



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

November 17, 2020

Bruce A. Radke
312-463-6211
312-819-1910 Direct Fax
bradke@polsinelli.com

Via Email (ATTORNEYGENERAL@DOJ.NH.GOV)

Attorney General Gordon J. MacDonald
Office of the Attorney General
Attn: Security Incident Notification
33 Capitol Street
Concord, NH 03301

Re: Notification of a Computer Security Incident Involving Personal Information Pursuant to N.H. Rev. Stat. § 359-C:20

Dear Attorney General MacDonald:

We represent Avon Old Farms School (“Avon”) in connection with an incident that involved the personal information of fifty-seven (57) New Hampshire residents, and provide this notice on behalf of Avon pursuant to N.H. Rev. Stat. § 359-C:20(I)(b). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Avon is notifying you of this incident, Avon does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY INCIDENT OR UNAUTHORIZED ACCESS

Avon contracts with Blackbaud, Inc. (“Blackbaud”) to manage its donor database within Blackbaud’s self-hosted environment. On July 16, 2020, Blackbaud notified Avon that it was impacted by a ransomware event in May 2020. Blackbaud prevented the ransomware from deploying, but the unauthorized third party exfiltrated data, including some of Avon’s student, donor, and vendor data, out of Blackbaud’s systems starting on or around April 18, 2020 through May 7, 2020. In this original communication, Blackbaud informed Avon that it encrypted the sensitive data contained within its systems. However, on October 6, 2020, Blackbaud notified Avon that it discovered the personal information, it previously believed to be encrypted prior to the incident, was unencrypted and accessible to the unauthorized third party. Upon learning of the potentially unencrypted information, Avon determined that the incident impacted certain individuals’ personal information, including, depending on the individual, their name and either their Social Security number or tax identification number.

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Washington, D.C. Wilmington
Polsinelli PC, Polsinelli LLP in California



November 17, 2020

Page 2

While Avon is not aware of any fraud or identity theft to any individual as a result of the incident, Avon provided notice of the incident to the potentially impacted New Hampshire residents.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Avon determined that the incident potentially impacted fifty-seven (57) New Hampshire residents. Avon notified the potentially impacted New Hampshire residents of the incident by letter today. Enclosed is a copy of the notice that Avon is sending to the impacted individuals.

STEPS TAKEN RELATING TO THE INCIDENT

Upon becoming aware of the incident, Avon promptly investigated the incident to determine what, if any, personal information a third party might have accessed or acquired during the incident. Avon provided complimentary identity theft protection services, through Blackbaud, to the impacted individuals and provided the individuals with information on how they can protect themselves against fraudulent activity and identity theft.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Bruce A. Radke

Enclosure

██████████
██████████
██████████
██████████



November 17, 2020

██████████
██████████
██████████

E-11

Dear ██████,

Avon Old Farms values and respects the privacy of your information, which is why we are writing to advise you of a recent data security incident involving a company called Blackbaud, Inc. Avon Old Farms, like thousands of other schools, foundations, and non-profits, contracts with Blackbaud, Inc. to manage our donor and vendor databases. We are writing to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

On July 16, 2020, Blackbaud, Inc. notified us that it was impacted by a ransomware event. According to Blackbaud, Inc., in May 2020, an unauthorized third party attempted to deploy ransomware within Blackbaud, Inc.'s environment. Blackbaud, Inc. was able to prevent the ransomware from deploying, but the threat actor was able to exfiltrate some data out of its systems.

In its original communication to us, Blackbaud, Inc. informed us that it encrypted most of the data it stores, including tax identification numbers ("TIN"). However, on October 6, 2020, Blackbaud, Inc. informed Avon Old Farms that it discovered that the personal information it previously thought was encrypted prior to the incident, was actually unencrypted and potentially accessible to the unauthorized third party. The newly discovered unencrypted information was contained in a database field not known to Avon Old Farms. After receiving this additional information from Blackbaud, Inc., we determined that some of your personal information, including your name and TIN may have been impacted by the incident. In addition, if you use your Social Security number as your TIN, as it relates to your engagement with Avon Old Farms, your Social Security number may have also been impacted by the incident.

We take our responsibility to safeguard personal information seriously and apologize for any inconvenience or concern this incident might cause. Upon learning of the incident, we worked with Blackbaud, Inc. to obtain additional information about the nature of the event. Although we are not aware of any instances of fraud or identity theft, we are offering through Blackbaud, Inc. a complimentary two-year membership of Single Bureau Credit Monitoring from CyberScout, LLC ("CyberScout"). This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Single Bureau Credit Monitoring through CyberScout is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and Single Bureau Credit Monitoring through CyberScout, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter.**

We value the trust you place in us and take our responsibility to safeguard your personal information seriously. We apologize for any inconvenience or concern this incident might cause. We are committed to taking steps to help prevent this from happening again. For further assistance, please call 1-888-675-0090 from 8:00 AM ET to 5:00 PM ET Monday – Friday.

Sincerely,



Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports 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 should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

This notice was not delayed due to a law enforcement delay.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).