

CLARK HILL

Robert A. Stern
T 312.985.5940
F 312.985.5955
Email: rastern@clarkhill.com

Clark Hill
130 East Randolph Street
Suite 3900
Chicago, IL 60601
T 312.985.5900
F 312.985.5999

clarkhill.com

September 2, 2020

Attorney General Bob Ferguson

securitybreach@atg.wa.gov.

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Dear Attorney General Ferguson:

We represent Hamline University (“Hamline”) with respect to a data security incident involving Hamline’s third-party service provider, Blackbaud, Inc. (“Blackbaud”). Hamline is committed to answering any questions you may have about the data security incident, its response, and steps it has taken to prevent a similar incident in the future.

1. Nature of security incident.

On July 16, 2020, Blackbaud notified Hamline that it had experienced a ransomware attack in May 2020. As part of that communication, Blackbaud informed Hamline that it was able to detect and stop the attack prior to the deployment of ransomware, but its independent forensic investigation revealed that, prior to the attempted ransomware deployment, the threat actors successfully removed a copy of a database backup file containing a limited amount of Hamline alumni and donor information. Blackbaud also informed Hamline that all Social Security numbers, credit or debit card numbers, bank account information, and any usernames or passwords contained in the database were encrypted at rest and not at risk of compromise. After receipt of the notification from Blackbaud, Hamline reviewed the unencrypted data fields in the impacted database and discovered that a limited number of alumni and donor names, dates of birth, addresses, phone numbers, marital status, and information relating to donations and wealth status were present in the impacted database and not encrypted by Blackbaud. Blackbaud also informed Hamline that it paid the threat actors in exchange for assurances that any stolen data was deleted and received confirmation of the same after deletion.

2. Number of Washington residents affected.

Hamline sent written notice to one thousand and sixty-six (1066) Washington residents whose information was present in this Blackbaud database. The notification letter was sent to the

September 2, 2020

Page 2

potentially affected individuals on August 24, 2020 via regular mail (a copy of the form notification letter is enclosed).

3. Steps taken or plan to take relating to the incident.

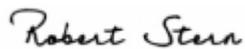
Hamline is working with Blackbaud to obtain more information about this incident, how it occurred, what improvements Blackbaud has made to its network and systems, and whether Blackbaud can encrypt all database fields going forward. Hamline also provided all recipients with contact information for the three major credit reporting bureaus, information on security freezes and fraud alerts, and contact information for Hamline if they have questions regarding this incident.

4. Contact information.

Hamline takes the security of personal information in its or its third-party service providers' control seriously and is committed to protecting the personal information of its community. If you have any questions or need additional information, please do not hesitate to contact me at Rastern@clarkhill.com or (312) 985-5940.

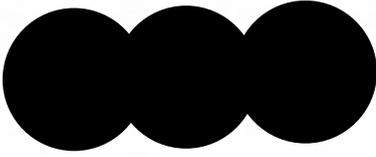
Very truly yours,

CLARK HILL



Robert A. Stern

Enclosure



August 24, 2020

Notice of Data Security Incident by Third-Party Service Provider

Dear John,

We are writing to inform you of a data security incident experienced by a third-party service provider of Hamline University (“Hamline”) that may have impacted a limited amount of your personal information, including your name, address, and date of birth. We take the privacy and security of your information seriously, and sincerely apologize for any inconvenience this may cause you. This letter explains the incident and our investigation and provides steps you can take to protect your information.

What happened?

On July 16, 2020, Hamline was notified by its third-party service provider, Blackbaud, Inc. (“Blackbaud”), that Blackbaud had experienced a ransomware attack in May 2020. Blackbaud told us that they were able to detect and stop the ransomware attack, but its independent forensic investigation revealed that the attackers had removed a copy of a backup containing a limited amount of Hamline alumni and donor information. Blackbaud is a software provider that assists Hamline with managing fundraising information for alumni and donors.

What information was involved?

The information at risk in the backup is limited to your name, address, date of birth, telephone number, email address, and information about any donations you may have made to Hamline. No Social Security numbers, bank account or credit or debit card data was at risk as this information was not stored in the database. Blackbaud advised us that they received assurances from the threat actor that the information taken from Blackbaud was deleted, but we wanted to let you know about this incident and inform you of steps we are taking in response to this incident.

What we are doing and what you can do:

The privacy and security of our alumni and donors’ information is important to us. Since learning of the incident, we are working with Blackbaud to obtain more information about the incident and steps they have taken to prevent something like this from happening again, and whether all data fields in the database and any backups can be encrypted going forward.

Blackbaud has also informed us that based on the nature of the incident, Blackbaud’s research, and third party (including law enforcement) investigation, Blackbaud has no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. While Blackbaud confirmed that limited information was impacted by this incident, it is always a good idea to remain vigilant and promptly report any suspicious activity to law enforcement.

For more information:

For questions related to this incident, please contact Denton Davidson, Director of Advancement Operations, at Hamline University by emailing ddavidson03@hamline.edu or calling (651) 523-2617. Your trust is a top priority for us, and we deeply regret any inconvenience this incident by Blackbaud may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Denton Davidson", with a long horizontal flourish extending to the right.

Denton Davidson
Director of Advancement Operations
Hamline University

Additional Information About Identity Theft Protection

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 by contacting any one or more of the following national consumer reporting agencies:

Equifax

P.O. Box 105139
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian

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

TransUnion

P.O. Box 6790
Fullerton, CA 92834
1-800-916-8800
www.transunion.com

You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Below is additional information on fraud alerts, security freezes, and steps you can take toward preventing identity theft:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via each credit bureau's website. 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. The contact information for all three credit bureaus is below. As of September 21, 2018, fraud alerts will now last one year, instead of 90 days. Fraud alerts will continue to be free and identity theft victims can still get extended fraud alerts for seven years.

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

Security Freeze: 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, each credit reporting agency has a dedicated web page for security freezes and fraud alerts or you can request a freeze by phone or by mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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 may also require 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. Effective September 21, 2018, placing a freeze on your credit report is now free for all United States citizens. Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://www.experian.com/freeze>

TransUnion

P.O. Box 2000
Chester, PA 19022
www.transunion.com/credit-freeze

More information on preventing identity theft can be obtained by contacting the Federal Trade Commission listed here:

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identityTheft.gov