Debevoise & Plimpton

Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022
+1 212 909 6000



**By First-Class Mail**

February 18, 2021

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

On behalf of Sequoia Capital Operations, LLC ("Sequoia"), and pursuant to N.H. Rev. Stat. Ann. § 359-C:20, this letter provides notice of a computer data security incident potentially affecting approximately 1,105 individuals in total, 2 of whom are residents of New Hampshire.

Sequoia is a venture capital firm headquartered in Menlo Park, California. On or about January 20, 2021, we learned that an unauthorized third party had gained remote access to the business email mailbox of one Sequoia employee, with the apparent aim of conducting a wire diversion scam. Our investigation has found no evidence of compromise beyond this single mailbox.

We discovered the incident after a Sequoia employee detected suspicious logins. We then quickly took steps to terminate that access and began a thorough investigation. Based on the findings of our investigation, we believe that the incident was likely the result of a phishing attack.

As part of our investigation, we engaged outside cybersecurity experts to help remediate any vulnerabilities and ensure the ongoing security of our systems, as well as conduct a detailed analysis of the contents of the affected email mailbox. We also contacted law enforcement about the incident. Our review of the mailbox, which contains over 80,000 emails, began on January 25, 2021.

Our analysis has identified that, depending on the individual in question, the unauthorized third party may have acquired a copy of the following categories of personal information of the affected New Hampshire residents: names, addresses, social security numbers, and passport numbers.

As an immediate response to the incident and to prevent recurrence of this type of incident in the future, Sequoia has enhanced its cybersecurity protections throughout its environment. Specifically, we have:

- Identified and remediated the configuration that permitted the initial access;

- Deployed additional prevention and detection technology at multiple layers to improve visibility into anomalous user activity and malicious email content;
- Reviewed the methods we use to store and share sensitive information inside and outside the company, including email message forwarding rules; and
- Refreshed our security training with additional emphasis on phishing awareness and proper data handling.

Out of an abundance of caution, Sequoia has also conducted dark web monitoring to determine whether any of the data from the mailbox has been sold or traded by cyber criminals, and we have not seen any indication that the email mailbox data is being exploited for any purpose.

While Sequoia cannot definitively determine whether any particular individual's data was acquired by the unauthorized third party, Sequoia is in the process of notifying potentially affected customers in accordance with applicable legal requirements. Sequoia anticipates sending notices via U.S. Mail beginning on or about February 19, 2021. A sample customer notification letter is attached. To protect individuals further, Sequoia has engaged Experian to provide 24 months of free credit monitoring and identity theft protection services to individuals whose personal information may have been acquired by the unauthorized third party.

Sequoia takes the protection of its customers' data seriously, and is committed to answering any questions your office may have. Please do not hesitate to contact me at the address above, at 1-212-909-6577, or agesser@debevoise.com.

Yours sincerely,

Avi Gesser

Avi Gesser

Partner

SEQUOIA CAPITAL

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

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

**NOTICE OF DATA BREACH**

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to notify you of a cybersecurity incident that occurred at Sequoia Capital Operations, LLC ("Sequoia"). Keeping personal information safe and secure is very important to us, and we deeply regret that this incident has occurred. Below you will find information about what happened, what we are doing, and what you can do.

**WHAT HAPPENED?**

On or about January 20, 2021, we learned that an unauthorized third party had gained remote access to the business email mailbox of one Sequoia employee, with the apparent aim of conducting a wire diversion scam. Our investigation has found no evidence of compromise beyond this single mailbox. We quickly took steps to secure our network and began to investigate the incident with the support of outside cybersecurity experts.

The unauthorized access to the mailbox might have allowed the third party to acquire a copy of files including certain individuals' personal information. As part of our investigation, we have analyzed the contents of the affected email mailbox and determined that it contained your personal information, and that the unauthorized third party might have accessed or acquired a copy of it.

**WHAT INFORMATION WAS INVOLVED?**

Based on our review, the unauthorized third party could have acquired personal information including your <<Insert Exposed PII>>.

**WHAT WE ARE DOING**

We took prompt steps to address this incident, including contacting law enforcement and engaging outside cybersecurity experts to help remediate and ensure the ongoing security of our systems. As part of these ongoing efforts, we have enhanced cybersecurity protections throughout our environment to detect any future anomalous activity. Specifically, we have:

- Identified and remediated the configuration that permitted the initial access;

- Deployed additional prevention and detection technology at multiple layers to improve visibility into anomalous user activity and malicious email content;
- Reviewed the methods we use to store and share sensitive information inside and outside the company, including email message forwarding rules; and
- Refreshed our security training with additional emphasis on phishing awareness and proper data handling.

