Lathrop GPM

80 South Eighth Street
500 IDS Center
Minneapolis, MN 55402
Main: 612.632.3000

Lathrop GPM LLP
lathropgpm.com

Michael R. Cohen
Counsel
Michael.Cohen@lathropgpm.com
612.632.3345

August 14, 2020

VIA U.S. Mail and email ndag@nd.gov

Office of the Attorney General
Consumer Protection and Antitrust
Gateway Professional Center
1050 E Interstate Avenue
Suite 200
Bismarck, ND 58503-5574

Re: Notice of Data Security Incident

Dear Sir or Madam:

We represent the University of Minnesota Foundation located at 200 SE Oak St #500, Minneapolis, MN 55455 ("**UMF**"). We are writing to notify your office of a data security incident that may have disclosed personal information of North Dakota residents. While we do not believe any of the information has been misused, will be used inappropriately, or that the incident is reasonably likely to subject North Dakota residents to a risk of harm, we are submitting this notice in accordance with statutory requirements and to be as transparent as we can about this incident.

On July 16, 2020, UMF was notified by its third-party database provider, Blackbaud, that it had experienced a ransomware attack. Cybercriminals removed backup files from Blackbaud's platform, which hosted personal information of donors to UMF. Blackbaud believes the incident occurred between February and May 2020, and discovered the incident in May 2020.

Notice to Residents

A sample copy of the notice being sent by UMF to all of those North Dakota residents whose personal information may have been affected by this incident is included with this correspondence.

What Information Was Involved?

The file that could have been subjected to unauthorized access contained the personal information of approximately 5,061 North Dakota residents, and was limited to names, addresses and/or date of birth. This incident did not involve any sensitive personal data like credit card numbers, financial account information, or social security numbers as this data was never provided by UMF to Blackbaud.

What Steps Have Been Taken in Response?

Upon discovering the event, UMF moved quickly to investigate and respond to the incident and prepare to notify potentially affected individuals. As part of the investigation, UMF followed up with Blackbaud to learn more about the incident and what responsive steps Blackbaud had taken and what security measures would be implemented to further protect and safeguard UMF data. Blackbaud informed UMF that they worked with law enforcement and third-party experts who received credible confirmation the stolen files had been destroyed. They also informed UMF that they have hired outside experts to monitor the Internet and have found no evidence that any information was ever released by the cybercriminal. Blackbaud has promised UMF that they will continue these monitoring activities for the foreseeable future. UMF has also been assured by Blackbaud that no further unauthorized disclosure or use was made of the data.

Contact Information

Should you have any questions regarding this incident or notification please contact me at (612) 632-3345

Very truly yours,

Michael R. Cohen

UNIVERSITY OF MINNESOTA
FOUNDATION

McNamara Alumni Center
200 Oak Street SE, Suite 500
Minneapolis, MN 55455-2010
driven.umn.edu

[[DATE]]
[[NAME]]
[[ADDRESS]]
[[CITY]], [[STATE]] [[ZIP]]

RE: Notice of Data Security Incident

Dear [[NAME]]:

We are writing to let you know of a data security incident that may have involved some of your personal information. The University of Minnesota Foundation ("UMF") 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. While we do not believe that this incident is reasonably likely to subject you to a risk of harm, we are providing you with this notice in an abundance of caution and transparency.

What Happened?
We were recently notified by one of our vendors, Blackbaud Inc., of a security incident in which they stopped a ransomware attack. However, prior to being locked out, the cybercriminals removed backup files from Blackbaud's platform, which hosted data for numerous colleges, universities, health care organizations, foundations, and other non-profit organizations around the world, including UMF. Blackbaud believes the breach occurred between February and May 2020. Blackbaud discovered the incident in May, conducted an investigation, and notified UMF on July 16, 2020.

What Information Was Involved?
After a careful review, we have determined that the copied file may have contained some of your information, which is limited to your name, address and/or date of birth. **Sensitive personal data like financial information, Social Security numbers, and passwords that are likely to lead to identity theft is not maintained by UMF and is not involved in this incident.** Also, Blackbaud worked with law enforcement and third-party experts who received credible confirmation that the stolen files had been destroyed.

Risk and Continued Mitigation
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. Unfortunately, these ransomware attacks are becoming more and more common. As a best practice in today's world of cybercrime, we recommend that you remain vigilant and report any suspicious activity or suspected identity theft to us and the proper law enforcement authorities. We also recommend that you review the enclosed *Preventing Identity Theft and Fraud* for more information on ways to protect yourself and your data.

For More Information
We sincerely regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact UMF at donorrelations@umn.edu or University of Minnesota Foundation, 200 Oak St SE, Suite 500, Minneapolis, MN 55455.

Sincerely,

Kathy Schmidlkofer
President and CEO
University of Minnesota Foundation

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 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 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: 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, 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.

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/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

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.