orrick
Orrick, Herrington & Sutcliffe LLP
405 Howard Street
San Francisco, CA 94105-2669
+1 415 773 5700
orrick.com

August 18, 2023

By Email

Office of the Attorney General
200 St. Paul Plaza
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

Orrick, Herrington & Sutcliffe, LLP ("Orrick") writes to provide supplemental notice of a security incident Orrick recently experienced and notified your Office about on July 20, 2023. Orrick is a law firm, headquartered at 405 Howard Street, San Francisco, CA 94105. Orrick is also making this supplemental notification on behalf of the entities listed on Exhibit A.

On March 13, 2023, Orrick detected that an unauthorized third party gained remote access to a portion of its network, including a file share that Orrick used to store certain client files. Upon detection, Orrick immediately took steps to block the unauthorized access and initiated its response process, including launching an investigation of the incident with the support of third party cybersecurity experts. Orrick also notified law enforcement. Orrick has identified no evidence of further unauthorized activity since detecting the security incident on March 13.

Once Orrick identified the affected files, it began a process to determine what personal information was impacted, and to whom it belonged. Orrick recently determined that primarily between February 28 and March 13, 2023, the unauthorized actor obtained files containing personal information. Orrick's clients were informed about the incident, and Orrick then worked with the clients to identify individuals with affected data and their contact information. Depending on the individual, the information affected may have included: name, date of birth, Social Security number, driver's license or other state identification number, tax identification number, financial account information, online account credentials, credit or debit card number, and health insurance information. The relevant data elements affected may differ by entity.

Orrick anticipates having made notification to 1,706 additional Maryland individuals with impacted personal information by August 18, 2023, some of whom were notified beginning July 20, 2023. Orrick is offering these individuals two years of complimentary identity monitoring services, including credit monitoring and identity theft protection services. Orrick has also established a dedicated call center to answer questions.

In addition to these actions, Orrick deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network. Orrick is not aware of any misuse of the affected personal information.

The information submitted herein is proprietary and confidential and should be afforded confidential treatment. If you have any questions, please do not hesitate to contact me at (206) 839-4340 or aswaminathan@orrick.com.

Respectfully yours,

Aravind Swaminathan

Partner

Orrick, Herrington & Sutcliffe, LLP

Enclosures

Exhibit A

Entities
Charles Schwab & Co., Inc.
Fujitsu North America, Inc.

Orrick, Herrington & Sutcliffe LLP
405 Howard Street
San Francisco, CA 94105-2669
+1 415 773 5700
orrick.com

August 18, 2023

[redacted]

Re: Notice of Data Breach

Dear [redacted],

Orrick, Herrington & Sutcliffe, LLP ("Orrick") recently experienced a security event. As a large international law firm, we occasionally receive information from our clients and other third parties, including personal information, which we possess in connection with the services we provide. During our representation of a client, Orrick obtained information about you that was recently impacted in a security event on Orrick systems. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing in response.

What happened?

On March 13, 2023, we detected that an unauthorized third party gained remote access to a portion of our network, including a file share that we used to store certain client files. Upon detection, we took immediate steps to block the unauthorized access and an investigation of the incident was launched with the support of leading outside cybersecurity experts. We also notified law enforcement. We recently determined that the unauthorized third party obtained files containing personal information primarily between February 28 and March 13, 2023.

What information was involved?

We recently determined that the information affected included: [redacted].

What are we doing?

Orrick is offering two years of complimentary identity monitoring services through Kroll. To take advantage of these free identity monitoring services, please follow the instructions in Attachment A. You must activate by November 16, 2023 to receive these services.

In addition to these actions, Orrick deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network.

What can you do?

Orrick is not aware of any misuse of your information. It is always advisable to remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing online and financial accounts, credit reports, and Explanations of Benefits ("EOBs") from your health insurers for suspicious activity. This is a best practice for all individuals. If you identify suspicious activity, you should contact the company that maintains the account on your behalf.

Additional information about how to protect your identity is contained in Attachment B.

For more information:

Orrick has established a dedicated call center to answer questions. If you have any questions regarding this incident or the services available to you, please call (866) 373-9174 Monday through Friday from 9:00 am to 6:30 pm Eastern Time, excluding major U.S. holidays.

