CONFIDENTIAL
OFFICIAL - Sensitive

PENALTY NOTICE

23andMe, Inc.

5 June 2025

TABLE OF CONTENTS

DATA PROTECTION ACT 2018

(PART 6, SECTION 155)

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

PENALTY NOTICE

To: 23andMe, Inc and 23andMe Holding Co.

FAO: [redacted] (Chief Information Security Officer)

Of: 870 Market Street
Room 415
San Francisco
California, 94102

I. INTRODUCTION

1. Pursuant to section 155(1)(a) of the Data Protection Act 2018 ("**DPA 2018**"), by this written notice ("**Penalty Notice**"), the Information Commissioner (the "**Commissioner**") requires 23andMe, Inc ("**23andMe**") to pay the Commissioner a penalty of £2,310,000.

2. This Penalty Notice is given in respect of infringements of Article 5(1)(f) and 32(1) of the UK General Data Protection Regulation ("**UK GDPR**").

3. This Penalty Notice follows an investigation which was carried out jointly by the Information Commissioner's Office ("**ICO**") and the Office of the Privacy Commissioner of Canada ("**OPC**") into a personal data breach which 23andMe first reported to both regulators in October 2023. This Penalty Notice sets out the Commissioner's conclusions and the reasons why the Commissioner has decided to impose a penalty, including the circumstances of the infringements and the nature of the personal data involved.

4. In accordance with paragraph 2 of Schedule 16 to the DPA 2018, the Commissioner issued a notice of intent ("**NOI**") to 23andMe on 4 March

2025, setting out the reasons why the Commissioner proposed to issue 23andMe with a penalty notice. In that NOI, the Commissioner indicated that the amount of the penalty he proposed to impose was £4,593,750.

5. On 18 April 2025, 23andMe made written representations (the **"Written Representations**") in response to the Commissioner's NOI. Oral representations were provided at a hearing on 30 April 2025 (the "**Oral Hearing**"). In reaching the decision to issue this Penalty Notice, the Commissioner has taken full account of 23andMe's representations and, where appropriate, the Penalty Notice makes specific reference to them.

6. On 6 February 2025, 23andMe Holding Co., of which 23andMe is a wholly owned subsidiary, filed its Form 10-Q[1] with the United States Securities and Exchange Commission. The Form 10-Q showed that as of 31 December 2024, 23andMe Holding Co. had accumulated a deficit of $2.4 billion and possessed unrestricted cash and cash equivalents of $79.4 million, a decline from $216,488,000 on 31 March 2024. At the time of filing the Form 10-Q, 23andMe Holding Co. stated that there was substantial doubt about the company's ability to continue as a going concern.[2]

7. On 23 March 2025, 23andMe Holding Co. and certain of its subsidiaries, including 23andMe, filed voluntary petitions seeking relief under Chapter 11 of Title 11 of the United States Bankruptcy Code in the United States Bankruptcy Court for the Eastern District of Missouri.[3] A hearing to approve the sale of 23andMe Holding Co., its subsidiaries and/or its assets is scheduled to take place on 17 June 2025.

8. The Commissioner finds that between 25 May 2018[4] and 31 December

[1] SEC Filing | 23andMe, Inc.
[2] 23andMe Written Representations, 18 April 2025: Paragraph 25
[3] 23andMe Written Representations, 18 April 2025: Paragraph 26
[4] 23andMe's obligations under the General Data Protection Regulation (Regulation 2016/679 of the European Parliament and Council) came into effect on 25 May 2018.

2024[5] ("**the Relevant Period**") 23andMe infringed Article 5(1)(f) and Article 32(1) of the UK GDPR (the "**Infringements**"), by failing to implement:

a) appropriate technical and organisational measures to ensure the ongoing confidentiality, integrity, availability and resilience of its processing systems and services (Article 5(1)(f) and Article 32(1)(b) UK GDPR); and

b) an appropriate process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures intended to ensure the security of its processing systems and services (Article 5(1)(f) and Article32(1)(d) UK GDPR).

9. 23andMe submitted that in light of the deterioration in its financial position, a monetary penalty is not warranted as it would further deplete the funds that may be used to compensate 23andMe customers who have filed several class action lawsuits and arbitration claims in the US, Canada and the UK.[6] The Commissioner has carefully considered these representations and concluded that a monetary penalty remains appropriate in order to provide an effective, proportionate and dissuasive response to the Infringements. However, when setting the amount of the penalty, the Commissioner has taken into account the latest financial information provided by 23andMe, including 23andMe Holding Co.'s projected annual turnover for its 2025 financial year, in order to ensure that the penalty is proportionate in light of the company's current and significantly deteriorated financial position.

10. This Penalty Notice is issued in respect of the Infringements on the basis that, in all the circumstances, and having regard to the matters listed in Article 83(1) and 83(2) UK GDPR, the Commissioner considers that the

[5] 23andMe confirmed that its security improvements had been materially implemented by this date.
[6] 23andMe Written Representations, 18 April 2025: Paragraph 30

imposition of a financial penalty in the sum of £2,310,000 is an effective, proportionate and dissuasive response to the Infringements.

II. EXECUTIVE SUMMARY

11. This Penalty Notice follows a joint investigation by the Information Commissioner's Office and the Office of the Privacy Commissioner of Canada. The findings in this Penalty Notice are those of the Commissioner only.

12. Following his investigation, the Commissioner has concluded that during the Relevant Period, 23andMe, a US-based consumer genetics and research company, infringed Article 5(1)(f) and Article 32(1)(b) and (d) UK GDPR by failing to implement:

    a) appropriate authentication and verification measures as part of its customer login process, including, but not limited to, mandatory multi-factor authentication ("**MFA**"), appropriate password security policies and procedures, the ability for customers to use unpredictable usernames and other additional controls, such as device, connection or address fingerprinting (Article 5(1)(f) and Article 32(1)(b) UK GDPR);

    b) appropriate security measures specifically focused on the access to, and download of, special category data[7] (Article 5(1)(f) and Article 32(1)(b) UK GDPR);

    c) measures which enabled 23andMe to monitor for, detect and appropriately respond to threats to its customers' personal data (Article 5(1)(f) and Article 32(1)(b) UK GDPR);

    d) an appropriate process for regularly testing and assessing the effectiveness of its technical and organisational security measures, specifically in relation to the threat posed to its customers' personal

[7] "*Special category data*" is defined in Article 9(1) UK GDPR

data by a credential stuffing attack[8] instigated by a third-party threat actor[9] (Article 5(1)(f) UK GDPR and Article 32(1)(d) UK GDPR).

13. As a result of the Infringements, a threat actor was able to perpetrate a credential stuffing attack over the course of at least five months (the "**Data Breach**"), during which they obtained access to personal data relating to 155,592 UK-based customers of 23andMe ("**Affected UK Data Subjects**"). The personal data exfiltrated by the threat actor was offered for sale on a number of online forums in August and October 2023, with the relevant posts indicating that the threat actor had targeted 23andMe customers according to their racial and ethnic background.

14. Whilst the nature of the personal data accessed by the threat actor will have varied between the Affected UK Data Subjects, at least some of it constituted special category data. This special category data included personal data relating to health and genetic data, as well as data relating to the racial or ethnic origin of some customers, which could be inferred from the personal data processed by 23andMe.

15. The Commissioner has obtained evidence from Affected UK Data Subjects which demonstrates the harm which arose, or could have arisen, from the Infringements, including feelings of extreme anxiety about the consequences for their personal, financial and family safety and concerns that the personal data accessed by the threat actor could be used to target specific groups.

[8] Credential stuffing takes advantage of people reusing username and password combinations. Attackers fraudulently obtain valid combinations for one site and then use them across others to try and gain access to accounts (Use of credential stuffing tools - NCSC.GOV.UK)

[9] For the purposes of this Penalty Notice, the Commissioner has referred to a "threat actor", however, the Commissioner has not been received conclusive evidence that the Data Breach (as defined in paragraph 13 above) and the related posts on the dark web were attributable to a single individual or group.

16. The Commissioner has concluded that the Infringements constituted a serious failure to comply with the requirements of Article 5(1)(f) and Article 32(1) UK GDPR. The seriousness of the Infringements was aggravated by the sensitivity of the personal data processed by 23andMe, the large number of Affected UK Data Subjects, the extended period of time during which the 23andMe failed to comply with its data protection obligations and the damage and distress suffered and likely to be suffered by Affected UK Data Subjects as a result of the unauthorised access to their personal data.

17. The seriousness of the Infringements was further aggravated by:

    a) 23andMe's failure to identify the Data Breach at an earlier stage, despite multiple indications of anomalous and unauthorised activity by the threat actor; and

    b) deficiencies in the content of 23andMe's notifications of the Data Breach to the Commissioner.

18. In light of the above, and having fully taken into account the representations received from 23andMe in relation to the NOI and penalty calculation, the Commissioner has concluded that a penalty of £2,310,000 adequately reflects the seriousness of the Infringements and is effective, proportionate and dissuasive.

III. RELEVANT LEGAL FRAMEWORK

19. Section 155 DPA 2018 provides that, if the Commissioner is satisfied that a person has failed, or is failing, as described in section 149(2) DPA 2018, the Commissioner may, by written notice, require the person to pay to the Commissioner an amount in sterling specified in the notice.

20. The types of failure described in section 149(2) DPA 2018, include, at section 149(2)(a), *"where a controller or processor has failed , or is failing, to comply with . . . a provision of Chapter II of the UK GDPR ... . principles of processing)"* and at section 149(2)(c), *"where a controller*

or processor has failed, or is failing, to comply with . . . a provision of Articles 25-39 of the UK GDPR . . . (obligations of controllers and processors).”

21. Chapter II of the UK GDPR sets out the principles relating to the processing of personal data that controllers must comply with. Article 5(1) UK GDPR lists these principles and at point (f) includes the requirement that “*personal data shall be… processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).”* This is referred to in the UK GDPR as the “integrity and confidentiality” principle.

22. Article 32(1) UK GDPR (security of processing) materially provides:

“(1) *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk . . .*

(2) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from . . . unauthorised disclosure of . . . personal data transmitted, stored or otherwise processed.”

23. The legal framework for imposing a penalty notice is set out below in **Section VII: Decision to Impose a Penalty**.

IV. BACKGROUND TO 23ANDME

24. This section summarises the corporate background of 23andMe, the services which it offers to its customers and how uninterpreted raw genotype data can be downloaded from its customer accounts.

A. Corporate background

25. 23andMe is a consumer genetics and research company which operates a direct-to-consumer genetic testing service available both through https://23andme.com and as a mobile application available on iOS and Android (together the "**Platform**").

26. 23andMe was incorporated on 28 April 2006 in Delaware in the United States of America and is a wholly owned subsidiary of 23andMe Holding Co., a company incorporated on 16 June 2021, also in the US state of Delaware.[10] Shares in 23andMe Holding Co. began trading on the Nasdaq Global Select Market ("**Nasdaq**") on 17 June 2021.[11] However, trading in 23andMe Holding Co.'s common stock was suspended on the NASDAQ on 31 March 2025. On the same date, trading in 23andMe Holding Co.'s common stock began on the OTC Pink Market.[12] On 27 May 2025, 23andMe Holding Co. announced its intention to voluntarily file a Form 25 Notification of Delisting with the US Securities and Exchange Commission which will remove its stock from listing and registration on the NASDAQ.[13]

B. 23andMe's services

27. 23andMe offers its services worldwide, although not all of its services are available in every location in which its services are offered. As of July 2024, 23andMe offered its services to individuals in 39 countries and territories, including the United States of America, the United

[10] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to question 1
[11] 23andMe Press release entitled, "23andMe Successfully Closes its Business Combination with VG Acquisition Corp", 16 June 2021 (accessed 4 February 2025)
[12] 23andMe Holding Co's Form 8-K dated 19 May 2025 states that on 24 March 2025, the NASDAQ informed 23andMe Holding Co, that, in connection with the company's announcement of its filing for insolvency protection under Chapter 11 of Title 11 of the US Bankruptcy Code and in accordance with the NASDAQ Listing Rules, the 23andMe Holding Co,'s securities would be delisted from the NASDAQ Stock Market.
[13] 23andMe Announces Intent to Voluntarily Delist from Nasdaq and Deregister with the SEC | 23andMe, Inc. (accessed 28 May 2025)

Kingdom and Canada.[14]

28. The following terms are defined by 23andMe on its website and should be interpreted as follows for the purposes of this Penalty Notice:

    a) "***Raw Genetic Data***" means all the uninterpreted raw genotype data relating to a particular customer including data that is used in the 23andMe reports defined in Annex 1. 23andMe allows its customers to view and download their Raw Genetic Data via its "*Browse Raw Data"* feature,[15] which produces a text file consisting of lines of genotype data displaying all of the customer's nucleotides and their position on each of the customer's chromosomes.[16]

    b) "***Ancestry Composition Reports***" "*shows the percentage of a particular customer's DNA that comes from each of the 47 populations*" which 23andMe has identified as genetically similar groups of people with a known common ancestry.[17]

29. Annex 1 contains further definitions of terms related to 23andMe's services which are used in this Penalty Notice.

30. During the Relevant Period, 23andMe offered the following three services to UK data subjects:

    a) **"Ancestry Service"** – This provides access to Ancestry Composition Reports and the DNA Relatives and Connections features (details regarding these two features are provided in paragraph 33 below).[18]

    b) **"Health + Ancestry Service"** – This includes the features provided as part of the Ancestry Service as well as access to Health

[14] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to question 1
[15] The Commissioner considers Raw Genetic Data to constitute "genetic data" as defined in Article 4(13) UK GDPR
[16] Accessing Your Raw Genetic Data – 23andMe Customer Care (accessed 4 February 2025)
[17] Ancestry Composition - 23andMe UK (accessed 4 February 2025)
[18] 23andMe: Ancestry Service (accessed 5 February 2025)

Predisposition Reports, Wellness Reports and Carrier Status Reports (as defined in Annex 1).

c) **"23andMe+ Premium"** – This includes the features provided as part of the Health+ Ancestry Service as well as access to additional health reports powered by 23andMe research, Pharmacogenetic Reports (as defined in Annex 1) and other health-focused features.[19]

31. As of 1 October 2023, 23andMe had approximately 14.9 million customers worldwide, with approximately 495,000 resident in the UK.[20]

32. 23andMe customers who have created an account, registered for a 23andMe test kit and provided a DNA sample have the option to consent to participate in 23andMe research projects.[21] Participating 23andMe customers answer online survey questions and their genetic data is combined with other data points by researchers in studies aimed at making medical and scientific discoveries.[22]

33. There are a number of features available within the Platform which 23andMe offers in the UK and which are designed to result in connections being made between customers who have a genetic relationship:

a) "***DNA Relatives***" is an optional feature which allows customers who have provided consent to match with their genetic relatives. The genetic relative must have also taken a 23andMe test, have an active 23andMe account and have consented to participate in DNA Relatives. Depending on the customer's service subscription, they can view either 1,500 or 5,000 "DNA Relatives". DNA Relatives

[19] 23andMe+ Premium Service (accessed 5 February 2025)
[20] Letter from Greenberg Traurig LLP to the ICO and OPC dated 16 July 2024 (response to letter from the ICO and OPC dated 20 June 2024), Response to question 1
[21] Letter from Greenberg Traurig LLP to the ICO and OPC,16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to Question 1
[22] Research - 23andMe United Kingdom (accessed 5 February 2025)

matches can view one another's display name,[23] most recent log-in date, relationship labels and predicted relationship. The "predicted relationship" uses the number of segments of DNA shared by relatives and the overall percentage of shared DNA to predict a likely relationship with that relative.[24] Customers may also choose to share their ancestry reports, matching DNA segments, self-reported postcode-level location, the birth locations of their ancestors and family names, profile picture, birth year, a weblink to their family tree and any other information included within the "*Introduce Yourself*" section of the customer's profile.[25]

b) The "***Family Tree***" feature is part of DNA Relatives and generates an individual's family tree based on their DNA Relatives matches. A customer's Family Tree profile contains their display name, relationship labels and percentage DNA shared with their DNA Relatives matches. Individual customers can also choose to share their self-reported postcode-level location and birth year.[26]

c) The "***Connections***" feature allows customers to share genetic ancestry information and their DNA Relatives profile and, if they choose to do so, their 23andMe health-related and trait reports with other customers to whom they are not genetically related on the basis of mutual agreement between the customers.[27]

C. Accessing and downloading Raw Genetic Data

34. 23andMe allows its customers to access and download their Raw Genetic

[23] Display names are selected by the user and comprise either initials only, first name and last initial, first initial and last name, and first and last name
[24] DNA Relatives: Detecting Relatives and Predicting Relationships – 23andMe Customer Care (accessed 5 February 2025)
[25] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 1
[26] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 1
[27] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 1

Data from their accounts at any time using the Browse Raw Data feature[28].

35. 23andMe provides this function to enable its customers to access, understand and benefit from the information their genetics can tell them. 23andMe informed the Commissioner that many customers wish to upload their data to third-party services, which offer to interpret their raw DNA data to find new genetic relatives or generate new genetic reports.[29]

36. As of 29 April 2023, the date identified by 23andMe as the beginning of the Data Breach described further at paragraphs 93 to 103 below,[30] a customer was able to access and download their Raw Genetic Data through 23andMe's "*Browse Raw Data"* feature.[31] The Commissioner notes that this feature was disabled on 2 November 2023[32], as part of 23andMe's response to the Data Breach. During the suspension, customers were required to authenticate their identities with 23andMe customer care to download their Raw Genetic Data. The feature was then reinstated on 27 February 2024 with the additional requirement that users had to provide the date of birth used to register their account before they could download their Raw Genetic Data[33]. At or around this time, 23andMe also introduced a 48-hour delay between a Raw Genetic Data download request being made and the notification email being sent

[28] Response from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to Question 37, footnote 1.
[29] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 5
[30] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 36
[31] Letter from Greenberg Traurig LLP to the ICO and OPC, 10 September 2024 (responding to a letter from the ICO and OPC dated 21 August 2024): Response to Clarification Question 12
[32] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to Question 12
[33] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to Question 12

to the customer.[34]

37. Until 2 November 2023, a customer could download their Raw Genetic Data in one of three ways:[35]

    a) by navigating directly to you.23andme.com/tools/data/;

    b) by clicking on their profile name on the top right-hand corner of their homepage, and selecting "Browse Raw Data" from the dropdown menu; or

    c) by visiting their "Account Settings" and clicking on "View" under "23andMe Data". Customers would then see a blue "Download Raw Data" button which would redirect them to the download raw data page.

38. When the file was available for download, 23andMe sent the customer an email alerting them. At the time of the Data Breach, there was a short delay following a Raw Genetic Data download request whilst the file was generated.[36] The customer then had to login to their account to download the compressed (.zip) file of Raw Genetic Data by navigating to the same location in their account settings.[37]

39. 23andMe confirmed in the Written Representations and at the Oral Hearing that in addition to the 48-hour delay that had been added, all

[34] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to Question 68
[35] Response from Greenberg Traurig LLP to the ICO and OPC, 10 September 2024 (responding to a letter from the ICO and OPC dated 21 August 2024): Response to Clarification Question 12
[36] Accessing Your Raw Genetic Data – 23andMe Customer Care | Europe (accessed 21 May 2025). At the time of the Data Breach, 23andMe's Customer Care page relating to Raw Genetic Data downloads stated that files were typically available within one hour of a request being made.
[37]Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to Clarification Question 12.

download actions for exome,[38] "PGS" raw data,[39] medical data and profile transfers now require additional verification in the form of the date of birth used to register for their customer account. In addition, only three incorrect attempts are permitted for this additional verification, after which a customer is prevented from initiating a Raw Genetic Data download request and directed to contact 23andMe's Customer Care team.

V. BACKGROUND TO THE INFRINGEMENTS

A. Relevant events prior to October 2023

40. This section summarises the relevant events which took place prior to 23andMe becoming aware of the Data Breach in October 2023 and which have been disclosed to the ICO and the OPC during the course of their joint investigation. It does not seek to provide an exhaustive account of all relevant events which took place prior to 29 April 2023.

(a) 2019 and 2020 credential stuffing attacks

41. In October 2023, a forensic team, instructed by 23andMe, commenced an investigation (the "**Internal Investigation**") into reports that personal data relating to 23andMe customers ("**Customer Personal Data**") had been exfiltrated from the Platform and offered for sale on the dark web.[40]

[38] The exome represents the protein-coding regions of genes, which make up only about 1-2% of the entire genome but contain the majority of genetic variants associated with disease risk. By selectively sequencing these regions, exome sequencing provides valuable insights into an individual's genetic makeup, identifying variations that may be linked to specific genetic disorders or conditions. This technique is particularly useful for diagnosing rare genetic diseases and conducting research into the genetic basis of various medical conditions, 23andMe+ Total Health - Build longevity with DNA, blood & more (accessed 2 June 2025).
[39] Polygenic scores (PGS) aim to quantify the cumulative effects of a number of genes, which may individually have a very small effect on susceptibility. They can be used to predict a person's likelihood of displaying any trait with a genetic component, Polygenic risk scores: how useful are they? - Genomics Education Programme (accessed 12 May 2025).
[40] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to Question 36

42. As part of the Internal Investigation, 23andMe analysed whether any credential stuffing attacks had taken place prior to 29 April 2023. The forensic team identified "*eight separate accounts that may have been accessed in isolated incidents of credential stuffing in 2019 and 2020*."[41] This was the first occasion on which 23andMe identified these earlier credential stuffing attacks.

(b) July 2023 Login Spike and July Attempted Profile Transfers

43. **6 July 2023** - The Platform was rendered temporarily inoperable as a result of over one million successful logins (as displayed in Figure 3 below), primarily to a single customer account in what was subsequently determined to be an unsuccessful attempt to transfer the ownership of customer profile data from the accessed customer account to other 23andMe accounts using 23andMe's profile transfer function[42] (the "**July Login Spike**").[43]

[41] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to Question 36
[42] A profile transfer is when a DNA profile associated to an account is transferred to a different account. This may take place, for example, when a child who has their profile associated to a shared family account (23andMe Family Account Options (accessed 5 February 2025)) becomes an adult and wishes to establish their own account. To initiate a profile transfer, a customer must be logged into the account with which the DNA profile is associated and enter the email address of the "destination account" (What is a Profile Transfer? – 23andMe Customer Care (accessed 5 February 2025))
[43] Letter from Greenberg Traurig LLP to the ICO and OPC, 14 October 2024 (responding to a letter from the ICO and OPC dated 20 September 2024): Response to question 7 of request for information relating to logs and other technical-related components and Exhibit V (Failed and Successful Logins 1 January 2019 – 31 December 2023)

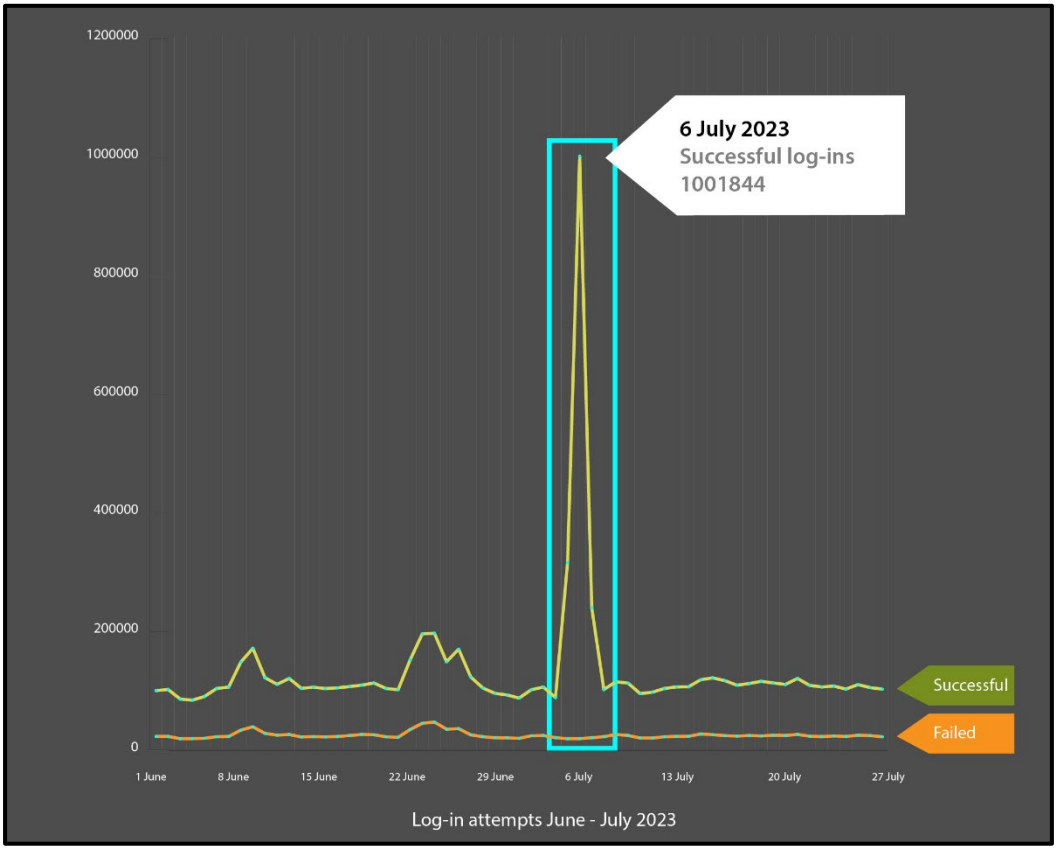


Figure 1: The July Login Spike[44]

44. **28 to 30 July 2023** - Further unsuccessful attempts were made to transfer ownership of profile data relating to approximately 400 customers from accounts which the threat actor had successfully accessed to other 23andMe accounts[45] (the "**July Attempted Profile Transfer**").[46]

45. Upon discovery of the July Attempted Profile Transfer, 23andMe disabled all profile transfer requests, placed a temporary lock on accounts suspected of attempting to perform an unauthorised profile transfer and initiated a mandatory password reset for the customers deemed to have

[44] Letter from Greenberg Traurig LLP to the ICO and OPC, 14 October 2024 (responding to a letter from the ICO and OPC dated 20 September 2024): Response to question 7 of request for information relating to logs and other technical-related components and Exhibit V (Failed and Successful Logins 1 January 2019 – 31 December 2023)
[45] The Commissioner has not received confirmation as to whether the destination accounts were other customer accounts that had been successfully credential stuffed, or the threat actor's own accounts.
[46] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to question 36

been affected. 23andMe also added a systems alert for [redacted] to detect abnormal rates of profile transfer requests ([redacted]) and undertook an internal investigation to determine whether Customer Personal Data had potentially been accessed by a third party. Based on its investigation, 23andMe determined that limited Customer Personal Data within 19 US-based 23andMe customers' accounts had been accessed by an unauthorised third party.[48]

(c) Customer contact portal messages – August 2023

46. **10 and 11 August 2023** - Messages were submitted via the 23andMe customer contact portal which were directed to 23andMe's former chief executive officer ("**CEO**"), [redacted], from an individual named "Anna" who claimed to have obtained the data of over 10 million 23andMe customers (the **"August 2023 Messages"**). It was claimed that the data amounted to over 300 terabytes, and included personal information, family background, ancestry composition, haplogroup information, health data, health traits, surveys and raw DNA data. The individual threatened to "*destroy"* 23andMe if the company was not "*honest*" with them.[49] "Anna" further threatened to share the DNA data of both [redacted] and her former husband, [redacted].

47. **14 - 18 August 2023** - The August 2023 Messages were identified and considered by 23andMe's Cyber Incident Response Team.[50] Further details of the August 2023 Messages are provided at paragraphs 53 to

[47] [redacted]

[48] 23andMe Written Representations, 18 April 2025, paragraph 11

[49] Letter from Greenberg Traurig LLP to the OPC and ICO, 23 October 2024 (responding to letters from the ICO and OPC dated 20 September and 11 October 2024): Exhibit AA

[50] A cyber incident response team consists of the people who will handle the response to an incident. It may include both internal and external teams and may differ based on the nature of the incident - Build: A cyber security incident response team (CSIRT) - NCSC.GOV.UK

61 below.

