WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

April 20, 2020

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Postal Mail Only

Attorney General Gordon J. MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent the Silicon Valley Community Foundation ("SVCF"), headquartered in Silicon Valley, California, with respect to a potential data security incident described in more detail below. SVCF takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

1. **Nature of the security incident.**

On or about August 23, 2018, SVCF's IT Department was notified of suspicious activity within their email environment. SVCF's IT Department conducted an investigation and concluded that three email accounts had been compromised which contained personally identifiability information ("PII"). These affected individuals were previously notified. However, on or about December of 2019, SVCF became aware that one of these mailboxes has access to a larger shared mailbox that was used to collect scholarship information also containing PII. SVCF discovered that this shared mailbox may or could have been accessed by an unauthorized user.

2. **Number of New Hampshire residents affected.**

A total of one (1) New Hampshire residents may have been potentially affected by this incident. Notification letters to these individuals were mailed on April 20, 2020, by first class mail. A sample copy of the notification letter is included with this letter.

3. **Steps taken.**

SVCF takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar event from occurring in the future, as well as to protect the privacy and security of potentially impacted individuals' information. The steps taken include conducting mandatory cybersecurity training annually, implementing multi-factor authentication, and reviewing data privacy practices for review and improvements. SVCF is also providing potentially impacted individuals with identity theft protection and credit monitoring services for a period of

twelve (12) months at no cost through Epiq.

4. Contact information.

SVCF remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

We are writing to inform you of a data security incident involving the Silicon Valley Community Foundation ("SVCF") that may have resulted in unauthorized access to some of your personal information. We take the privacy and protection of your personal information very seriously. We apologize and regret any inconvenience this may cause. This letter contains information about what happened, steps we have taken, and resources we are making available to you to help protect your identity.

On or about August 23, 2018, SVCF's IT Department was notified of suspicious activity within their email environment. SVCF's IT Department conducted an investigation and concluded that three email accounts had been compromised which contained personally identifiable information ("PII"). These affected individuals were previously notified. However, on or about December of 2019, SVCF became aware that one of these mailboxes has access to a larger shared mailbox that was used to collect scholarship information also containing PII. SVCF discovered that this shared mailbox may or could have been accessed by an unauthorized user. The personal information contained within the email account may include your name, address, photo, passport photo and number, drivers' license number, and/or school records, among other information. At this time, we have no evidence that the emails and attached documents were misused, but presume that each one has been accessed. While we are unaware of any misuse of anyone's information, we are notifying all individuals who are potentially affected by this incident.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<<6 Digit Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*:
It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Maryland, Rhode Island, Illinois, New York,* and *North Carolina*:
You can obtain information from the Maryland, Rhode Island, North Carolina, and New York Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General	**Rhode Island Office of the Attorney General**	**North Carolina Office of the Attorney General**	**Federal Trade Commission**	**New York Office of the Attorney General**
Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	Consumer Protection 150 South Main Street Providence, RI 02903 1-401-274-4400 www.riag.ri.gov	Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.gov	Consumer Response Center 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft	Bureau of Consumer Frauds & Protection The Capitol Albany, NY 12224-0341 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

---

For residents of *Massachusetts*:
It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:
Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.freeze.equifax.com	www.experian.com/freeze	freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.