Sincerely,

Orrick Client Support
Orrick, Herrington & Sutcliffe, LLP

[redacted]

Attachment A - Identity Monitoring Services

We have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

1. You must activate your identity monitoring services by **November 16, 2023.**

2. Visit **https://enroll.krollmonitoring.com** to activate your identity monitoring services.

3. Provide Your Membership Number: [redacted]

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Attachment B – Information for U.S. Residents

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	Experian:	TransUnion:
equifax.com	experian.com	transunion.com
equifax.com/personal/credit-report-services	experian.com/help	transunion.com/credit-help
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
800-685-1111	888-397-3742	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580.

Additional Information

If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

For Massachusetts residents: You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New York residents: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at http://www.dos.ny.gov/consumerprotection or (800) 697-1220 or NYS Attorney General at http://www.ag.ny.gov/home.html or (800) 771-7755.

For New Mexico Residents: You have rights pursuant to the FCRA, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_ your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Business Services website at https://dfr.oregon.gov/financial/protect/Pages/stolen-identity.aspx and click "Place a credit freeze."

For Rhode Island residents: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

Orrick, Herrington & Sutcliffe LLP
405 Howard Street
San Francisco, CA 94105-2669
+1 415 773 5700
orrick.com

July 31, 2023

By Email

Office of the Attorney General
200 St. Paul Plaza
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

Orrick, Herrington & Sutcliffe, LLP ("Orrick") writes to provide supplemental notice of a security incident Orrick recently experienced and notified your Office about on July 20, 2023. Orrick is a law firm, headquartered at 405 Howard Street, San Francisco, CA 94105. Orrick is making this supplemental notification on behalf of Cigna Healthcare & Life Insurance Company.

On March 13, 2023, Orrick detected that an unauthorized third party gained remote access to a portion of its network, including a file share that Orrick used to store certain client files. Upon detection, Orrick immediately took steps to block the unauthorized access and initiated its response process, including launching an investigation of the incident with the support of a third-party forensics firm. Orrick also notified law enforcement. Orrick has identified no evidence of further unauthorized activity since detecting the security incident on March 13.

Once Orrick identified the affected files, it began a process to determine what personal information was impacted, and to whom it belonged. Orrick recently determined that primarily between February 28 and March 13, 2023, the unauthorized actor obtained files containing personal information. Orrick's client's customers were informed about the incident, and Orrick then worked with the client to identify individuals with affected data and their contact information, which was provided to the customers in early June. The information affected may have included: full name, address, date of birth, email address, claims information, health insurance identification number, healthcare provider, medical record number, and Social Security number.

Orrick anticipates notifying 11 additional Maryland individuals with impacted personal information beginning July 31, 2023. Orrick is offering these individuals two years of complimentary identity monitoring services, including credit monitoring and identity theft protection services. Orrick has also established a dedicated call center to answer questions.

In addition to these actions, Orrick deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network. Orrick is not aware of any misuse of the affected personal information.

The information submitted herein is proprietary and confidential and should be afforded confidential treatment. If you have any questions, please do not hesitate to contact me at (206) 839-4340 or aswaminathan@orrick.com.

Respectfully yours,

Aravind Swaminathan

Partner

Orrick, Herrington & Sutcliffe, LLP

Enclosure

Orrick, Herrington & Sutcliffe LLP
405 Howard Street
San Francisco, CA 94105-2669
+1 415 773 5700
orrick.com

September 6, 2023

By Email

Office of the Attorney General
200 St. Paul Plaza
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

Orrick, Herrington & Sutcliffe, LLP ("Orrick") writes to provide supplemental notice of a security incident Orrick recently experienced and notified your Office about on July 20, 2023. Orrick is a law firm, headquartered at 405 Howard Street, San Francisco, CA 94105. Orrick is making this supplemental notification on behalf of the entities listed on Exhibit A.

On March 13, 2023, Orrick detected that an unauthorized third party gained remote access to a portion of its network, including a file share that Orrick used to store certain client files. Upon detection, Orrick immediately took steps to block the unauthorized access and initiated its response process, including launching an investigation of the incident with the support of a third-party forensics firm. Orrick also notified law enforcement. Orrick has identified no evidence of further unauthorized activity since detecting the security incident on March 13.