(d) The Hydra Post

48. **11 August 2023** - Customer Personal Data was offered for sale on the Hydra Market platform[51] by a customer operating under the pseudonym Dazhbog (the "**Hydra Post**"). In the Hydra Post, Dazhbog claimed to have access to 10 million DNA records, and offered them for sale for US$50 million. Dazhbog claimed that the file contained over 300 terabytes of data, and included "*personal information, family background, ancestry composition, haplogroup, health, traits, surveys [and] raw DNA data*." Dazhbog also offered to separate the data specifically based on location and ethnicity if the purchaser was willing to pay an additional fee.[52]

49. A copy of this post is displayed at Figure 2 below:

[51] Hydra Market was an online criminal marketplace that enabled users in mainly Russian-speaking countries to buy and sell illicit goods and services, including illegal drugs, stolen financial information, fraudulent identification documents and money laundering and mixing services, anonymously and beyond the reach of law enforcement. Hydra Market was disabled in April 2022 after the US Department of Justice seized its servers and cryptocurrency wallets containing US$25 million in a coordinated international law enforcement operation - Office of Public Affairs | Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace | United States Department of Justice (accessed 5 February 2025). Despite this, the [redacted] Report dated 19 October 2023 (Exhibit N of the Letter from Greenberg Traurig LLP to the OPC and ICO, 13 August 2024) attributed the Dazhbog posts to the Hydra Market platform. The Commissioner has not investigated the accuracy of the attribution of the Dazhbog posts to the Hydra Market platform

[52] Letter from 23andMe to the ICO and OPC, 13 August 2024 (in response to a letter from the ICO and OPC dated 20 June 2024): Response to question 47 and Exhibit N

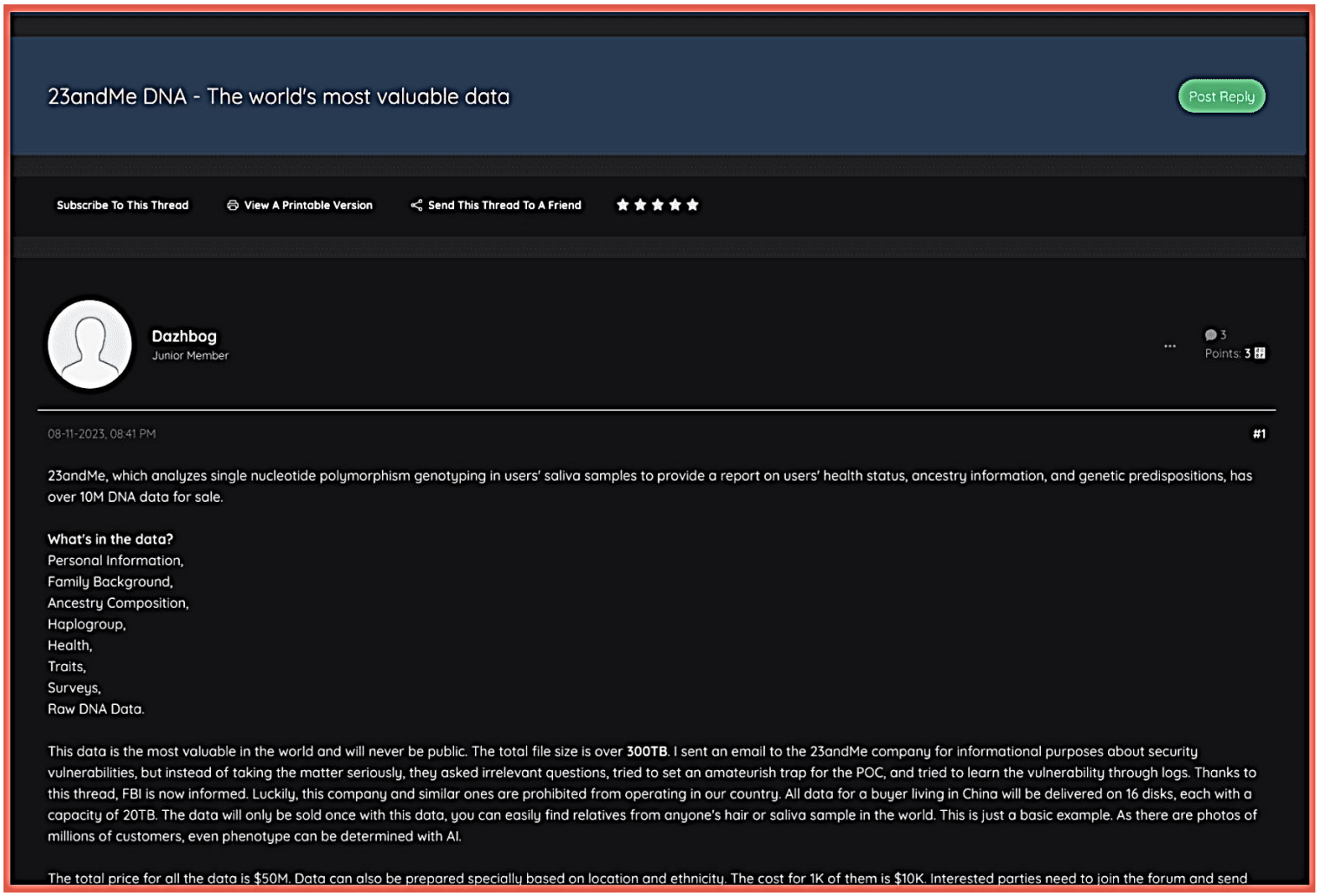


Figure 2: The Hydra Post

50. Dazhbog has not been identified, but they did indicate in their post that 23andMe was not allowed to operate in their country and gave specific instructions on how the data would be sent to a purchaser in China.

51. A subsequent post, apparently by the same user, on 14 August 2023 on the Hydra Market platform claimed that the entire dataset had been sold to an Iranian national who had requested that the original post be removed.[53] A copy of this post is displayed at Figure 3 below:

[53] How can a DNA firm lose half its users' data to 'Jew-hating' hackers? (accessed 5 February 2025)

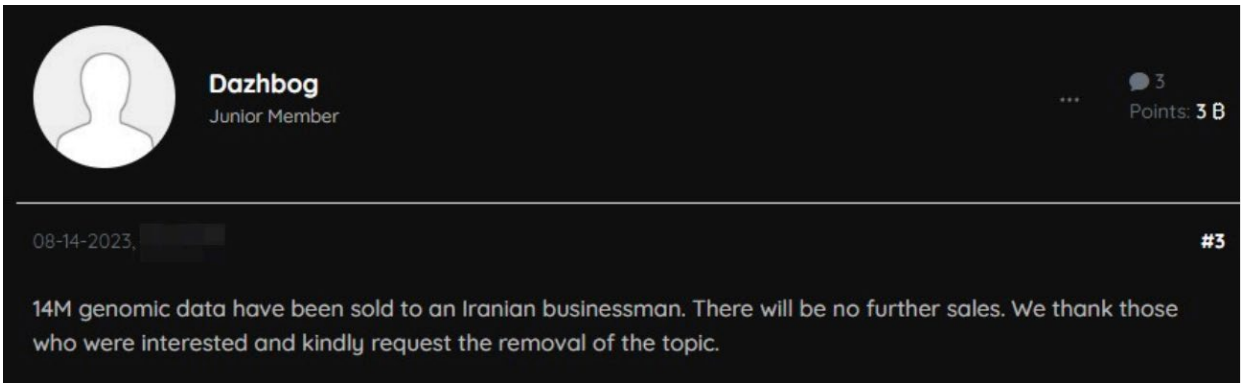


Figure 3: Hydra Post dated 14 August 2023

52. The Commissioner notes reports from The Times that Dazhbog provided links to the personal data of [redacted] (CEO of 23andMe) and [redacted] (Co-founder of [redacted] and former husband of [redacted]) as proof of the data obtained.[54] As noted above, in the August 2023 Messages, "Anna" had threatened to publish the DNA data of [redacted] and [redacted].

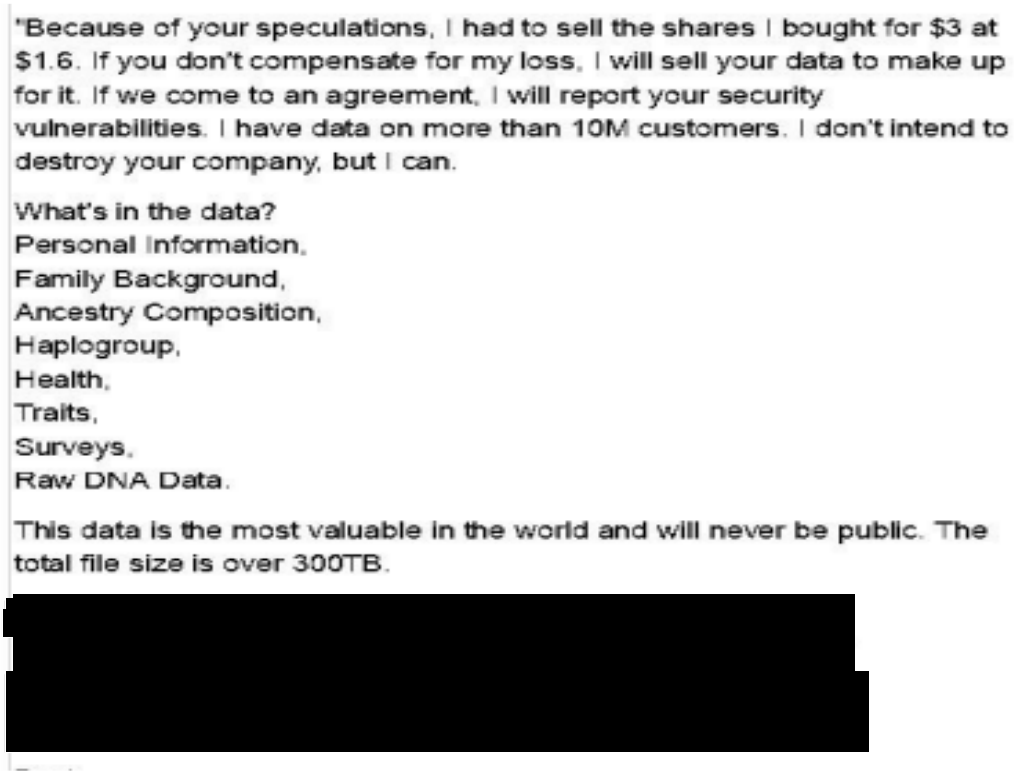
(e) The [redacted] Ticket

53. [redacted] is a third-party customer service software solution. [redacted] provides a ticketing system which provides its clients with a means of centralising the handling of questions, requests and concerns they receive from their customers via email, webchats, telephone or other channels.[55]

54. **14 August 2023** - The Hydra Post and the August 2023 Messages were raised as a security concern in an internal [redacted] Ticket (a form of security incident log), numbered [redacted] ("the [redacted] **Ticket**") by 23andMe's Cyber Incident Response Team.[56]

55. The text from some of the August 2023 Messages, which was copied into the [redacted] Ticket, is displayed at Figure 4 below:

[54] How can a DNA firm lose half its users' data to 'Jew-hating' hackers? (accessed 29 January 2025)
[55] [redacted]
[56] Letter from Grenberg Traurig LLP to the ICO and OPC, 23 October 2024 (in response to letters from the ICO and OPC dated 20 September 2024 and 11 October 2024): Exhibit AL


"Because of your speculations, I had to sell the shares I bought for $3 at $1.6. If you don't compensate for my loss, I will sell your data to make up for it. If we come to an agreement, I will report your security vulnerabilities. I have data on more than 10M customers. I don't intend to destroy your company, but I can.

What's in the data?
Personal Information,
Family Background,
Ancestry Composition,
Haplogroup,
Health,
Traits,
Surveys,
Raw DNA Data.

This data is the most valuable in the world and will never be public. The total file size is over 300TB.

[redacted]

Figure 4: August 2023 Messages as copied into the [redacted] Ticket

56. The [redacted] Ticket was linked to two other incidents previously considered by 23andMe's Cyber Incident Response Team entitled "Suspicious Raw data Downloads [redacted]" and "Data Sharing on Reddit [redacted]". Despite a request from the ICO and the OPC during their joint investigation, 23andMe refused to disclose the incident logs relating to [redacted] and [redacted] claiming that, under US law, they were protected by the work-product doctrine and attorney-client privilege.[57]

57. **14 August 2023** - The [redacted] Ticket was updated to state that "*A user on Reddit by the same name [*Anna*] made a post on the 23andMe Subreddit, but it has since been deleted. Based on the comments, it appears that they* [sic] *poster was providing evidence of a data breach. While the evidence provided in the Reddit post has been deleted, another customer reposted the image with annotations on it.*

[57] Letter from Greenberg Traurig LLP to the ICO and OPC, 17 January 2025

Unfortunately, the original image has not yet been recovered."

58. The [redacted] Ticket shows that a number of immediate actions were identified and allocated to individual members of 23andMe's Cyber Incident Response Team. These actions included conducting an analysis of the email headers within the August 2023 Messages, checking access patterns to identify any irregularities and searching the dark web for any information related to the incident and to data alleged to have been obtained from the Platform in general.

59. **15 August 2023** - A screenshot of the Reddit post referred to in the comments added to the [redacted] Ticket on 14 December 2023 was obtained and added to the [redacted] Ticket.

60. Members of 23andMe's Cyber Incident Response Team added comments to the [redacted] Ticket stating that analysis of the image of the Reddit post did not reveal a discrepancy from the ones on the *"legit DNAR[58] pages*," indicating that the Cyber Incident Response Team believed that the Reddit post included genuine data extracted from the DNA Relatives feature.

61. **18 August 2023** - The [redacted] Ticket was closed by the Cyber Incident Response Team on the basis that it, *"looks to have been a hoax."*[59]

B. The October 2023 Online Forum Posts and 23andMe's initial response

62. Between 1 and 17 October 2023, Customer Personal Data was offered for sale in a number of posts uploaded to online forums (the "**October 2023 Online Forum Posts**").[60] The data offered for sale included the personal data of Affected UK Data Subjects. 23andMe indicated that

[58] DNAR is a reference to 23andMe's DNA Relatives finder, a feature which enables opted in customers to find relatives and compare ancestries or traits
[59] Letter from Grenberg Traurig LLP to the ICO and OPC, 23 October 2024 (in response to letters from the ICO and OPC dated 20 September 2024 and 11 October 2024): Exhibit AL
[60] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Exhibit N

there were further posts across online forums relating to Customer Personal Data and offering it for sale, but the Commissioner has not been provided with copies of such posts.

63. **1 October 2023** - A subreddit user operating under the pseudonym "Green-Prompt6762" posted on the unofficial 23andMe subreddit, claiming to have breached 23andMe's systems, offering Customer Personal Data for sale and posting a sample of the alleged stolen Customer Personal Data ("the **Subreddit Post**").[61] 23andMe informed the Commissioner that its security team monitor activity on the unofficial 23andMe subreddit[62] and that it was through this monitoring that the Subreddit Post was discovered on 1 October 2023.[63]

64. **3 October 2023** - A post was published by an unknown user on the BreachForums[64] platform offering Customer Personal Data for sale. The user later deleted the post.[65]

65. **4 October 2023** - A user operating under the pseudonym "Golem" posted on BreachForums. The post is displayed at Figure 5 below.

[61] A subreddit is a smaller, sub-community within Reddit which is created and moderated by Reddit users. There are communities dedicated to specific topics, where Reddit users can post content and interact with one another. What are communities or "subreddits"? – Reddit Help (accessed 5 February 2025)
[62] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to Question 31.
[63] Third Data Breach Report Form (as defined in paragraph 106 below)
[64] On 24 March 2023, the US Federal Bureau of Investigations, in confirming the arrest of Data BreachForum's founder, described BreachForums as a "*marketplace for cybercriminals to buy, sell and trade hacked or stolen data and other contraband since March 2022*"[64].
[65] Cyber Threat Intelligence Dark Web Report, prepared for 23andMe, dated 10 October 2023 (disclosed as Exhibit N to 23andMe's response dated 13 August 2024 to the letter from the ICO and the OPC dated 20 June 2024)

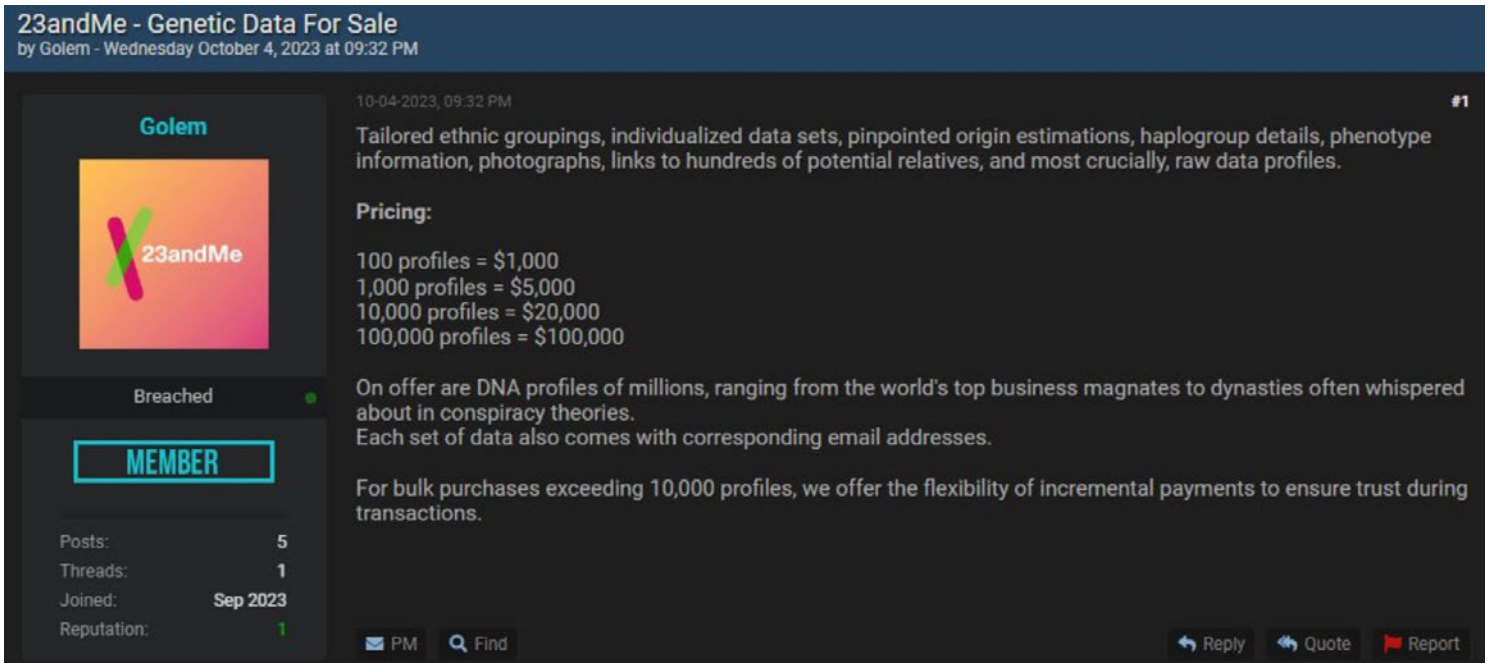


Figure 5: The BreachForums post dated 4 October 2023[66]

66. The post offered for sale the DNA profiles of millions of 23andme customers with "*tailored ethnic groupings, individualized data sets, pinpointed origin estimations, haplogroup details, phenotype information, photographs, links to hundreds of potential relatives, and most crucially, raw data profiles.*"

67. **5 October 2023** - 23andMe confirmed that the Subreddit Post was genuine and commenced the Internal Investigation.[67]

68. **6 October 2023** - 23andMe announced in a blog that customer profiles had been accessed without authority.[68] 23andMe stated that whilst the Internal Investigation was ongoing, it believed that a personal data breach had occurred in which a threat actor had accessed certain 23andMe customer accounts in instances where customers had recycled their login credentials from other websites that had previously been

[66] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Exhibit N
[67] Third Data Breach Report Form (as defined in paragraph 106 below)
[68] Addressing Data Security Concerns - Action Plan - 23andMe Blog (accessed 5 February 2025)

hacked.[69]

69. **8 October 2023** - The [redacted] Ticket was updated by 23andMe's Cyber Incident Response Team to include:

    a) the Hydra Post;

    b) an undated message on an unknown forum addressed to [redacted] which alleged to "write the security vulnerability;"

    c) a post dated 12 August 2023 on an unknown forum offering 23andMe data for sale;

    d) the additional Hydra Market post dated 14 August 2023 from the user operating under the pseudonym "Dazhbog," stating that "*14m genomic data have been sold to an Iranian businessman. There will be no further sales. We thank those who were interested and kindly request the removal of the topic"*; and

    e) a post dated 23 August 2023 from a customer operating under the pseudonym "hiyibef" on an unknown forum stating that, "*I wrote to you via a PM and didn't receive a response. Are you still making sales? We are genuinely interests* [sic]*."*[70]

70. **9 October 2023** - 23andMe disabled all active logged-in customer sessions[71] and published a further blog post which confirmed that the Internal Investigation had been commenced and that the company was working with third-party forensic experts and federal law enforcement officials.[72] This blog page was maintained and updated with further details of the Data Breach and findings of the Internal Investigation up until 5 December 2023.

[69] Addressing Data Security Concerns - Action Plan - 23andMe Blog (accessed 5 February 2025)
[70] Letter from Grenberg Traurig LLP to the ICO and OPC, 23 October 2024 (in response to letters from the ICO and OPC dated 20 September 2024 and 11 October 2024): Exhibit AL
[71] Third Data Breach Report Form (as defined in paragraph 106 below)
[72] Addressing Data Security Concerns - Action Plan - 23andMe Blog (accessed 5 February 2025)

71. **10 October 2023** - 23andMe emailed its customers to inform them of the Data Breach and mandated a password reset using a word or phrase that "*is not easy to guess and* [is] *not used for other accounts.*" 23andMe also encouraged its customers to enable two-factor MFA on their accounts.[73]

72. This was followed by a series of email notifications to customers whose DNA Relatives and Family Tree profiles had been accessed by the threat actor.[74]

73. **15 October 2023** - 23andMe first notified the Commissioner of a personal data breach by submitting a breach report (the "**First Data Breach Report Form**"). 23andMe stated that it had discovered the breach on 5 October 2023 but the date of the breach itself was said to be unknown.

74. The First Data Breach Report Form stated that on 1 October 2023 a customer by the name of Green-Prompt6762 posted on the unofficial 23andMe subreddit claiming to have breached 23andMe's systems. The post offered Customer Personal Data for sale and included a sample of the allegedly stolen data. The First Breach Report Form stated that 1,103,647 data subjects could have been affected in the course of the breach of whom 18,856 were located in the UK.

75. **17 October 2023** - A further post was made by "Golem" on BreachForums (the "**BreachForums Post Dated 17 October 2023**") (displayed at Figure 6 below). This was entitled, "23andMe- Great Britain- Originated 4M Genetic Dataset."

[73] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Exhibit C
[74] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (responding to a letter from the ICO and ICO dated 20 June 2024): Response to question 58 and Exhibit C

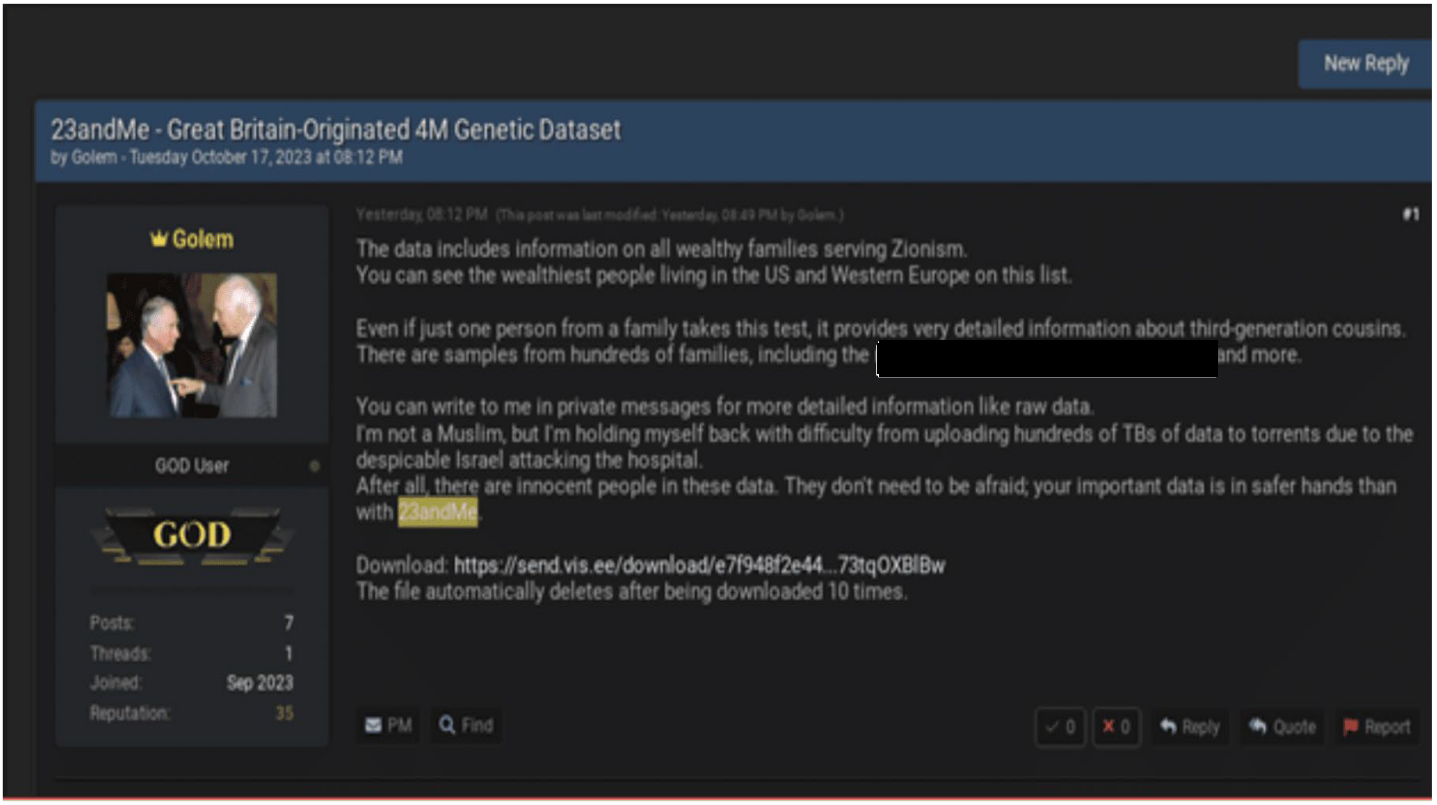


Figure 6: The BreachForums Post Dated 17 October 2023

76. The BreachForums Post Dated 17 October 2023 offered for sale a genetic dataset relating to 4 million customers originating from Great Britain.

77. "Golem" publicly stated that the dataset included, "*information on all wealthy families serving Zionism*" and that, "*even if just one family takes this test, it provides verydetailed information about third-generation cousins*."

78. "Golem" further stated that he/she was "*holding (myself) back with difficulty from uploading hundreds of TBs of data to torrents due to the despicable Israel attacking the hospital. After all, there are innocent people in these data. They don't need to be afraid, your important data is in safer hands than with 23andMe.*"[75]

79. **20 October 2023** - 23andMe temporarily disabled some of the features within the DNA Relatives tool, stating that this was intended as an

[75] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (in response to a letter from the ICO and OPC dated 20 June 2024): Exhibit N

"*additional precaution to protect the privacy of* [its] *customers."*[76]

80. **27 October 2023** – 23andMe submitted a supplementary Data Breach Report Form to the ICO on 27 October 2023 (the "**Second Data Breach Report Form**"). The Second Data Breach Report Form stated that, on 17 October 2023, 23andMe had become aware of the BreachForums Post Dated 17 October 2023 in which a customer by the name "Golem" had posted data which they claimed was from 23andMe, calling it the "*Great Britain-Originated 4M Genetic Dataset*."

81. The Second Data Breach Report Form confirmed that by 23 October 2023, 23andMe had verified that the data referred to in the BreachForums Post Dated 17 October 2023 was genuine. The total number of 23andMe customers thought to be affected was 5,621,179 (including the 1,103,647 reported in the First Data Breach Report Form), including 77,412 in the UK (including the 18,856 UK data subjects reported in the First Data Breach Report Form).

82. **2 November 2023** - 23andMe temporarily disabled its self-service Raw Genetic Data download feature, with customers required to verify their identities with the company's Customer Care team in order to download their Raw Genetic Data during the period of suspension.

83. The self-service functionality was re-enabled on 27 February 2024, with 23andMe introducing a 48-delay between a Raw Genetic Data download request being submitted and the notification email being sent to the customer to inform them that the data is available for download.[77] At or around this time, 23andMe also introduced an additional requirement for customers to provide the date of birth used to register their account when attempting to complete a data download. The Commissioner understands that, as of the date of this Penalty Notice, this verification

[76] Addressing Data Security Concerns - Action Plan - 23andMe Blog: Update: 20 October 2023 (9:35pm PST), (accessed 5 February 2025)
[77] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to Question 68

step continues to apply to the self-service Raw Genetic Data download feature.[78]

C. The ICO's initial enquiries and the introduction of mandatory MFA

84. **3 November 2023 -** The ICO sent initial enquiries to 23andMe following receipt of the First and Second Data Breach Report Forms.

85. **9 November 2023** - 23andMe mandated the use of MFA for all new and existing customer accounts. Customers were also able to login to their accounts using Google and Apple single sign-on systems[79] ("**SSO**").[80]

86. **11 November 2023** - 23andMe responded to the initial enquiries sent by the ICO on 3 November 2023.

