[redacted]

From: Dunn, Amy Grewal <amy.dunn@faegredrinker.com>
Sent: Thursday, October 15, 2020 10:39 PM
To: DOJ: Attorney General <attorneygeneral@doj.nh.gov>; DOJ: Consumer Protection Bureau <DOJ-CPB@doj.nh.gov>
Cc: Cain, Doriann H. <doriann.cain@faegredrinker.com>
Subject: RE: Notice of Data Incident

To Whom It May Concern:

We represent Scholarship America and are writing on their behalf to provide a supplement notice in connection a recent vendor data security incident at Blackbaud, Inc. that may impact the personal information of an additional New Hampshire resident.

As provided in our initial notice to your office (please see below), Blackbaud is a data service provider for Scholarship America, and provides cloud-based data management services for hundreds of colleges, universities, foundations, and non-profits like Scholarship America. Blackbaud notified us on July 16, 2020 that it had stopped and recovered from an intrusion and ransomware attack that occurred between February and May 2020 and affected hundreds of their nonprofit clients—including Scholarship America. When making this disclosure, Blackbaud stated that it had encrypted certain data fields in the backup files, including fields containing Social Security numbers, so the cybercriminal was unable to access this information. However, on September 29, 2020, Blackbaud notified Scholarship America that this information was not encrypted, as initially disclosed. Consequently, the cybercriminal may have had access to it.

Based on our review, we have determined the unencrypted files contained personal information including names, addresses, and Social Security Numbers. Specifically, this included personal information of one (1) New Hampshire resident.

As provided in our initial notice, there is no indication that any of the compromised information is subject to further disclosure or misuse, as Blackbaud informed us that it paid a ransom to the cybercriminal after working with third-party experts and received credible confirmation that the stolen files had been destroyed. Blackbaud has also assured us that they are enhancing their safeguards to mitigate the risk of future attacks, including paying a third party service to periodically review the dark web to confirm whether any of Scholarship America's information is for sale.

A template copy of the Data Breach Notification Letter being mailed to the New Hampshire resident is attached. While Scholarship America and Blackbaud are not aware of any instances of fraud or identity theft as a result of this incident, we have again arranged for identity protection and credit monitoring services through Experian for one year for the individual in New Hampshire that was impacted.

Please contact us if you have any further questions about this incident.

Regards,
Amy

Amy Grewal Dunn
Associate
amy.dunn@faegredrinker.com
+1 317 237 1057 direct

From: Dunn, Amy Grewal
Sent: Wednesday, September 09, 2020 8:03 AM
To: 'attorneygeneral@doj.nh.gov' <attorneygeneral@doj.nh.gov>; 'doj-cpb@doj.nh.gov' <doj-cpb@doj.nh.gov>
Cc: Cain, Doriann H. <doriann.cain@faegredrinker.com>
Subject: Notice of Data Incident

To Whom It May Concern:

We represent Scholarship America and are writing on their behalf to notify you of an incident that affected the personal information of some New Hampshire residents as a result of a service provider's breach.

As background, Scholarship America was notified on July 16, 2020 by Blackbaud, a large provider of cloud-based data management services to Scholarship America and many educational institutions and other not-for-profit organizations, that it had discovered and stopped a ransomware attack that occurred from February 2020 to May 2020. Blackbaud's systems that were affected by the attack included databases containing certain information about Scholarship America's contractors, vendors and employees.

Although some information was encrypted, Scholarship America's information in one of the systems was unencrypted and was potentially acquired by the cybercriminal. This information included names, mailing addresses, email addresses, Social Security Numbers, and financial information, such as routing and account numbers and bank names. Specifically, this included personal information of 5 New Hampshire residents.

According to Blackbaud, and as far as we know, there is no indication that any of the compromised information is subject to further disclosure or misuse, as Blackbaud informed us that it paid a ransom to the cybercriminal after working with third-party experts and received credible

confirmation that the stolen files had been destroyed. Blackbaud has also assured us that they are enhancing their safeguards to mitigate the risk of future attacks, including paying a third party service to periodically review the dark web to confirm whether any of Scholarship America's information is for sale. A template copy of the Data Breach Notification Letter is attached.

Individual notifications detailing the incident are being mailed to New Hampshire residents on September 9, 2020. While Scholarship America and Blackbaud are not aware of any instances of fraud or identity theft as a result of this incident, we have arranged for identity protection and credit monitoring services for one year for the individuals in New Hampshire that were impacted.

Please contact us if you have any further questions about this incident.

Regards,
Amy

Amy Grewal Dunn
Associate
amy.dunn@faegredrinker.com
Connect: vCard

+1 317 237 1057 direct

Faegre Drinker Biddle & Reath LLP
300 N. Meridian Street, Suite 2500
Indianapolis, Indiana 46204, USA

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

October 14, 2020

F8857-L01-0000001 P001 T00001 **********MIXED AADC 159
SAMPLE A SAMPLE
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

RE: Notice of Data Breach

Dear Sample A Sample:

We are writing to notify you of a Blackbaud data security incident that may have involved some of your personal information. Scholarship America takes the protection and proper use of your information very seriously; therefore, we are contacting you to explain the incident and measures taken to protect your information.

