From: **23andMe**
Date: xxxxxx
Subject: Notice of Data Breach
To: xxxxxxx

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 your Family Tree profile information 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 Family Tree profile, specifically your display name, relationship labels, and percentage DNA you share with the credential stuffed account holder through which your information was accessed. The following information may have also been accessed in relation to the Family Tree profile if you chose to share this information in the DNA Relatives feature: self-reported location (city/zip code) and birth year.

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 during the period from May 2023 through September 2023 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

When 23andMe became aware of the incident, we immediately began working with third-party security experts to investigate the incident, and we contacted 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 our Customer Care article here. We also recommend you review our guidance here on how to keep your 23andMe account secure and for additional steps you can take to safeguard your account.

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.

From: **23andMe**
Date: xxxxxx
Subject: Notice of Data Breach
To: xxxxxxx

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 the credential stuffed account holder through which your information was accessed. 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 during the period from May 2023 through September 2023 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

When 23andMe became aware of the incident, we immediately began working with third-party security experts to investigate the incident, and we contacted 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 our Customer Care article here. We also recommend you review our guidance here on how to keep your 23andMe account secure and for additional steps you can take to safeguard your account.

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.

From: **23andMe**
Date: xxxxxx
Subject: 23andMe Account Update
To: xxxxxxx

23andMe, Inc. ("23andMe") takes the privacy and confidentiality of your information very seriously. We are writing to update you regarding our October incident. Based upon our investigation of this incident, we believe a threat actor orchestrated a credential stuffing attack during the period from May 2023 through September 2023 and gained access to your account.

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 was able to gain access to your account because the username and password that you used on 23andMe.com were the same as those that you used on other websites that were previously compromised or otherwise available.

What you can do

On October 10, 23andMe required all users to change their passwords. On November 6, 23andMe required all new and existing customers to login using two-step verification. However, if you are currently using the same username and password that you were using on 23andMe.com prior to October 10, on other websites, we recommend you immediately change your passwords on the other websites.

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 certain 23andMe accounts including your account. Once the threat actor accessed your account they

also accessed certain information in your account.

What information was involved?
Our investigation determined that a threat actor accessed your settings, which includes information such as your height, weight, self-reported ethnicity, current zip code, and birth date. To review the information in your settings page, please sign in to your account and go to your settings page.

We recommend you review our guidance here on how to keep your 23andMe account secure and for additional steps you can take to safeguard your account.

What have we done?
23andMe worked 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. We have also temporarily paused certain functionality within the 23andMe platform.

23andMe is here to support you. Please contact Customer Care at customercare@23andme.com if you need assistance. Protecting our customers' privacy and security continues to be a top priority. We sincerely apologize for any inconvenience caused to you by this incident.

Sincerely,
23andMe, Inc.

Secure Processing Center
20 Oser Ave
Suite 100
Hauppauge, NY 11788

<<Date>>

<<Name 1>> <<Name 2>>
<<Address_1>>
<<Address_2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Breach

Dear <<Name 1>>,

23andMe, Inc. ("23andMe") takes the privacy and confidentiality of your information very seriously. We are writing to update you regarding the incident that took place in October. Based upon our investigation of this incident, we believe a threat actor orchestrated a credential stuffing attack during the period from late April 2023 through September 2023 and gained access to your account.

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 was able to gain access to your account because the username and password that you used on 23andMe.com were the same as those that you used on other websites that were previously compromised or otherwise available. Based upon our investigation of this incident, we believe only your Family Tree profile information was involved.

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 certain 23andMe accounts including your account. Once the threat actor accessed your account they also accessed certain information in your account.

What information was involved?

Our investigation determined that a threat actor accessed certain information about your ancestry that you chose to share in your Family Tree profile, specifically your display name, relationship labels, and percentage DNA you share with your DNA Relatives matches. The following information may have also been accessed in relation to the Family Tree profile if you chose to share this information in the DNA Relatives feature: self-reported location (city/zip code) and birth year.

What have we done?

23andMe worked 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. We have temporarily paused certain functionality within the 23andMe platform.

What you can do

If you are currently using the same username and password that you were using on 23andMe.com prior to October 10, 2023 on other websites, we recommend you immediately change your passwords on those other websites.

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.

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 by this incident.

Sincerely,

23andMe, Inc.

Secure Processing Center
20 Oser Ave
Suite 100
Hauppauge, NY 11788

<<Date>>

<<Name 1>> <<Name 2>>
<<Address_1>>
<<Address_2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Breach

Dear <<Name 1>>,

23andMe, Inc. ("23andMe") takes the privacy and confidentiality of your information very seriously. We are writing to update you regarding the incident that took place in October. Based upon our investigation of this incident, we believe a threat actor orchestrated a credential stuffing attack during the period from late April 2023 through September 2023 and gained access to your account.