87. **1 December 2023** – 23andMe and its third-party forensic provider completed the Internal Investigation.[81]

D. Updates to regulators and additional findings following the Internal Investigation

88. **4 December 2023 -** 23andMe provided further updates to the OPC and other data protection regulators, but not the ICO, regarding the Data Breach. This represented the first occasion on which 23andMe reported

[78] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 12
[79] Single sign-on is an authentication method that allows users to sign in using one set of credentials across multiple independent software systems. Using an SSO system means that a user does not have to sign into every application they use separately and enables them to access several applications without being required to complete separate authentication processes for each application using different credentials.
[80] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 28
[81] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 54. 23andMe informed the Commissioner that additional information came to light in January 2024 which resulted in 23andMe further investigating the credential stuffed profiles and finding that the threat actor had accessed the DNA Relatives profile information and/or health reports of an additional 46 customers who had shared this information with credential stuffed profiles through the Connections feature on the Platform.

the fact that Raw Genetic Data had been accessed and downloaded by the threat actor. 23andMe explained in its Written Representations that it had notified the OPC and 70 other data protection regulators within 72 hours of finalising the Internal Investigation and the failure to notify the ICO at the same time was an unintentional omission.[82]

89. **12 December 2023** - The [redacted] Ticket was updated to state that, *"no evidence of the exfiltration of 10M customers' raw DNA data was found. While* [redacted] *shows that some data was accessed, it was not to the levels outlined in this claim. If this is related to* [redacted]*, then it is likely an exaggeration of the actual data obtained."*[83]

90. **January 2024** - "*Additional information came to light*" that, *"some ungenotyped accounts are set up specifically to receive the DNA Relatives profile and health reports of another customer through the Connections feature."*[84] Despite requests from the Commissioner, 23andMe failed to confirm how this additional information "*came to light*."[85] 23andMe stated that during the Internal Investigation in October and November 2023, prior to receipt of this additional information, it had assumed that only the accounts of those customers who had submitted DNA for testing would contain genetic data.

91. As a result of this additional information coming to light, 23andMe investigated the credential stuffed accounts to determine which accounts contained other customers' information which had been shared through the Connections feature.[86] This led to 23andMe identifying an

[82] 23andMe Written Representations, 18 April 2025: paragraph 8
[83] Letter from Grenberg Traurig LLP to the ICO and OPC, 23 October 2024 (in response to letters from the ICO and OPC dated 20 September 2024 and 11 October 2024): Exhibit AL
[84] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 54
[85] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to request for clarification of original response to question 54
[86] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 54

additional UK customer, in January 2024, whose personal data was accessed through the account of another customer whose account had been credential stuffed and with whom they had shared their data through the Connections feature. The customer was then sent a notification letter by 23andMe to inform them that the data they had shared through the Connections feature had been accessed by the threat actor.[87]

92. **3 to 30 January 2024** - 23andMe emailed customers whose accounts the threat actor had successfully accessed by way of credential stuffing to confirm which categories of their profile information had been affected.[88]

E. 23andMe's Internal Investigation – reported findings

93. In December 2023, the Internal Investigation determined that the threat actor had been able to obtain access to certain 23andMe accounts by way of a credential stuffing attack.

94. Credential stuffing is a form of brute force attack which involves the automated injection of stolen credentials (usernames or email addresses and passwords) into website login forms in order to fraudulently gain access to the customer's account.[89] Many internet customers re-use the same credentials across multiple different online accounts, meaning that when those credentials are exposed, an attacker can use those credentials across multiple other sites in order to compromise other accounts belonging to the same individual. Credential stuffing is one of the most common techniques used to gain unauthorised access to customer accounts and, once the attacker knows that they have access to an account, potential next steps include making purchases, accessing

[87] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Updated response to question 54
[88] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 58 and Exhibit C
[89] Brute force attacks | ICO (accessed 5 February 2025)

sensitive information (such as credit card numbers and private messages), sending phishing messages or spam, and selling known valid credentials for other attackers to use. Multi-factor authentication is regarded as the primary means of defending against credential stuffing attacks.[90]

95. The Internal Investigation found that the threat actor used credential stuffing to gain access to the accounts of 611 Affected UK Data Subjects.[91]

96. The threat actor's first activity occurred on or about 29 April 2023, when, up until 6 May 2023, they logged into six accounts with separate email addresses that were likely to have been used by the threat actor to create their own 23andMe accounts.[92]

97. In the period from 1 – 16 May 2023, the threat actor carried out 183,380 failed and 9,974 successful login attempts, whilst also scraping[93] DNA Relatives profile information, ancestry composition information and health data contained in the credential stuffed accounts that were successfully accessed.[94]

98. Between 11 and 16 June 2023, the threat actor continued to scrape DNA Relatives profile information via the credential stuffed accounts that had opted into this feature.[95]

99. This occurred again on 27 and 28 August 2023, whilst on 29 August

[90] Credential stuffing | OWASP Foundation (accessed 5 February 2025)
[91] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 37
[92] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 36
[93] Data scaping generally involves the automated extraction of data from the internet. Scraped personal data can be exploited for various purposes, such as monetisation through re-use on third-party websites, sale to malicious actors, or private analysis or intelligence gathering, resulting in serious risks to individuals - Joint statement on data scraping and the protection of privacy (24 August 2023) (accessed 4 March 2025)
[94] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 36
[95] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 36

2023, the threat actor scraped Family Tree profile information using the credential stuffed accounts.[96]

100. Further incidents of data scraping from DNA Relatives and Family Tree profiles, as well as the scraping of data from Ancestry Composition Reports, was identified as having taken place between 28 August and 3 September 2023, and on 20 September 2023.[97]

101. Overall, 23andMe found that during the period between 1 May and 18 September 2023, the threat actor conducted approximately 14,601 successful logins and approximately 273,465 unsuccessful logins.[98]

102. In total, the Internal Investigation found that the DNA Relatives profiles of 120,031 Affected UK Data Subjects were unlawfully accessed in the course of the Data Breach, with 35,561 Affected UK Data Subjects' Family Tree profiles accessed by the threat actor. The threat actor also gained access to the Ancestry Reports of 120,504 Affected UK Data Subjects, the Health Reports of 320 Affected UK Data Subjects, the self-reported health conditions of three Affected UK Data Subjects and the Raw Genetic Data of two Affected UK Data Subjects.[99]

103. Based on the Internal Investigation, 23andMe informed the Commissioner on 16 July 2024 that it had found no evidence that the threat actor had downloaded Raw Genetic Data relating to any Affected UK Data Subjects.[100]

F. The Commissioner's investigation

104. On 7 June 2024, the ICO and the OPC informed 23andMe of the launch

[96] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 36
[97] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 36
[98] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 36
[99] These figures are not mutually exclusive.
[100] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 60

of a joint investigation into the Data Breach.

105. On 20 June 2024, the ICO and the OPC jointly sent a first round of questions to 23andMe seeking information about its data processing policies and procedures, the Data Breach and how it had responded.[101] 23andMe stated that this letter from the ICO and the OPC alerted it to its failure to submit a supplementary personal data breach report form to the Commissioner in December 2023.[102]

106. On 24 June 2024, 23andMe submitted an updated supplementary personal data breach report form to the ICO (the "**Third Data Breach Report Form**"), which stated that the breach had begun on 1 May 2023 via a credential stuffing attack.

107. The Third Data Breach Report Form stated, inter alia, that:

a) The type of personal data affected depended on the customer groups impacted by the Data Breach. However, the threat actor had accessed the Raw Genetic Data of two Affected UK Data Subjects and the self-reported health conditions of three Affected UK Data Subjects.

b) 156,204 Affected UK Data Subjects could have been affected by the Data Breach. This total figure included 611 Affected UK Data Subjects whose accounts the threat actor had been able to access via credential stuffing, 120,031 Affected UK Data Subjects whose DNA Relatives profiles had been accessed, 35,561 Affected UK Data Subjects whose Family Tree profiles had been accessed and 1 Affected UK Data Subject whose Connections profile had been accessed.

108. 23andMe responded to the ICO and OPC's initial round of questions in

[101] Letter from the ICO and OPC to 23andMe and Greenberg Traurig LLP, 20 June 2024
[102] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 57

three tranches in July and August 2024.[103] The ICO and OPC issued requests for clarification on elements of 23andMe's responses,[104] to which 23andMe responded in September and October 2024.[105]

109. Between 18 and 20 November 2024, the ICO and OPC jointly conducted interviews by video calls with three 23andMe employees: the company's Software Architect, its Head of Security and its Data Privacy Officer. 23andMe provided follow-up written responses to a number of the questions asked during the interviews.[106]

VI. THE COMMISSIONER'S FINDINGS OF INFRINGEMENT

A. Controllership and jurisdiction

110. The Commissioner finds that during the Relevant Period 23andMe was the controller, as defined in Article 4(7) UK GDPR and sections 3(6), 5(1) and 6 DPA 2018,[107] of the personal data relating to the Affected UK Data Subjects. The Commissioner's finding is based on evidence which indicates that 23andMe determined both the means by which the personal data of the Affected UK Data Subjects was processed and the purposes for which such processing took place. For example, 23andMe determined the type of personal data that a customer was required to provide when setting up an account, how such personal data was stored and the categories of personal data that could be shared with other customers through the DNA Relatives, Family Tree and Connections features. 23andMe designed these features and processed personal data to fulfil its stated aim of offering a service which enables individuals to

[103] Letters from Greenberg Traurig LLP to the ICO and OPC dated 16 July, 26 July and 13 August 2024 (response to a letter from the OPC and ICO dated 20 June 2024)
[104] Letters from the ICO and OPC to 23andMe and Greenberg Traurig LLP dated 19 July and 21 August 2024
[105] Letters from Greenberg Traurig LLP to the ICO and OPC dated 10 September, 14 September, 14 October and 18 October 2024
[106] Letter from Greenberg Traurig LLP to the ICO and OPC dated 17 January 2025
[107] "*Controller*" is defined in Article 4(7) UK GDPR as "*the natural or legal person, public authority, agency or ither body which, alone or jointly with others, determines the purposes and means of the processing of personal data.*"

"*access, understand and benefit from the human genome.*"[108] 23andMe also controlled the use of customers' personal data for research purposes (where customers provided their consent to such processing).

111. This is reflected in 23andMe's EEA, UK and Switzerland Privacy Notice, which states that the company is the "*controller of* [customers'] *Personal Information because we determine the means and purposes of processing your information when using our Services.*"[109]

112. The processing operations performed by 23andMe in the course of providing its services to its customers and carrying out its research activities fall within the material scope of the UK GDPR and Part 2 of the DPA 2018 pursuant to Article 2(1) UK GDPR and section 4(2)(a) DPA 2018 respectively, as they constitute the "*automated or structured processing of personal data.*"[110]

113. The UK GDPR applies to 23andMe's processing of the personal data relating to the Affected UK Data Subjects pursuant to Article 3(2)(a) UK GDPR as although 23andMe is not established within the UK, it processes the personal data of the Affected UK Data Subjects for the purposes of offering goods or services to those individuals.

B. Nature of the personal data affected

114. On 16 July 2024,[111] 23andMe confirmed that the threat actor had accessed the DNA Relatives profiles of 120,031 Affected UK Data Subjects. This provided the threat actor with access to the Affected UK Data Subjects' display names, relationship label and their predicted

[108] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 1
[109] Legal - Privacy Notice for European Residents - 23andMe (as of 21 December 2024) (accessed 5 February 2025)
[110] "*The automated or structured processing of personal data*" is defined in Article 2(5)(a) UK GDPR as "*(i) the processing of personal data wholly or partly by automated means, and (ii) the processing otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system*."
[111] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 37

relationship and percentage of DNA shared with their DNA Relatives matches. In respect of the Affected UK Data Subjects who chose to share such information with their matches, the threat actor would also have had access to their Ancestry Reports, matching DNA segments, self-reported city or postcode-level location, ancestor birth location and family names, profile picture, birth year, family tree and contents of the customer's "*Introduce Yourself*" section of their profile.[112]

115. The threat actor accessed the Ancestry Reports relating to 120,504 Affected UK Data Subjects. 23andMe explained that Ancestry Reports are the same as DNA Relatives profiles, but the Ancestry Reports number is larger because it includes customers who had their accounts credential stuffed and customers whose Ancestry Reports were accessed because they shared it via their Connections feature with a Credential Stuffed Profile.[113]

116. The threat actor also accessed the Family Tree feature for 35,561 Affected UK Data Subjects. This provided the threat actor with access to these individuals' display names, relationship labels and percentage of DNA shared with their matches. Where the customers had chosen to share this information through the Family Tree feature, the threat actor would also have had access to the customers' self-reported city or postcode-level location and birth year.[114]

117. The threat actor also accessed personal data relating to the health of 323 Affected UK Data Subjects. This figure included:

    a) three Affected UK Data Subjects whose self-reported health conditions were accessed by the threat actor; and

[112] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Responses to questions 1 and 37
[113] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2023 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 37.
[114] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Responses to questions 1 and 37

b) 320 Affected UK Data Subjects whose 23andMe generated Health Reports were accessed in the course of the Data Breach.[115]

118. The threat actor also accessed, but did not download, Raw Genetic Data relating to two Affected UK Data Subjects.

119. The information that was available to the threat actor as a result of their access to the Affected UK Data Subjects' DNA Relatives profiles, Ancestry Reports and Family Tree profiles constitutes personal data within the meaning of Article 4(1) UK GDPR and section 3(2) DPA 2018 as it relates to the individual customer and could, either directly or indirectly, when combined with other information, identify them.

120. Article 4(13) UK GDPR defines "*genetic data*" as "*personal data relating to the inherited or acquired characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question*."

121. Affected UK Data Subjects' Raw Genetic Data therefore constitutes "*genetic data"* within the meaning of Article 4(13) UK GDPR, as it is generated using a DNA sample provided by the customer and displays the unique configuration of nucleotides within the customer's DNA which determines the genetic characteristics they inherit from their biological ancestors.

122. Furthermore, both genetic data and data relating to the health of Affected UK Data Subjects constitute special category data within the meaning of Article 9(1) UK GDPR.

123. All three of the 23andMe services available in the UK[116] include, as

[115] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Responses to questions 1 and 37
[116] (Ancestry Service, Ancestry + Health Service and 23andMe+ Premium)

standard, Ancestry Composition, Ancestry Reports and Trait Reports.[117] 23andMe uses this information to connect customers to one another where the customer has opted into its DNA Relatives feature. Customers are then able to find their genetic relatives, message such relatives directly and compare their respective ancestries and traits.

124. In the "*Before You Buy*" section of its "*Customer Care*" information, 23andMe includes a specific FAQ entitled "*Can 23andMe identify Jewish ancestry?*",[118] which demonstrates the ability to infer Jewish ancestry about 23andMe customers from the information contained within their profile. The response to the FAQ confirms that *"DNA clearly shows connections among those who consider themselves to be Ashkenazi Jewish: two Ashkenazi Jewish people are very likely to be "genetic cousins" sharing long stretches of identical DNA. This reflects the fact that the Ashkenazi Jewish population expanded relatively recently from a small initial population."* This means that if a customer is connected to an Ashkenazi Jew via the DNA Relatives feature, it is possible to infer that they (i.e. the customer) are also an Ashkenazi Jew.

125. 23andMe confirmed that as the impacted individuals were genetically related, the information the threat actor accessed included groups of customers who shared a common genetic ancestry. 23andMe confirmed that the threat actor had posted links to .csv files with the labels *"Ashkenazi DNA Data of Celebrities"; "Chinese Ancestry"; "British Ancestry";* and *"Germany Ancestry".*[119]

C. The Infringements

126. The Commissioner has considered whether the facts set out above

[117] See, for example, the description of the information available for subscribers to the Ancestry Service (accessed 5 February 2025)
[118] Can 23andMe Identify Jewish Ancestry? – 23andMe Customer Care | Europe (accessed 5 February 2025)
[119] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 39

constitute an infringement of the UK GDPR and/or DPA 2018 (together the "**data protection legislation**").

127. The Commissioner has conducted an assessment of the facts set out in paragraphs 41 to 109 above and finds that during the Relevant Period 23andMe infringed Article 5(1)(f) UK GDPR and Article 32(1)(b) and (d) UK GDPR.

128. As part of this assessment, the Commissioner has carefully considered and made reference to the ICO's *Guidance on Data Security*[120] which includes detailed guidance on *Passwords in Online Services*[121] and *Security Outcomes*[122]. This Guidance was produced with assistance from the National Cyber Security Centre ("**NCSC**")[123], part of the Government Communications Headquarters and the UK's technical authority for tackling cyber threats. As part of his assessment, the Commissioner has also, in addition, carefully considered relevant guidance produced by NCSC. The Commissioner has also referred, where relevant, to other authoritative and well-known guidance relating to technical and organisational security measures, such as that published by the Open Worldwide Application Security Project ("**OWASP**"), a non-profit foundation which works to improve the security of software through community-led open-source software projects and other initiatives.[124]

129. Whilst the Commissioner acknowledges that 23andMe did implement some technical and organisational security measures during the Relevant Period, he finds that, taken collectively, these were not *"appropriate technical and organisational measures to ensure a level of security appropriate to the risk"* posed to the Affected UK Data Subjects'

[120] A guide to data security | ICO (accessed 5 February 2025)
[121] Passwords in online services | ICO (accessed 5 February 2025)
[122] Security outcomes | ICO (accessed 5 February 2025)
[123] A guide to data security | ICO (accessed 5 February 2025)
[124] OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation

personal data by 23andMe's processing.

130. The Infringements involved serious deficiencies in the technical and organisational security measures implemented by 23andMe when processing Customer Personal Data.

131. Specifically, the Commissioner finds that during the Relevant Period 23andMe infringed Article 5(1)(f) UK GDPR and Article 32(1)(b) and (d) UK GDPR by failing to implement:

a) appropriate technical and organisational measures to "*ensure the ongoing confidentiality, integrity, availability and resilience of its processing systems and services*" (Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR), including by failing to implement:

i. appropriate authentication and verification measures as part of its customer login process, including, but not limited to, multi-factor authentication, secure password requirements, unpredictable usernames, or other measures recognised as effective defences against credential stuffing attacks;

ii. additional appropriate security measures specifically focused on the access to and download of Raw Genetic Data, despite the fact that genetic data is special category data by virtue of Article 9(1) UK GDPR and therefore merits specific protection.[125]

iii. measures which enabled 23andMe to monitor for, detect and appropriately respond to threats to its customers' personal data;

b) an appropriate process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational

[125] Recital 51 to the UK GDPR states that "*Personal data which are, by their nature, particularly sensitive in relation to the fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.*"

measures intended to ensure the security of its processing systems and services (Article 5(1)(f) UK GDPR and Article 32(1)(d) UK GDPR). Specifically, prior to the Data Breach, none of 23andMe's penetration tests or security exercises simulated a credential stuffing attack despite such attacks being widely recognised as a prominent cybersecurity risk to organisations offering online account-based products and services. The Commissioner notes that one of the company's security software providers, [redacted], describe such attacks as *"widespread"* and *"a popular attack vector."*[126]

(a) Failure to implement appropriate mitigations against credential stuffing attacks

132. Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR require controllers and processors to implement appropriate technical and organisational measures that ensure appropriate security of personal data. In accordance with Article 32(1) UK GDPR, the level of security should be appropriate to the risks posed to the rights and freedoms of natural persons by its processing activities. This includes, inter alia, implementing measures which ensure the ongoing confidentiality, integrity, availability and resilience of the controller or processor's processing systems and services (Article 32(1)(b) UK GDPR).

133. The Commissioner finds that 23andMe failed to implement appropriate technical and organisational measures to ensure the ongoing confidentiality and integrity of Affected UK Data Subjects' personal data by failing to:

a) enable the use of unpredictable usernames in lieu of email addresses;

126 [redacted]

b) impose appropriate requirements regarding the security and complexity of passwords; and

c) mandate the use of MFA.

i. Usernames

134. For the reasons set out below, the Commissioner finds that during the Relevant Period 23andMe infringed Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR by failing to enable the use of unpredictable usernames in lieu of email addresses for login purposes,[127] which would have been an appropriate technical measure to ensure an appropriate level of security.

135. Advice published by OWASP[128] on the prevention of credential stuffing attacks advises that customers create their own usernames when registering on a website rather than simply using their email address, as this "*makes it harder for an attacker to obtain valid username and password pairs for credential stuffing, as many of the available credential lists only include email addresses.*"[129]

136. Therefore, whilst a requirement for customers of online services to create their own usernames distinct from their email address is neither an explicit requirement within the UK GDPR, nor a failsafe means of protecting customer accounts against credential stuffing attacks, the Commissioner's view is that providing an option for customers to create unpredictable usernames in lieu of email addresses would have been an appropriate technical measure, in accordance with Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR, for 23andMe to have implemented

[127] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (Response to ICO & OPC letter of 20 June 2024): Response to question 67
[128] The *ICO Security Outcomes* recommend that organisations ensure that their web services are protected from common security vulnerabilities, including those described in widely-used publications such as the OWASP Top-10. Identification and authentication failures, previously known as broken authentication, includes credential stuffing and other brute force attacks and has featured in the OWASP Top-10 since 2003
[129] Credential Stuffing Prevention - OWASP Cheat Sheet Series (accessed 5 February 2025)

to ensure an appropriate level of security for the personal data held within its customers' accounts.

137. The Commissioner's view is that enabling the use of unpredictable usernames would, in addition to secure password requirements and compulsory MFA, have represented an appropriate technical measure to increase the level of protection afforded to customer accounts against unauthorised access, particularly credential stuffing attacks.

ii. Secure passwords

138. The Commissioner notes that during the Relevant Period 23andMe failed to enforce appropriate minimum password length[130] and complexity requirements, and failed to prevent customers from using either weak or compromised passwords. The Commissioner finds that this represented a failure to implement appropriate technical measures, in accordance with Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR, which would have ensured an appropriate level of security for its customers' accounts and enhanced protections against brute force attacks such as credential stuffing.

139. The UK GDPR does not specifically prescribe how organisations should configure their password systems. However, providers of online services must ensure that the configuration and operation of their password systems comply with their obligations under Article 5(1)(f) UK GDPR and Article 32 UK GDPR and are appropriate to ensure a level of security which is appropriate to the risk, taking into account the context of the personal data being processed and the associated risks to the rights and freedoms of their customers.

140. ICO Guidance on *Password Requirements for Online Services*[131] states

[130] This finding applies from the start of the Relevant Period until 23andMe increased the minimum length for customer account passwords to 12 characters following the Data Breach.
[131] Passwords in online services | ICO (accessed 5 February 2025)

that there are three general requirements for any password system that providers of online services need to consider: password length, special characters and password strength. Operators of online services are advised to set a minimum but not a maximum password length; allow, but not mandate, the use of special characters; and prevent customers from using common, weak passwords by screening passwords against a password "*deny list*" featuring the most commonly used passwords, leaked passwords from website breaches and common words or phrases related to the relevant service.

141. In assessing 23andMe's password policy by reference to this ICO guidance, the Commissioner notes that, at the time of the Data Breach, 23andMe's password policy for customer accounts:

a) only included a minimum character requirement of eight characters, albeit that, following the Data Breach, this was increased to a minimum of 12 characters;[132]

b) did not include password complexity requirements; and

c) contained insufficient measures to prevent the use of common words or known compromised credentials.[133]

142. In addition, 23andMe initially informed the Commissioner that there were measures in place to prevent a customer submitting a previously used password when resetting their password.[134] However, 23andMe later confirmed that this measure wasn't introduced until August 2023, after the Data Breach began, and that prior to that date, customers could reset their passwords to any previously used password.[135]

[132] This was confirmed in an interview with 23andMe software architect [redacted] on 18 November 2024
[133] This was confirmed in an interview with 23andMe software architect [redacted] on 18 November 2024
[134] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to question 17
[135] This was confirmed in an interview with 23andMe software architect [redacted] on 18 November 2024

143. Although 23andMe stated that it had repeatedly warned customers about the risks of reusing their passwords[136], the Commissioner notes that customers were not directed to these resources when creating or changing their passwords. Instead, these warnings were contained in the "*Password Tips*" section of the 23andMe Privacy and Security Help Centre[137] and on a 23andMe Blog.[138] The Commissioner finds that 23andMe would not have been able to ensure that its customers had accessed and read this information when creating or changing passwords.

144. Furthermore, 23andMe failed to maintain a comprehensive password "deny list" of commonly used words or phrases which could not be used by customers when creating their passwords, nor implement measures to assist customers to choose strong passwords, both of which are recommended in the ICO *Guidance on Passwords in Online Services*. This ICO guidance also recommends that controllers consult the NCSC's guidance when devising their password policies. The Commissioner notes that the maintenance of a password "deny list" and measures to assist customers in improving the strength of their passwords are amongst the password-related measures which are recommended in guidance from the NCSC on password strategies that can help organisations remain secure.[139]

145. The *ICO Guidance on Passwords in Online Services* states that operators of online services should screen passwords against a password "deny list'" of the most commonly used passwords and leaked passwords from website breaches, citing SecLists and HIBP as examples of such lists which are available online.[140]

[136] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 16
[137] Privacy and Security Help Center – 23andMe Customer Care
[138] The 23andMe privacy team answers 10 common questions - 23andMe Blog
[139] Password policy: updating your approach - NCSC.GOV.UK
[140] Passwords in online services | ICO

146. During the Relevant Period (and prior to the introduction of measures to prevent customers reusing previous passwords in August 2023), the only password complexity check implemented by 23andMe was the [redacted] default password validation function.[141] The [redacted] default password validation function[142] includes basic complexity checks, such as confirming that a password is not comprised solely of integer values nor contains elements of a customer's email address or name. 23andMe also utilised an in-built feature within the [redacted] web framework which enables a comparison of customer passwords against only 20,000 passwords collected in 2021 from the https://haveibeenpwned.com ("**HIBP**") dataset of approximately 500 million compromised credentials.[143]

147. In addition, during the Relevant Period, 23andMe maintained a [redacted] subscription which would have allowed it to access the [redacted] which offers a database of over 14 billion compromised credentials compared with the database of 20,000 offered by [redacted] The Commissioner notes that the [redacted] was not enabled[144] during the Relevant Period and 23andMe's Head of Security was not aware of this feature of the [redacted] until being informed of it at an interview with the ICO and OPC on 19 November 2024.[145] 23andMe later stated in correspondence that the [redacted]

[141] Email from Greenberg Traurig LLP to the ICO and OPC, 19 November 2024 (00:45): Response to question 1 of interview with 23andMe software architect [redacted] on 18 November 2024
[142] [redacted]
[143] Email from Greenberg Traurig LLP to the ICO and OPC, 19 November 2024 (00:45): Response to question 1 of interview with 23andMe software architect [redacted] on 18 November 2024
[144] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024: Response to ICO & OPC letter of 20 June 2024: Exhibit I
[145] Interview with [redacted], 23andMe Head of Security, 19 November 2024

"*is not a viable option for 23andMe because of the structure of its customised website.*"[146] No further information or explanation was provided in support of this statement.

148. The Commissioner finds that had 23andMe implemented the [redacted], it would have significantly increased the strength of 23andMe's password controls by automating the screening of passwords against the entire dataset of known compromised credentials within the HIPB database.[147]

149. In the alternative, if 23andMe had not considered the [redacted] to be a viable option, the Commissioner finds that 23andMe should have implemented an alternative means of effectively checking for previously compromised customer passwords and from a database of significantly more than 20,000 compromised passwords as was offered by [redacted]. For example, HIBP offers a free service which compares customer passwords against over 500 million compromised credentials. 23andMe could also have downloaded the full HIBP database of compromised passwords and integrated the checks within its own Platform.[148]

150. The Commissioner considers that 23andMe's reliance upon the provision of customer credentials as the sole customer authentication measure (in the absence of mandatory MFA) further supports his conclusion that it would have been appropriate for 23andMe to have implemented an alternative system of credential checks which utilised a far more extensive database of known compromised credentials as part of its technical security measures designed to protect its customers against the risk of brute force attacks such as credential stuffing. The Commissioner considers that the implementation of such a system would

[146] Letter from Greenberg Traurig LLP to the ICO and OPC, 17 January 2025
[147] https://haveibeenpwned.com/ (accessed 5 February 2025)
[148] Have I Been Pwned: Pwned Passwords (accessed 5 February 2025)

not only have been more effective than the [redacted] web framework in preventing 23andMe customers from reusing compromised credentials and thus protecting them against the risk of brute force attacks such as credential stuffing, but would also not have affected the usability of the Platform, which 23andMe cited when seeking to explain its decision not to implement mandatory MFA.[149]

151. The Commissioner notes that since October 2023, 23andMe has reviewed and updated its password requirements. This includes increasing the minimum password length to 12 characters; preventing customers from repeating any of their previous five passwords; reminding customers to use a unique password; and preventing customers using repeated characters, sequences of characters or contextual strings in their passwords.[150] In addition, 23andMe now checks customer passwords against the entire HIBP database (nearly 1 billion passwords, updated monthly) when customers register, sign-in and reset their passwords.[151]

iii. Multi-factor authentication

152. For the reasons set out below, the Commissioner finds that 23andMe's failure to mandate MFA on customer accounts during the Relevant Period constituted a failure to implement appropriate technical measures to ensure the ongoing confidentiality and integrity of Affected UK Data Subjects' personal data and thereby infringed Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR.

153. NCSC guidance, to which the Commissioner's *Guidance on Passwords in Online Services* directs controllers,[152] confirms that MFA is one of the most effective ways of providing additional protection to a password

[149] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 28
[150] 23andMe Written Representations 18 April 2025: Paragraph 16
[151] Email from Greenberg Traurig LLP to the ICO and OPC, 6 May 2025 (20:15)
[152] Passwords in online services | ICO (accessed 5 February 2025)

protected account.[153] MFA is a strong authentication method which requires two or more factors to gain access to a network, system or application. Each factor must come from a different category of the three recognised authentication methods (i.e. knowledge, possession and inheritance or traits).[154] This is in contrast to single-factor authentication ("**SFA**"), which is regarded as a low-security method of authentication which only requires one factor, such as a username and password[155] to gain access to a system. Whilst SFA systems may require two pieces of information, such as a username and password, this is still regarded as a single factor because they both fall within the same category of authentication methods set out above.[156]

154. In 2018, the NCSC published guidance for organisations about implementing MFA to protect against password guessing and theft on online services.[157] The Commissioner directs controllers to the NCSC's guidance when they are considering implementing an extra factor for authentication.[158] This NCSC guidance states that "*Passwords have a limited ability to protect your data and systems. Even when implemented correctly, passwords are limited in helping prevent unauthorised access. If an attacker discovers or guesses the password, they are able to impersonate a user… One of the most effective ways of providing additional protection to a password protected account is to use MFA… MFA is best used where there may be additional risk (such as logging into an account on a new device, internet facing systems or for priority accounts)*."[159]

[153] Password policy: updating your approach - NCSC.GOV.UK (accessed 5 February 2025)
[154] These factors are otherwise referred to as something you know, something you have and something you are.
[155] Both usernames and passwords are examples of "something you know".
[156] CEG Enhancement Guide: Implementing Strong Authentication (accessed 5 February 2025)
[157] Multi-factor authentication for online services - NCSC.GOV.UK (accessed 5 February 2025)
[158] Passwords in online services | ICO (accessed 5 February 2025)
[159] Password policy: updating your approach - NCSC.GOV.UK (accessed 11 February 2025)

155. From 2019 onwards, 23andMe offered MFA to its customers as an optional feature, with customers also able to access their accounts using single sign-on services offered by Google and Apple.[160] 23andMe informed the Commissioner that in light of the fact that its "*customer base tends to be older and less likely to possess even basic digital skills, 23andMe decided to make MFA optional to ensure that customers could easily access their accounts.*"[161] The Commissioner has not been presented with any evidence to indicate that 23andMe conducted customer surveys, performed trials or researched customer opinions when considering whether to mandate the use of MFA.

156. In any case, the Commissioner regards 23andMe's reference to the proportion of its userbase aged over 65 and who were therefore assumed to lack basic digital skills as an inadequate explanation for its decision not to introduce MFA as a mandatory part of its login process.

157. 23andMe's decision not to mandate the use of MFA indicates that it prioritised customer convenience and ease of use of the Platform over the security of customer accounts, which the Commissioner finds is not compliant with the company's obligations under Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR, particularly when taking into account the sensitivity of the personal data accessible via customer accounts.

158. The guidance from the NCSC and the ICO referred to in paragraphs 153 and 154 above, clearly indicates that MFA is the most effective means of protecting against the risk of credential stuffing attacks. At the time of the Data Breach, only 0.2% of 23andMe's global customer base had MFA enabled on their 23andMe accounts and a further 21.5% used SSO services offered by Google and Apple. Notably none of those accounts

[160] Enhanced Customer Security at 23andMe with 2-Step Verification - 23andMe Blog (Accessed 12 February 2025)
[161] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 28

were successfully accessed by the threat actor.[162]

159. The Commissioner considers that this constitutes clear evidence of the effectiveness of MFA (and SSO systems) in protecting against credential-based attacks and indicates that the Data Breach could have been avoided if MFA had been mandated on all customer accounts. This is further supported by research carried out by Microsoft in 2019, which suggested that online accounts are 99.9% less likely to be compromised where MFA is used.[163]

160. 23andMe clearly possessed the technological capacity to require all customers to use MFA when accessing their accounts, as it was offered as an optional security feature, and the Commissioner does not consider that mandating its use would have resulted in any significant additional cost to 23andMe.

161. The Commissioner notes that since 9 November 2023, 23andMe has required all customers to use email-based two-factor authentication[164] when logging into the Platform, whilst customers continue to be able to use single sign-on services offered by Apple and Google to access their accounts.

iv. Lack of compensatory controls

162. For the reasons set out below, the Commissioner finds that, taking into account the absence of mandatory MFA prior to 9 November 2023, 23andMe's failure to implement alternative technical and organisational measures to ensure appropriate security of the personal data, in the form of device, browser or connection fingerprinting and access to device history, constitutes an infringement of Article 5(1)(f) UK GDPR and

[162] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 28
[163] Your Pa$$word doesn't matter - Microsoft Community Hub (accessed 5 February 2025)
[164] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to Question 13

Article 32(1)(b) UK GDPR.

163. In relation to device, browser, connection or other fingerprinting, the ICO *Security Outcomes* state that controllers should "*detect security events that affect the systems that process personal data"* and "*monitor authorised customer access to that data, including anomalous customer activity."* The guidance further states that controllers should "*record customer access to personal data"* and "*where unexpected events or indications of a personal data breach are detected,* [controllers should] *have processes in place to act upon these events as necessary in an appropriate timeframe."*[165]

164. Furthermore, NCSC *Guidance on Logging and Protective Monitoring*[166] to which controllers are directed by the ICO *Security Outcomes*[167], states that organisations should conduct "*monitoring of device state and compliance"*, whilst also recommending that organisations "*log device events, including customer activity, network communications authentication and access, to both devices and services."* Doing so will, according to the NCSC, provide organisations with "*the ability to detect and respond to security events. Where possible* [organisations] *should automate detection and remediation."*[168]

165. The Commissioner's view is that implementation of device, browser or connection fingerprinting would have been appropriate technical measures to mitigate the risk of unauthorised access to customer accounts, particularly as compensatory measures in light of the absence of mandatory MFA.

166. During the Relevant Period, 23andMe failed to conduct any form of

[165] Security outcomes | ICO (accessed 5 February 2025)
[166] Logging and protective monitoring - NCSC.GOV.UK (accessed 5 February 2025)
[167] Security outcomes | ICO (accessed 5 February 2025)
[168] Logging and protective monitoring - NCSC.GOV.UK (accessed 5 February 2025)

device, browser, connection or other fingerprinting.[169] 23andMe informed the Commissioner that it elected not to implement device, browser or connection fingerprinting due to the other security controls it had implemented as well as privacy concerns regarding the collection of additional information from customers.[170] The Commissioner considers this to be an inadequate explanation for the failure to implement these measures. The Commissioner notes that 23andMe's Privacy Policy states that it collects "*Web-Behaviour Information: Information on how you use our Services or about the way your devices use our Services is collected through log files, cookies, web beacons, and similar technologies (e.g. device information, device identifiers, IP address, browser type, location, domains, page views).*"[171] Therefore, it is clear that 23andMe already collected the personal data required in order to produce and verify a customer's device or connection, but did not use this information for the purposes of verifying that an attempt to log into a customer's account was genuine.

167. In addition to the lack of fingerprinting, 23andMe did not allow customers to view a device history indicating what devices had accessed, and were currently being used to access, the Platform with their credentials.[172]

168. Whilst this is not a specific requirement under the UK GDPR, the Commissioner regards such a system of device visibility as one of the range of possible technical security measures that it would have been appropriate for 23andMe to implement in this context. The ICO guidance on steps that individuals should take if they experience a personal data

[169] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to question 18
[170] Letter from Greenberg Traurig LLP to the ICO and OPC, 17 January 2025
[171] Privacy Policy - 23andMe UK (Version last updated on 14 December 2022)
[172] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (responding to a letter from the ICO and OPC Dated 20 June 2024): Response to question 19

breach[173] directs them to the NCSC's guidance for individuals and families on how to protect themselves from the impact of data breaches, which recommends that customers check whether there have been any logins or attempted logins into their accounts from strange locations or at unusual times.[174]

169. If such a system had been in place, it may have enabled 23andMe customers whose accounts were successfully credential stuffed to identify the threat actor's activity as an anomalous and unexplained entry in the list of devices used to access the customers' accounts. This, in turn, could have led to the customers themselves reporting such irregularities to 23andMe in advance of the actual discovery of the Data Breach in October 2023.

170. The Commissioner is of the view that had these compensatory controls been implemented they would have constituted appropriate technical measures which, when combined with the other necessary technical and organisational measures would have ensured an appropriate level of security to protect the integrity and confidentiality of the Affected UK Data Subjects' personal data.

171. The Commissioner notes that as of 31 December 2024, 23andMe has implemented a number of additional monitoring and alerting measures which are intended to detect unauthorised activity in customer accounts. This includes deploying [redacted] and carrying out risk-based activity monitoring. In addition, 23andMe has

[173] What steps should I take if I have experienced a data breach? | ICO (accessed 5 February 2025)
[174] Data breach guidance for individuals - NCSC.GOV.UK (accessed 5 February 2025)
[175] [redacted]

implemented a trusted browser functionality, which allows customers to register a "trusted device" used to access their 23andMe account for a period of 400 days and offers an "Account Event History" report which customers can download and which displays every login, attempted login and download with the associated IP address and approximate location (based on the IP address).[176]

(b) Failure to implement additional protections for Raw Genetic Data

172. The Commissioner finds that by failing to operate any additional verification steps prior to customers accessing or downloading Raw Genetic Data during the Relevant Period, 23andMe failed to comply with its obligations under Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR to implement technical and organisational measures to ensure a level of security of Affected UK Data Subjects' personal data which was appropriate to the risk of varying likelihood and severity for the rights and freedoms of natural persons when taking into account the sensitive nature of such personal data and the context and purposes of the processing.

173. The Commissioner finds that this failure exposed the Raw Genetic Data of customers whose accounts had been credential stuffed to unauthorised access and processing by the threat actor. In addition, the Commissioner regards this failure as particularly significant in light of the lack of default technical security measures applied during the login process at the time of the Data Breach, particularly the absence of mandatory MFA.

174. As explained in **Section VI(B)** above, the Raw Genetic Data processed by 23andMe constitutes genetic data within the meaning of Article 4(13) UK GDPR, which is listed as a form special category data under Article

[176] What's In Your Account Settings? – 23andMe Customer Care (accessed 8 May 2025)

9(1) UK GDPR[177] and thus "*merit*[s] *higher protection*."[178] This enhanced level of protection is required for genetic data due to its unique and unchanging nature, as well as its commonality among related persons. In the Commissioner's view, in light of the higher level of protection that special category data requires and the inherent sensitivity of genetic data, it would have been appropriate for 23andMe to have implemented additional verification measures before customers were able to access or download their Raw Genetic Data.

175. When assessing the Infringements, it is necessary to consider not only the information which was actually obtained in the course of the Data Breach, but also the personal data which was put at risk by 23andMe's failure to comply with the requirements of Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR.

176. As explained at paragraph 38 above, during the Relevant Period there was a short delay following a Raw Genetic Data download request whilst the file was generated.[179] 23andMe customers were sent an email alert when the file was available for download, with the customer required to log back into their account in order to complete the process.[180] 23andMe also confirmed that at the time of the Data Breach, once an individual logged into their account (including after completing a MFA check, if enabled by the customer), there were no additional authentication steps before the customer could access their Raw Genetic Data, self-reported

[177] Article 9(1) UK GDPR provides that "*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."* This is subject to Article 9(2) UK GDPR.
[178] Recital 53 to the UK GDPR
[179] Accessing Your Raw Genetic Data – 23andMe Customer Care | Europe (accessed 21 May 2025). At the time of the Data Breach, 23andMe's Customer Care page relating to Raw Genetic Data downloads stated that files were typically available for download within one hour of a request being made.
[180] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 12

health conditions or 23andMe generated Health Reports.[181]

177. Following the Data Breach, on 2 November 2023, 23andMe temporarily disabled its self-service Raw Genetic Data download feature. During the period of suspension, customers were required to authenticate their identities with the company's Customer Care team in order to download their Raw Genetic Data. The self-service Raw Genetic Data download service was re-enabled on 27 February 2024, at which time 23andMe introduced an additional verification step requiring customers to provide the date of birth used to register for their account before the download could be initiated.[182]

178. The Commissioner notes that there are industry concerns regarding the use of dates of birth as a method of verification because birth dates can often be found in public records, ascertained from intelligence research, or exposed in previous data breaches, meaning that this information may be otherwise available to a threat actor.[183]

179. 23andMe informed the Commissioner that in August 2023, the company "*analysed the possibility of requiring customers to take additional steps prior to being able to download their uninterpreted genotype data*."[184] However, no additional steps were implemented until after the Data Breach was discovered and operation of the self-service download feature was suspended on 2 November 2023. 23andMe has not provided its rationale for the decision in August 2023 not to require customers to

[181] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 13

[182] Letter from Greenberg Traurig LLP to the ICO and OPC), 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 12

[183] For example, the US National Institute of Standards and Technology's Digital Identity Guidelines (Special Publication 800-63B) states that security questions, including date of birth checks, are no longer recognised as an acceptable authentication measure (section 5.1.1.2 paragraph 4), whilst OWASP's "*Choosing and Using Security Questions Cheat Sheet*" labels "*What is your date of birth?*" as a bad security question on the basis that it is easy for an attacker to discover.

[184] Letter from Greenberg Traurig LLP to the ICO and OPC, 10 September 2024 (response to letters from the ICO and OPC dated 20 June and 21 August 2024): Response to clarification question 15

complete additional verification or authentication measures when downloading their Raw Genetic Data despite requests having been made by the Commissioner for information regarding the decision-making that took place at this time

180. The appropriateness of the technical and organisational security measures which a controller is required to implement in accordance with Article 32(1)(b) UK GDPR must be considered in light of the type of personal data being processed and the risks posed by such processing to the rights and freedoms of data subjects. Therefore, where special category data or other forms of sensitive personal data are processed and, as a result, the risks posed to the rights and freedoms of data subjects are greater, the controller must implement additional or more stringent measures in order to ensure the integrity and confidentiality of the personal data in question.

181. 23andMe informed the Commissioner that the Internal Investigation found that no Affected UK Data Subjects' Raw Genetic Data had been downloaded by the threat actor.

182. However, the Commissioner's investigation identified significant concerns regarding the methodology used by 23andMe to identify both credential stuffed accounts and, in particular, attempts by the threat actor to access and download individuals' Raw Genetic Data.

183. 23andMe informed the Commissioner that it identified IP addresses used by the threat actor on the basis of one of two indicators:

a) the IP address was used to log into a customer account and, when it did so, the HTTP referrer field was empty and a specific customer agent string was provided; or

b) the IP address was observed scraping data from an endpoint containing the unique signature "/p/1/".

184. 23andMe then examined the login history for compromised accounts and

identified logins from IP addresses associated with the threat actor which were followed by a Raw Genetic Download event from the same account within a six-hour period. If there was such a login from a known threat actor IP address within the six-hours prior to a Raw Genetic Data download event, this was considered to be potentially attributable to the threat actor.[185]

185. 23andMe also informed the Commissioner that when a customer requested a full download of their Raw Genetic Data, it routinely placed the data into an [redacted]. However, 23andMe did not collect the logs available from [redacted] which were created when this data was subsequently downloaded. Instead, 23andMe created its own bespoke log of such download events. Due to a "bug in the system", the bespoke log entry generated when Raw Genetic Data was downloaded incorrectly recorded an internal IP Address (127.0.0.1), rather than the IP address associated with the customer who initiated the download request.[186] This misconfiguration in 23andMe's logging system remained undetected until it was identified in the course of the Internal Investigation.

186. As a result of this misconfiguration, 23andMe was not able to establish which IP addresses were being used to initiate each download of Raw Genetic Data. This prevented 23andMe from searching for Raw Genetic Data downloads linked to IP addresses known to have been used by the threat actor, resulting in it employing the methodology set out above.

[185] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to questions 35 and 39. 23andMe initially indicated in its response to question 35 that it only searched for Raw Genetic Data download events which occurred within [redacted] of a login from an IP address associated with the threat actor, but later revised this response in a letter from Greenberg Traurig LLP to the ICO and OPC dated 22 November 2024, confirming that a [redacted] window was analysed

[186] Letter from Greenberg Traurig LLP to the ICO and OPC, 10 September 2024 (response to question 2 in a letter from the ICO and OPC to 23andMe and Greenberg Traurig LLP dated 21 August 2024)

187. Furthermore, the methodology employed by 23andMe during the Internal Investigation failed to account for multiple viable methods which the threat actor could have used in order to initiate a Raw Genetic Data download.

188. As a result, the Commissioner proposed an alternative methodology, pursuant to which any Raw Genetic Data download event which occurred after an account was compromised would be regarded as a potentially unauthorised download by the threat actor.

189. At the Commissioner's request, 23andMe confirmed that of the additional 257 accounts[187] which the Commissioner had identified as having recorded a Raw Genetic Data download event after the date on which they were credential stuffed, nine accounts related to Affected UK Data Subjects.[188]

190. However, in its Written Representations, 23andMe explained that it had further reviewed evidence of Raw Genetic Data downloads in credential stuffed accounts and provided a report detailing the methodology that was used.[189] Applying its revised methodology, 23andMe found that the threat actor downloaded Raw Genetic Data relating to four customers worldwide, none of whom were in the UK.[190]

191. However, regardless of the number of 23andMe customers whose Raw Genetic Data was downloaded by the threat actor, the absence of additional step-up authentication measures in the download process, at the time of the Date Breach, meant that Raw Genetic Data was available to the threat actor once they had successfully credential stuffed an

[187] These 257 accounts were in addition to the originally reported figure of 18 individuals who were identified in the Internal Investigation as having had their Raw Genetic Data downloaded by the threat actor - Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the ICO and OPC dated 20 June 2024): response to question 37
[188] Email from Greenberg Traurig LLP to the ICO and OPC, 23 January 2025 (18:50)
[189] 23andMe Written Representations, 18 April 2025: Exhibit 1
[190] 23andMe Written Representations, 18 April 2025: Paragraph 2

account.

192. As explained at paragraphs 185 to 186 above, at the time of the Data Breach 23andMe's security measures did not allow it to accurately verify that Raw Genetic Data downloads were initiated by genuine 23andMe customers. This not only prevented 23andMe from detecting the threat actor's activity in real time, but also inhibited the subsequent Internal Investigation. Furthermore, regardless of the extent to which Raw Genetic Data was downloaded by the threat actor, they were able to obtain sensitive personal data relating to large numbers of 23andMe customers via the DNA Relatives feature on the Platform. This information would have enabled the threat actor to draw inferences regarding the racial and ethnic origins of 23andMe customers and therefore constitutes inferred special category data.[191]

(c) Failure to prepare for a credential stuffing attack

193. For the reasons set out below, the Commissioner finds that 23andMe infringed Article 5(1)(f) UK GDPR and Article 32(1)(d) UK GDPR, by failing to implement an appropriate process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of its processing systems and services. Specifically, prior to the Data Breach, 23andMe failed to carry out any form of environmental scanning for potential risks to its systems, whilst its penetration and security testing did not simulate a credential stuffing attack, despite this being widely recognised as a significant risk to providers of customer facing online services which has affected multiple organisations operating in many sectors of the

[191] *ICO Guidance on Special Category Data* states that "*The UK GDPR is clear that special category data includes not only personal data that specifies relevant details, but also personal data revealing or concerning these details… If the information itself does not clearly reveal or concern something about one of the special categories, it may still be possible to infer or guess details about someone that do fall within those categories.*"

economy.[192]

194. *ICO Guidance on Data Security* under the UK GDPR[193] states that controllers should "*have a process for regularly testing, assessing and evaluating the effectiveness of any measures* [they] *put in place. What these tests look like, and how regularly* [the controller] *does them will depend on* [the controller's] *own circumstances… whatever scope* [the controller] *chooses for this testing should be appropriate to what* [it is] *doing, how* [it is] *doing it, and the data that* [it is] *processing."* The ICO guidance further states that controllers can discharge this obligation by using a number of techniques, "*such as vulnerability scanning and penetration testing*", with these techniques functioning as "*stress tests of* [the controller's] *network and information systems which are designed to reveal areas of potential risk and things that* [the controller] *can improve."*

195. Penetration testing is defined by the NCSC as, "*a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might… A well scoped penetration test can give confidence that the products and security controls tested have been configured in accordance with good practice."* When scoping a penetration test, NCSC guidance states that "*where the goal of the test is to ensure good vulnerability management… risk owners should outline any areas of special concern."*[194]

[192] For example, video streaming service Netflix experienced a credential stuffing attack in 2019, whilst approximately 160,000 Nintendo account users were affected in a credential stuffing attack in 2020. Also in 2020, hackers used compromised credentials to target 300,000 Spotify accounts and the login credentials of an estimated 500,000 Zoom users were extracted from a database and placed for sale on crime forums and dark web markets. More recently, payment services provider PayPal was targeted by a credential stuffing attack in December 2022 which affected an estimated 34,942 of its users, whilst in December 2023 restaurant chain Jason's Deli alerted members of its rewards scheme that their personal data had potentially been exposed in a credential stuffing attack.
[193] A guide to data security | ICO (accessed 5 February 2025)
[194] Penetration testing - NCSC.GOV.UK (accessed 5 February 2025)

196. Furthermore, regardless of the form of testing which is undertaken, ICO *Guidance on Data Security* confirms that controllers should "*document the results and make sure that* [they] *act upon any recommendations, or have a valid reason for not doing so and implement appropriate safeguards. This is particularly important if your testing reveals potential critical flaws that could result in a personal data breach."*[195]

197. The guidance referred to above indicates that a controller may discharge its obligations under Article 32(1)(d) UK GDPR by regularly performing vulnerability or environmental scanning in order to identify the internal and external sources of risk to the security of its processing operations, and by using penetration testing as a means of evaluating the effectiveness of its security measures in defending against the risks identified.

198. 23andMe informed the Commissioner that, prior to the Data Breach, none of its penetration tests or security exercises simulated a credential stuffing attack.[196] Nor did 23andMe prepare any reports in relation to its penetration testing which is inconsistent with the ICO guidance referred to above.[197]

199. The Commissioner finds that 23andMe's failure to incorporate testing for a credential stuffing attack within its vulnerability assessment and penetration testing procedures constituted a failure to implement an appropriate process for regularly testing, assessing and evaluating the effectiveness of its technical and organisational security measures, as required by Article 32(1)(d) UK GDPR. Whilst it is ultimately for the controller to determine how such assessments and tests are conducted, including which threats are simulated and how often they are performed,

[195] A guide to data security | ICO
[196] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 29
[197] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 66

the ICO *Security Outcomes* state that organisations should ensure that "*web services are protected from common security vulnerabilities such as SQL injection and others described in widely-used publications, such as the OWASP Top 10".*[198] Identification and authentication failures (previously known as broken authentication), including credential stuffing, featured in the OWASP Top-10 throughout the Relevant Period.[199]

200. 23andMe's failure to account for the threat of credential stuffing attacks within its vulnerability assessments and penetration tests resulted in a failure to test the robustness of the security measures integrated into its login process, evaluate the effectiveness of the measures employed to detect unauthorised activity on customer accounts, and improve the speed and effectiveness of its incident response processes, all of which left the Platform more vulnerable to a credential stuffing attack.

201. The increase in credential stuffing attacks in recent years,[200] and the clear trend of threat actors targeting organisations offering online account-based services, such as PayPal,[201] Spotify,[202] Nintendo[203] and

[198] Security outcomes | ICO
[199] OWASP Top Ten 2017 | A2:2017-Broken Authentication | OWASP Foundation and A07 Identification and Authentication Failures - OWASP Top 10:2021
[200] The European Union Agency for Cybersecurity (ENISA) "Main Incidents in the EU and Worldwide: January 2019 to April 2020" Report (accessed 5 February 2025) stated that "*companies experience an average of 12 credential-stuffing attacks each month, wherein the attacker is able to identify valid credentials",* whilst the Securities and Exchange Commission's Office of Compliance Inspectors and Examinations issued a risk alert on 15 September 2020 (accessed 5 February 2025) warning of a rise in credential stuffing attacks. The Global Privacy Assembly's Credential Stuffing Guidelines (dated 27 June 2022) (accessed 5 February 2025) states that the threat to personal data from credential stuffing attacks is, for many organisations, "*now no longer a 'threat' but an unavoidable reality"* and that "*organisations should implement measures to mitigate the risks of, and arising from, such attacks."*
[201] Thousands Of PayPal Accounts Data Breached—Is Yours One Of Them? (forbes.com) (accessed 5 February 2025)
[202] Credential Stuffing Attack Targeted Spotify, Affecting More Than 300,000 Accounts - CPO Magazine (accessed 5 February 2025)
[203] 300,000 Nintendo Users Hacked: What Gamers Need To Know (forbes.com) (accessed 5 February 2025)

Zoom,[204] should have resulted in 23andMe being aware of the risk of such an attack targeting its Platform and customers' accounts. In addition, 23andMe's Internal Investigation identified "ei*ght separate accounts that may have been accessed in isolated incidents of credential stuffing in 2019 and 2020*,"[205] indicating that the Data Breach did not constitute the first occasion on which the Platform had been targeted by this form of attack and further reinforcing the seriousness of its failure to implement and test the effectiveness of its technical and organisational measures against credential-based attacks.

202. The Commissioner notes that since October 2023, 23andMe has used generated accounts to test against credential stuffing attacks.[206] At the Oral Hearing, 23andMe informed the Commissioner that it had carried out five cyber security tabletop exercises in the company's 2025 financial year and had updated its product alerts to detect abuse by potential threat actors, including alerts which are designed to detect incidents of [redacted] and [redacted][207]. At the Oral Hearing, 23andMe also stated that since the Data Breach it has held incident response preparedness sessions with its internal incident response team and updated its vulnerability reporting management processes.

(d) Failure to implement appropriate and effective measures to monitor for, detect and respond to unauthorised activity

203. For the reasons set out below, the Commissioner finds that, in breach of Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR, 23andMe failed

[204] An Analysis of the 2020 Zoom Data Breach | CSA (cloudsecurityalliance.org) (accessed 5 February 2025)
[205] Response from Greenberg Traurig LLP to the ICO and OPC dated 16 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to Question 36
[206] Letter from Greenberg Traurig LLP to the ICO and OPC dated 13 August 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to Question 66
[207] The NCSC define "*password spraying*" as the use of a small number of commonly-used passwords in an attempt to access a large number of accounts - Password policy: updating your approach - NCSC.GOV.UK

to ensure the confidentiality and integrity of Affected UK Data Subjects' personal data by failing to implement appropriate measures to monitor for and detect unauthorised third-party activity on customer accounts. Specifically, 23andMe's rate-limiting rules, managed and operated on its behalf by [redacted], failed to detect and alert either 23andMe or [redacted] to the high volume of both successful and unsuccessful login attempts by the threat actor.

204. The Commissioner finds that 23andMe:

a) missed multiple opportunities to identify the Data Breach prior to October 2023;

b) failed to appropriately investigate evidence provided directly to the company in August 2023 of a large-scale personal data breach affecting the Platform; and

c) deployed an organisational response to the eventual discovery and verification of the Data Breach in October 2023 which was not appropriate in light of the risks posed by its processing operations to the rights and freedoms of its customers.

205. The following four sub-sections set out the reasons for the Commissioner's findings, and specifically address 23andMe's failure to:

a) implement a system of device or connection monitoring or suspicious activity alerts;

b) implement effective rate-limiting rules and alerts;

c) monitor for and detect anomalous customer activity; and

d) implement an appropriate organisational response to evidence of a personal data breach.

i. Lack of device or connection monitoring or suspicious activity alerts

206. The Commissioner finds that 23andMe failed to implement appropriate technical and organisational security measures as required by Article

5(1)(f) UK GDPR and Article 32(1) UK GDPR by failing to implement device or connection monitoring or suspicious activity alerts. This failure had the effect of leaving the Platform exposed to a preventable brute force cyberattack, whilst also depriving customers of the ability to monitor and protect the security of their accounts.

207. Customers were not alerted when a new device, IP address or browser was used to access the Platform using their credentials. The *ICO Guidance on Passwords in Online Services* states that organisations should consider implementing a "*risk-based approach to verifying authentication attempts. For example, if a customer logs in from a new device or IP address [the organisation] might consider requesting a second authentication factor and informing the customer by another contact method of the login attempt*." The ICO guidance also recommends that organisations should "*consider providing customers with the facility to review a list of unsuccessful login attempts. This will allow people who might be specifically targeted to check for potential attacks manually. However, this will only be useful if* [the organisation] *pays attention to reports from individuals that their accounts are being attacked."* [208]

208. Alerts regarding login attempts from an unrecognised device or IP address are used by a range of other organisations operating online account-based services, for example Google[209] and Microsoft,[210] in order to alert customers to unusual activity on their account, such as a login from a new device or previously unused email address. These alerts may instruct customers to contact the organisation in question or take steps to protect their accounts (such as changing their login credentials)

[208] Passwords in online services | ICO (accessed 5 February 2025)
[209] Protect your account if there's unfamiliar activity - Google Account Help (accessed 5 February 2025)
[210] What happens if there's an unusual sign-in to your account - Microsoft Support (accessed 5 February 2025)

where they do not recognise the activity in question.

209. Such a system could have been used to alert 23andMe customers whose accounts were credential stuffed when the threat actor logged into their accounts from a device and IP address which had not previously been used to access the Platform using their credentials. This could also have resulted in customers reporting such suspicious activity to 23andMe itself and enabled the detection of the Data Breach at an earlier stage, thus reducing the duration and severity of the Infringements.

