

Appendix

Pennington Biomedical Research Foundation (“Pennington”) received notice from its third-party vendor, Blackbaud, Inc. (“Blackbaud”) about a data security incident that occurred at Blackbaud. Blackbaud is a cloud-based software company that provides customer relationship management and financial services tools to thousands of schools, hospitals, and non-profits globally, including Pennington. On July 16, 2020, Blackbaud informed Pennington, along with numerous other institutions, it had discovered that an unauthorized individual had gained access to its systems between February 7 and May 20, 2020. Blackbaud further advised that the unauthorized individual acquired backup copies of databases used by its customers, including a backup of Pennington’s accounting and donor databases.

On August 3, 2020, Pennington’s investigation and review of the Blackbaud database revealed that it contained some information belonging to one (1) Maine resident, including the individual’s name and Social Security number. Pennington mailed notification letters to the Maine resident on September 28, 2020 in accordance with Me. Rev. Stat. Tit. 10, §1348,¹ and offered the resident twelve months of complimentary identity monitoring services through Experian. A copy of the notification letter is enclosed.

To help prevent this from happening again, Pennington is evaluating its institutional relationship with Blackbaud, Blackbaud’s security measures, and the scope of data Pennington stores within Blackbaud’s system.

¹ This report is not, and does not constitute, a waiver of Pennington’s objection that Maine lacks personal jurisdiction over Pennington regarding any claims related to this data security incident.

<<Letterhead>>

<<FIRST NAME>> <<LAST NAME>>

<<ADDRESS 1>>

<<ADDRESS 2>>

<<CITY>>, <<STATE>> <<ZIP CODE>>

Dear <<FIRST NAME>> <<LAST NAME>>

Pennington Biomedical Research Foundation (“Pennington”) is committed to protecting the security and privacy of personal information. Regrettably, this notice is regarding a ransomware attack that occurred at one of our third-party software providers, Blackbaud, Inc. (“Blackbaud”) that may have involved some of your personal information.

What Happened

Blackbaud is a cloud-based software company that provides customer relationship management and financial services tools to thousands of schools, hospitals, and non-profits globally, including Pennington. On July 16, 2020, Blackbaud informed us, along with numerous other institutions, it had discovered that an unauthorized individual had gained access to its systems between February 7 and May 20, 2020. Blackbaud advised us that the unauthorized individual acquired backup copies of databases used by its customers, including a backup of our accounting and donor databases.

Upon learning of the incident from Blackbaud, we immediately began conducting our own investigation of the Blackbaud services we use, as well as the information provided by Blackbaud to determine what information was involved in the incident.

What Information Was Involved

Based on our review of the database, we determined on August 3, 2020 that the stolen information unfortunately contained some of your personal information including your name and <<affected data sets>>.

What You Can Do

Though we have no evidence that your personal information has been misused, and Blackbaud informed us that they believe the actors involved destroyed the information when the ransom was paid, we wanted to let you know this happened and assure you we are taking this incident very seriously. As a precaution, we are offering you a complimentary membership of Experian’s® IdentityWorksSM. This product provides you with identity detection and resolution of identity theft. IdentityWorks is completely free to you and enrolling in this program will not hurt your credit score. For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the additional information provided in the following pages.

What We Are Doing

We are notifying you of this incident and sharing the steps that we, and Blackbaud, are taking in response to this incident. Blackbaud has informed us that they identified and fixed the vulnerability associated with this incident and are implementing additional security enhancements. To help prevent this from

happening again, we are evaluating our institutional relationship with Blackbaud, their security measures, and the scope of data we store within Blackbaud's system.

For More Information

We sincerely regret that this incident occurred through our third-party vendor and apologize for any inconvenience. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact us directly at 225-763-2684 or info@pbrf.org.

Sincerely,

[signature image]
Janet L. Olson
Board Chair

[signature image]
Rebecca F. Schutte
President/CEO

[signature image]
Brad Jewell
Senior Vice President/CFO & COO

Activate IdentityWorks Now in Three Easy Steps

1. ENROLL by: **[Date]** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: www.experianidworks.com/3bcredit
3. PROVIDE the **Activation Code**: **[Code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(877) 890-9332**. Be prepared to provide engagement number **[Engagement #]** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud. Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at www.experianidworks.com/3bcredit or call (877) 890-9332 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **(877) 890-9332**.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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 bureau will provide you with 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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov. You may contact Pennington Biomedical Research Foundation for more information by mail at 6400 Perkins Road, Baton Rouge, LA 70808 or by phone at (225) 763-2511.

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us. You may contact Pennington Biomedical Research Foundation for more information by mail at 6400 Perkins Road, Baton Rouge, LA 70808 or by phone at (225) 763-2511.

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov