Maryland Office of Attorney General:

On behalf of 23andMe, Inc., we write to advise of a security incident that impacted Maryland residents. Attached is a copy of the notification that 23andMe, Inc. will be mailing to Maryland residents tomorrow, and that certain Maryland residents received on November 26, advising them the personal information they made available through 23andMe's optional DNA Relatives feature was accessed by a threat actor. 23andMe will be providing email notice to 49,848 Maryland residents.

Nature of the Security Breach

On October 1, 2023, a third party posted on the unofficial 23andMe subreddit site claiming to have 23andMe customers' information and posting a sample of the stolen data. Upon learning of the incident, 23andMe immediately commenced an investigation, engaged third party incident response experts to assist in determining the extent of any unauthorized activity and contacted federal law enforcement.

Based on our investigation, 23andMe determined that a threat actor orchestrated a credential stuffing attack to gain access to certain 23andMe accounts that are connected to certain customers through 23andMe's optional DNA Relatives feature. The threat actor accessed those accounts where the usernames and passwords that were used on 23andMe.com were the same as those used on other websites that were previously compromised or otherwise available. Using this access, the threat actor was able to access information that included certain customers' DNA Relatives profile information. The threat actor then created posts on a website entitled BreachForums that included links to a file containing the data points of certain customers' DNA Relatives profile.

Information Accessed

Customers who participate in 23andMe's DNA Relatives feature can see the DNA Relatives profile information for up to 1,500 of their genetic relatives, and if they are a subscriber, customers can view the DNA Relative profile information of up to 5,000 of their genetic relatives. A customer's DNA Relatives profile

information includes a user's DNA Relatives display name, how recently the user logged into their account, their relationship labels, and their predicted relationship and percentage DNA shared with their DNA Relatives matches. The following information may have also been accessed by the threat actor if the customer chose to share this information through the DNA Relatives feature: their ancestry reports and matching DNA segments (specifically where on their chromosomes they and their relative had matching DNA), self-reported location (city/zip code), ancestor birth locations and family names, profile picture, birth year, a weblink to a family tree the user created, and anything else the customer may have included in the "Introduce yourself" section of their profile. For more information about what information is a part of a customer's DNA Relatives profile visit: https://customercare.23andme.com/hc/en-us/articles/18262768896023.

Steps Taken

On October 10, 23andMe required all customers to reset their password. On November 6, 23andMe required all new and existing customers to login using two-step verification.

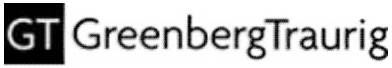
Some of the DNAR Profile information that the threat actor posted on BreachForums that has been re-posted on other websites, and 23andMe is taking steps to have the re-posted DNAR Profile information removed from the other websites.

Please reach out if you have further questions. Thank you.

Sincerely,

Gretchen A. Ramos
Shareholder

Greenberg Traurig, LLP
101 2nd Street | Suite 2200 | San Francisco, CA 94105-3668
T +1 415.655.1319
ramosg@gtlaw.com | www.gtlaw.com | View GT Biography



SUBJECT LINE: Notification Regarding Your Account

Dear <<first_name>>,

23andMe, Inc. ("23andMe") takes the privacy and confidentiality of your information very seriously. We are writing to update you regarding an incident involving the personal information you made available through 23andMe's optional DNA Relatives feature, further described below. Based upon our investigation of this incident, we believe only the profile information that you chose to share through our DNA Relatives feature was involved. There is no evidence that your 23andMe account, or any other information in your account was accessed in this incident.

What information was involved?

Our investigation determined that a threat actor accessed certain information about your ancestry that you chose to share in our DNA Relatives feature, specifically, your DNA Relatives display name, how recently you logged into your account, your relationship labels, and your predicted relationship and percentage DNA shared with your DNA Relatives matches. The following information may have also been accessed by the threat actor if you chose to share this information through the DNA Relatives feature: your ancestry reports and matching DNA segments (specifically where on your chromosomes you and your relative had matching DNA), self-reported location (city/zip code), ancestor birth locations and family names, profile picture, birth year, a weblink to a family tree you created, and anything else you may have included in the "Introduce yourself" section of your profile.

What happened?

On October 1, 2023, a third party posted on the unofficial 23andMe subreddit site claiming to have 23andMe customers' information and posting a sample of the stolen data. Upon learning of the incident, we immediately commenced an investigation and engaged third party incident response experts to assist in determining the extent of any unauthorized activity.

Based on our investigation, we believe a threat actor orchestrated a credential stuffing attack to gain access to one or more 23andMe accounts that are connected to you through our optional DNA Relatives feature. Credential stuffing is a method of attack where threat actors use lists of previously compromised user credentials to gain access to another party's systems. The threat actor accessed those accounts where the usernames and passwords that were used on 23andMe.com were the same as those used on other websites that were previously compromised or otherwise available.

Using this access, the threat actor was able to access information that included certain customers' DNA Relatives profile information, including yours (collectively, the "DNAR Profile File"). The threat actor then created posts on a website entitled BreachForums that included links to the DNAR Profile File, which may have included your DNA Relatives profile information. These links expired within 24 hours of being made available. We have identified other websites where the DNAR Profile File has been re-posted. 23andMe is taking steps to have the re-posted DNAR Profile File removed from other websites.

What we are doing

23andMe is working with third-party security experts on this investigation, as well as federal law enforcement. On October 10, we required all 23andMe customers to reset their password. On November 6, we required all new and existing customers to login using two-step verification. While we continue our investigation, we have also temporarily paused certain functionality within the 23andMe platform. We are also taking steps to have the re-posted DNAR Profile File removed from other websites.

What you can do

For more information about what information is a part of your DNA Relatives profile and how to manage your preferences visit: https://customercare.23andme.com/hc/en-us/articles/18262768896023. We also recommend you review our guidance on how to keep your 23andMe account secure for additional steps you can take to safeguard your account. See

https://customercare.23andme.com/hc/en-us/articles/360062175913-Privacy-and-Security-Help-Center.

While we do not believe this incident is likely to result in identity theft or fraud, we encourage you to review the Additional Resources appendix to this letter as it contains additional information on how to protect yourself against identity theft and fraud.

For more information

If you have additional questions you may email us at customercare@23andme.com, or call us at 1-800-239-5230 on weekdays from 6am to 5pm PT. You may also write to 23andMe at Attn: Legal, 349 Oyster Point Blvd, South San Francisco, CA 94080.

Protecting our customers' privacy and security continues to be a top priority. We will continue to invest in protecting our systems and data. We sincerely apologize for any inconvenience caused to you by this incident.

Sincerely,

23andMe, Inc.

23andMe

Additional Resources

Free Credit Report. You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free at 1-877-322-8228, or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually. They provide free annual credit reports only through the website or toll-free number.

If you see anything on your credit report that you do not understand, you should notify the credit bureau that sent you the report immediately. If you find any suspicious activity on your credit report, call your local police or sheriff's office, and file a police report for identity theft. You have a right to obtain a copy of the police report, which you may need to provide to creditors to clear up your records.

Equifax P.O. Box 105069 Atlanta, GA 30348 800-525-6285 www.equifax.com	Experian P.O. Box 2002 Allen, TX 75013 888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19022-2000 800-680-7289 www.transunion.com

Fraud Alerts. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Security Freeze. You may wish to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. The credit bureaus may charge a reasonable fee to place a freeze on your account and may require that you provide proper identification prior to honoring your request. You can request a security freeze by contacting the credit bureaus.

Additional Information. Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement. A checklist of the steps listed above and links to forms and other helpful information can be found on the site at https://IdentityTheft.gov/steps.

For Maryland Residents: The Maryland Office of the Attorney General Identity Theft Unit (https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx) may be contacted at 200 St. Paul Place 25th Floor, Baltimore, MD 21202; 1-410-576-6491; and idtheft@oag.state.md.us.