210. As referred to at paragraph 171 above, the Commissioner notes that 23andMe now provides a trusted browser functionality, which allows customers to register a "trusted device" used to access their 23andMe account for a period of 400 days and offers an "Account Event History" report which customers can download and which displays every login, attempted login and download with the associated IP address and approximate location (based on the IP address).[211]

ii. Ineffective rate-limiting rules and alerts

211. The Commissioner finds that 23andMe failed to implement appropriate technical and organisational security measures as required by Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR by failing to implement effective rate-limiting rules and alerts.

212. *The ICO Security Outcomes* state that organisations should "*ensure that* [they] *are rate-limiting or throttling the number and frequency of incorrect login attempts. The precise number of attempts and the consequences of exceeding these limits will be for* [the organisation] *to decide based on the specific requirements of* [the] *organisation, but limiting to a certain number per hour, day and month is a good idea."*[212]

213. At the time of the Data Breach, 23andMe had service level agreements

[211] What's In Your Account Settings? – 23andMe Customer Care
[212] Security outcomes | ICO (accessed 5 February 2025)

in place with three third-party security providers: [redacted] and [redacted].[215] [redacted] was engaged for the purposes of protecting the Platform against malicious activity such as distributed denial of service attacks, malicious bots and other intrusions. 23andMe used [redacted] to detect and generate notifications regarding security events, as well as for the management of security incidents. [redacted] services were used to log all events within the 23andMe Platform, with such events then being correlated and stored within the [redacted] software.[216]

214. 23andMe informed the Commissioner that a range of [redacted] managed rules were in place at the time of the Data Breach to detect and respond to potential attacks. In addition, 23andMe stated that it implemented a range of rate-limiting rules which were set up in order to limit the amount of traffic from a given IP address. These rules looked for patterns, and, based on the frequency of these patterns, blocked the flow of traffic to and from a particular IP address for a given period of time.[217] 23andMe further stated that its alert system sufficiently detected breached credential testing by identifying multiple authentications from the same IP source within a certain time period.[218]

215. 23andMe explained that its Internal Investigation found that its rate-

[213] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the ICO and OPC dated 20 June 2024): [redacted]

[214] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the ICO and OPC dated 20 June 2024): [redacted]

[215] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the ICO and OPC dated 20 June 2024): [redacted]

[216] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 22

[217] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 22

[218] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 43

limiting rules had not been triggered by the threat actor's activity due to their rotation of thousands of unique IP addresses when accessing accounts during the Data Breach, meaning that the login activity was not detected as being irregular or unusual. 23andMe cited the fact that in May 2023, the threat actor had conducted successful login attempts from 7,813 IP addresses and had attempted further unsuccessful login attempts from 4,156 IP addresses. The threat actor was also found to have used approximately 2,000 IP addresses to scrape DNA Relatives profile information.[219] 23andMe further stated that the rate-limiting requests to access Raw Genetic Data would not have had any effect on the detection of the Data Breach given the threat actor downloaded and accessed the Raw Genetic Data for a small number of customers.

216. However, 23andMe previously informed the Commissioner that between 1 May and 16 May 2023, the threat actor carried out approximately 183,380 failed logins and 9,974 successful logins, whilst between 12 September and 18 September 2023, the threat actor carried out a further 89,762 unsuccessful and 4,500 successful login attempts (see Figure 7 below).[220]

[219] Letter from Greenberg Traurig LLP to the ICO and OPC, 10 September 2024 (response to letters from the ICO and OPC dated 20 June and 1 August 2024): Response to clarification question 64-64a
[220] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 36

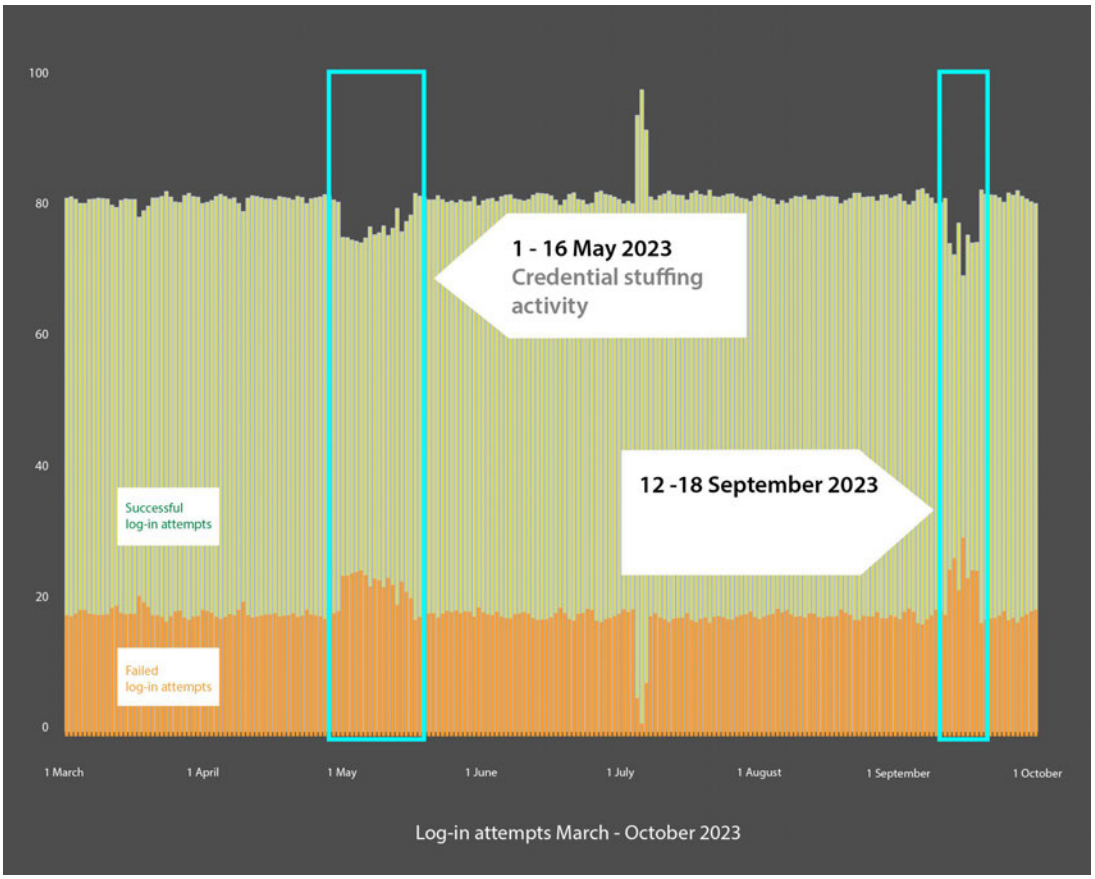


Figure 7: Ratio of successful to unsuccessful login attempts 1 March – 1 October 2023[221]

217. Therefore, whilst the threat actor's rotation of large numbers of IP addresses may have prevented 23andMe's rate-limiting rules from detecting the unauthorised activity, 23andMe failed to identify a significant distortion of the ratio of successful to unsuccessful login attempts in favour of the latter, when this ratio should, in ordinary circumstances and as illustrated in Figure 7 above, remain relatively stable at approximately 80% successful and 20% unsuccessful. In comparison, Figure 7 above illustrates that during the peak of the threat actor's credential stuffing activity this ratio fell to approximately 70% successful and 30% unsuccessful logins. Whilst 23andMe's security

[221] Figure 7 was produced using a list of the failed and successful logins to the Platform each day for the period 1 January 2019 to 31 December 2023: Letter from Greenberg Traurig LLP to the ICO and OPC, 18 October 2024 (response to letters from the ICO and OPC dated 20 September and 11 October 2024) Exhibit V

system failed to detect any unusual or suspicious activity at the relevant time, the Internal Investigation retrospectively uncovered "*large spikes of failed and unsuccessful logins for the certain periods in 2023 between May 1 and September 18.*"[222]

218. 23andMe's rate-limiting rules were not capable of detecting the threat actor's attempts to access and download customers' Raw Genetic Data. 23andMe's measures failed to detect, in real time, the abnormally large number of account login attempts, both successful and unsuccessful, and the significant changes to the ratio between the two. If the threat actor's login attempts had been detected at this stage and an investigation initiated, this could have resulted in 23andMe detecting the Data Breach and taking measures in response at a far earlier stage.

219. In light of the deficiencies in 23andMe's rate-limiting system and broader monitoring measures, the Commissioner finds that either such measures were ineffective as a means of alerting 23andMe's security team to potentially unauthorised and illegitimate activity on the Platform, or its organisational measures did not ensure that indicators of malicious activity were investigated in a prompt and appropriate manner. The Commissioner also understands that the thresholds applied by 23andMe for triggering detection alerts were set manually, resulting in those thresholds lacking flexibility to respond to changes in usage patterns and quickly becoming outdated. The Commissioner's view is that the manual setting of thresholds increased the risk of alerts not being triggered or alerts being triggered in inappropriate circumstances.

220. The Commissioner finds that 23andMe's failure to detect the threat actor's activity represents further evidence of its failure to implement appropriate technical and organisational measures which ensured a level of confidentiality and integrity of Affected UK Data Subjects' personal

[222] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 25

data when taking into account the nature of 23andMe's processing operations and the risks posed to its customers' rights and freedoms. However, the Commissioner notes 23andMe's update at the Oral Hearing that, as of 31 December 2024 it had:

a) reconfigured its internal logs so that its Security Team can better track and identify malicious activities [redacted];

b) introduced over [redacted] SIEM (security information and event management) detection alerts and [redacted] new product rules; and

c) created various new rate-limiting rules through [redacted].[223] At the Oral Hearing 23andMe also confirmed that it has continued to adjust these rate-limiting rules based on traffic activities or indication of attack.

iii. Failure to monitor and detect anomalous customer activity

221. The Commissioner finds that 23andMe failed to implement appropriate technical and organisational security measures as required by Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR by failing to implement an appropriate and effective system to monitor for, detect and investigate evidence of anomalous and potentially unauthorised activity on the Platform.

222. *The ICO Security Outcomes*[224] state that controllers and processors are expected to detect security events that affect the systems that process personal data and to monitor authorised customer access to that data.[225] This includes recording customer access to personal data, with processes in place to act upon unexpected events or indications of personal data breaches that are detected within the appropriate

[223] 23andMe Written Representations, 18 April 2025: Paragraph 16
[224] Security outcomes | ICO
[225] Security outcomes | ICO

timeframe.[226] The Commissioner's *Accountability Framework* also states that controllers should take steps to prevent unauthorised access to systems and applications, including by logging and monitoring user and system activity to detect anything unusual.[227]

223. 23andMe informed the Commissioner that in the course of the Internal Investigation it reviewed login patterns to identify any irregularities. 23andMe indicated that it was aware of normal patterns of customer behaviour on the Platform, stating that when customers access the login page from the main 23andMe.com site, the HTTP referrer is the main login page. However, during the Internal Investigation, 23andMe identified a login pattern where attempts were made to log in to accounts, but the HTTP referrer was empty. Following further analysis, 23andMe identified large increases in both successful and unsuccessful login attempts which did not display a HTTP referrer for certain periods between 1 May and 18 September 2023.[228]

224. This indicates that the threat actor's pattern of activity on the Platform deviated from that observed when legitimate customers accessed their accounts. However, this abnormal pattern of activity was only detected during the Internal Investigation, with 23andMe having no system in place to monitor and investigate such deviations from standard customer behavioural patterns in real time during the Relevant Period.

225. 23andMe informed the Commissioner that it engaged [redacted] to protect the Platform against malicious activity, such as [redacted] and [redacted], whilst [redacted] was used for the detection and notification of security events and incident management across the Platform.[229] However, on the basis of the

[226] Security outcomes | ICO
[227] Records management and security | ICO
[228] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 25
[229] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the OPC and ICO dated 20 June 2024): Response to question 22

information provided to the Commissioner, it appears that 23andMe did not proactively monitor for, detect or investigate unusual patterns of customer behaviour, such as that displayed by the threat actor.

226. The Commissioner acknowledges that monitoring and logging of abnormal customer behaviour is not a specific requirement set out in the UK GDPR. However, the Commissioner's Accountability Framework[230] confirms that implementing such a monitoring and logging system is expected as part of the measures a controller must put in place to prevent unauthorised access to their systems, as required by Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR. The Commissioner therefore regards the absence of such monitoring and logging measures as further evidence in support of his finding that the technical and organisational measures implemented by 23andMe were not appropriate to ensure the ongoing confidentiality, integrity and resilience of its processing systems and services.

227. The fact that the threat actor's activity was detected as anomalous in the course of the Internal Investigation indicates that 23andMe both understood how its customers generally accessed their accounts and possessed the technical ability and means of detecting abnormal use patterns within the Platform.

228. Therefore, the Commissioner's view is that neither the costs of implementing such a system of proactive monitoring and investigation of potential security events, nor the availability of the required software and technology are factors that would have prevented the adoption of such a system, whether through a third-party service or internally, as part of a range of appropriate technical and organisational security measures as required by Article 32(1)(b) UK GDPR.

229. This failure to implement appropriate technical and organisation

[230] Records management and security | ICO

measures to monitor and detect anomalous customer activity is evidenced by the multiple opportunities which 23andMe missed to detect the Data Breach prior to October 2023. The *ICO Security Outcomes* state that controllers should have processes in place to detect unexpected events or indications of a personal data breach and processes in place to act upon those events as necessary in an appropriate timeframe.[231] When assessing 23andMe's processes for detecting unexpected events or indications of a personal data breach, the Commissioner notes that, between 28 July and 30 July 2023, the threat actor unsuccessfully attempted to automate the transfer of ownership of approximately 400 customer profiles. 23andMe confirmed in its Written Representations that it took various steps in response to the July Attempted Profile Transfers including mandating a password reset for 400 customers, disabling all profile transfer requests, placing a temporary lock on accounts suspected of having attempted a malicious transfer and introducing a new systems alert for [redacted]. However, the Commissioner notes that despite undertaking an internal investigation after discovering the July Attempted Profile Transfers, 23andMe failed to detect the threat actor's wider activity on the Platform, or launch a wider investigation into potential unauthorised access to customer accounts, resulting in the Data Breach continuing for a further two months.

230. Furthermore the Commissioner notes that there were deficiencies in 23andMe's logging and event monitoring. As stated at paragraph 185 above, 23andMe did not collect the logs generated by [redacted] when a customer requested a download of their Raw Genetic Data, whilst 23andMe's bespoke logging system erroneously recorded an internal IP

[231] Security outcomes | ICO
[232] 23andMe Written Representations, 18 April 2025: Paragraph 11

address, rather than the IP address associated with the customer who initiated the Raw Genetic Data download.[233] This misconfiguration in 23andMe's logging system was only discovered during the Internal Investigation in October and November 2023.

231. As a result of this misconfiguration, 23andMe was unable to establish which IP address had been used to initiate each download of Raw Genetic Data, meaning that it was unable to search for Raw Genetic Data downloads linked to IP addresses known to have been used by the threat actor. This meant that 23andMe was forced to employ the methodology explained at paragraphs 183 and 184 above in an attempt to retrospectively identify Raw Genetic Data downloads by the threat actor.

232. In the Commissioner's view, 23andMe's failure to collect and store direct logs generated by [redacted] when a customer initiated a Raw Genetic Data download represents a significant omission. The logging of such access requests in the [redacted] is not technically complex, particularly as the security products provided to 23andMe by [redacted] and [redacted] are both designed to be compatible with [redacted]. Meanwhile, Raw Genetic Data downloads by 23andMe customers were relatively infrequent,[234] meaning that retaining the logs would not have been likely to result in 23andMe incurring significant additional costs. Furthermore, directly generating the logs from the [redacted] would have reduced the potential for error and would have enabled a more expeditious and effective investigation by 23andMe.

233. The Commissioner notes that, as explained at paragraph 220 above, since the Data Breach 23andMe has reconfigured its internal logs so that its security team can better track and identify malicious activities [redacted]

[233] Letter from Greenberg Traurig LLP to the ICO and OPC, 10 September 2024 (Response to question 2 in a letter from the ICO and OPC to 23andMe and Greenberg Traurig LLP dated 21 August 2024)unauthorised
[234] Interview with [redacted], 23andMe Software Architect, 18 November 2024

[redacted]

iv. Failure to implement an appropriate organisational response to evidence of a personal data breach

234. As set out below, the Commissioner finds that 23andMe failed to implement appropriate organisational security measures in accordance with Article 5(1)(f) UK GDPR and Article 32(1)(b) UK GDPR by failing to respond appropriately to evidence of a personal data breach by:

a) deciding to allocate the August 2023 Messages the lowest level of priority rating within the 23andMe Cyber Incident Response Procedure;

b) undertaking limited investigations following receipt of the August 2023 Messages; and

c) failing to consider that these incidents constituted potential evidence of genuine malicious activity.

235. 23andMe informed the Commissioner that it only became aware of the Data Breach on 1 October 2023 after an employee reported seeing a post on the Reddit platform offering data allegedly stolen from the Platform for sale, with this subsequently leading to the Internal Investigation being initiated.[236]

236. However, the Commissioner finds that 23andMe missed multiple opportunities before this date to detect and respond to the threat actor's attack.

237. The Commissioner notes that 23andMe's response to the August 2023 Messages demonstrated an organisational failure by 23andMe to respond to evidence of a personal data breach. 23andMe opened an incident log following receipt of the August 2023 Messages, in the form

[235] 23andMe Written Representations, 18 April 2025: Paragraph 16.6
[236] Third Data Breach Report Form

of the [redacted] Ticket.[237] The incident was only allocated a severity rating of "should have", which, according to 23andMe's Cyber Incident Response Procedure,[238] is the lowest level of priority classification available, with other examples of "should have" incidents including a lost laptop or ID badge.

238. The low level of priority classification attributed to the August 2023 Messages was inappropriate given that the [redacted] Ticket contained reference to the Subreddit Post, including screenshots of posts containing images of the DNA Relatives profiles of [redacted] and her former husband [redacted]. The responses within the [redacted] Ticket indicate that 23andMe's Cyber Incident Response Team attributed a low level of priority to the August 2023 Messages on the basis that [redacted] and [redacted] had publicly shared their 23andMe profile, meaning that this information would be visible to any of either individual's DNA Relatives, and therefore did not constitute evidence of "*outside access to* [23andMe customer] *account*[s]."[239]

239. A comment on the [redacted] Ticket dated 15 August 2023, stated that any stolen data from 23andMe systems would presumably have been posted on an invite-only dark net site, which the Cyber Incident Response Team did not have the capability to access. The [redacted] Ticket did not contain any response to, or follow up on this comment. Had 23andMe's security team arranged for other dark net platforms to be checked at this time, there is a significant possibility that they would have seen the Hydra Post which contained content and wording which

[237] Letter from Greenberg Traurig LLP to the ICO and OPC, 23 October 2024 (Exhibit AL) (Responding to letters to Greenberg Traurig LLP and 23andMe from the ICO and OPC dated 20 September and 11 October 2024)
[238] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (Responding to a letter to Greenberg Traurig LLP and 23andMe from the ICO and OPC dated 20 June 2024) (Exhibit E)
[239] Letter from Greenberg Traurig LLP to the ICO and OPC, 23 October 2024 (Exhibit AL) (Responding to letters to Greenberg Traurig LLP and 23andMe from the ICO and OPC dated 20 September and 11 October 2024)

was very similar to the August 2023 Messages and the posts on the 23andMe Subreddit. 23andMe only established a link between the Hydra Post and the August 2023 Messages on 8 October 2023 when the [redacted] Ticket was updated with a link to the Hydra Post.[240]

240. On 18 August 2023, the [redacted] Ticket was closed by the Cyber Incident Response Team on the basis that the August 2023 Messages were deemed to have been a "*hoax,*" with one comment stating that there was "*no evidence of unauthorised data exposure*" and another that whilst "*some data was accessed, it was not to the levels outlined in this claim.*"[241] There is no evidence to suggest that the [redacted] Ticket was escalated beyond the Cyber Incident Response Team.

241. Whilst the figures quoted in the August 2023 Messages, which claimed that the personal data relating to 10 million 23andMe customers had been exfiltrated, were exaggerated, the updates added to the [redacted] Ticket on 12 December 2023 demonstrate that 23andMe later established that they related to the same security incident which was subsequently identified and verified as genuine in October 2023. Furthermore, the [redacted] Ticket failed to include reference to the July Login Spike and the July Attempted Profile Transfer, with there being no indication that 23andMe ever considered that the events may be linked.

242. 23andMe did not disclose the August 2023 Messages to the Commissioner until October 2024.[242] The August 2023 Messages did not feature in the personal data breach reports submitted by 23andMe to the Commissioner, nor in the company's initial responses to requests for

[240] Letter from Greenberg Traurig LLP to the ICO and OPC, 23 October 2024 (Exhibit AL) (Responding to letters to Greenberg Traurig LLP and 23andMe from the ICO and OPC dated 20 September and 11 October 2024)
[241] Letter from Greenberg Traurig LLP to the ICO and OPC, 23 October 2024 (Exhibit AL) (Responding to letters to Greenberg Traurig LLP and 23andMe from the ICO and OPC dated 20 September and 11 October 2024)
[242] Letter from Greenberg Traurig LLP to the ICO and OPC, 23 October 2024 (Responding to letters to Greenberg Traurig LLP and 23andMe from the ICO and OPC dated 20 September and 11 October 2024)

information from the ICO and the OPC. The only indication that the threat actor had made contact with 23andMe in August 2023 was a reference to the threat actor having emailed 23andMe in the Hydra Post which was visible in a screenshot within an [redacted] Report dated 19 October 2023[243] which was disclosed to the ICO and OPC as an exhibit to 23andMe's letter dated 13 August 2024.

243. 23andMe informed the Commissioner that it did not consider implementing any additional security or monitoring measures following the August 2023 Messages as "*there was no indication of unauthorised access.*"[244] However, the proximity of the July Login Spike, the July Attempted Profile Transfer and the August 2023 Messages should have been sufficient to increase 23andMe's alert level and could reasonably have been expected to have led to a full investigation being commissioned into the accumulating evidence of malicious activity in August 2023. Furthermore, the fact that the August 2023 Messages contained claims of a theft of significant amounts of customer data should, according to the 23andMe Cyber Incident Response Procedure, have led to the messages being classified as a high priority incident.[245]

244. In addition, 23andMe's response to the August 2023 Messages focused solely on the accounts of [redacted] and [redacted] on the basis that they were named in the August 2023 Messages, which also included extracts of their DNA Relatives Profile information. The investigation focused exclusively on evidence of unauthorised access to these two accounts and, when none was found, was quickly closed, with the August 2023 Messages being dismissed as a hoax. The Commissioner

[243] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter to Greenberg Traurig LLP and 23andMe from the OPC and ICO dated 20 June 2024) (Exhibit N: Figure 2)
[244] Letter from Greenberg Traurig LLP to the ICO and OPC, 17 January 2025
[245] Figure 17 in Section 6.4.5 of the 23andMe Cyber Incident Response Procedure states that the highest priority incidents require an immediate fix, with the examples given of such incidents including "breaches" and "lost customer data."

has not been presented with any evidence to indicate that 23andMe conducted a broader search for any other indicators of unauthorised activity, such as analysis of patterns of successful and unsuccessful login attempts.

245. The fact that such steps were taken in October 2023 and ultimately led to the confirmation of a credential stuffing attack, demonstrates that 23andMe had the resources and technical ability to conduct such an investigation. The Commissioner therefore finds that the failure to do so in August 2023 constitutes evidence of 23andMe's failure to implement organisational measures which ensured that actual or potential security incidents were identified, logged and investigated in a manner which was appropriate in light of the sensitivity of such data and the potential consequences of a personal data breach affecting the Platform.

246. 23andMe's inadequate response to the accumulated evidence of unauthorised activity on the Platform, including the July Login Spike, the July Attempted Profile Transfer and the August 2023 Messages meant that the company's limited and insufficient security controls and authentication measures remained in place for a further two months, during which time Customer Personal Data remained accessible to the threat actor.[246]

(e) Assessment of compliance as of 31 December 2024

247. On 4 March 2025, the Commissioner informed[247] 23andMe that he intended to issue an enforcement notice pursuant to section 149 DPA 2018 (in addition to a penalty notice pursuant to section 155 DPA 2018).

248. The proposed enforcement notice would have required 23andMe to implement appropriate technical and organisational measures in accordance with Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR.

[246] For example, there were 84 downloads of Raw Genetic Data from compromised accounts after the [redacted] Ticket was closed on 18 August 2023.
[247] By way of a "preliminary" enforcement notice.

249. On 18 April 2025, the Commissioner received the Written Representations from 23andMe, which set out the company's response to his intention to impose a penalty and issue an enforcement notice. 23andMe provided further detail at the Oral Hearing and by way of written correspondence dated 6 May 2025.

250. Having considered both the written and oral representations, the Commissioner finds that by 31 December 2024, 23andMe had implemented appropriate measures to ensure appropriate security of the personal data which was subject to the Relevant Processing. The ongoing infringements of Article 5(1)(f) UK GDPR and Article 32 UK GDPR were therefore remedied by that date.[248]

VII. DECISION TO IMPOSE A PENALTY

251. For the reasons set out below, the Commissioner has decided to impose a penalty of £2,310,000 on 23andMe in respect of the infringements of Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR during the Relevant Period, as described in this Penalty Notice.

A. Legal framework - Penalties

252. Section 155(1)(a) DPA 2018 provides that, if the Commissioner is satisfied that a person has failed, or is failing, as described in section 149(2) DPA 2018, the Commissioner may, by written notice, require the person to pay to the Commissioner an amount in sterling specified in the notice.

253. When deciding whether to issue a penalty notice to a person, and determining the appropriate amount of the penalty, section 155(2)(a) DPA 2018 requires the Commissioner to have regard to the matters listed in Article 83(1) and (2) UK GDPR, in so far as they are relevant in the circumstances of the case.

[248] As a result, there are no longer grounds to give the proposed enforcement notice.

254. Article 83(1) UK GDPR requires any penalty imposed by the Commissioner to be effective, proportionate and dissuasive in each individual case.

255. Article 83(2) UK GDPR requires the Commissioner to have due regard to the following factors when determining whether to issue a penalty notice and the appropriate amount of any such penalty in each individual case:

a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

b) the intentional or negligent character of the infringement;

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

e) any relevant previous infringements by the controller or processor;

f) the degree of cooperation with the Commissioner, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the manner in which the infringement became known to the Commissioner, in particular whether, and if so to what extent, the controller or processor notified the infringement;

i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

j) adherence to approved codes of conduct pursuant to Article 40, or approved certification mechanisms pursuant to Article 42; and

k) *any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoid, directly or indirectly, from the infringement.*[249]

B. The Commissioner's decision on whether to impose a penalty

256. Paragraphs 258 to 368 below set out the Commissioner's assessment of whether it is appropriate to issue a penalty in relation to the Infringements set out above. This assessment involves consideration of the factors in Article 83(1) and (2) UK GDPR. Those considerations are considered in the following order, which follows the *Commissioner's Data Protection Fining Guidance* (the "**Fining Guidance**")[250]:

a) Seriousness of the infringement (Article 83(2)(a), (b) and (g) UK GDPR);

b) Relevant aggravating or mitigating factors (Article 83(2)(c)-(f), (h)-(k) UK GDPR); and

c) Effectiveness, proportionality and dissuasiveness (Article 83(1) UK GDPR).

257. The Commissioner's decision is to impose a penalty.

Seriousness of the Infringements

(a) The nature, gravity and duration of the Infringements (Article 83(2)(a) UK GDPR)

258. In assessing the seriousness of the Infringements, the Commissioner

[249] Section 155(2)(a) DPA 2018 states that when deciding whether to issue a penalty notice and determining the amount of the penalty, the Commissioner must have regard to the matters listed in Article 83(1) and (2) UK GDPR to the extent that the penalty notice concerns a matter to which the UK GDPR applies.
[250] Data Protection Fining Guidance | ICO (March 2024)

has given due regard to their nature, gravity and duration.

i) *Nature of the Infringements*

259. The Commissioner has made a finding of infringement of Article 5(1)(f) UK GDPR, which sets out the integrity and confidentiality principle for the processing of personal data. As stated above, an infringement of this provision is subject to the higher maximum statutory penalty,[251] which is indicative of its seriousness.

260. The Commissioner finds that 23andMe's failure to implement such authentication and verification measures, both as part of the general login process and the self-service Raw Genetic Data download feature, represented a significant failure to implement technical security measures which were appropriate in light of the risks posed by 23andMe's processing operations to Customer Personal Data, as required by Article 32(1) UK GDPR. The Commissioner considers that, had 23andMe mandated MFA for all customer accounts, and/ or implemented alternative access controls, this would have significantly decreased the likelihood of the Platform being successfully targeted by a credential stuffing attack. Furthermore, requiring an additional step-up authentication measure before enabling access to the most sensitive data within a customer account would have significantly decreased the likelihood of the threat actor accessing and exfiltrating Raw Genetic Data and health data.

