andMe's statements describing the "DNA Relatives" feature assured 23andMe customers that the "DNA Relatives" feature was limited only to other 23andMe who had opted into the feature and actually matched to them as a DNA relative. As 23andMe customers could choose to opt into the "DNA Relatives" feature, as such promises were important to many consumers, particularly those deciding whether to share some of their sensitive personal information and genetic data with other 23andMe customers who are relatives. However, 23andMe deceived consumers because the "DNA Relatives" feature was not so limited.

104. 23andMe told consumers that: "If you choose to opt in and participate in DNA Relatives, all of your matches will be able to view the following information about you: Your display name; Your profile sex (Male/Female); Your predicted relationship; The percent DNA and number of segments you share, but not the location of those segments; Relatives in Common." 23andMe also told consumers that: "Choosing this option [of showing your genetic ancestry results] also makes the location of shared DNA segments available to your matches in a chromosome diagram that includes the X chromosome(s). Please note that sharing this

information may reveal your genetic sex by showing segments on one or more multiple copies of the X chromosome."

105. 23andMe also told consumers who opted into the "DNA Relatives" feature that: "The DNA Relatives feature includes a few ways to help you filter and sort your list of genetic matches" and "Search can be used in conjunction with other filters and sorting. Search for surnames, locations, or other information about relatives to narrow your list by that criteria."

106. As a result, 23andMe customers were assured that the "DNA Relatives" feature and its search function were meant to be limited such that an opted-in 23andMe customer was only able to view and search for 23andMe customers who had both opted-in to the "DNA Relatives" feature and appeared on the querying 23andMe's customer's "DNA Relatives" list because they were a match.

107. In reality, 23andMe deceived customers because there was a coding error in the "DNA Relatives" feature that allowed a user to submit a doctored query to the 23andMe database that would search for and return results on ***any*** 23andMe customer who had opted-into the "DNA Relatives" feature even if that customer was not on the query user's "DNA Relatives" list.

FIRST CAUSE OF ACTION

VIOLATIONS OF THE GENETIC INFORMATION PRIVACY ACT

(CIVIL CODE SECTION 56.18 ET SEQ.)

108. The People reallege and incorporate by reference each of the paragraphs above as though fully set forth herein.

109. At all times relevant, 23andMe was a "direct-to-consumer genetic testing company" because it was an entity that (a) sold, marketed, interpreted, or otherwise offered consumer-initiated genetic testing products or services directly to consumers; (b) analyzed genetic data obtained from a consumer; or (c) collected, used, maintained, or disclosed genetic data collected or derived from a direct-to-consumer genetic testing product or service, or was directly provided by a consumer. (Civ. Code, § 56.18, subd. (b)(5).) "Genetic data" is defined as "any data that results from the analysis of a biological sample from a consumer … and concerns

genetic material," such as deoxyribonucleic acids (DNA), genes, chromosomes, genomes, and "any information extrapolated, derived, or inferred therefrom." (*Id.*, subd. (b)(7)(A).)

110. Civil Code section 56.181, subdivision (d)(1) requires a direct-to-consumer genetic testing company to implement and maintain reasonable security procedures and practices to protect a consumer's genetic data against unauthorized access, destruction, use, modification, or disclosure.

111. Defendants failed to implement and maintain reasonable security procedures and practices to protect consumers' genetic data against unauthorized access, destruction, use, modification, or disclosure as described in Paragraphs 34-87. Defendants' failure was negligent. As a result, Defendants violated Civil Code section 56.181, subdivision (d)(1).

SECOND CAUSE OF ACTION

VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT

(CIVIL CODE SECTION 1798.100 ET SEQ.)

112. The People reallege and incorporate by reference each of the paragraphs above as though fully set forth herein.

113. At all times relevant, 23andMe was a "business" that collected consumers' personal information. (Civ. Code, § 1798.140, subd. (d).) "'Personal information' means 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." (*Id.*, subd. (v)(1).) "Personal information" is defined to include, among other things, "[i]dentifiers, such as a real name, alias, postal address, [or] unique personal identifier," "sensitive personal information," and "[i]nferences drawn from" any such information "to create a profile about a consumer reflecting," among other things, the consumer's "characteristics, . . . intelligence, abilities, and aptitudes." (*Id.*, subds. (v)(1)(A), (v)(1)(K), (v)(1)(L).) "Sensitive personal information" is defined to include personal information that reveals "a consumer's racial or ethnic origin," "a consumer's genetic data," and "personal information collected and analyzed concerning a consumer's health." (*Id.*, subds. (ae)(1)(D), (ae)(1)(F), (ae)(2)(B).)

114. Civil Code section 1798.100, subdivision (e) requires a business that collects a consumer's personal information to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

115. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it maintained to protect the personal information from unauthorized access, destruction, use, modification, or disclosure as described in Paragraphs 34-87. As a result, Defendants violated Civil Code section Civil Code section 1798.100, subdivision (e).

THIRD CAUSE OF ACTION

VIOLATIONS OF THE FALSE ADVERTISING LAW

(BUSINESS AND PROFESSIONS CODE SECTION 17500 ET SEQ.)

116. The People reallege and incorporate by reference each of the paragraphs above as though fully set forth herein.

117. Defendants engaged in acts or practices that constitute violations of Business and Professions Code section 17500 *et seq.* by making or disseminating, or causing to be made or disseminated, untrue or misleading statements with the intent to induce members of the public to use 23andMe's services or products.