What Happened?
Scholarship America was recently notified this past July by its financial system database provider, Blackbaud, of a security incident in which they discovered and stopped a ransomware attack. However, prior to being locked out, the cybercriminal removed backup files from Blackbaud's cloud-based platform, which hosted data for numerous colleges, universities, health care organizations and other non-profit organizations, including Scholarship America. Blackbaud stated the hackers gained access to certain Blackbaud datacenters in February 2020, and it discovered the incident in May 2020.

When making this initial disclosure, Blackbaud stated that it had encrypted certain data fields in the backup files, including fields containing Social Security numbers, so the cybercriminal was unable to access this information. However, on September 29, 2020, Blackbaud notified Scholarship America that this information was not encrypted, as initially disclosed. Consequently, the cybercriminal may have had access to it.

What Information Was Involved?
As noted above, we have determined that the stolen Scholarship America data may have contained some of your personal information, including your name, address, and Social Security number. Blackbaud paid a ransom to the cybercriminal after working with third-party experts who received credible confirmation that the stolen files had been destroyed.

What's Being Done?
Blackbaud has hired outside experts to continue to monitor the Internet, including the dark web, and they have found no evidence that any information was ever released by the cybercriminal. Furthermore, Blackbaud plans to continue such monitoring activities for the foreseeable future.

What Can You Do?
As a best practice in today's world of cybercrime, we recommend that you continue to remain vigilant and report any suspicious activity or suspected identity theft to us and the proper law enforcement authorities.

We recommend that you review the attachment called Preventing Identity Theft and Fraud for more information on ways to protect yourself and your data. Also, to assist you in protecting your information, we are offering you a complimentary #-year membership in in Experian's® IdentityWorks℠. This product provides you with identity protection services focused on immediate identification and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by: 1/31/2021 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your activation code: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by January 31, 2021. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the identity restoration services by Experian.

The Terms and Conditions for this service 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
In summary, our database provider, Blackbaud, had a data security incident that may have included some of your personal information, but Blackbaud confirmed that stolen files were ultimately destroyed. In an abundance of caution we are offering free credit monitoring services. We regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, you may contact Scholarship America at inquiries@scholarshipamerica.org or at 1-800-279-2039.

Sincerely,

Robert C. Ballard
President and CEO
Scholarship America, Inc.

Preventing Identity Theft and Fraud

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud 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 your local police or sheriff's office and your state's attorney general, as well as the Federal Trade Commission ("FTC"). You have a right to a copy of the police report, and you may need to give copies of the police report to creditors to clear up your records and access some services that are free to identity theft victims.

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps to 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: 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 www.identitytheft.gov/Know-Your-Rights or https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf. You can also request information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

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 http://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/cra/requestformfinal.pdf.

Alternatively, you may elect to obtain or purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact these national credit reporting agencies to request a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files. Contact information for these agencies is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. 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 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 http://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 free of charge, 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 using the contact information above.

You can use the following addresses and contact information to place a security freeze with each major credit bureau:

- Equifax Security Freeze. 1-800-685-1111. P.O. Box 105788, Atlanta, GA 30348-0241. www.equifax.com/personal/credit-report-services;
- Experian Security Freeze. 1-888-EXPERIAN or 1-888-397-3742. P.O. Box 9554, Allen, TX 75013. www.experian.com; or
- TransUnion. 1-800-680-7289. Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000. www.transunion.com/credit-help

In order to request a security freeze, you may need to supply your full name (including middle initial, as well as Jr., Sr., II, III, etc.), date of birth, Social Security number, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement to show proof of your current address. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning your identity theft.

The credit reporting agencies must place a security freeze on your credit report within one (1) business day after receiving a request by phone or secure electronic means, and within (3) business days after receiving your request by mail. The credit bureaus must then send written confirmation to you within five (5) business days of placing the security freeze, along with information about how to remove or lift the security freeze in the future.

Other Important State Information

You may also file a report with your local police or the police in the community where the identity theft took place. Further, you are entitled to request a copy of the police report filed in this matter.

For Maryland Residents:
You may obtain information about avoiding identity theft at: Office of the State of Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202, 1-888-743-0023 www.marylandattorneygeneral.gov.

For Washington D.C. Residents:
You obtain information about avoiding identity theft at: Office of the Attorney General for the District of Columbia 441 4th Street, NW, Washington, DC 20001, 202-727-3400 https://oag.dc.gov/.

For North Carolina Residents:
You may obtain information about avoiding identity theft at: North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001, 919-716-6400 www.ncdoj.gov.

For New Mexico Residents:
The Fair Credit Reporting Act provides certain rights in addition to the right to receive a copy of your credit report (including a free copy once every 12 months), including the right to ask for a credit score, dispute incomplete or inaccurate information, limit "prescreened" offers of credit and insurance, and seek damages from violators. 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 California Residents:
You can visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Iowa Residents:
You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Georgia, Maine, Maryland, Massachusetts, 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).