

RECEIVED

By Consumer Protection at 11:19 am, Sep 08, 2020



A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248-220-1356
E-mail: dpaluzzi@mcdonaldhopkins.com

September 2, 2020

VIA U.S. MAIL

Office of Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188

Re: University of North Dakota Alumni Association and Foundation – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents University of North Dakota Alumni Association and Foundation (“UNDAAF”). I am writing to provide notification of an incident at Blackbaud, a third party service provider, that may affect the security of personal information of two thousand six hundred eighty-seven (2,687) Washington residents. UNDAAF uses UNDAAF uses a Blackbaud application, and Blackbaud recently experienced an incident impacting that application. UNDAAF was one of many schools, colleges, and nonprofits that were a part of this incident. UNDAAF’s investigation is ongoing and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, UNDAAF does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

On July 16, 2020, Blackbaud notified UNDAAF of a security incident affecting educational institutions and other nonprofits across the United States. Upon learning of the issue, UNDAAF commenced an investigation, which is still ongoing. Blackbaud reported to UNDAAF that Blackbaud identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed UNDAAF that they stopped the ransomware attack with the help of forensics 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. That investigation concluded that the cybercriminal removed data from Blackbaud’s systems intermittently 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.

Chicago | Cleveland | Columbus | Detroit | West Palm Beach

{9066176: }

mcdonaldhopkins.com

Office of Washington Attorney General
Consumer Protection Division
September 2, 2020
Page 2

UNDAAF learned on August 11, 2020 that it is possible that the cybercriminal may have gained access to the Washington residents' names and dates of birth. The cybercriminal did not access financial account information, credit card account information or social security number information because UNDAAF does not maintain this information.

UNDAAF has no indication that any of the information has been misused. Nevertheless, out of an abundance of caution, UNDAAF wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. UNDAAF is providing the affected residents with written notification of this incident commencing on or about September 2, 2020 in substantially the same form as the letter attached hereto. UNDAAF is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At UNDAAF, protecting the privacy of personal information is a top priority. UNDAAF is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. UNDAAF continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at 248.220.1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,



Dominic A. Paluzzi

Encl.



[REDACTED]

[REDACTED]

Dear [REDACTED]:

We are writing to let you know of a data security incident at a third-party service provider that may have involved some of your personal information. The University of North Dakota Alumni Association & Foundation ("UNDAAF") 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 have no information indicating that your personal information was misused, 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 UNDAAF. Blackbaud believes the incident occurred between February and May 2020. Blackbaud discovered the incident in May, conducted an investigation, and notified UNDAAF on July 16, 2020.

What Information Was Involved?

After a careful review, on August 11, 2020 we determined that the information removed by the threat actor may have contained some of your information, which is limited to [REDACTED]. **Sensitive personal data like financial account information, Social Security numbers, and payment card information is NOT maintained by UNDAAF and is NOT involved in this incident.** Also, Blackbaud worked with law enforcement and third-party experts and informed us that they paid the threat actor to ensure that the data was permanently destroyed.

Risk and Continued Mitigation

According to Blackbaud, there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Blackbaud indicates that it has hired a third-party team of experts, including a team of forensics accountants, to continuing monitoring for any such activity. 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 the proper law enforcement authorities. We also recommend that you review *Preventing Identity Theft and Fraud* by visiting [REDACTED] for more information on ways to protect yourself and your data.

For More Information

We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We sincerely regret any inconvenience this incident may cause you. Should you have any

[REDACTED]

[REDACTED]

further questions or concerns regarding this matter, please do not hesitate to contact our [REDACTED],
[REDACTED] at [REDACTED] or by calling [REDACTED].

Sincerely,

[REDACTED]

University of North Dakota
Alumni Association & Foundation

[REDACTED]

[REDACTED]

- 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 all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all 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.