Once Orrick identified the affected files, it began a process to determine what personal information was impacted, and to whom it belonged. Orrick recently determined that primarily between February 28 and March 13, 2023, the unauthorized actor obtained files containing personal information. Orrick's client's customers were informed about the incident, and Orrick then worked with the client to identify individuals with affected data and their contact information, which was provided to the customers in early June. The information affected may have included: full name, address, date of birth, email address, claims information (date, cost of services, and claims identifiers), health insurance identification number, healthcare provider, medical record number, and Social Security number.

Orrick anticipates notifying 9 additional Maryland individuals with impacted personal information beginning September 6, 2023. Orrick is offering these individuals two years of complimentary identity monitoring services, including credit monitoring and identity theft protection services. Orrick has also established a dedicated call center to answer questions.

In addition to these actions, Orrick deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network. Orrick is not aware of any misuse of the affected personal information.

The information submitted herein is proprietary and confidential and should be afforded confidential treatment. If you have any questions, please do not hesitate to contact me at (206) 839-4340 or aswaminathan@orrick.com.

Respectfully yours,

Aravind Swaminathan

Partner

Orrick, Herrington & Sutcliffe, LLP

Enclosures

Exhibit A

Entities
Care Ventures Accountable Health Plan
Sheppard Pratt Health System Life, Accident and Health Plan
University of Maryland-Upper Chesapeake Health

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>

Notice of Data Breach

Dear <<first_name>>,

Orrick, Herrington & Sutcliffe, LLP ("Orrick") writes to inform you that Orrick, a downstream service provider of <<b2b_text_1 (covered entity)>>, recently experienced a security incident that involved your personal information. Orrick has served as legal counsel for MultiPlan, Inc. ("MultiPlan"), which provides services to <<b2b_text_1 (covered entity)>>. In connection with Orrick's representation of MultiPlan, Orrick stored files that included plan participant information related to a prior security incident for which notification was previously made. Those files were recently impacted in a security incident on Orrick's systems. This incident did not impact MultiPlan's or <<b2b_text_1 (covered entity)>>'s systems. Please read this notice carefully, as it provides up-to-date information on what happened and what Orrick is doing in response.

What happened?

On March 13, 2023, Orrick detected that an unauthorized third party gained remote access to a portion of Orrick's network, including a file share that Orrick used to store certain client files. Upon detection, Orrick took immediate steps to block the unauthorized access and an investigation of the incident was launched with the support of leading outside cybersecurity experts. Orrick also notified law enforcement. Through its investigation, Orrick recently determined that on March 10, 2023, the unauthorized third party obtained files containing personal information. The health insurance plan in which you are or were enrolled was informed about the incident and Orrick has been working to identify individuals with impacted data and their contact information, which was provided to your health insurance plan in early June.

What information was involved?

Orrick recently determined that your information impacted includes: <<b2b_text_2 (data elements)>>.

What are we doing?

Orrick is offering two years of complimentary identity monitoring services through Kroll. To take advantage of these free identity monitoring services, please follow the instructions in Attachment A. You must activate by <<b2b_text_6 (activation date)>> to receive these services.

In addition to these actions, Orrick deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network.

What can you do?

Orrick is not aware of any misuse of your information. Your financial information, such as financial account information or credit card numbers, was not involved in this incident. It is always advisable to remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing online and financial accounts, credit reports, and Explanations of Benefits ("EOBs") from your health insurers for suspicious activity. This is a best practice for all individuals. If you identify suspicious activity, you should contact the company that maintains the account on your behalf.

Additional information about how to help protect your information is contained in Attachment B.

For more information:

Orrick has established a dedicated call center to answer questions. If you have any questions regarding this incident or the services available to you, please call <<TFN>>, Monday through Friday from 9:00am to 6:30pm Eastern Time, excluding major U.S. holidays. Callers who are deaf, hard-of-hearing, or speech-disabled may utilize their TeleTYpewriter (TTY) or Telecommunication Device (TDD) to access an operator at <<TFN>>, Monday through Friday from 9:00am to 6:30pm Eastern Time, excluding major U.S. holidays.