Out of an abundance of caution, Sequoia has also conducted dark web monitoring to determine whether any of the data from the business email mailbox is being sold or traded by cyber criminals, and **we have not seen any indication that the email mailbox data is being exploited for any purpose.**

To protect you further, we are offering credit monitoring and identity theft protection services through Experian for 24 months, free of charge. You can find further details below on how to sign up.

**WHAT YOU CAN DO**

We strongly encourage you to contact Experian and take advantage of the credit monitoring and identity theft protection services we are providing to you free of charge. Remain vigilant and carefully review your accounts for any suspicious activity.

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained and any relevant government agency, such as the IRS, SSA, or state DMV, as applicable.

If you would like to take additional steps to protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

**CREDIT MONITORING**

To help relieve concerns and restore confidence following this incident, we have secured the services of Experian's® IdentityWorks℠ to provide identity monitoring at no cost to you for 24 months. Experian 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, Identity Detection, and Identity Theft Restoration.

Visit https://www.experianidworks.com/3bcredit to activate and take advantage of your identity monitoring services.
You have until May 31, 2021 to activate your identity monitoring services.
Activation Code: <<######>>
Engagement Number: <<######>>

Your Experian® IdentityWorks℠ membership provides you with the following key features:

- A credit card is not required for enrollment in Experian IdentityWorks.
- You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:
    - **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
    - **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
    - **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
    - **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
    - **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.[2]

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (833) 339-1511 Monday to Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number: <<#######>>. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

**FOR MORE INFORMATION**

We know you put a great deal of trust in Sequoia, and we sincerely regret that this incident has occurred. We are very sorry for any inconvenience or concern it may have caused you. If you have any questions about the incident, please contact us at privacy@sequoiacap.com or 1-800-991-3121.

Avon Puri

---

1 Offline members will be eligible to call for additional reports quarterly after enrolling.

2 The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Global Chief Digital Officer

Sequoia Capital Operations, LLC

## Additional Resources

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 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. You can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
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<br>equifax.com/personal/credit-report-services<br>P.O. Box 740241<br>Atlanta, GA 30374<br>866-349-5191 | experian.com<br>experian.com/help<br>P.O. Box 2002<br>Allen, TX 75013<br>888-397-3742 | transunion.com<br>transunion.com/credit-help<br>P.O. Box 1000<br>Chester, PA 19016<br>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; 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 Ave. N.W., Washington, D.C. 20580.

**Additional Information**

You have the right to obtain any police report filed in regard to this incident. 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 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 or to the Iowa 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.

**For New York residents:** You may contact the Office of the New York Office of the Attorney General, The Capitol, Albany NY 12224-0341, https://www.ag.ny.gov/, 1-800-771-7755.

**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.

**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 Colorado, Georgia, Maine, Maryland, New Jersey, and Vermont 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).

**For Tennessee residents:**

**TENNESSEE CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE**

You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze must be requested in writing by certified mail or by electronic means as provided by a consumer reporting agency. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. If you are actively seeking a new credit, loan, utility, or telephone account, you should understand that the procedures involved in lifting a security freeze may slow your applications for credit. You should plan ahead and lift a freeze in advance of actually applying for new credit. When you place a security freeze on your credit report, you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or authorize the release of your credit report for a period of time after the

freeze is in place. To provide that authorization you must contact the consumer reporting agency and provide all of the following:

(1) The personal identification number or password;

(2) Proper identification to verify your identity; and

(3) The proper information regarding the period of time for which the report shall be available.

A consumer reporting agency must authorize the release of your credit report no later than fifteen (15) minutes after receiving the above information.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account, that requests information in your credit report for the purposes of fraud control, or reviewing or collecting the account. Reviewing the account includes activities related to account maintenance.

You should consider filing a complaint regarding your identity theft situation with the federal trade commission and the attorney general and reporter, either in writing or via their web sites.

You have a right to bring civil action against anyone, including a consumer reporting agency, which improperly obtains access to a file, misuses file data, or fails to correct inaccurate file data.

***