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 was able to gain access to your account because the username and password that you used on 23andMe.com were the same as those that you used on other websites that were previously compromised or otherwise available. Based upon our investigation of this incident, we believe only your DNA Relatives profile information was involved.

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. The threat actor also created posts on a website entitled BreachForums that included links to a file, which may have included your DNA Relatives profile information. These links expired within 24 hours of being made available.

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 certain 23andMe accounts including your account. Once the threat actor accessed your account they also accessed certain information in your account.

What information was involved?

Our investigation determined the threat actor downloaded or 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 have we done?

23andMe worked 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. We have temporarily paused certain functionality within the 23andMe platform. We have identified other websites where the file containing certain DNA Relatives profiles has been re-posted. 23andMe is taking steps to have the re-posted file containing DNA Relatives profiles removed from other websites.

What you can do

If you are currently using the same username and password that you were using on 23andMe.com prior to October 10, 2023 on other websites, we recommend you immediately change your passwords on those other websites.

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.

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 by this incident.

Sincerely,

23andMe, Inc.

Secure Processing Center
20 Oser Ave
Suite 100
Hauppauge, NY 11788

<<Date>>

<<Name 1>> <<Name 2>>
<<Address_1>>
<<Address_2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Breach of Security

Dear <<Name 1>>,

23andMe, Inc. ("23andMe") takes the privacy and confidentiality of your information very seriously. We are writing to update you regarding the incident that took place in October. Based upon our investigation of this incident, we believe a threat actor orchestrated a credential stuffing attack during the period from late April 2023 through September 2023 and gained access to your account.

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 was able to gain access to your account because the username and password that you used on 23andMe.com were the same as those that you used on other websites that were previously compromised or otherwise available.

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. The threat actor also created posts on a website entitled BreachForums that included links to a file, which may have included your DNA Relatives profile information. These links expired within 24 hours of being made available.

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 certain 23andMe accounts including your account. Once the threat actor accessed your account they also accessed certain information in your account.

What information was involved?

Our investigation determined the threat actor downloaded or accessed information in your account, such as certain health reports derived from the processing of your genetic information, including health-predisposition reports, wellness reports, and carrier status reports. If you participated in the 23andMe DNA Relatives feature, the threat actor may have also accessed your DNA Relatives profile information, and your Family Tree profile information.

If your DNA Relatives profile information was accessed, the threat actor was able to view your 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.

If your Family Tree profile information was accessed, the threat actor accessed your display name, relationship labels, and percentage DNA with your DNA Relatives matches. The following information may have also been accessed in relation to the Family Tree profile if you chose to share this information in the DNA Relatives feature: self-reported location (city/zip code) and birth year.

The threat actor may have also accessed information in your settings, which may include information such as your height, weight, self-reported ethnicity, current zip code, and birth date.

What have we done?

23andMe worked 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. We have temporarily paused certain functionality within the 23andMe platform. We have identified other websites where the file containing certain DNA Relatives profiles has been re-posted. 23andMe is taking steps to have the re-posted file containing DNA Relatives profiles removed from other websites.

What you can do

If you are currently using the same username and password that you were using on 23andMe.com prior to October 10, on other websites, we recommend you immediately change your passwords on those other websites.

For a list of 23andMe's health reports depending upon your level of service, see https://www.23andme.com/dna-reports-list/. To learn 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. To review the information in your settings page, please sign in to your account and go to your settings page. 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 resulted in identity theft or fraud since no social security numbers, driver's license numbers or financial information were accessed, 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 by this incident.

Sincerely,

23andMe, Inc.

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.

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392 or 1-503-378-4400; www.doj.state.or.us.

For Washington D.C. Residents: You can obtain additional information about the steps you can take to avoid identity theft from the DC Office of the Attorney General at https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft. You may also contact the DC Office of the Attorney General at 400 6th Street NW, Washington, D.C. 20001; (202) 727-3400; and oag@dc.gov.

Secure Processing Center
20 Oser Ave
Suite 100
Hauppauge, NY 11788

<<Date>>

<<Name 1>> <<Name 2>>
<<Address_1>>
<<Address_2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Breach of Security

Dear <<Name 1>>,

23andMe, Inc. ("23andMe") takes the privacy and confidentiality of your information very seriously. We are writing to update you regarding the incident that took place in October. Based upon our investigation of this incident, we believe a threat actor orchestrated a credential stuffing attack during the period from late April 2023 through September 2023 and gained access to your account.

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 was able to gain access to your account because the username and password that you used on 23andMe.com were the same as those that you used on other websites that were previously compromised or otherwise available.

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. The threat actor also created posts on a website entitled BreachForums that included links to a file, which may have included your DNA Relatives profile information. These links expired within 24 hours of being made available.

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 certain 23andMe accounts including your account. Once the threat actor accessed your account they also accessed certain information in your account.

What information was involved?