Sincerely,

Orrick Client Support

Orrick, Herrington & Sutcliffe, LLP

Attachment A - Identity Monitoring Services

Orrick has secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services. *You have until **<<b2b_text_6 (Activation Deadline)>>** to activate your identity monitoring services.*

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

Take Advantage of Your Identity Monitoring Services

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Attachment B – Information for U.S. Residents

Below are additional helpful tips you may want to consider to help protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, Orrick recommends that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	Experian:	TransUnion:
equifax.com	experian.com	transunion.com
equifax.com/personal/credit-report-services	experian.com/help	transunion.com/credit-help
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
800-685-1111	888-397-3742	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be

provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Additional Information

If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

For Massachusetts residents: You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New York residents: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at http://www.dos.ny.gov/consumerprotection or (800) 697-1220 or NYS Attorney General at http://www.ag.ny.gov/home.html or (800) 771-7755.

For New Mexico Residents: You have rights pursuant to the FCRA, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the FTC and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Commercial Services website at www.dfcs.oregon.gov/id_theft.html and click "How to get a security freeze."

For Rhode Island residents: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

Orrick, Herrington & Sutcliffe LLP
405 Howard Street
San Francisco, CA 94105-2669
+1 415 773 5700
orrick.com

August 21, 2023

By Email

Office of the Attorney General
200 St. Paul Plaza
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

Orrick, Herrington & Sutcliffe, LLP ("Orrick") writes to provide supplemental notice of a security incident Orrick recently experienced and notified your Office about on July 20, 2023. Orrick is a law firm, headquartered at 405 Howard Street, San Francisco, CA 94105. Orrick is making this supplemental notification on behalf of Oscar Garden State Insurance Corporation.

On March 13, 2023, Orrick detected that an unauthorized third party gained remote access to a portion of its network, including a file share that Orrick used to store certain client files. Upon detection, Orrick immediately took steps to block the unauthorized access and initiated its response process, including launching an investigation of the incident with the support of a third-party forensics firm. Orrick also notified law enforcement. Orrick has identified no evidence of further unauthorized activity since detecting the security incident on March 13.

Once Orrick identified the affected files, it began a process to determine what personal information was impacted, and to whom it belonged. Orrick recently determined that primarily between February 28 and March 13, 2023, the unauthorized actor obtained files containing personal information. Orrick's client's customers were informed about the incident, and Orrick then worked with the client to identify individuals with affected data and their contact information, which was provided to the customers in early June. The information affected may have included: full name, address, date of birth, email address, claims information (date, cost of services, and claims identifiers), health insurance identification number, healthcare provider, medical record number, and Social Security number.

Orrick anticipates notifying 1 additional Maryland individual with impacted personal information beginning August 21, 2023. Orrick is offering this individual two years of complimentary identity monitoring services, including credit monitoring and identity theft protection services. Orrick has also established a dedicated call center to answer questions.

In addition to these actions, Orrick deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network. Orrick is not aware of any misuse of the affected personal information.

The information submitted herein is proprietary and confidential and should be afforded confidential treatment. If you have any questions, please do not hesitate to contact me at (206) 839-4340 or aswaminathan@orrick.com.

Respectfully yours,

Aravind Swaminathan

Partner

Orrick, Herrington & Sutcliffe, LLP

Enclosure

orrick
Orrick, Herrington & Sutcliffe LLP
405 Howard Street
San Francisco, CA 94105-2669
+1 415 773 5700
orrick.com

October 11, 2023

By Email

Office of the Attorney General
200 St. Paul Plaza
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

Orrick, Herrington & Sutcliffe, LLP ("Orrick") writes to provide supplemental notice of a security incident Orrick recently experienced and notified your Office about on July 20, 2023. Orrick is a law firm, headquartered at 405 Howard Street, San Francisco, CA 94105. Orrick is making this supplemental notification on behalf of Sentara Health Plans.

On March 13, 2023, Orrick detected that an unauthorized third party gained remote access to a portion of its network, including a file share that Orrick used to store certain client files. Upon detection, Orrick immediately took steps to block the unauthorized access and initiated its response process, including launching an investigation of the incident with the support of a third-party forensics firm. Orrick also notified law enforcement. Orrick has identified no evidence of further unauthorized activity since detecting the security incident on March 13.