261. In addition, simulating a credential stuffing attack as part of its security testing programme would have alerted 23andMe to its level of exposure to such an attack and enabled it to devise and implement measures in response to that risk, as required by Article 32(1)(b) and (d) UK GDPR. During the Internal Investigation, 23andMe identified eight separate accounts that may have been accessed in isolated incidents of credential

[251] Article 83(5)(a) UK GDPR

stuffing in 2019 and 2020,[252] which its security and monitoring measures failed to detect at the time. If 23andMe had detected these attacks at the time, this would have presented the company with an opportunity to review and address the deficiencies in its security measures, including the lack of mandatory MFA, which the threat actor subsequently exploited in the course of the Data Breach.

262. As stated above, at the time of the Data Breach 23andMe did not have any form of browser, device or connection fingerprinting in place on the Platform.[253] Neither did it allow customers to monitor the devices used to access the Platform using their credentials.[254] 23andMe also failed to detect significant changes in the ratio of successful to unsuccessful login attempts, with significant increases in the latter compared to the former, when this figure should, in ordinary circumstances, have remained relatively stable.

263. Furthermore, the Commissioner's investigation revealed evidence of the inappropriateness and ineffectiveness of 23andMe's logging, monitoring and organisational security measures, with numerous missed opportunities to detect the threat actor's activities.

264. The Commissioner finds that 23andMe's failure to (a) detect the incidents of credential stuffing in 2019 and 2020, and (b) identify and investigate the anomalous usage patterns displayed by the threat actor, represent further evidence of 23andMe's failure to implement appropriate technical measures designed to monitor for, detect and appropriately respond to threats to the integrity and confidentiality of its processing systems and services, in breach of Article 5(1)(f) UK GDPR

[252] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to question 34
[253] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to question 18
[254] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to question 20

and Article 32(1)(b) UK GDPR.

265. Furthermore, 23andMe stated that it only became aware of the Data Breach on 1 October 2023.[255] However, the Commissioner finds that both the July Login Spike and the July Attempted Profile Transfers constituted evidence of unauthorised activity on the Platform which it is reasonable to expect should have triggered a broader investigation into suspected unauthorised and illegitimate activity on the Platform in July 2023. Furthermore, the August 2023 Messages directly indicated that a significant personal data breach had occurred. Whilst an internal incident log was created in response to the August 2023 Messages,[256] 23andMe:

a) did not commission a full investigation;

b) dismissed the claims as a hoax after conducting only a limited analysis of the August 2023 Messages;

c) did not undertake a broader review of its technical and organisational security measures; and

d) did not make any changes to its authentication and verification measures in order to enhance the security of its login and Raw Genetic Data download processes.

266. The Commissioner finds that 23andMe's response to the identification and verification of the Data Breach was inadequate given its seriousness. In particular, the Commissioner notes 23andMe's failure to take urgent steps to reestablish the integrity and confidentiality of Customer Personal Data. For example, it took 23andMe four days after verification of the Data Breach to disable active customer sessions on the Platform[257]

[255] 15 October 2023 Data Breach Report Form
[256] Letter from Greenberg Traurig LLP to the ICO and OPC, 23 October 2024 (responding to letters from the ICO and OPC dated 20 September and 11 October 2024 (See Exhibit AL)
[257] Third Data Breach Report Form

and mandate a password reset for all customers.[258] It took 23andMe until 2 November 2023 to disable its self-service Raw Genetic Data download feature, almost one month after the Data Breach had been detected and verified as genuine. Mandatory MFA was only implemented for all new and existing customer accounts on 9 November 2023, despite 23andMe almost immediately attributing the Data Breach to a credential stuffing attack[259] and MFA being widely recognised as the most effective means of protection against such attacks.[260]

267. In light of the above, the Commissioner finds that the Infringements are of a serious nature as 23andMe's failure to implement appropriate technical and organisational security measures exposed its customers' highly sensitive personal data, including their special category data, to the risk of unauthorised access and use, whilst also significantly inhibiting its ability to detect anomalous and potentially malicious activity on the Platform.

ii) *Gravity of the Infringements*

268. When assessing the gravity of the Infringements, the Commissioner has considered the nature, scope and purposes of 23andMe's processing, as well as the number of data subjects affected and the level of any damage or distress they have suffered.[261]

269. As regards the **nature** of 23andMe's processing activities, it is of particular significance that 23andMe customers who complete and return a saliva collection kit entrust the company with their genetic data. Genetic data is listed as a form of special category data in Article 9(1)

[258] 23andMe Written Representations, 19 April 2025: Paragraph 12
[259] Interview with [redacted] (23andMe Software Architect), 18 November 2024
[260] The Global Privacy Assembly's Credential Stuffing Guidelines (dated June 2022) (accessed 5 February 2025) state that "MFA is considered to be the most effective measure in securing online accounts against credential stuffing… analysis by Microsoft suggests that MFA would stop virtually all credential stuffing account compromises… MFA should be considered as an essential measure for any accounts that contain sensitive information."
[261] Fining Guidance, paragraph 58

UK GDPR and, in light of its inherent sensitivity, merits specific protection.[262] Furthermore, and as explained at paragraph 318 below, the Commissioner's view is that the personal data contained in a customer's DNA Relatives profile could be inferred special category data where it is used to make inferences about a customer's racial or ethnic origin based on their connections within the feature and the traits that they share.

270. Therefore, the Commissioner considers that when devising and implementing its technical and organisational security measures, 23andMe should have given particular consideration to:

a) the highly sensitive nature of the personal data processed on the Platform, including genetic and other special category data;

b) the reasonable expectations of 23andMe customers who shared their genetic and other special category data with the company regarding the security measures in place to protect such highly sensitive data; and

c) the extensive amounts of data sharing between customers that takes place on the Platform which would significantly increase the number of customers and volume of personal data which could be affected in the event of a third-party obtaining unauthorised access to customer accounts.

271. As regards the **purposes** of the processing, paragraph 59 of the *Fining Guidance*[263] states that the Commissioner may give greater weight to this factor if the relevant processing is central to a controller or processor's main business and commercial activities.

272. The Commissioner considers that the purposes of 23andMe's processing is a relevant factor which increases the seriousness of the

[262] Recital 51 UK GDPR
[263] Seriousness of the infringement | ICO

Infringements. 23andMe's business model is predicated upon processing personal data supplied by its customers, including Raw Genetic Data, in order to generate further information about their ancestral, racial and genetic origins, and using that information to establish connections between customers on the basis of their shared genetic ancestry, primarily through the DNA Relatives and Family Tree features. These features of the Platform enable customers to view the personal data within the DNA Relatives profiles of other customers with whom they are connected and are a central element of 23andMe's marketing of the Platform.[264]

273. This meant that when the threat actor successfully credential stuffed a 23andMe customer account, they were not only able to access personal data relating to the owner of that account, but also the personal data relating to the customer's DNA Relatives connections which they shared on their profile.

274. This ability for 23andMe customers to share highly sensitive personal data with 23andMe, which was then visible to their connections within the DNA Relatives, Family Tree and Connections features, meant that 23andMe was required, pursuant to Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR to implement particularly robust technical and organisational measures in order to ensure the integrity and confidentiality of its customer's personal data. However, the Commissioner finds that the technical and organisational measures in place throughout the Relevant Period fell far below this standard and therefore could not be considered "appropriate" for the purposes of Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR, resulting in serious infringements of these Articles.

[264] 23andMe's description of its Ancestry Service informs customers that the optional DNA Relatives feature allows them to "*Find your matches. Compare ancestries and traits. Message relatives directly to better understand your family connection.*"

275. Therefore, the Commissioner finds that, in light of the considerations set out above, the nature and purpose of 23andMe's processing increased the seriousness of the Infringements.

276. When considering the **scope** of the processing, the Commissioner has assessed both the territorial scope and the extent and scale of 23andMe's processing.[265]

277. The Commissioner finds that 23andMe, Inc is the controller[266] directly responsible for the personal data of the company's approximately 495,000 customers in the UK. As stated at paragraph 113 above, the UK GDPR applies to 23andMe under Article 3(2)(a), as whilst not established in the UK, it offers services to data subjects in the UK.

278. Paragraph 59 of the *Fining Guidance* states that the greater the **number** of data subjects affected by the infringement, the more weight the Commissioner will give to this factor.[267] In making this assessment, the Commissioner takes into account both the number of data subjects potentially affected, as well as those actually affected, by an infringement.

279. In this case, 23andMe's failure to implement appropriate technical and organisational security measures put at risk the personal data of the majority of its customer base. In particular, 23andMe's failure to mandate the use of MFA, or implement appropriate compensatory controls, placed the 78.3% of its customers who, at the time of the Data Breach, had not enabled MFA and did not use a form of SSO service on their 23andMe accounts[268] at a greater risk of exposure to brute force attacks.

---

[265] Fining Guidance, paragraph 59
[266] As defined in Article 4(7) UK GDPR as the "*natural or legal person, public authority, agency or other body which alone, or jointly with others, determines the purposes and means of the processing of personal data.*"
[267] Seriousness of the infringement | ICO
[268] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 28

280. The number of data subjects whose personal data was actually affected in the course of the Data Breach varied according to the type of personal data that was accessed by the threat actor. 23andMe informed the Commissioner that a total of 155,592 Affected UK Data Subjects were affected by the Data Breach, with the threat actor having accessed:

a) Ancestry Reports relating to 120,504 Affected UK Data Subjects;

b) the DNA Relatives profiles of 120,031 Affected UK Data Subjects;

c) the Family Tree profiles of 35,561 Affected UK Data Subjects;[269]

d) 23andMe Health Reports relating to 320 Affected UK Data Subjects;

e) the details of health conditions self-reported by three Affected UK Data Subjects; and

f) the Raw Genetic Data of two Affected UK Data Subjects. [270]

281. Paragraph 59 of the *Fining Guidance* states that the Commissioner may have regard to the number of complaints received from data subjects about the conduct that has led to findings of infringement. However, the absence of such complaints will not be regarded as an indication that conduct found to infringe the UK GDPR or DPA 2018 is less serious.

282. 23andMe informed the Commissioner that its Customer Care team received approximately 360 enquiries from UK customers relating to the Data Breach.[271] However, 23andMe has not confirmed the proportion of these enquiries which were negative in nature, or which were treated as complaints. In addition, 11 Affected UK Data Subjects complained to the ICO in October 2023 following 23andMe's initial public statements

[269] The figures for the number of Affected UK Data Subjects whose DNA Relatives profiles and those whose Family Tree profiles were accessed by the threat actor are mutually exclusive.
[270] Third Data Breach Report Form and a letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 37
[271] Letter from Greenberg Traurig LLP and 23andMe to the ICO and OPC, 10 September 2024 (responding to letters from the ICO and OPC dated 20 June and 21 August 2024): Clarified response to question 61

relating to the Data Breach.

283. 23andMe informed the Commissioner that the Internal Investigation indicated that the threat actor did not download Raw Genetic Data relating to any Affected UK Data Subjects.[272] 23andMe reached the same conclusion after re-examining Raw Genetic Data downloads in the credential stuffed accounts during the period in which the Data Breach occurred, claiming that its original analysis had been over-inclusive and that only four customers globally had, in fact, had their Raw Genetic Data downloaded by the threat actor.[273] However, at the Oral Hearing, 23andMe accepted that whilst there was a small time delay as the file was generated, there were no additional step-up authentication measures in place which would have impeded the threat actor from downloading Raw Genetic Data from credential stuffed accounts, had the threat actor attempted to do so.

284. The Commissioner finds that, when assessing the seriousness of the Infringements, it is significant that personal data relating to the majority of 23andMe's customer base was vulnerable to unauthorised access as a result of 23andMe's failure to implement appropriate technical and organisational security measures as part of its login process. Therefore, the Commissioner finds that the fact that a greater number of customers were not actually affected by the Infringements was not attributable to the effectiveness of 23andMe's technical and organisational security measures.

285. Furthermore, whilst 23andMe informed the Commissioner that the threat actor accessed Raw Genetic Data relating to only two Affected UK Data Subjects, the Commissioner considers this to be a serious consequence of the Infringements given the particular sensitivity of

[272] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 37
[273] 23andMe Written Representations, 18 April 2025: Paragraph 2

genetic data and the requirement in Recital 51 of the UK GDPR for it to be given specific protection as a result.

286. In assessing the **level of damage suffered** the Commissioner has had regard to both the actual damage suffered and the potential damage and distress which could have resulted from the Infringements. In particular, the Commissioner has considered the extent to which the Infringements affected the rights and freedoms of Affected UK Data Subjects, or otherwise led to them suffering, or being likely to suffer harm, in the form of physical, material or non-material damage.[274]

287. Evidence which the Commissioner obtained from Affected UK Data Subjects, which is set out in full in Annex 3 of this Penalty Notice, demonstrated the harm that arose, or which could have arisen, as a result of the Infringements. One Affected UK Data Subject described feeling "*extremely anxious about what* [the Data Breach] c*ould mean to my personal, financial and family safety in future.*"

288. An Affected UK Data Subject also stated that their 23andMe account had "*a Jewish identifier associated with it*", and that in the context of what they described as "*the conflict between Zionism and the Arab world,*" which they believed had "*resulted in increases in antisemitic violence in the UK*" the ability, as they believed existed, to "*target a specific group using their DNA data*" was "*very concerning*."

289. Another Affected UK Data Subject stated that they "*expected rigorous privacy controls to be in place due to the nature of the information* [23andMe] *collected*," adding that "*unlike usernames, passwords and email addresses, you can't change your genetic makeup when a data breach occurs.*"

290. The Commissioner finds that the statements above from Affected UK Data Subjects demonstrate that the Infringements and the Data Breach

[274] Seriousness of the infringement | ICO

which followed caused significant distress to some 23andMe customers.

291. In addition to the distress reported by Affected UK Data Subjects, the Commissioner has considered the potential harm to 23andMe customers which may have resulted, and which may yet result, from the Infringements.[275]

292. The combination of personal data found in a DNA Relatives profile could provide a detailed profile of an individual, including details of their race, ethnic origin and genetic relatives. Such a combination of information, if exploited by a maliciously motivated threat actor, could be used to cause emotional and psychological harm, especially if used to target individuals. The Commissioner considers that this is particularly relevant in this case in light of the evidence in the October 2023 Online Forum Posts that the threat actor targeted 23andMe customers of an Ashkenazi Jewish descent.[276]

293. 23andMe acknowledged that customers could experience anxiety and embarrassment if the personal data within their DNA Relatives profile was made public. However, 23andMe considered this to be "*unlikely",* stating that "*if the impacted individuals had anxiety or embarrassment about such information being made public, or thought making such information publicly available would harm them in some way, they would not have shared such information with thousands of individuals on the DNA Relatives feature."*[277] 23andMe also recognised that customers whose health-related information was accessed by the threat actor may be concerned and experience anxiety, but stated that this only applied

[275] When considering the potential harms to Affected UK Data Subjects resulting from the Infringements, the Commissioner has taken into account the categories of harm set out in the ICO's Data Protection Harms Taxonomy.
[276] For example, the BreachForums Post Dated 17 October referred to prominent Jewish families and an alleged Israeli attack on a hospital during the conflict between Israel and Hamas in Gaza which began earlier that month
[277] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 55

to a small subset of the customers affected by the Data Breach.[278] 23andMe submitted that over 99% of Affected UK Data Subjects had consented to making the information contained in their DNA Relatives Profile, Family Tree Profile and/or Ancestry Reports available to their genetic relatives through the DNA Relatives feature and that "*for the vast majority of 23andMe customers, 90% or more of the individuals on their DNA Relatives list are strangers who they will never know*." 23andMe also submitted that by agreeing to participate in the DNA Relatives feature, these customers had agreed to share their personal data with "*complete strangers"* and that any claims of anxiety or fear "*seem disingenuous, especially where a customer's physical address was not part of the information disclosed*".[279]

294. However, the Commissioner considers that there is a significant difference between 23andMe customers voluntarily electing to share their personal data with other customers in what they believed to be the secure environment of the Platform and that personal data being accessible to a maliciously motivated threat actor and subsequently posted on open forums on the internet. When sharing their personal data within the DNA Relatives feature, 23andMe customers did not consent to, nor can they be said to have reasonably expected, their personal data to be disclosed to a potentially unlimited and unknown number of persons outside the Platform and in a manner which significantly increased the risk of such data being used in a manner which could cause them harm.

295. Therefore, the Commissioner finds that participating in the DNA Relatives feature and sharing the personal data within their profiles with their genetic relatives, Affected UK Data Subjects cannot be said to have demonstrated a reduced expectation of privacy in respect of such

[278] 23andMe Written Representations, 18 April 2025: Paragraph 21
[279] 23andMe Written Representations, 18 April 2025: Paragraph 22

personal data. The Commissioner's view is that Affected UK Data Subjects had a legitimate expectation that 23andMe would have implemented measures to ensure that such personal data was not accessible to third parties such as the threat actor, to whom they were not connected on the Platform.

296. In addition, in respect of some of the Affected UK Data Subjects whose accounts were credential stuffed, the threat actor accessed their Raw Genetic Data, personal data relating to their racial and ethnic origin, and/or personal data relating to their health, including information on their genetic health risks and self-reported health conditions. The Commissioner finds that such information becoming publicly available could lead to stigmatisation, discrimination and reputational damage, particularly if used to target members of a particular racial or ethnic group, or those with particular health conditions.

297. Affected UK Data Subjects who have a predisposition to, or who self-reported a serious medical condition, could also face serious harms as a result of such information being made public, including adverse treatment from employers or service providers if such information was used to assist in their decision-making regarding those individuals. Furthermore, uses for genetic data are continuing to emerge, with the potential for such personal data to be used by companies to develop bio-informed and personalised products, services and advertisements, thus exacerbating the seriousness of a loss of control over and unauthorised access to such information. Whilst genetic information is not currently widely used for the purposes of identification, its unique and unalterable nature means that, in future, organisations may use it for identification purposes in systems similar to those which currently rely on biometric data. Therefore, unauthorised access to Raw Genetic Data could, in future, place Affected UK Data Subjects at risk of impersonation, identity theft and fraud.

298. 23andMe acknowledged that, in respect of customers whose Raw Genetic Data and / or health data was accessed by the threat actor, "*the most severe outcome of the* [Data Breach] *could potentially be discrimination or reputational damage due to an individual's genotype and / or health data becoming public.*" However, 23andMe considered that it was "*highly improbable that such information will ever be used to cause harm*" as "*it does not seem probable (or legal) for insurance companies or employers to search the dark web for such information*" and that, on that basis, "*there is no real risk of significant harm.*"[280]

299. The Commissioner considers that this demonstrates 23andMe's failure to appreciate the extent of the distress suffered by 23andMe customers as a result of the loss of control over their highly sensitive personal data, whilst it also ignores the risks which are inherent in such data being made available on the dark web and thereby becoming accessible to maliciously motivated third parties who may seek to use it to cause harm, either now or in the future.

300. Finally, the Infringements and the Data Breach which followed, could have placed Affected UK Data Subjects at risk of extortion should the threat actor, or another maliciously motivated third party, have demanded payment in exchange for not releasing the highly sensitive personal data contained within 23andMe accounts into the public domain.

301. Therefore, the Commissioner finds that the seriousness of the Infringements was exacerbated by the actual harm suffered by Affected UK Data Subjects and the potential for further significant psychological, reputational and financial harm to have been caused by the highly sensitive personal data within 23andMe accounts entering the public domain and potentially being exploited by maliciously motivated third

[280] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 55

parties. 23andMe failed to recognise the potential for such harm and emphasised the voluntary nature of the sharing of personal data within the DNA Relatives feature, in a manner which failed to account for the distress caused to customers as a result of the loss of control over their sensitive personal data and the significantly greater risk of harm once such personal data was made publicly available outside of the Platform. Furthermore, it appears that 23andMe relied upon assurances from the threat actor that all personal data in their possession which had been obtained from the Platform had been destroyed and had not been sold on as evidence of the lack of harm caused to its customers, despite, by its own admission, being unable to confirm the veracity of those representations.[281]

iii) Duration of the Infringements

302. As stated at paragraph 59 of the *Fining Guidance*, the longer the duration of an infringement, the greater the weight the Commissioner is likely to attribute to this factor due to the greater potential for harm to have occurred.

303. As stated at paragraph 8 above, the Commissioner finds that, the Infringements commenced on 25 May 2018 when 23andMe's obligations under Article 5(1)(f) UK GDPR and 32(1) GDPR (as it then was) came into force. After considering 23andMe's Written Representations and the submissions made at the Oral Hearing, the Commissioner finds that the additional measures 23andMe has implemented since the Data Breach, including but not limited to:

a) revising its password requirements;

b) introducing mandatory two-factor verification as part of the login process;

[281] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 55

c) improving its credential checking processes, including checking customer passwords against the HIBP database;

d) implementing the "Account Event History" feature;

e) implementing a date of birth check before customers can download Raw Genetic Data, with only three attempts permitted before a user is referred to 23andMe's customer care team;

f) updating its product alerts to detect multiple scenarios of product abuse, including alerts intended to respond to evidence of [redacted] and [redacted]. 23andMe also adjusted its [redacted] rate-limiting rules and continues to adjust these rules based on traffic activities or indications of attack;

g) engaging a third-party to monitor and report on any dark web posts relating to 23andMe;

h) carrying out tabletop cyber security exercises, including five in the company's 2025 financial year;

i) reconfiguring its internal logs to enable the 23andMe security team to better track and identify malicious activities [redacted]

j) implementing [redacted] and risk-based activity monitoring; and

k) updating its cyber incident response procedures,

mean that as of 31 December 2024, 23andMe had implemented appropriate technical and organisational measures to ensure a level of security for Customer Personal Data which was appropriate in light of the risks posed by the processing it performs, as required by Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR. Therefore, the Commissioner finds that the Infringements were no longer ongoing as of this date.

304. 23andMe's failure to implement appropriate technical and organisational security measures throughout the Relevant Period placed its customer's personal data at risk of unauthorised access and use over an extended period of time, as demonstrated by the Data Breach.

305. Therefore, the Commissioner finds that the extended duration of the Infringements are a further indication of their seriousness as they exposed 23andMe customers to an increased risk of harm to their rights and freedoms in relation to their personal data over a significant period of time.

(b) The intentional or negligent character of the Infringements (Article 83(2)(b) UK GDPR)

306. The Commissioner finds that the Infringements are negligent, rather than intentional, in nature because 23andMe unintentionally breached the duty of care it owed to its customers pursuant to the UK GDPR and DPA 2018.[282] Pursuant to Article 24(1) and (2) UK GDPR, controllers are responsible for implementing appropriate technical and organisational measures to enable and allow them to demonstrate that processing is performed in accordance with the UK GDPR, including, where proportionate, the implementation of appropriate data protection policies. It follows that 23andMe is responsible for ensuring that Customer Personal Data is processed in a manner that ensures an appropriate level of security of that personal data, including protection against unauthorised or unlawful processing (Article 5(1)(f) UK GDPR) and through the use of appropriate technical and organisational security measures (Article 32(1) UK GDPR).

307. Negligent infringements can be serious and the *Fining Guidance* indicates that the Commissioner may decide to issue a penalty notice in cases where a controller or processor is found to have acted

[282] Fining Guidance, Paragraph 66

negligently.[283]

308. When assessing 23andMe's negligence, the Commissioner has considered all of the relevant evidence regarding whether it breached the duty of care it owed to its customers, taking into account the specific circumstances of this case.[284]

309. The Commissioner considers that when taking into account the sensitivity of the personal data processed by 23andMe, including special category data; the fact that the company's processing operations were intended to facilitate the sharing of information between customers; and the risk of significant damage or distress resulting from a personal data breach affecting the Platform, 23andMe could reasonably have been expected to have implemented appropriate measures to prevent unauthorised access to customer accounts and to enable the prompt detection of and effective response to any incident which compromised, or potentially compromised, the integrity and confidentiality of Customer Personal Data.

310. The Commissioner also finds that the Infringements resulted from 23andMe's failure to implement technical and organisational security measures which included basic protections, such as mandatory MFA, which are widely recommended by regulators and other public agencies, including the ICO and NCSC. Prior to the Data Breach, 23andMe also failed to carry out any form of simulation or penetration testing which focused on credential stuffing attacks, despite this being recognised in the OWASP top-10 web-application security risks since 2003.[285]

311. In addition, the Commissioner finds that 23andMe negligently failed to

[283] Fining Guidance, Paragraph 63
[284] Fining Guidance, Paragraph 67
[285] The NCSC recommends that organisation use the OWASP top-10 list of security risks when developing their applications and states that defending against these risks should be considered throughout the development of the system - Building and operating a secure online service - NCSC.GOV.UK (accessed 5 February 2025)

respond in an appropriate and timely manner when it first received indications in July and August 2023 that the Platform had been subject to personal data breach. The July Login Spike, the July Attempted Profile Transfer and the August 2023 Messages were all dealt with by 23andMe's security team as isolated incidents and a detailed internal investigation was not commissioned until October 2023. In particular, the August 2023 Messages featured explicit claims that a widescale personal data breach had occurred and that Customer Personal Data was being sold on the dark web.[286] However, the August 2023 Messages were not linked to the July Login Spike or the July Attempted Profile Transfer, a full investigation was not commissioned, the claims were dismissed as a "*hoax*" within four days and no review of the company's technical and organisational security measures was undertaken, despite the increasing evidence of a risk to Customer Personal Data.[287]

312. Furthermore, the failure to update 23andMe's technical and organisational security measures following the receipt of the August 2023 Messages must be considered in the context of the almost simultaneous discussions relating to the launch of the Total Health service, which indicated that 23andMe's senior management were aware of security risks affecting the Platform and the deficiencies in 23andMe's technical and organisational security measures. Specifically, 23andMe's Chief Product Officer highlighted security concerns related to the profile transfer and Raw Genetic Data download features, referred to the potential value of 23andMe customers' genetic data to malicious actors and recognised that MFA would be the most effective means of improving the security of customers' accounts.[288] However, despite these concerns being raised and recommendations being made

[286] Letter from Greenberg Traurig LLP to the ICO and OPC, 23 October 2024 (responding to letters from the ICO and OPC dated 20 September and 11 October 2024 (See Exhibit AL)
[287] Letter from Greenberg Traurig LLP to the ICO and OPC, 23 October 2024 (responding to letters from the ICO and OPC dated 20 September and 11 October 2024 (See Exhibit AL)
[288] Letter from Greenberg Traurig LLP to the ICO and OPC, 17 January 2025: Exhibit AS

regarding how to strengthen the security of 23andMe customers' accounts, 23andMe failed to take steps to ensure that its technical and organisational security measures were appropriate in light of the risks posed to Customer Personal Data.

313. Therefore, the Commissioner finds that whilst the Infringements are negligent, rather than intentional, in nature, they nonetheless constitute a serious breach of the duty of care 23andMe owes to its customers in respect of the protection of their personal data.

(c) Categories of personal data affected (Article 83(2)(g) UK GDPR)

314. The categories of personal data affected by the Infringements are also relevant to the assessment of its seriousness. In particular, the Commissioner considers infringements of data protection legislation which involve the processing of special category data to be particularly serious because the UK GDPR makes clear that such data merits specific protection.[289]

315. As stated at paragraph 122 above, during the Relevant Period 23andMe processed special category data, within the meaning of Article 9(1) UK GDPR. Specifically, 23andMe processed genetic data supplied by customers who submitted their DNA to 23andMe when completing saliva testing kits and data concerning health in the form of self-reported health conditions, as well as 23andMe generated Health Reports in respect of customers who subscribed to the "*Health + Ancestry*" or "*23andMe+ Premium*" services.

316. 23andMe reported that the threat actor accessed the Raw Genetic Data

[289] Paragraph 71 of the Fining Guidance states that "*The Commissioner is likely to consider infringements involving the processing of* special category data within the meaning of Article 9(1) UK GDPR). This accords with Recital 51 to the UK GDPR, which states that *"Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.* [This] *personal data should include personal data revealing racial or ethnic origin."*

of two Affected UK Data Subjects in the course of the Data Breach.[290] Furthermore, whilst 23andMe's analysis indicates that the threat actor did not download Raw Genetic Data relating to any Affected UK Data Subjects, as the threat actor had demonstrated their ability to successfully access credential stuffed accounts, the Commissioner finds that the integrity and confidentiality of Raw Genetic Data relating to Affected UK Data Subjects whose accounts were credential stuffed was nonetheless compromised.

317. Moreover, it is clear that special category data includes not only personal data that explicitly relates to the categories of information specified in Article 9(1) UK GDPR, but also personal data which reveals or concerns those categories of information, including where the data allows inferences to be drawn about a data subject which fall within the categories specified in Article 9(1) UK GDPR.[291]

318. The Commissioner finds that the personal data contained within customers' accounts which is processed for the purposes of matching customers within the DNA Relatives, Family Tree and Connections features of the Platform may also be regarded as special category data, as the processing of such personal data enables, and is in fact intended, to allow inferences to be drawn regarding the shared racial or ethnic origin of matched customers, thus bringing it within the scope of Article 9 UK GDPR.

[290] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 60
[291] By analogy, in Judgment of 4 October 2024, *ND v DR (Lindenapotheke) C-21/23, EU:ECLI:2024:846*, at [82] – [83] the Court of Justice of the European Union ("CJEU"), held that Article 9(1) GDPR cannot be interpreted to mean that the processing of personal data which only indirectly reveals sensitive information about a natural person is exempt from the increased level of protection afforded to special category data. Therefore, in the view of the CJEU, personal data will be considered special category data where it is possible to infer from it, by association or deduction, information within the categories specified in Article 9(1) GDPR. Although CJEU judgments are no longer binding following the UK's exit from the European Union, pursuant to section 6(2) of the European Union (Withdrawal) Act 2018, UK courts and tribunals may have regard to them so far as they are relevant to the matter before the court of tribunal.

319. The Commissioner regards this as significant in this context, as the threat actor appeared to have specifically targeted 23andMe customers of particular ethnic or racial origins, including those of an Ashkenazi Jewish background. For example, the BreachForums Post Dated 17 October referred to prominent Jewish families and an alleged Israeli attack on a hospital.

320. The Commissioner considers that 23andMe should have specifically considered its processing of special category data when deciding on what level of technical and organisational measures were appropriate in order to ensure the integrity and confidentiality of its processing systems and services pursuant to Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR.

321. In addition, the Commissioner considers that the adequacy and appropriateness of such measures should have been reassessed following the receipt of the August 2023 Messages and the associated posts identified by 23andMe's Cyber Incident Response Team which contained explicit references to inferences drawn regarding connected customers' common Ashkenazi Jewish ancestry and indicated that Customer Personal Data was being offered for sale on the dark web.

322. Therefore, the Commissioner finds that the highly sensitive nature of the personal data processed by 23andMe, which was placed at risk as a result of the lack of appropriate technical and organisational security measures, constitutes further evidence of the seriousness of the Infringements.

Conclusion on the seriousness of the Infringements

323. Having considered the nature, gravity and duration of the Infringements, as well as their negligent nature and the categories of personal data affected, the Commissioner has categorised the Infringements as having a high degree of seriousness.

324. In reaching his conclusion, the Commissioner has allocated particular weight to:

a) the extent of 23andMe's failure to implement appropriate technical and organisational security measures, particularly when taking into account applicable guidance and best practice throughout the Relevant Period and the multiple incidents which ought reasonably to have led to 23andMe reviewing and revising such measures;

b) the nature of 23andMe's processing activities, including the processing of genetic data, data relating to health and inferred special category data;

c) the direct links between the Infringements and the purposes of 23andMe's processing activities, specifically the use of customer personal data to reveal further information about them and facilitate the sharing of highly sensitive personal data between large numbers of customers, and the importance of such processing to 23andMe's business model;

d) the extended duration of the Infringements, which resulted in the integrity and confidentiality of the majority of 23andMe customers' personal data being placed at risk of unauthorised access and use for a significant period of time;

e) the documented evidence of actual non-material damage suffered by Affected UK Data Subjects as a result of the Infringements and the ongoing potential for further, serious material or non-material harm to be suffered; and

f) the negligent nature of the Infringements, specifically the clear breach of the duty of care owed by 23andMe to its customers in respect of maintaining the integrity and security of their personal data.

Relevant aggravating and/or mitigating factors:

(a) Any action taken by the controller or processor to mitigate the damage suffered by the data subjects (Article 83(2)(c) UK GDPR)

325. Paragraph 77 of the *Fining Guidance* states: "*The Commissioner is more likely to take into account measures implemented prior to the controller or processor becoming aware of the Commissioner's investigation as a mitigating factor. Measures that are only implemented after the start of the Commissioner's investigation are less likely to be regarded as a mitigating factor.*"

326. 23andMe's initial response to the Data Breach is set out at paragraphs 62 – 83 above.

327. 23andMe also informed the Commissioner that it searched for and requested the removal of Customer Personal Data from dark web sites. The Commissioner understands that 23andMe believed that these requests were actioned in some cases, but notes that there is no objective means of verifying how successful 23andMe were in ensuring the removal of Customer Personal Data from the dark web.

328. Under Article 34(1) UK GDPR, a controller is required to inform data subjects whose personal data has been affected in a personal data breach, without undue delay, if it is likely to result in a high risk to their rights and freedoms. The communication sent by the controller to the affected data subjects must include the information relating to the personal data breach and the measures taken, or which the controller proposes to take in response which are referred to in Article 33(3)(b), (c) and (d) UK GDPR.[292]

329. On 6 October 2023, 23andMe created a public blog discussing the details and impacts of the Data Breach, as well as recommending steps customers could take to keep their accounts and passwords secure,

[292] Article 34(2) UK GDPR

including the use of strong, unique passwords and enabling MFA.[293] The blog was updated as more information about the Data Breach was discovered during the course of the Internal Investigation, with the final update dated 5 December 2023.[294]

330. 23andMe informed the Commissioner that it met with numerous impacted individuals to respond to their questions relating to the Data Breach and offered dark web monitoring.[295] 23andMe's Data Privacy Officer subsequently clarified that dark web monitoring was only offered to a limited number of customers who contacted the company about the Data Breach and where it was deemed to be appropriate on the basis of the nature of the customer's enquiry and the specific impact the Data Breach had on them.[296]

331. In addition to the public blog on the 23andMe website, between 10 October 2023 and 30 January 2024, 23andMe sent a series of emails to the customers it believed had been affected by the Data Breach.[297]

332. The content of these emails varied, but those initially sent in October 2023 to all current or former customers whose DNA Relatives profile data had either been posted on the dark web, or was deemed to have been accessed by the threat actor included a high-level description of the Data Breach, a link to the type of information which may be found within a DNA Relatives profile, details of 23andMe's initial response to the Data Breach and recommendations as to what steps the customers could take in order to enhance the security of their accounts, including

[293] Addressing Data Security Concerns - Action Plan - 23andMe Blog
[294] Addressing Data Security Concerns - Action Plan - 23andMe Blog
[295] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 61
[296] Interview with [redacted] (23andMe Data Privacy Officer and Senior Product Counsel) on 20 November 2024
[297] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to question 58 and Exhibit C

avoiding repeat use of passwords and enabling MFA.[298]

333. Whilst the Commissioner acknowledges that 23andMe took steps to inform Affected UK Data Subjects of the Data Breach, he also finds that these emails failed to fully inform the affected data subjects of the nature of the Data Breach to the extent required by Article 34(2) UK GDPR. Specifically, the email notifications sent by 23andMe to its customers prior to January 2024 did not:

a) include the period within which the Data Breach occurred. Whilst some of the emails included the date upon which the threat actor posted samples of Customer Personal Data on the dark web, 23andMe did not include the period during which the threat actor accessed Customer Personal Data;

b) disclose the possibility that Raw Genetic Data and other special category data may have been accessed by the threat actor. Whilst 23andMe did not confirm that Raw Genetic Data had been accessed by the threat actor until the conclusion of the Internal Investigation in December 2023,[299] 23andMe was aware of the possibility that such data had been compromised, not least as a result of the claims made in the threat actor's posts on the dark web. The seriousness with which 23andMe treated this possibility was demonstrated by the fact that it disabled the Raw Genetic Data download feature on 2 November 2023, prior to the Internal Investigation confirming that such data had been accessed and, in some cases, downloaded by the threat actor.[300] The potential for Raw Genetic Data to have been accessed by the threat actor significantly impacted upon the likely consequences of the Data Breach, which 23andMe was

[298] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Exhibit C
[299] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to question 54
[300] Letter from Greenberg Traurig LLP to the ICO and OPC, 26 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to question 12

required to describe when notifying data subjects pursuant to Article 34(2) UK GDPR;[301] or

c) provide any information as to what could happen as a result of the personal data exfiltrated by the threat actor becoming public. Article 33(3)(c) UK GDPR and Article 34(2) UK GDPR required 23andMe to describe the likely consequences which could result from the Data Breach when notifying Affected UK Data Subjects. Whilst 23andMe did alert customers to the fact that the threat actor had posted samples of Customer Personal Data on the dark web, the Commissioner's view is that 23andMe was required to provide a greater level of detail as to the potential consequences for Affected UK Data Subjects, particularly in light of the sensitivity of the data involved.

334. The Commissioner's view is that 23andMe's response to the identification and verification of the Data Breach did not fully reflect the urgency of the situation and had only a limited, if any, effect on mitigating the damage suffered by Affected UK Data Subjects. However, the Commissioner also acknowledges that 23andMe did investigate and take steps in response to the July Attempted Profile Transfers and that the measures taken in response to the Data Breach were ultimately successful in bringing to an end the threat actor's unauthorised access to Customer Personal Data. Therefore, following consideration of 23andMe's representations, the Commissioner finds that the action 23andMe took in an attempt to mitigate the damage to Affected UK Data Subjects should be treated as a neutral factor, rather than an aggravating factor.

335. As stated at paragraph 303 above, 23andMe informed the Commissioner

[301] Article 34(2) UK GDPR requires communications sent to affected data subjects to include, inter alia, the information specified in Article 33(3)(c), namely, "*the likely consequences of the personal data breach.*"

of the additional security measures that it had implemented as of 31 December 2024. However, whilst the Commissioner considers that these measures, when assessed collectively, mean that as of 31 December 2024, 23andMe's processing is compliant with Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR, they are focused on reducing the likelihood of a similar event occurring in the future, or at least limiting its impact. Therefore, the Commissioner finds that such measures should not be regarded as attempts to mitigate the damage suffered by data subjects as a result of the Infringements. Consequently, such steps will not be treated as a mitigating factor.

(b) The degree of responsibility of the controller or processor (Article 83(2)(d) UK GDPR)

336. At paragraph 81, the *Fining Guidance* refers to the level of accountability expected of controllers and processors under the UK GDPR and indicates that it is more likely that the degree of responsibility will be considered an aggravating, or, at most, a neutral factor.[302]

337. Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR require 23andMe to implement technical and organisational security measures which ensure a level of security which is appropriate in light of the sensitivity of the personal data it processes and the nature, purpose and context of its processing operations.

338. When assessing the appropriateness of such measures, the Commissioner considers that it is necessary to have regard, in particular, to:

a) the significant volumes of highly sensitive special category data processed by 23andMe;

b) the risks posed by the processing of such special category data to the fundamental rights and freedoms of 23andMe customers in the

[302] Relevant aggravating or mitigating factors | ICO

event of a personal data breach;[303]

c) the nature and purposes of 23andMe's processing, specifically the processing of sensitive personal data, including special category data, to enable its customers to learn about their genetic, racial and ethnic origins, and connect and share such information with their genetic relatives; and

d) the reasonable expectations of 23andMe customers regarding the measures in place to protect the personal data they shared with the company and their genetic relatives.

339. When assessing 23andMe's degree of responsibility for the Infringements, the Commissioner has considered the extent to which 23andMe did what it could be expected to do in terms of implementing technical and organisational security measures, taking into account its size and resources and the nature and purposes of its processing.[304] The Commissioner finds that in light of 23andMe's position as a leading global provider of direct-to-consumer genetic testing services, its technical capacity to implement appropriate security measures, the nature of its processing activities, including the processing of highly sensitive personal data, and the importance of the relevant processing to its business model, its responsibility for the Infringements should be regarded as an aggravating factor.

(c) Any relevant previous infringements by the controller or processor (Article 83(2)(e) UK GDPR)

340. The Commissioner is not aware of any relevant previous infringements of the UK GDPR or DPA 2018 committed by 23andMe. Therefore, this factor is not relevant to the Commissioner's decision.

(d) The degree of cooperation with the Commissioner (Article 83(2)(f)

[303] Article 32(2) UK GDPR
[304] Fining Guidance, Paragraph 79

UK GDPR)

341. Pursuant to Article 31 UK GDPR, controllers and processors are required to cooperate with the Commissioner, on request, in the performance of his tasks. The Commissioner's tasks include the monitoring and enforcement of the UK GDPR[305] and the conduct of investigations into the application of the Regulation.[306] Such cooperation may include, for example, responding to requests for information and attending meetings. The Commissioner considers that as this duty of cooperation is required by law, meeting this standard should not be regarded as a mitigating factor. [307]

342. Paragraph 89 of the *Fining Guidance* states that "*the Commissioner may view persistent and repeated behaviour that delays regulatory action as an aggravating factor. Examples of such behaviour include not engaging with the Commissioner during the investigation or repeatedly failing to meet deadlines set by the Commissioner without reasonable excuse.*"

343. 23andMe responded to requests for information during the Commissioner's investigation. However, 23andMe:

a) failed, on occasion, to provide information in the format explicitly requested by the ICO and the OPC;

b) frequently failed to respond to enquiries within the specified timescales; and

c) requested multiple extensions to deadlines citing staff absences, ongoing legal proceedings in the US and a reduction in workforce numbers.

344. 23andMe's responses to the Commissioner's enquiries were, at times, insufficiently detailed, necessitating multiple follow-up questions and

[305] Article 57(1)(a) UK GDPR and s.115(2)(a) DPA 2018
[306] Article 57(1)(h) UK GDPR and s.115(2)(a) DPA 2018
[307] Fining Guidance, Paragraph 87

requests for clarification in order to obtain the information required. 23andMe's responses to such follow-up questions and requests for clarification often revised or amended previous responses, which, in some cases, resulted in a substantially different position being put forward to that which had earlier been set out. This not only created confusion, but also created uncertainty as to the validity and accuracy of the information provided to the Commissioner.

345. For example, 23andMe initially stated that during the Internal Investigation it had identified suspicious Raw Genetic Data downloads by searching for download events instigated from an IP address associated with the threat actor which occurred within one hour of a known threat actor login, with the one hour period used because 23andMe automatically logs customers out of the Platform after one hour of inactivity.[308] However, 23andMe later revised this response, stating that "*if the web request* [to download Raw Genetic Data] *was made within 6 hours, 23andMe marked it as downloaded by the threat actor.*"[309]

346. 23andMe also delayed the disclosure of key information which was of direct relevance to the Commissioner's investigation. For example, in relation to the process used to attribute Raw Genetic Data downloads to the threat actor, 23andMe did not disclose the error that meant that the actual IP address associated to a download event was not recorded in its database until its response to a request for clarification on 10 September 2024,[310] despite 23andMe having multiple opportunities to

[308] Letter from Greenberg Traurig LLP to the ICO and OPC, 13 August 2024 (response to a letter from the ICO and OPC dated 20 June 2024): Response to question 35 and Letter from Greenberg Traurig LLP to the ICO and OPC, 10 September 2024 (response to letters from the ICO and OPC dated 20 June and 21 August 2024): Response to request for additional materials (2)
[309] Letter from Greenberg Traurig LLP to the ICO and OPC, 22 November 2024: Responses to undertakings given at interviews carried out on 18, 19 and 20 November 2024
[310] Letter from Greenberg Traurig LLP to the ICO and OPC, 10 September 2024 (response to letters from the ICO and OPC dated 20 June and 21 August 2024): Response to request for additional materials (2)

provide this highly relevant information to the Commissioner prior to this point.

347. 23andMe also failed to inform the Commissioner of the August 2023 Messages until 23 October 2024,[311] when this information should have been included in the First and Second Data Breach Report Forms.[312]

348. Furthermore, whilst 23andMe agreed to the ICO and OPC conducting interviews by video call with senior 23andMe employees in November 2024, the interviews were repeatedly delayed on the grounds of a lack of availability. 23andMe later informed the Commissioner that the delays were due to a significant workforce reduction which was approved by the company's Board of Directors on 8 November 2024 and resulted in the closure of substantially all of 23andMe's therapeutics operating division and an overall headcount reduction in excess of 200 employees, representing approximately 40% of the workforce at the time.[313] 23andMe also failed to put forward [redacted], its Chief Product Officer, for interview, despite the Commissioner having seen internal documentation in which [redacted] raised a number of security concerns relating to the Platform and advocated for the implementation of mandatory MFA in advance of the launch of the 23andMe Total Health service in August 2023.[314]

349. The Commissioner has considered the broader circumstances facing 23andMe during the period of the investigation. In its Written Representations and at the Oral Hearing 23andMe highlighted that in

[311] Letter from Greenberg Traurig LLP to the ICO and OPC, 23 October 2024 (response to letters from the ICO and OPC dated 20 September and 11 October 2024): Exhibits AA – AF and AH - AJ
[312] Article 33(3)(a) UK GDPR requires a notification of a personal data breach to describe the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned. The Commissioner finds that the August 2023 Messages were indicative of the overall nature of the Data Breach and should therefore have been disclosed within 23andMe's initial personal data breach reports
[313] 23andMe Written Representations, 18 April 2025: Paragraphs 17 and 24
[314] Letter from Greenberg Traurig LLP to the ICO and OPC, 17 January 2025: Exhibit AS

addition to responding the Commissioner's investigation, it was simultaneously:

a) defending numerous class action and arbitration claims in the US, Canada and the UK;

b) engaged in multiple investigations initiated by US regulators; and

c) dealing with the resignation of the company's entire Board of Directors in September 2024.

350. 23andMe also highlighted how its ability to respond to the Commissioner's enquiries was inhibited by the departure of key employees involved in the Internal Investigation, including the data protection officer and chief information security officer.[315]

351. The Commissioner finds that the lack of cooperation on the part of 23andMe would, in normal circumstances, be regarded as an aggravating factor. However, following consideration of the representations made by 23andMe in response to the NOI, the Commissioner considers that the extreme financial and commercial challenges experienced by 23andMe during the period of the investigation represent exceptional circumstances which must be taken into account when assessing 23andMe's compliance with its obligations under Article 31 UK GDPR. Therefore, the Commissioner finds that 23andMe's level of cooperation should be treated as a neutral factor.

(e) The manner in which the Infringements became known to the Commissioner (Article 83(2)(h) UK GDPR)

352. Article 33(1) UK GDPR requires a controller to notify the Commissioner of a personal data breach without undue delay and, where feasible, within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of data subjects. Where the

[315] 23andMe Written Representations, 18 April 2025: Paragraphs 18 - 20

notification is not made within 72 hours of the controller becoming aware of the breach, it must be accompanied by reasons for the delay.

353. 23andMe initially notified the Commissioner of a personal data breach on 15 October 2023,[316] 10 days after it verified the reports of the Data Breach in the Subreddit Post as genuine and 14 days after it was first alerted to the Subreddit Post in which Customer Personal Data was offered for sale. The delay was attributed to the fact that it took 23andMe until 12 October 2023 to determine what personal data and which customers had been affected and to identify the regulators it was required to notify.[317] Therefore, whilst the submission of 23andMe's first notification relating to the Data Breach fell outside the statutory 72 hour window, the Commissioner finds that 23andMe has provided an explanation for this delay, as required by Article 33(1) UK GDPR.

354. Article 33(3)(a) and (c) UK GDPR require a notification of a personal data breach to include a description of the nature of the personal data affected and the likely consequences of the breach. However, the First and Second Breach Report Forms failed to refer to the possibility that Raw Genetic Data may have been compromised. 23andMe sought to explain this omission by stating that it was only after the conclusion of the Internal Investigation in December 2023 that it was able to confirm that Raw Genetic Data had been accessed and, in some cases, downloaded by the threat actor.[318] However, the Commissioner finds that this is indicative of a misunderstanding of the requirements of Article 33(3)(c) UK GDPR, which specifically requires the controller to provide a description of the likely consequences of the breach.

355. The Commissioner considers that 23andMe was required to disclose the fact that there was at least the potential for Raw Genetic Data to have

[316] First Data Breach Report Form
[317] First Data Breach Report Form
[318] Letter from Greenberg Traurig LLP to the ICO and OPC, 16 July 2024 (responding to a letter from the ICO and OPC dated 20 June 2024): Response to question 56

been affected when it first notified the Commissioner of the Data Breach in October 2023. The disclosure of this information in October 2023 could have allowed the Commissioner's investigation to be expedited and could potentially have avoided, or at least mitigated, some of the challenges that the Commissioner encountered during the investigation, including the departure of multiple senior individuals from relevant roles at 23andMe in the period between the discovery of the Data Breach and the opening of the Commissioner's investigation.

356. The Commissioner finds that 23andMe's failure to include reference to the potential for Raw Genetic Data to have been accessed or downloaded by the threat actor in the First and Second Data Breach Report Forms delayed and rendered more difficult the Commissioner's investigation of the Infringements and should be treated as an aggravating factor.

(f) Measures previously ordered against the controller or processor (Article 83(2)(i) UK GDPR)

357. The Commissioner has not previously imposed measures referred to in Article 58(2) UK GDPR on 23andMe. Therefore, this factor is not relevant to the Commissioner's decision.

(g) Adherence to approved codes of conduct or certification mechanisms (Article 83(2)(j) UK GDPR)

358. There are no relevant codes of conduct or approved certification mechanisms in this case. Therefore, this factor is not relevant to the Commissioner's decision.

(h) Any other applicable aggravating or mitigating factors (Article 83(2)(k) UK GDPR)

359. The Commissioner has considered whether 23andMe benefitted from any financial gain in not implementing appropriate technical and organisational measures to ensure the integrity and confidentiality of its processing operations. The Commissioner considered that 23andMe

would have benefitted from some savings as a result of the Infringements. However, the Commissioner finds that such savings were unlikely to have been significant and therefore this was not deemed to be relevant to the Commissioner's decision to issue a penalty.

360. 23andMe provided the ICO and OPC with copies of the August 2023 Messages which referred to a personal data breach affecting the Platform and threatened the sale of Customer Personal Data on the dark web.[319] These messages coincided with the Hydra Post in which the author claimed to have access to the data of 10 million 23andMe customers and subsequently indicated that the data had been sold to an Iranian national.

361. The [redacted] Ticket indicated that an internal investigation was conducted following the receipt of the August 2023 Messages, but that this involved only a limited examination of the potential personal data breach, and focused on the profiles of the 23andMe CEO and her then husband, before being closed after only four days on the basis that there was "*no evidence of the exfiltration of 10M customers' raw DNA data.*" 23andMe's Security and Engineering Team concluded that whilst there was evidence that "*some data was accessed, it was not to the levels outlined in* [the Hydra Post]" and the claims were considered to be "*an exaggeration of the actual data obtained*,"[320] which did not merit either a more in-depth investigation, nor a wider review of 23andMe's technical and organisational security measures. Furthermore, 23andMe did not consider the possibility that the July Login Spike and the July Attempted Profile Transfers could have been linked to the alleged personal data breach which was referred to in the August 2023 Messages.

362. On the basis of this information, the Commissioner finds that, as of 14

[319] Letter from Greenberg Traurig LLP to the ICO and OPC, 23 October 2023 (Exhibits AA, AB, AC, AD, AE, AF, AH and AI)
[320] Letter from Greenberg Traurig LLP to the ICO and OPC, 23 October 2023 (Exhibit AL)

August 2023, 23andMe was aware, or was at least in possession of significant volume of evidence of a personal data breach affecting the Platform. However, 23andMe failed to launch a full investigation, did not report the incidents to appropriate regulators, including the Commissioner, and did not reconsider whether its technical and organisational measures were appropriate to ensure the integrity and confidentiality of its processing systems and services in light of the cumulative indicators of unauthorised access to Customer Personal Data. As at the date of this Penalty Notice 23andMe continues to maintain that there was *"no indication of unauthorised access"* at the time.[321]

363. The Commissioner finds that 23andMe's failure to connect or fully investigate evidence of the threat actor's activity in August 2023 Messages, its failure to commission an investigation or review the security measures in place on the Platform following the receipt of the August 2023 Messages and the delayed disclosure of these incidents to the Commissioner should be regarded as an aggravating factor.

(i) Effectiveness, proportionality and dissuasiveness (Article 83(1) UK GDPR)

364. The Commissioner considers that the imposition of a penalty would be effective as it would represent an appropriate sanction when considering the seriousness of the Infringements and would emphasise to 23andMe the importance of complying with its obligations under Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR.

365. Taking into account:

a) the seriousness and duration of the Infringements;

b) the highly sensitive nature of the personal data processed by

[321] Letter from Greenberg Traurig LLP to the ICO and OPC, 17 January 2025

23andMe;

c) the scale of the company's processing operations;

d) 23andMe's position as a multinational provider of direct-to-consumer genetic testing services;

e) the nature and purposes of its processing;

f) the distress caused to Affected UK Data Subjects; and

g) the potential harm which may have resulted, or which may in future result from the Infringements;

the Commissioner considers that the imposition of a penalty would be proportionate. A penalty would not exceed what is appropriate and necessary in the circumstances of the case to promote compliance with data protection legislation and to provide an appropriate sanction for the Infringements.

366. 23andMe continues to process its customers' personal data. Therefore, the Commissioner considers that there is a need to deter 23andMe from committing any further infringements of Article 5(1)(f) UK GDPR and Article 32 UK GDPR in the future. There is also a need to deter other controllers and processors operating within the genetic testing sector from committing similar infringements.

367. The Commissioner considers that the proposed penalty will also have a general dissuasive effect as it will raise awareness of the need for controllers and processors, both within the sector and more broadly, to ensure that they implement appropriate technical and organisational security measures which take into account the nature, scope, context and purposes of their processing, as well as the risks this poses to the interests and fundamental rights and freedoms of data subjects.

C. The Commissioner's conclusions on whether to impose a penalty

368. In light of the above, the Commissioner has decided to impose a penalty.

VIII. CALCULATION OF THE PROPOSED PENALTY

369. The *Fining Guidance* sets out a five-step approach which the Commissioner proposes to apply to calculate the amount of a penalty:

a) Step 1: An assessment of the seriousness of the infringement.

b) Step 2: Accounting for the turnover (where the controller or processor is part of an undertaking).

c) Step 3: Calculation of the starting point for the penalty having regard to the seriousness of the infringement and, where relevant, the turnover of the undertaking.

d) Step 4: Adjustment to take account of any aggravating or mitigating factors.

e) Step 5: Adjusting the penalty to ensure that it is effective, proportionate and dissuasive,[322] whilst not exceeding the relevant statutory maximum.

370. Whilst the Commissioner has applied this approach, the overall assessment of the appropriate level of penalty which the Commissioner has imposed involved evaluation and judgment, taking into account all the relevant circumstances of the individual case.

Statutory maximum penalty

371. The Commissioner finds that 23andMe infringed Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR.

372. An infringement of Article 5(1)(f) UK GDPR is subject to the higher maximum statutory penalty of £17.5 million, or, in the case of an undertaking, 4% of the worldwide annual turnover in the preceding

[322] As required by Article 83(1) UK GDPR

financial year, whichever is higher.[323]

373. An infringement of Article 32(1) UK GDPR is subject to the standard maximum statutory penalty of £8.7 million, or, in the case of an undertaking, 2% of the worldwide annual turnover in the preceding financial year, whichever is higher.[324]

374. Pursuant to Article 83(3) UK GDPR, if a controller or processor intentionally or negligently, in the course of the same or linked processing operations, infringes several provisions of the UK GDPR, the total amount of any penalty imposed cannot exceed the amount specified for the gravest infringement.[325] Therefore, the Commissioner has based his assessment of the level of the proposed penalty on the higher statutory maximum of £17.5 million, or, in the case of an undertaking, 4% of the worldwide turnover in the preceding financial year.

375. The *Fining Guidance* considers the concept of an undertaking for the purpose of imposing a penalty at paragraphs 23 – 31. Where a controller or processor forms part of an undertaking, the Commissioner will calculate the maximum penalty on the basis of the turnover of the undertaking as a whole. Whether or not an individual controller or processor forms part of an undertaking depends on whether another legal or natural person, for example, a parent company, exercises decisive influence over it.

376. Paragraph 30 of the *Fining Guidance* states:

"*Where a parent company owns all, or nearly all, the voting shares in a subsidiary, there is a presumption that the parent company exercises decisive influence over the subsidiary's conduct. This presumption may be rebutted. However, the burden is on the parent company to provide*

[323] Section 157(1)(a) DPA 2018 and Article 83(5)(a) UK GDPR
[324] Section 157(1)(a) DPA 2018 and Article 83(4)(a) UK GDPR
[325] Also see paragraph 33 of the Fining Guidance

sufficient evidence to demonstrate that the subsidiary acts independently."

377. The relevant legal entity responsible for the Infringements is 23andMe. 23andMe is a wholly-owned subsidiary of 23andMe Holding Co., which is also the parent company of Lemonaid Health Inc. and 23andMe Pharmacy Holdings Inc.[326] Therefore, the Commissioner has relied upon the presumption referred to above that the parent company, 23andMe Holding Co., exercises decisive influence over its wholly owned subsidiary, 23andMe. The Commissioner is therefore entitled to calculate the maximum penalty on the basis of the turnover of 23andMe Holding Co.

378. As 23andMe Holding Co.'s shares were listed for trading on the NASDAQ stock exchange until 31 March 2025, the company's 2023/24 annual report was published and stated that, for the year ending 31 March 2024, it generated turnover of US$219,638,000 (approximately £168,251,493).[327] 4% of this figure is £6,730,060, which is less than the higher maximum statutory penalty of £17.5 million. Therefore, the higher statutory maximum penalty of £17.5 million applies in this case.

A. Step 1: Assessment of the seriousness of the Infringements

379. As set out at paragraphs 109 to 115 of the *Fining Guidance,* the Commissioner determines a starting point for the penalty by first assessing the seriousness of the infringement. The Commissioner categorises the infringement according to its degree of seriousness and then selects a starting point based on a percentage of the relevant applicable statutory maximum.

380. As stated at paragraph 323 of this Penalty Notice, the Commissioner has categorised the Infringements as having a high degree of seriousness.