Our investigation determined the threat actor downloaded or accessed information in your account, such as certain health reports derived from the processing of your genetic information, including health-predisposition reports, wellness reports, and carrier status reports. To the extent your account contained such information, the threat actor may have also accessed self-reported health condition information, and information in your settings. If you participated in the 23andMe DNA Relatives feature, the threat actor may have also accessed your DNA Relatives profile information, and your Family Tree profile information.

If your DNA Relatives profile information was accessed, the threat actor was able to view your 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.

If your Family Tree profile information was accessed, the threat actor accessed your display name, relationship labels, and percentage DNA with your DNA Relatives matches. The following information may have also been accessed in relation to the Family Tree profile if you chose to share this information in the DNA Relatives feature: self-reported location (city/zip code) and birth year.

The threat actor may have also accessed information in your settings, which may include information such as your height, weight, self-reported ethnicity, current zip code, and birth date.

What have we done?

23andMe worked 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. We have temporarily paused certain functionality within the 23andMe platform. We have identified other websites where the file containing certain DNA Relatives profiles has been re-posted. 23andMe is taking steps to have the re-posted file containing DNA Relatives profiles removed from other websites.

What you can do

If you are currently using the same username and password that you were using on 23andMe.com prior to October 10, on other websites, we recommend you immediately change your passwords on those other websites.

For a list of 23andMe's health reports depending upon your level of service, see https://www.23andme.com/dna-reports-list/. To learn 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. To review the information in your settings page, please sign in to your account and go to your settings page. 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 resulted in identity theft or fraud since no social security numbers, driver's license numbers or financial information were accessed, 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 by this incident.

Sincerely,

23andMe, Inc.

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.

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392 or 1-503-378-4400; www.doj.state.or.us.

For Washington D.C. Residents: You can obtain additional information about the steps you can take to avoid identity theft from the DC Office of the Attorney General at https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft. You may also contact the DC Office of the Attorney General at 400 6th Street NW, Washington, D.C. 20001; (202) 727-3400; and oag@dc.gov.

Secure Processing Center
20 Oser Ave
Suite 100
Hauppauge, NY 11788

<<Date>>

<<Name 1>> <<Name 2>>
<<Address_1>>
<<Address_2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Breach of Security

Dear <<Name 1>>,

23andMe, Inc. ("23andMe") takes the privacy and confidentiality of your information very seriously. We are writing to update you regarding the incident that took place in October. Based upon our investigation of this incident, we believe a threat actor orchestrated a credential stuffing attack during the period from late April 2023 through September 2023 and gained access to your account.

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 was able to gain access to your account because the username and password that you used on 23andMe.com were the same as those that you used on other websites that were previously compromised or otherwise available.

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. The threat actor also created posts on a website entitled BreachForums that included links to a file, which may have included your DNA Relatives profile information. These links expired within 24 hours of being made available.

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 certain 23andMe accounts including your account. Once the threat actor accessed your account they also accessed certain information in your account.

What information was involved?

Our investigation determined the threat actor downloaded or accessed your uninterrupted raw genotype data, and may have accessed other sensitive information in your account, such as certain health reports derived from the processing of your genetic information, including health-predisposition reports, wellness reports, and carrier status reports. To the extent your account contained such information, the threat actor may have also accessed self-reported health condition information, and information in your settings. If you participated in the 23andMe DNA Relatives feature, the threat actor may have also accessed your DNA Relatives profile information, and your Family Tree profile information.

If your DNA Relatives profile information was accessed, the threat actor was able to view your 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.

If your Family Tree profile information was accessed, the threat actor accessed your display name, relationship labels, and percentage DNA with your DNA Relatives matches. The following information may have also been accessed in relation to the Family Tree profile if you chose to share this information in the DNA Relatives feature: self-reported location (city/zip code) and birth year.

The threat actor may have also accessed information in your settings, which may include information such as your height, weight, self-reported ethnicity, current zip code, and birth date.

What have we done?

23andMe worked 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. We have temporarily paused certain functionality within the 23andMe platform. We have identified other websites where the file containing certain DNA Relatives profiles has been re-posted. 23andMe is taking steps to have the re-posted file containing DNA Relatives profiles removed from other websites.

What you can do

If you are currently using the same username and password that you were using on 23andMe.com prior to October 10, on other websites, we recommend you immediately change your passwords on those other websites.

For a list of 23andMe's health reports depending upon your level of service, see https://www.23andme.com/dna-reports-list/. To learn 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. To review the information in your settings page, please sign in to your account and go to your settings page. 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 resulted in identity theft or fraud since no social security numbers, driver's license numbers or financial information were accessed, 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 by this incident.

Sincerely,

23andMe, Inc.

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.

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392 or 1-503-378-4400; www.doj.state.or.us.

For Washington D.C. Residents: You can obtain additional information about the steps you can take to avoid identity theft from the DC Office of the Attorney General at https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft. You may also contact the DC Office of the Attorney General at 400 6th Street NW, Washington, D.C. 20001; (202) 727-3400; and oag@dc.gov.