Once Orrick identified the affected files, it began a process to determine what personal information was impacted, and to whom it belonged. Orrick recently determined that primarily between February 28 and March 13, 2023, the unauthorized actor obtained files containing personal information. Orrick's client's customers were informed about the incident, and Orrick then worked with the client to identify individuals with affected data and their contact information, which was provided to the customers in early June. The information affected may have included: full name, address, date of birth, phone number, email address, vision insurance account/identification number, health insurance account/identification number, and Social Security number.

Orrick anticipates notifying 3 additional Maryland individuals with impacted personal information beginning October 11, 2023. Orrick is offering these individuals two years of complimentary identity monitoring services, including credit monitoring and identity theft protection services. Orrick has also established a dedicated call center to answer questions.

In addition to these actions, Orrick deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network. Orrick is not aware of any misuse of the affected personal information.

The information submitted herein is proprietary and confidential and should be afforded confidential treatment. If you have any questions, please do not hesitate to contact me at (206) 839-4340 or aswaminathan@orrick.com.

Respectfully yours,

Aravind Swaminathan

Partner

Orrick, Herrington & Sutcliffe, LLP

Enclosures

Orrick, Herrington & Sutcliffe LLP
405 Howard Street
San Francisco, CA 94105-2669
+1 415 773 5700
orrick.com

October 24, 2023

By Email

Office of the Attorney General
200 St. Paul Plaza
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

Orrick, Herrington & Sutcliffe, LLP ("Orrick") writes to provide supplemental notice of a security incident Orrick recently experienced and notified your Office about on July 20, 2023. Orrick is a law firm, headquartered at 405 Howard Street, San Francisco, CA 94105. Orrick is making this supplemental notification on behalf of the entities listed on Exhibit A.

On March 13, 2023, Orrick detected that an unauthorized third party gained remote access to a portion of its network, including a file share that Orrick used to store certain client files. Upon detection, Orrick immediately took steps to block the unauthorized access and initiated its response process, including launching an investigation of the incident with the support of a third-party forensics firm. Orrick also notified law enforcement. Orrick has identified no evidence of further unauthorized activity since detecting the security incident on March 13.

Once Orrick identified the affected files, it began a process to determine what personal information was impacted, and to whom it belonged. Orrick recently determined that primarily between February 28 and March 13, 2023, the unauthorized actor obtained files containing personal information. Orrick's client's customers were informed about the incident, and Orrick then worked with the client to identify individuals with affected data and their contact information, which was provided to the customers in early June. The information affected may have included: full name, address, date of birth, email address, claims information (date, cost of services, and claims identifiers), health insurance identification number, healthcare provider, medical record number, prescriber name, and Social Security number.

Orrick notified 22 additional Maryland individuals with impacted personal information on our about September 8 and 29, 2023 and October 19, 2023. Orrick is offering these individuals two years of complimentary identity monitoring services, including credit monitoring and identity theft protection services. Orrick has also established a dedicated call center to answer questions.

In addition to these actions, Orrick deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network. Orrick is not aware of any misuse of the affected personal information.

The information submitted herein is proprietary and confidential and should be afforded confidential treatment. If you have any questions, please do not hesitate to contact me at (206) 839-4340 or aswaminathan@orrick.com.

Respectfully yours,

Aravind Swaminathan

Partner

Orrick, Herrington & Sutcliffe, LLP

Enclosures

Exhibit A

Entities
Independent Health
The Ohio State University Health Plan Inc.
Sentara Health Plans

Orrick, Herrington & Sutcliffe LLP
405 Howard Street
San Francisco, CA 94105-2669
+1 415 773 5700
orrick.com

December 28, 2023

By Email

Office of the Attorney General
200 St. Paul Plaza
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

Orrick, Herrington & Sutcliffe LLP ("Orrick") writes to provide supplemental notice of a security incident Orrick recently experienced and first notified your Office about on July 20, 2023. Orrick is a law firm, headquartered at 405 Howard Street, San Francisco, CA 94105. Orrick is making this supplemental notification on behalf of itself and the entities listed on Exhibit A.

On March 13, 2023, Orrick detected that an unauthorized third party gained remote access to a portion of its network, including a file share that Orrick used to store certain client files. Upon detection, Orrick immediately took steps to block the unauthorized access and initiated its response process, including launching an investigation of the incident with the support of third party cybersecurity experts. Orrick also notified law enforcement. Orrick has identified no evidence of further unauthorized activity since detecting the security incident on March 13.

Once Orrick identified the affected files, it began a process to determine what personal information was impacted, and to whom it belonged. Orrick determined that primarily between February 28 and March 13, 2023, the unauthorized actor obtained files containing personal information. Orrick's clients and, where relevant, Orrick's clients' customers were informed about the incident, and Orrick then worked with the clients to identify individuals with affected data and their contact information, which was provided to the customers in early June. An analysis of personal information in certain unstructured data, such as emails and attachments to emails, was completed in mid-October and the impacted health plans have been notified.

Depending on the individual, the information affected may have included: name, address, email address, date of birth, Social Security number, driver's license or other government-issued identification number, passport number, financial account information, tax identification number, medical treatment and/or diagnosis information, claims information (date, cost of services, and claims identifiers), health insurance identification number, healthcare provider, medical record number, prescriber name, healthcare provider license number, incidental health reference, online account credentials, and credit or debit card number. The relevant data elements affected may differ by entity.

Orrick notified approximately 1,851 additional Maryland individuals with impacted personal information between August 31, 2023 and December 12, 2023. Orrick is offering these individuals two years of complimentary identity monitoring services, including credit monitoring and identity theft protection services. Orrick has also established a dedicated call center to answer questions. Several class action complaints have been filed in connection with this security incident. These cases were recently consolidated, and on December 21, 2023, a notice and joint stipulation was filed that the parties have reached a settlement in principle.

In addition to these actions, Orrick deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network. Orrick is not aware of any misuse of the affected personal information.

At this time, Orrick does not anticipate providing notifications on behalf of additional businesses.

The information submitted herein is proprietary and confidential and should be afforded confidential treatment. If you have any questions, please do not hesitate to contact me at (206) 839-4340 or aswaminathan@orrick.com.

Respectfully yours,

Aravind Swaminathan

Partner

Orrick, Herrington & Sutcliffe, LLP

Enclosures

Exhibit A

Entities
Benveo (OK)
Roberts Oxygen Company Inc
Small Business Administration

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>

Notice of Data Breach

Dear <<first_name>>,

Orrick, Herrington & Sutcliffe, LLP (“Orrick”) writes to inform you that Orrick, a downstream service provider of <<b2b_text_1 (covered entity)>>, recently experienced a security incident that involved your personal information. Orrick has served as legal counsel for MultiPlan, Inc. (“MultiPlan”), which provides services to <<b2b_text_1 (covered entity)>>. In connection with Orrick’s representation of MultiPlan, Orrick stored files that included plan participant information related to a prior security incident for which notification was previously made. Those files were recently impacted in a security incident on Orrick’s systems. This incident did not impact MultiPlan’s or <<b2b_text_1 (covered entity)>>’s systems. Please read this notice carefully, as it provides up-to-date information on what happened and what Orrick is doing in response.

What happened?

On March 13, 2023, Orrick detected that an unauthorized third party gained remote access to a portion of Orrick’s network, including a file share that Orrick used to store certain client files. Upon detection, Orrick took immediate steps to block the unauthorized access and an investigation of the incident was launched with the support of leading outside cybersecurity experts. Orrick also notified law enforcement. Through its investigation, Orrick recently determined that on March 10, 2023, the unauthorized third party obtained files containing personal information. The health insurance plan in which you are or were enrolled was informed about the incident and Orrick has been working to identify individuals with impacted data and their contact information, which was provided to your health insurance plan in early June.

What information was involved?

Orrick recently determined that your information impacted includes: <<b2b_text_2 (data elements)>>.

What are we doing?

Orrick is offering two years of complimentary identity monitoring services through Kroll. To take advantage of these free identity monitoring services, please follow the instructions in Attachment A. You must activate by <<b2b_text_6 (activation date)>> to receive these services.

In addition to these actions, Orrick deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network.

What can you do?

Orrick is not aware of any misuse of your information. Your financial information, such as financial account information or credit card numbers, was not involved in this incident. It is always advisable to remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing online and financial accounts, credit reports, and Explanations of Benefits (“EOBs”) from your health insurers for suspicious activity. This is a best practice for all individuals. If you identify suspicious activity, you should contact the company that maintains the account on your behalf.

Additional information about how to help protect your information is contained in Attachment B.

For more information:

Orrick has established a dedicated call center to answer questions. If you have any questions regarding this incident or the services available to you, please call <<TFN>>, Monday through Friday from 9:00am to 6:30pm Eastern Time, excluding major U.S. holidays. Callers who are deaf, hard-of-hearing, or speech-disabled may utilize their TeleTYpewriter (TTY) or Telecommunication Device (TDD) to access an operator at <<TFN>>, Monday through Friday from 9:00am to 6:30pm Eastern Time, excluding major U.S. holidays.

Sincerely,

Orrick Client Support

Orrick, Herrington & Sutcliffe, LLP

Attachment A - Identity Monitoring Services

Orrick has secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services. *You have until* ***<<b2b_text_6 (Activation Deadline)>>*** *to activate your identity monitoring services*.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

Take Advantage of Your Identity Monitoring Services

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Attachment B – Information for U.S. Residents

Below are additional helpful tips you may want to consider to help protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, Orrick recommends that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	Experian:	TransUnion:
equifax.com	experian.com	transunion.com
equifax.com/personal/credit-report-services	experian.com/help	transunion.com/credit-help
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
800-685-1111	888-397-3742	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be

provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Additional Information

If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

For Massachusetts residents: You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New York residents: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at http://www.dos.ny.gov/consumerprotection or (800) 697-1220 or NYS Attorney General at http://www.ag.ny.gov/home.html or (800) 771-7755.

For New Mexico Residents: You have rights pursuant to the FCRA, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the FTC and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Commercial Services website at www.dfcs.oregon.gov/id_theft.html and click “How to get a security freeze.”

For Rhode Island residents: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>

Re: Notice of Data Breach

Dear <<first_name>>,

Orrick, Herrington & Sutcliffe, LLP ("Orrick") writes to inform you that we experienced a security incident that involved your personal information. Orrick has served as legal counsel for an entity that provides benefits administration services to health insurers (the "Client"). In connection with Orrick's representation of its Client, Orrick stored files, including files containing certain provider information, related to a prior representation of its Client. Those files were impacted in a security incident on Orrick's systems. Please read this notice carefully, as it provides up-to-date information on what happened and what Orrick is doing in response.

What happened?

On March 13, 2023, Orrick detected that an unauthorized third party gained remote access to a portion of Orrick's network, including a file share that Orrick used to store certain client files. Upon detection, Orrick took immediate steps to block the unauthorized access and an investigation of the incident was launched with the support of leading outside cybersecurity experts. Orrick also notified law enforcement. Through its investigation, Orrick determined that on March 10, 2023, the unauthorized third party obtained files containing personal information. The investigation has remained ongoing, and certain information that was contained in unstructured data, such as email and attachments to email, that belongs to you recently was identified. The effort to review and analyze the volume of unstructured data to identify impacted individuals and their contact information was completed in mid-October.

What information was involved?

We recently determined that your impacted information includes: <<b2b_text_2 (data elements)>>.

What are we doing?

Orrick is offering two years of complimentary identity monitoring services through Kroll. To take advantage of these free identity monitoring services, please follow the instructions in Attachment A. You must activate by <<b2b_text_6 (activation deadline)>> to receive these services.

In addition to these actions, Orrick deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network.

What can you do?

Orrick is not aware of any misuse of your information. Your financial information, such as financial account information or credit card numbers, was not involved in this incident. It is always advisable to remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing online and financial accounts and credit reports for suspicious activity. This is a best practice for all individuals. If you identify suspicious activity, you should contact the company that maintains the account on your behalf.

Additional information about how to help protect your information is contained in Attachment B.

For more information:

Orrick has established a dedicated call center to answer questions. If you have any questions regarding this incident or the services available to you, please call (866) 676-3916, Monday through Friday from 9:00 am to 6:30 pm Eastern Time, excluding major U.S. holidays. Callers who are deaf, hard-of-hearing, or speech-disabled may utilize their TeleTYpewriter (TTY) or Telecommunication Device (TDD) to access an operator at (866) 676-3916, Monday through Friday from 9:00 am to 6:30 pm Eastern Time, excluding major U.S. holidays.

