

**RECEIVED**

By Consumer Protection at 11:54 am, Jan 19, 2021



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

January 5, 2021

**VIA U.S. MAIL**

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

**Re: Grinnell College – Incident Notification**

Dear Sir or Madam:

McDonald Hopkins PLC represents Grinnell College. I am writing to provide notification of an incident at Blackbaud, Grinnell College's third-party software and service provider, that may affect the security of personal information of approximately 2,465 Washington residents. Grinnell College'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, Grinnell College does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

On July 16, 2020, Blackbaud notified Grinnell College of a security incident that impacted its clients across the world. Blackbaud reported to Grinnell College that they identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed Grinnell College that they stopped the ransomware attack and engaged forensic experts to assist in their internal investigation. That investigation concluded that the threat actor intermittently removed data from Blackbaud's systems between February 7, 2020 and May 20, 2020.

Upon learning of the issue, Grinnell College commenced an immediate and thorough investigation. That investigation is still ongoing. As a part of its investigation, in addition to demanding detailed information from Blackbaud about the nature and scope of the incident, Grinnell College engaged outside experts experienced in handling these types of incidents to help determine the impact to its stakeholders and appropriately notify them. On September 29, 2020, Grinnell College determined that the information removed by the threat actor may have contained a limited amount of personal information, including the affected residents' full names and dates of birth and/or student identification number.

According to Blackbaud, they paid the threat actor to ensure that the data was permanently destroyed, and there is no evidence to believe that any data will be misused, disseminated, or

otherwise made publicly available. Blackbaud also indicates that it has hired a third-party team of experts, including a team of forensics accountants, to continue monitoring for any such activity. Nevertheless, out of an abundance of caution, Grinnell College 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. Grinnell College is providing the affected residents with written notification of this incident commencing on or about January 5, 2021, in substantially the same form as the letter attached hereto. Grinnell College 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 Grinnell College, protecting the privacy of personal information is a top priority. Grinnell College remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Blackbaud has assured Grinnell College that they closed the vulnerability that allowed the incident and that they are enhancing their security controls and conducting ongoing efforts against incidents like this in the future. Grinnell College continually evaluates and modifies its practices, and those of its third party service providers, 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](mailto:dpaluzzi@mcdonaldhopkins.com). Thank you for your cooperation.

Sincerely,



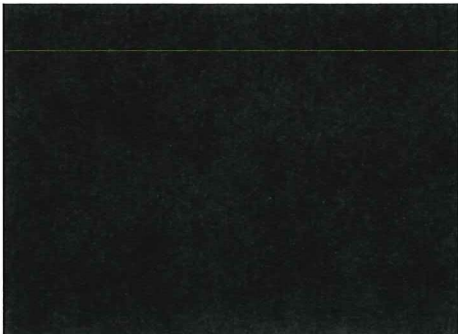
Dominic A. Paluzzi

Encl.





Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336



Dear <img alt="Redacted name" data-bbox="115 342 205 359"/>

The privacy and security of the personal information we maintain is of the utmost importance to Grinnell College. We are writing with important information regarding a data security incident at Blackbaud, a third party service provider, which may have involved some of the information that you provided to Grinnell College. Blackbaud is a software and service provider that is widely used for fundraising and alumni or donor engagement efforts at non-profits and universities world-wide. Grinnell College uses several Blackbaud applications, and Blackbaud experienced an incident impacting one or more of those applications. We want to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

*What Happened?*

On July 16, 2020, Blackbaud notified Grinnell College of a security incident that impacted its clients across the world. 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 and engaged forensic experts to assist in their internal investigation. That investigation concluded that the threat actor intermittently removed data from Blackbaud's systems between February 7, 2020 and May 20, 2020. According to Blackbaud, they paid the threat actor to ensure that the data was permanently destroyed.

*What We Are Doing.*

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 cybersecurity professionals experienced in handling these types of incidents.

*What Information Was Involved.*

On September 29, 2020, following an extensive review and analysis of the data at issue, we determined that the information removed by the threat actor may have contained some of your personal information, including your full name and date of birth. **Your Social Security number was not exposed since it was not stored by Grinnell College in the Blackbaud application. Additionally, financial account information and/or payment card information were not exposed, as they were encrypted.** Your demographic information, contact information, and/or philanthropic giving history, such as donation dates and amounts, may have also been removed by the threat actor.

*What You Can Do.*

**According to Blackbaud, there is no evidence to support the belief 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.** Nevertheless, out of an abundance of caution, we want to make you aware of the incident. 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 and report any suspicious activity to the proper authorities.

– 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](http://www.equifax.com)  
1-800-525-6285

**Experian**  
P.O. Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742

**TransUnion LLC**  
P.O. Box 2000  
Chester, PA 19016  
[www.transunion.com](http://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](http://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](http://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.