[326] Letter from Greenberg Traurig LLP to the ICO and OPC: Initial Responses to Questions (Tranche 1), 16 June 2024
[327] Microsoft Word - 23andMe 10-K Wrap - 2024 (accessed 5 February 2025)

This means that the starting point will be between 20% and 100% of the relevant statutory maximum.

381. The Commissioner finds that the Infringements warrant a starting point of 60% of the statutory maximum. A starting point lower than 60% is not warranted due to the seriousness of the Infringements, as determined by reference to their nature, gravity and extended duration; the sensitive nature of the personal data affected; and the nature and purposes of the processing performed by 23andMe. The Commissioner's full assessment of the seriousness of the Infringements is set out at paragraphs 258 to 324 above.

382. In deciding that a starting point higher than 60% is not warranted in the circumstances of this case, the Commissioner has taken into account the fact that the Infringements were not committed intentionally.

B. Step 2: Accounting for turnover

383. Having assessed the seriousness of the infringement, the Commissioner next determines any adjustments to account for turnover, as set out in paragraphs 116 to 129 of the *Fining Guidance*. This step permits the Commissioner to adjust the starting point to reflect the size of the undertaking.

384. Paragraph 121 of the *Fining Guidance* states that "*the relevant turnover of the undertaking for the purpose of calculating the maximum amount of the fine is the total worldwide turnover in its previous financial year,*" whilst paragraph 123 further provides that "*the Commissioner will generally base turnover figures used for the purpose of calculating the fine on the consolidated turnover recorded in the undertaking's audited accounts.*"

385. As referred to in paragraph 378 above, 23andMe Holding Co.'s turnover for the year ending 31 March 2024 was US$219,638,000 (approximately £168,251,493). However, the *Fining Guidance* also states that "*the*

Commissioner may adjust the turnover figure used to ensure it reflects the true scale of the undertaking (for example, by using more recent management accounts or forecast figures where available."[328] In light of this discretion, the Commissioner has considered 23andMe Holding Co.'s Form 10-Q, which was filed with the United States Securities and Exchange Commission on 6 February 2025 and documents the company's financial results for the three and nine month periods ending 31 December 2024 (the "**Q3 Filing**").

386. The Q3 Filing recorded a total quarterly turnover of $60,262,000, with a total comprehensive loss of $53,035,000, whilst it also showed that as of 31 December 2024, 23andme held $93,288,00 in cash, cash equivalents and restricted cash, compared to $250,791,000 as of 31 December 2023. The Q3 Filing was submitted shortly before 23andMe Holding Co. and certain of its subsidiaries, including 23andMe Inc, filed voluntary petitions seeking relief under Chapter 11 of Title 11 of the US Bankruptcy Code in the United States Bankruptcy Court of the Eastern District of Missouri.[329] The Q3 Filing stated that "[23andMe Holding Co.] *has incurred significant operating losses as reflected in its accumulated deficit and negative cash flows from operations. As of December 31, 2024,* [23andMe holding Co.] *had an accumulated deficit of $2.4 billion, and unrestricted cash and cash equivalents of $79.4 million.* [23andMe Holding Co.] *will need additional liquidity to fund its necessary expenditures and financial commitments for 12 months after the date that the unaudited interim condensed consolidated financial statements included in this report are issued.* [23andMe holding Co.] *has determined that, as of the filing date of this report, there is substantial doubt about the company's ability to continue as a going concern."*

387. The Commissioner has considered the evidence of the significant

[328] Fining Guidance, paragraph 123
[329] Kroll Restructuring: Administration: 23andMe Holding Co,: Case No. 25-40976 (accessed 9 May 2025)

deterioration in 23andMe Holding Co.'s financial position, as demonstrated in the Q3 Filing and the petition for relief under Chapter 11 of the US Bankruptcy Code. In accordance with paragraph 123 of the *Fining Guidance,* the Commissioner has decided that in order to reflect 23andMe's current financial position it is appropriate to calculate the starting point for the penalty on the basis of 23andMe Holding Co.'s projected annual turnover, as calculated by reference to the latest financial results recorded in the Q3 Filing. At the Oral Hearing, 23andMe projected that 23andMe Holding Co.'s annual turnover for its 2025 financial year is likely to be close to the lower end of the £100 - £250 million range.

388. This means that the range of adjustment based on the turnover of the undertaking is between 20% and 50%.[330]

389. As set out in paragraph 128 of the *Fining Guidance*: "*the Commissioner is likely to choose a higher amount for undertakings with higher turnover within the applicable range. However, these ranges are only indicative. The Commissioner will reach a decision on a case-by-case basis as to whether it is appropriate to adjust the starting point of the fine in this way, having regard to the need for the fine to be effective, proportionate and dissuasive. Therefore, the Commissioner retains the discretion to impose a fine up to the applicable statutory maximum.*"

390. In this case, the projected turnover of 23andMe Holding Co. is expected to fall close to the lower end of the applicable range (£100 million to £250 million) specified in the *Fining Guidance*.[331] Therefore, following consideration of 23andMe's representations in respect of the current size of the 23andMe Holding Co. undertaking, the deterioration in its financial position and its projected turnover for its 2025 financial year, the

[330] Fining Guidance: Table B: Ranges for adjustment based on the turnover of the undertaking
[331] Step 2: Accounting for turnover | ICO: Table B: Ranges for adjustment based on the turnover of the undertaking

Commissioner has reduced the turnover adjustment factor from 35%, as specified in the NOI, and now finds that a factor of 20% should be applied in this case.

C. Step 3: Calculation of the starting point

391. The starting point for the penalty is calculated as follows: higher statutory maximum amount (£17.5 million) x turnover adjustment (20%) x adjustment for seriousness (60%) = £2,100,000.

D. Step 4: Adjustment to take into account any aggravating or mitigating factors

392. The Commissioner next takes into account any aggravating or mitigating factors. These factors may warrant an increase or decrease in the penalty calculated at the end of Step 3 (the starting point of £2,100,000).

393. On this occasion, the Commissioner has decided to account for the aggravating factors considered at paragraphs 325 to 363 above, by applying an increase of 10% to the starting point calculated at Step 3. Therefore, the proposed penalty increases to **£2,310,000**.

394. In the NOI, the Commissioner provisionally applied an increase of 25% to account for aggravating factors. However, after considering 23andMe's representations, the Commissioner finds that the measures taken by 23andMe to mitigate the harm which resulted from the Data Breach and 23andMe's level of cooperation should be treated as neutral, rather than aggravating factors. Therefore, the Commissioner has reduced the increase in the penalty to 10% increase in order to account for the remaining aggravating factors, specifically:

a) the deficiencies in the content of the First and Second Breach Report Forms sent by 23andMe to the Commissioner regarding the Data Breach in October 2023;

b) 23andMe's degree of responsibility for the Infringements when

taking into account the extent of its failure to implement appropriate technical and organisational security measures as required by Article 5(1)(f) UK GDPR and Article 32(1) UK GDPR; and

c) 23andMe's multiple failures to review and revise its technical and organisational security measures despite increasing evidence of a significant risk to the integrity and confidentiality of Customer Personal Data.

E. Step 5: Adjustment to ensure the penalty is effective, proportionate and dissuasive

395. As set out in paragraph 142 of the *Fining Guidance*, "*The aim of Steps 1 to 4 of the calculation is to identify a fine that is effective, proportionate and dissuasive. The purpose of Step 5 is to provide the opportunity for the Commissioner to check that is the case.*"

396. The Commissioner considers that a penalty of £2,310,000 will be effective, proportionate and dissuasive. A penalty in this amount will have a genuine deterrent effect, taking into account both the specific deterrent to 23andMe and the general deterrence to other organisations.

397. The penalty amount is designed to reflect the serious nature of the Infringements, especially when considered in the context of the extent of 23andMe's failure to implement appropriate technical and organisational security measures, the nature and purposes of its processing, the sensitive nature of the personal data affected, the distress caused to Affected UK Data Subjects and the potential harm which may have resulted from the Infringements.

398. The Commissioner has exercised his judgment and discretion and finds that the proposed penalty is proportionate when taking into account the seriousness of the Infringements, the aggravating factors present in this case, and 23andMe's position as a prominent provider of direct-to-

consumer genetic testing services in multiple countries and territories around the world.

399. The Commissioner considers that the proposed penalty is proportionate to the current financial position of 23andMe and its parent undertaking, 23andMe Holding Co. Specifically, the penalty represents approximately 2.3% of 23andMe Holding Co.'s projected turnover for its 2025 financial year and whilst the Commissioner is aware of the significant deterioration in the financial position of 23andMe Holding Co., he finds that a lower penalty would fail to reflect the seriousness of the Infringements and the significant aggravating factors present in this case.

F. Conclusion - Penalty

400. For the reasons set out above, the Commissioner has decided to impose an administrative penalty on 23andMe, Inc in the amount of **£2,310,000**.

IX. FINANCIAL HARDSHIP

401. The *Fining Guidance* outlines that, in exceptional circumstances, the Commissioner may reduce a penalty where an organisation is unable to pay due to its financial position.

402. The Commissioner has considered 23andMe's representations, including the submission that the company's current financial position constitutes exceptional circumstances which warrant not imposing any monetary penalty. However, the Commissioner considers that the deterioration in 23andMe's and 23andMe Holding Co's financial position, has been adequately accounted for as part of the calculation of the penalty in **Section VIII** above and that the seriousness of the Infringements, as well as the need to provide an effective, proportionate and dissuasive response to the Infringements, justify the imposition of a monetary penalty for the reasons set out in **Section VII(B)** above.

403. Paragraph 152 of the *Fining Guidance* states that the Commissioner will only grant a reduction for financial hardship on the basis of objective evidence that imposing the proposed fine would irretrievably jeopardise an organisation's economic viability. In light of this, when finding that no further reduction to the penalty is necessary on the basis of financial hardship, the Commissioner has taken into account the fact that 23andMe Holding Co, "*is using the Chapter 11 proceedings to facilitate a sale process to maximise the value of its business*" and "*intends to continue operating its business in the ordinary course throughout the sale process.*"[332]

404. Therefore, the Commissioner finds that no further reduction to the penalty should be made on the basis of financial hardship.

X. PAYMENT OF THE PENALTY

405. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by 10 July 2025.

406. Under paragraph 9(1) of Schedule 16 to the DPA 2018, the Commissioner cannot take action to recover a penalty unless:

a) the period specified in this Penalty Notice (i.e. by 10 July 2025) has ended;

b) any appeals against this Penalty Notice have been decided or otherwise ended;

c) if this Penalty Notice has been varied, any appeals against the penalty variation notice have been decided or otherwise ended; and

d) the period for 23andMe to appeal this Penalty Notice, and any variation of it, has ended.

407. Under paragraph 9(2) of Schedule 16 to the DPA 2018, in England and

[332] Kroll Restructuring: Administration: 23andMe Holding Co,: Case No. 25-40976 (accessed 9 May 2025)

Wales, the Commissioner is able to enforce the payment of the penalty. The penalty is recoverable:

a) if the County Court so orders, as if it were payable under an order of that court; or

b) if the High Court so orders, as if it were payable under an order of that court.

XI. RIGHTS OF APPEAL

408. By virtue of section 162 DPA 2018, 23andMe may appeal to the First-tier Tribunal (General Regulatory Chamber) (Information Rights) against this Penalty Notice. 23andMe may appeal to the Tribunal against the amount of the penalty regardless of whether or not it appeals against this Penalty Notice.

409. Information about the appeals process is set out in Annex 2 to this Penalty Notice. Any notice of appeal should be sent or delivered to the Tribunal so that it is received within 28 days of the date of this Penalty Notice.

Dated 5 June 2025

Stephen Bonner
Deputy Commissioner, Regulatory Supervision
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1
DEFINITIONS

The following definitions are provided by 23andMe on its website and relate to the services offered by 23andMe. They are used throughout this Penalty Notice, in addition to those set out in paragraph 28 of the Penalty Notice:

1. "***haplogroups***" are "*genetic classifications or ancestral groupings within a population, typically defined by shared, inherited genetic markers or mutations.*"[333]
2. "***Neanderthal Ancestry Reports***" provide "*information about how much of your ancestry can be traced back to the Neanderthals. The analysis includes the review of over 2,000 genetic variants of known Neanderthal origin that are scattered across the genome*"[334].
3. "***parental inheritance information***" determines how DNA was inherited and displays which portions of a customer's ancestry came from which parent. This forms part of the 23andMe Ancestry Report in circumstances where a biological parent is also on the 23andMe database and shares their information with the customer.[335]
4. "***Health Predisposition Reports***" inform customers if they "*have genetic variants associated with an increased risk of developing certain health conditions but do not report on* [the customer's] *entire genetic profile.*"[336]
5. "***Wellness Reports***" are intended to help customers "*make more informed choices that may relate to healthy living.*" Wellness reports also allow customers to "*learn how* [their] *DNA may influence* [their] *caffeine consumption, lactose digestion and your muscle*

[333] Haplogroups Explained - 23andMe Blog (accessed 5 February 2025)
[334] Neanderthal Ancestry Report Basics – 23andMe Customer Care (accessed 5 February 2025)
[335] DNA Phasing and Inheritance – 23andMe Customer Care (accessed 5 February 2025)
[336] Navigating and Understanding Health Predisposition Reports – 23andMe Customer Care (accessed 5 February 2025)

composition."[337]

6. ***Carrier Status Reports***" inform customers "*about variants that may not affect* [their] *health, but could affect the health of your future family."*[338]
7. "***Pharmacogenetic Reports***" inform customers "*about DNA variants that may influence [their] body's ability to process some medications*."[339].
8. "***exome sequencing***" is defined as "*an advanced, comprehensive genetic testing method that analyses the protein coding regions of* [a customer's] *genome, known as the exome. The exome is where the majority of known genetic variants associated with disease risk are located."* 23andMe use exome sequencing as part of its Total Health service.[340]
9. "***phenotypes***" are "*observable traits*" which "*result from interactions between* [an individual's] *genes and the environment. Differences in some phenotypes, like height, are determined mostly by genes… the influence of genes on other traits, such as personality, is less well understood."*[341]

[337] Getting Started with Your 23andMe Reports – 23andMe Customer Care (accessed 5 February 2025)
[338] Carrier Status Reports – 23andMe Customer Care (accessed 5 February 2025)
[339] Getting Started with Your 23andMe Reports – 23andMe Customer Care (accessed 5 February 2025)
[340] How Exome Sequencing Unlocks Deeper Genetic Insights - 23andMe for Healthcare Professionals (accessed 5 February 2025)
[341] 23andMe - Genetics 101: What are phenotypes? UK (accessed 5 February 2025)

ANNEX 2

DATA PROTECTION ACT 2018 (PART 6, SECTION 162)

RIGHTS OF APPEAL

1. By virtue of section 162(1) DPA 2018, you may appeal to the Tribunal against this Penalty Notice. By virtue of section 162(3) DPA 2018, you may appeal to the Tribunal against the amount of the penalty specified in this Penalty Notice, whether or not you appeal against this Penalty Notice.

2. If you appeal and if the Tribunal considers:

   a) that the notice or decision against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently,

   the Tribunal must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.

3. You may bring an appeal by sending a notice of appeal to the Tribunal at:

   grc@justice.gov.uk

   or

   General Regulatory Chamber
   HM Courts and Tribunals Service
   PO Box 11230
   Leicester
   LE1 8FQ
   UK
   (Telephone: 0300 123 4504)

4. The notice of appeal should be received by the Tribunal within 28 days of the date of this Penalty Notice (which is the date that this Penalty Notice was sent).

5. If your notice of appeal is late, the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule.

6. The notice of appeal **must** include:

   a) your name and address;

   b) the name and address of your representative (if any);

   c) an address where documents may be sent or delivered to you;

   d) the name and address of the respondent (the Information Commissioner);

   e) details of the decision to which the proceedings relate;

   f) the result you are seeking;

   g) the grounds on which you rely;

   h) a full copy of this Penalty Notice; and

   i) (if the notice of appeal is late) a request for an extension of time, giving the reason(s) why the notice of appeal is late and why the Tribunal should accept it.

7. Before deciding whether or not to appeal, you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct their case themselves, or may be represented by any person whom they may appoint for that purpose.

8. The statutory provisions concerning appeal to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the DPA 2018 and The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).

ANNEX 3

RESPONSES TO AN ICO QUESTIONNAIRE FROM AFFECTED UK DATA SUBJECTS

Response 1

1) Are you able to confirm when and describe why you first registered as a customer with 23andMe?

I ordered my kit on the 6th of June 2021, I would've created my account around this time.

I did so as I was interested in finding out any genetic health risks I have, as I do not have contact with my parents or extended family.

2) Are you able to confirm which level of service you had with 23andMe (e.g. Ancestry Service, Health + Ancestry Service or 23andMe+ Premium?

To the best of my knowledge I had the Health + Ancestry service.

3) Please explain when and how you first became aware of the breach. If possible, please confirm what information was provided by 23andMe directly and what you learnt from other sources (eg news reports).

I found out late 2023 that a breach had occurred on several tech link sharing websites (e.g. Hacker News). By my rough understanding they had an information sharing feature between relatives where a subset of your genetic profile would be shared to a related user. Exploiting this allowed a portion of the 23andme user data to be exfiltrated and leaked.

I remember that 23andme were very late to notify users of the breach. I submitted an ICO complaint on the 8th of October 2023, and received a boilerplate notification from 23andme on the 24th of that month which did nothing to reassure me about the security of my PII.

4) Are you able to describe your concerns about the 23andMe breach?

As a past 23andme user, I expected rigorous privacy controls to be in place due to the nature of the information collected. Unlike usernames, passwords and e-mail addresses, you can't change your genetic makeup when a data breach occurs.

Unfortunately, I was left sorely disappointed when news of 23andme's data breach surfaced. Following on from that, further reports in the news of 23andme potentially being sold to a third party leave me deeply concerned about the potential for my genetic records to be misused and shared without my consent. (See https://www.theatlantic.com/health/archive/2024/09/23andme-dna-data-privacy-sale/680057/ for one example).

I do have concerns about my genetic information being shared amongst private companies to make risk assessments on me without my knowledge. With the way large private corporations operate today, I imagine it wouldn't be beyond the realm of possibility.

Whilst I did delete my 23andme account fairly recently, I have serious doubts on whether my genetic records and DNA samples were actually destroyed. From what I've seen, it seems that there is a tendency for US-based companies to flagrantly disregard UK and EU privacy laws. I have no doubt that regardless of any outcome from any investigation or penalties put in place, my genetic information will ultimately make its way to several private companies and foreign entities.

The tech industry, from my own experience as an IT professional, has a tendency to 'move fast and break things', but in matters like this where incredibly sensitive private information is concerned, that doesn't really work.

5) To your knowledge, were any of your relatives also impacted by the breach?

From what I remember no direct relatives used the service.

6) Please explain why you decided to raise your concerns relating to the 23andMe with the ICO?

The ICO I view as one of the only government entities interested in maintaining the privacy of British citizens. I have the utmost respect for what you do, and in any matter like this my first thought is to notify you so you can review as appropriate to hopefully prevent it happening to anyone else.

7) Have you raised concerns with 23andMe directly? If so, what, if any, response have you received?

I have not raised concerns directly, mainly because past experience with large tech companies dictates they'll reply with a boilerplate response and ignore any attempts to get a real answer.

8) Have you raised concerns relating to the 23andMe breach with any other organisation or body?

No, I only considered the ICO at the time.

9) How did you feel when you first became aware of the breach?

Shocked, and violated. I also felt a bit stupid considering how diligent I am about my privacy. In retrospect, it was inevitable this would happen.

10) Would you say that your feelings changed over time at all? If so, if possible, please explain how.

Not really, although I've mostly pushed it to the back of my mind. I've accepted that my information is possibly out there in the wild and there's nothing I can do about it.

11) Have you taken any steps in response to the breach in respect of your 23andMe account?

Yes, I deleted my account after you sent a follow up e-mail this year.

12) Have you taken any steps in response to the breach in respect of any other online accounts?

Over the past year I've deleted as many online accounts as possible, including all big tech social media.

13) Has the breach changed your views about with whom you share your personal information and your approach to doing so?

I'm very careful now about which companies I share PII with, as it seems to be that even with the GDPR in place, a lot of companies choose to ignore it and hold onto your information regardless of the consequences.

14) Is there any additional information that you feel is relevant to your personal experience of the 23andMe data breach and that you would like the ICO to consider?

The main issue I have is how 23andme handled this issue. As a tech worker I know first hand that bugs and mis-designed features can and do happen, this is understandable albeit unfortunate.

The real issue here is they delayed issuing a notice for weeks and left everyone in the dark. Data breaches of this severity should be handled with an immediate response and ability to directly contact the respective company and reach a real human being to answer any questions.

Response 2

1) Are you able to confirm when and describe why you first registered as a customer with 23andMe?

Have asked 23andMe - awaiting reply with details

At the time I registered for 23&Me, genetic technology was relatively novel and although there was a lot of excitement about the potential of the sector, I wanted insights into where the majority of my ancestors came from.

2) Are you able to confirm which level of service you had with 23andMe (e.g. Ancestry Service, Health + Ancestry Service or 23andMe+ Premium?

What level of service did you purchase (eg Ancestry Service, Health + Ancestry Service or 23&me premium) Have asked 23andMe - awaiting reply with details

3) Please explain when and how you first became aware of the breach. If possible, please confirm what information was provided by 23andMe directly and what you learnt from other sources (eg news reports).

I can't quite remember how I became aware of the data breach. I do however remember that once I was aware, I couldn't find details of the breach in local news, which shocked me.

4) Are you able to describe your concerns about the 23andMe breach?

Once I had contacted 23andMe asking whether my data had been compromised, I was disappointed by their response. I asked that my data be removed from their databases. As I understand computing, most individualised records are stored in arrays/databases - I specifically asked that 23andMe delete my data. I didn't want 23andMe to simply hide/prevent my own access to my record under the guise of a user-triggered account "deletion", rather I wanted 23andMe to delete my DNA sequence, destroy any samples it had, remove the added benefit my data had made to any models they have/will have in the future, etc, and no longer process my data.

The idea that my genetic information could be used forever by a possibly incompetent Data Controller, who is one of the biggest corporations on Earth, scared me. No terms and conditions could fairly allow 23andMe to retain my data forever, given the advances in CRISPR (clustered regularly interspaced short palindromic repeats) gene editing, RNAi innovations and 23andMe's data breaches. Given the exponential advances in the technology, such a contract is unreasonable. 23andMe being hacked is one thing, but 23andMe's refusal to respect a data subject's right to request the deletion of their data shows contempt for British law, in my opinion. Has 23anM3 [sic] ever been

audited? I doubt their processes can even facilitate the removal of a genetic contributor's DNA (from their models, etc), which has to be a data compliance issue. It appears as though this company's whole model is to exploit users to create a library of genetic code, then make associations between specific code and correlated real-world traits. The pharmacogenomic potential of 23andMe was expressed in a 23andMe blog on 26 October 2011 (https://blog.23andme.com/articles/a-prescription-for-personalizing-medicine). The fact that 23andMe has lost over 95% of it's peak value and may well sell it's data, should be a concern to every customer in Britain. (And Canada, if your remit extends to this jurisdiction).

Now regarding the hack itself. We should all be concerned that incredibly sensitive information was allegedly accessed nefariously. It is understood that Semitic and Oriental groups were targeted. China has been accused of carrying out genocide on its ethnic Uyghur population. Since 2014, the Chinese government has committed a series of ongoing human rights abuses against Uyghurs and other Turkic Muslim minorities in Xinjiang which has often been characterized as persecution or as genocide (https://en.wikipedia.org/wiki/Persecution_of_Uyghurs_in_China).

Similarly, the conflict between Zionism and the Arab world has resulted in increases in antisemitic violence in the UK. Being able to target a specific group using their DNA data is very concerning. My 23andM3 [sic] account has a Jewish identifier associated with it.

5) To your knowledge, were any of your relatives also impacted by the breach?

According to 23andMe's own website, I have 1500 relatives who are their customers, 719 who are 3-4th cousins - it stands to reason that some were affected to some extent. But in terms of immediate family, not to my knowledge.

6) Please explain why you decided to raise your concerns relating to the 23andMe with the ICO?

I raised my concerns with the ICO because I was concerned that 23andMe had potentially failed in it's responsibilities as a data controller by being hacked, and had failed to process my request to delete all my data from it's systems.

7) Have you raised concerns with 23andMe directly? If so, what, if any, response have you received?

I have raised my concerns with 23andMe and have sent you some of our exchange. There's just too many messages. 23andMe suggested I delete my account, but will not confirm whether this means all my data will be removed.

8) Have you raised concerns relating to the 23andMe breach with any other organisation or body?

I contacted win-no-fee solicitors.

9) How did you feel when you first became aware of the breach?

Concerned.

10) Would you say that your feelings changed over time at all? If so, if possible, please explain how.

I would say that I am more cynical: in the battle that rages between the "Individual" and the "Corporation", the corporation seems to have an advantage in law. People are real, but corporations are flexible etheric things: how can it be fair that people are worth so little and the game is so skewed? If I commit an offense or refuse to pay certain fines, my very liberty is at stake. When corporations cover buildings in flammable materials, rig diesel engines to present them to the consumer as greener and more economical than they are, when individuals are mis-sold insurance or financial products, what happens to corporations? Banks conspired to rig the LIBOR rate,

affecting the interest rate on mortgages for tens of thousands of Britains [sic], and cause cost of living crisis after cost of living crisis. Where are the regulators? Where are the repercussions?

And what happens when individuals lose faith in corporations (who basically fund/influence regulators through lobbyists) to "police" themselves? I'd argue that tragedies like the killing of UnitedHealth CEO Brian Thompson become more likely, as shocking as that sounds.

11) Have you taken any steps in response to the breach in respect of your 23andMe account?

The only step that I have taken is to request that 23andMe, the data controller, delete the data it processes that relates to me.

12) Have you taken any steps in response to the breach in respect of any other online accounts?

I periodically change passwords on my accounts.

13) Has the breach changed your views about with whom you share your personal information and your approach to doing so?

Yes.

14) Is there any additional information that you feel is relevant to your personal experience of the 23andMe data breach and that you would like the ICO to consider?

i)Are 23andMe's terms and conditions "reasonable"?

ii)Does 23andMe respect and comply with the UK's DPA?

iii)given the speed at which it handled the breach in the US, settling class actions etc, did 23andMe treat it's UK/Canada customers fairly?

iv) Should 23andMe be able to sell it's UK customer data?

v)if a decision is taken to not fine 23andMe, what would a company have to do to earn a fine?

Response 3

1. Are you able to confirm when and describe why you first registered as a customer with 23andMe?

I believe I signed up for 23andme sometime around 2018. My wife is a cystic fibrosis gene carrier and we were using the service to understand if I also could be a carrier. I was also interested in my family ancestry.

2. Are you able to confirm which level of service you had with 23andMe (e.g. Ancestry Service, Health + Ancestry Service or 23andMe+ Premium?

Health + Ancestry Service

3. Please explain when and how you first became aware of the breach. If possible, please confirm what information was provided by 23andMe directly and what you learnt from other sources (eg news reports).

Press reports in October 2023 alerted me and then an email from 23andme confirmed the breach

4. Are you able to describe your concerns about the 23andMe breach?

Disgusted that my dna data could be out there in the wild and been exposed to bad actors. In the wrong hands, an individual's genetic information could be misused for surveillance or discrimination.

Extremely anxious about what this could mean to my personal, financial and family safety in the future.

Anxious about my 23andme connections, who may have been impacted and what this may mean further down the line for me. I am not clear on any repercussions I could be exposed to which is distressing.

Worried about the lack of communication and transparency from 23andme about who or what could be using my deeply personal information

5. To your knowledge, were any of your relatives also impacted by the breach?

I am not clear about this

6. Please explain why you decided to raise your concerns relating to the 23andMe with the ICO?

The careless handling of my personal information has caused me immense distress, and I find it totally unacceptable that such a breach could occur in an organisation that claims to put security as a priority! I demand immediate action to rectify the situation and a detailed explanation of how this violation of my privacy occurred.

In the wrong hands, an individual's genetic information could be misused for surveillance or discrimination. This is deeply concerning and needs to be swiftly rectified.

7. Have you raised concerns with 23andMe directly? If so, what, if any, response have you received?

Yes. I sent emails to 23and me on 8/12/23 and 28/12/23 and received no direct response from 23andme

8. Have you raised concerns relating to the 23andMe breach with any other organisation or body?

Yes the ICO

I sought independent legal advice from Rocket Lawyer

9. How did you feel when you first became aware of the breach?

Distressed, anxious, upset, angry, confused, violated

10. Would you say that your feelings changed over time at all? If so, if possible, please explain how.

No! I still feel this way

11. Have you taken any steps in response to the breach in respect of your 23andMe account?

I upgraded my security with them, and then deleted my account and all data

12. Have you taken any steps in response to the breach in respect of any other online accounts?

Updated passwords across a number of accounts

13. Has the breach changed your views about with whom you share your personal information and your approach to doing so?

Yes totally

14. Is there any additional information that you feel is relevant to your personal experience of the 23andMe data breach and that you would like the ICO to consider?

Happy to share emails I sent to 23andme. I believe [ICO case officer] may have copies already