Sincerely,

Orrick Client Support

Orrick, Herrington & Sutcliffe, LLP

Attachment A - Identity Monitoring Services

Orrick has secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who experienced an unintentional exposure of confidential data. Your identity monitoring services[1] include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services. *You have until* ***<<b2b_text_6 (Activation Deadline)>>*** *to activate your identity monitoring services*.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

Take Advantage of Your Identity Monitoring Services

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Attachment B – Information for U.S. Residents

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, Orrick recommends that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	Experian:	TransUnion:
equifax.com	experian.com	transunion.com
equifax.com/personal/credit-report-services	experian.com/help	transunion.com/credit-help
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
800-685-1111	888-397-3742	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be

provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Additional Information

If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

For Massachusetts residents: You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New York residents: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at http://www.dos.ny.gov/consumerprotection or (800) 697-1220 or NYS Attorney General at http://www.ag.ny.gov/home.html or (800) 771-7755.

For New Mexico Residents: You have rights pursuant to the FCRA, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the FTC and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Commercial Services website at www.dfcs.oregon.gov/id_theft.html and click "How to get a security freeze."

For Rhode Island residents: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

Orrick, Herrington & Sutcliffe LLP
405 Howard Street
San Francisco, CA 94105-2669
+1 415 773 5700
orrick.com

[redacted]

Re: Notice of Data Breach

Dear [redacted]

Orrick, Herrington & Sutcliffe, LLP ("Orrick") recently experienced a security event. As a large international law firm, we occasionally receive information from our clients and other third parties, including personal information, which we possess in connection with the services we provide. During our representation of a client, Orrick obtained information about you that was recently impacted in a security event on Orrick systems. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing in response.

What happened?

On March 13, 2023, we detected that an unauthorized third party gained remote access to a portion of our network, including a file share that we used to store certain client files. Upon detection, we took immediate steps to block the unauthorized access and an investigation of the incident was launched with the support of leading outside cybersecurity experts. We also notified law enforcement. We recently determined that the unauthorized third party obtained files containing personal information primarily between February 28 and March 13, 2023.

What information was involved?

We recently determined that the information affected included: [redacted]

What are we doing?

Orrick is offering two years of complimentary identity monitoring services through Kroll. To take advantage of these free identity monitoring services, please follow the instructions in Attachment A. You must activate by [redacted] to receive these services.

In addition to these actions, Orrick deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network.

What can you do?

Orrick is not aware of any misuse of your information. It is always advisable to remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing online and financial accounts, credit reports, and Explanations of Benefits ("EOBs") from your health insurers for suspicious activity. This is a best practice for all individuals. If you identify suspicious activity, you should contact the company that maintains the account on your behalf.

Additional information about how to protect your identity is contained in Attachment B.

For more information:

Orrick has established a dedicated call center to answer questions. If you have any questions regarding this incident or the services available to you, please call (866) 373-9174 Monday through Friday from 9:00 am to 6:30 pm Eastern Time, excluding major U.S. holidays.

Sincerely,

Orrick Client Support
Orrick, Herrington & Sutcliffe, LLP

[redacted]

Attachment A - Identity Monitoring Services

We have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

1. You must activate your identity monitoring services by [redacted]
2. Visit **https://enroll.krollmonitoring.com** to activate your identity monitoring services.
3. Provide Your Membership Number: [redacted]

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Attachment B – Information for U.S. Residents

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	Experian:	TransUnion:
equifax.com	experian.com	transunion.com
equifax.com/personal/credit-report-services	experian.com/help	transunion.com/credit-help
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
800-685-1111	888-397-3742	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be

provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580.

Additional Information

If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

For Massachusetts residents: You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New York residents: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at http://www.dos.ny.gov/consumerprotection or (800) 697-1220 or NYS Attorney General at http://www.ag.ny.gov/home.html or (800) 771-7755.

For New Mexico Residents: You have rights pursuant to the FCRA, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Business Services website at https://dfr.oregon.gov/financial/protect/Pages/stolen-identity.aspx and click "Place a credit freeze."

For Rhode Island residents: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).