Southern New Hampshire University

August 24, 2020

securitybreach@atg.wa.gov
Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100 Olympia, WA 98504-0100

BY ELECTRONIC MAIL TO SECURITYBREACH@ATG.WA.GOV

Re: Blackbaud Data Security Incident: Southern New Hampshire University

Dear Attorney General Furguson:

I am writing to you on behalf of Southern New Hampshire University (SNHU), to notify you of a recent security incident involving unauthorized access to records in the custody of Blackbaud, a third-party alumni software services provider utilized by SNHU. This incident was the result of a criminal attack on the IT systems of Blackbaud. It occurred outside of SNHU's technology environment, and SNHU's internal security systems were not affected. It affected a backup file containing the records of 1,826 Washington residents.

SNHU was informed of this incident by Blackbaud on July 16, 2020. According to information provided by Blackbaud, the attacker may have been in their systems as early as February of 2020. Information provided to their customers states that they discovered and responded to the incident in May of 2020.

According to Blackbaud, after identifying the intrusion, they swiftly locked down their system and expelled the intruder. They involved external law enforcement and an independent forensics team to assist with response and remediation, and prevented further access or damage. They indicate they have taken significant steps to prevent similar future attacks and harden their systems.

Nature of the Security Incident: Based on information provided by the vendor, prior to being expelled from the system, the cybercriminal exported a backup file containing the following personal information:

- Biographical data: Name, Gender, Date of Birth, Marital status, Ethnicity
- Contact data: address, phone, email, communication preferences,
- Relationship data: spouse info, employment info,
- Education data: degree, major, grad date, campus, GPA
- Activity data: Event and Volunteer participation, outreach (notes on meetings, surveys sent, etc.)
- Donation data: Gift info (amount, date, fund, etc.),
- Research data: public data regarding wealth, assets, giving to other organizations, etc.
- Donor engagement information.

Blackbaud has represented to us that additional data points in the database including any payment card or financial account information, usernames, and passwords, were encrypted at all relevant times, and therefore not subject to unauthorized access.

I have attached a template copy of the notification that was sent to all affected Washington residents, by mail on August 13, 2020.

Office of General Counsel & Compliance
2500 North River Road | Manchester, NH 03106 | T: 603-665-7120 | F: 603-665-7151 | snhu.edu

Southern New Hampshire University takes incidents involving our community members' data very seriously. We are still actively processing this incident under our Incident Management Policy and procedures. The information we have at this time is subject to change as we further analyze this matter and seek additional information from the affected vendor.

Should you have any questions in follow-up to this incident, please contact me directly.

Sincerely,

Evan M. Lowry, Esq.

Assistant General Counsel
Office of General Counsel and Compliance
Southern New Hampshire University

Southern New Hampshire University
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

[redacted]

August 13, 2020

RE: Notice of Third-Party Data Security Incident

Dear [redacted],

We are writing to let you know about a data security incident at Blackbaud, a third-party vendor. Blackbaud is a software and service provider that is widely used for fundraising and alumni or donor engagement efforts at non-profits and universities, including Southern New Hampshire University ("SNHU"). SNHU first learned of this incident on July 16, 2020 when it was notified by Blackbaud.

SNHU takes the protection and proper use of your information very seriously. We are therefore contacting you out of an abundance of caution to explain the incident and timely provide you with the information that Blackbaud has provided its customers.

The incident included personal information of SNHU community members, **but the cybercriminal did not access Social Security numbers, banking, or payment card information**.

What Happened

On July 16, 2020 Blackbaud notified SNHU of a ransomware attack on their internal systems. Upon learning of the issue, we commenced an immediate and thorough investigation. That investigation is still ongoing. As part of our investigation, in addition to demanding detailed information from Blackbaud about the nature and scope of the incident, we engaged external cybersecurity professionals experienced in handling these types of incidents.

Blackbaud reported to us that they identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed us that they stopped the ransomware attack with the help of forensic experts and law enforcement, and that they prevented the cybercriminal from blocking or accessing encrypted files that contain sensitive data. Blackbaud engaged forensic experts to assist in their internal investigation. The investigation concluded that the cybercriminal removed data from Blackbaud's systems sometime between February 7, 2020 and May 20, 2020. A backup file containing certain information was removed by the cybercriminal. According to Blackbaud, they paid the cybercriminal to ensure that the backup file was permanently destroyed.

What Information Was Involved

We have determined that the compromised file may have contained your date of birth, Student ID, demographic information and philanthropic giving history, such as donation dates and amounts. **The threat actor did not access your credit card information or bank account information. As a policy, Southern New Hampshire University does not store Social Security numbers in this database.**

Blackbaud's Response and Remediation

Blackbaud has stated that their teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. They have engaged multiple third parties, including the appropriate platform vendors, to test their system security against this and other similar attack tactics. Additionally, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms. For additional information about this incident and Blackbaud's response, please visit Blackbaud's webpage dedicated to this incident at https://www.blackbaud.com/securityincident.

What You Can Do

Again, according to Blackbaud, there is no evidence to believe that any data was misused, disseminated, or otherwise made publicly available. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. As required by state law, this letter provides precautionary measures that you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

We sincerely apologize for any inconvenience this incident may cause you. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices, and those of our third-party services providers, to enhance the security and privacy of your personal information.

Should you have any further questions or concerns regarding this matter, please do not hesitate to contact our Institutional Advancement office directly at alumni@snhu.edu.

Sincerely,

Kristi Durette
Associate Vice President | Institutional Advancement / Alumni Engagement
Southern New Hampshire University

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

You may place an initial one (1) year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

2. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting each of the three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to each of the three credit reporting companies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-349-9960

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.