118. Defendants' untrue or misleading statements include, but are not limited to: its statements regarding 23andMe's security measures in place at the time of the data breach; post-breach statements regarding the severity of the breach and the adequacy of 23andMe's security measures and investigation; and statements made regarding the "DNA Relatives" feature. (See, e.g., Paragraphs 34-107.)

119. At the time these representations were made, Defendants knew or by the exercise of reasonable care should have known that these representations were untrue or misleading.

FOURTH CAUSE OF ACTION

VIOLATIONS OF THE UNFAIR COMPETITION LAW

(BUSINESS & PROFESSIONS CODE SECTION 17200 ET SEQ.)

120. The People reallege and incorporate by reference each of the paragraphs above as though fully set forth herein.

121. Defendants have engaged in unlawful, unfair, or fraudulent acts or practices, which constitute unfair competition within the meaning of Section 17200 of the Business and Professions Code. Defendants' violations of Section 17200 of the Business and Professions Code include but are not limited to:

a. Violation of the Genetic Information Privacy Act (Civ. Code, § 56.18 *et seq.*), as alleged in the First Cause of Action.

b. Violation of the California Consumer Privacy Act (Civ. Code, § 1798.100 *et seq.*), as alleged in the Second Cause of Action.

c. Violation of Civil Code section 1798.81.5. At all times relevant, 23andMe was a business that maintained personal information, which includes genetic data and medical information, about California residents. 23andMe failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it maintained to protect the personal information from unauthorized access, destruction, use, modification, or disclosure as described in Paragraphs 34-87.

d. Violation of the California Online Privacy Protection Act (CalOPPA, Bus. & Prof. Code, § 22575 *et seq.*). At all times relevant, 23andMe was an operator of a commercial online service that collected personally identifiable information through the Internet about individual consumers residing in California who used its commercial online service. (§ 22575, subd. (a).) 23andMe's posted privacy policy discussed their privacy and data security practices. 23andMe's failure to comply with their posted privacy policy was negligent and material. (§ 22576, subd. (b).)

e. Violation of California consumers' right to privacy as established in article I, section 1 of the California Constitution by failing to protect genetic data and personal information from unauthorized access, destruction, use, modification, or disclosure.

f. Violation of Business and Professions Code section 17500 et seq., as alleged in the Third Cause of Action.

g. Engaging in unfair business acts or practices, fraudulent acts or practices, and unfair, deceptive, untrue or misleading advertising including but not limited to 23andMe's data security practices at the time of the data breach, statements regarding its security measures in place at the time of the data breach, statements regarding the nature and severity of the breach after it was disclosed, and statements regarding the "DNA Relatives" feature.

PRAYER FOR RELIEF

WHEREFORE, the People pray for judgment as follows:

122. Pursuant to Civil Code section 1798.199.90, that the Court enter an injunction to prevent 23andMe, their successors, agents, representatives, employees, and all persons who act in concert with 23andMe from engaging in any act or practice that violates Civil Code section 1798.100 *et seq.* (CCPA), including but not limited to, as alleged in this Complaint;

123. Pursuant to Business and Professions Code section 17203, that the Court enter all orders necessary to prevent 23andMe, their successors, agents, representatives, employees, and all persons who act in concert with 23andMe from engaging in any act or practice that constitutes unfair competition in violation of Business and Professions Code section 17200, including, but not limited to, as alleged in this Complaint;

124. Pursuant to Business and Professions Code section 17535, that the Court enter all orders necessary to prevent 23andMe, their successors, agents, representatives, employees, and all persons who act in concert with 23andMe from making any untrue or misleading statements in violation of Business and Professions Code section 17500, including, but not limited to, as alleged in this Complaint;

125. Pursuant to Civil Code section 56.182, subdivision (a), that the Court assess a civil penalty of One Thousand Dollars ($1,000) for each violation of GIPA, as proved at trial;

126. Pursuant to Civil Code section 1798.199.90, that the Court assess a civil penalty of Two Thousand Five Hundred dollars ($2,500) for each violation of the CCPA, or Seven Thousand Five Hundred dollars ($7,500) for each intentional violation and each violation involving the personal information of minor consumers, as proven at trial;

127. Pursuant to Business and Professions Code section 17206, that the Court assess a civil penalty of Two Thousand Five Hundred Dollars ($2,500) for each violation of Business and Professions Code section 17200, as proved at trial;

128. Pursuant to Business and Professions Code section 17206.1, subdivision (a), that the Court assess a civil penalty of Two Thousand Five Hundred Dollars ($2,500) for each violation of Business and Professions Code section 17200 perpetrated again a senior citizen (person who is 65 years of age or older), as proved at trial;

129. Pursuant to Business and Professions Code section 17536, that the Court assess a civil penalty of Two Thousand Five Hundred Dollars ($2,500) for each violation of Business and Professions Code section 17500, as proved at trial;

130. That the People recover their cost of suit herein, including costs of investigation;

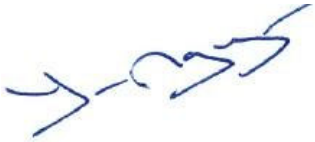
131. That the People receive all other relief to which they are legally entitled; and

132. For such other and further relief as the Court deems just and proper.

Dated: May 27, 2026

Respectfully submitted,

ROB BONTA
Attorney General of California
NICKLAS A. AKERS
Senior Assistant Attorney General



YEN P. NGUYEN
Deputy Attorney General
Attorneys for The People of the State of California