

17474



UNIVERSITY OF  
**South Carolina**

**Business Partnership Foundation**

Name

Address

August 18, 2020

RE: Notice of Third-Party Vendor Data Incident

Dear Name,

The University of South Carolina – Business Partnership Foundation and its wholly-owned subsidiary, Corporate Solutions, LLC, are writing to notify you that Blackbaud, Inc., one of our vendors, recently made us aware of a data security incident that may have affected some of your personal data.

**What Happened?**

On July 16, 2020, we were notified that Blackbaud, an outside vendor, discovered and stopped a ransomware attack of Blackbaud's self-hosted platform in May 2020. Blackbaud is a global market leader in third-party applications used by many charities, health, and educational organizations in the U.S. and abroad.

According to Blackbaud, prior to being locked out, the cybercriminal removed a copy of a subset of data from its self-hosted environment which contained information related to individuals affiliated with multiple charitable institutions. Blackbaud reports that it paid the cybercriminal's demand and received confirmation that the copy of the data removed has been destroyed. According to Blackbaud, this incident occurred at some point between February 7, 2020 and May 20, 2020 and was discovered in May of 2020.

**What Information Was Involved?**

Based on review of our records your name, address and social security number may have been involved in the incident.

Based on the nature of the incident, Blackbaud's research, and third-party investigation, including investigation by law enforcement, Blackbaud has stated that it 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. Blackbaud reports it has hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

### **What Are We Doing?**

We are offering you two (2) years of free credit monitoring and \$1 million in identity theft insurance through Experian - to give you peace of mind. You must activate the Experian product by the activation date in order for it to be effective. The activation instructions are included with this notification.

Additionally, we are reviewing all relevant practices regarding the security of Blackbaud data. Blackbaud reported that it has implemented numerous security changes. Blackbaud stated that it quickly identified the vulnerability associated with this incident and took swift action to fix it. Blackbaud stated that it has confirmed through testing by multiple third parties that its fix withstands all known attack tactics. Finally, Blackbaud asserted that it is further hardening its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.

As we continue to monitor this incident, we will update you to the extent that we are legally required.

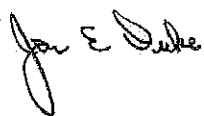
### **What Can You Do?**

While Blackbaud has stated that it 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, we still recommend you take precaution and activate the free credit monitoring. Also, we have included some additional steps that you can take to protect yourself, as you deem appropriate.

**For More Information About This Incident**, you can consult the Blackbaud website at <https://www.blackbaud.com/securityincident>. If you have additional questions about this incident, please email us at [foundation@moore.sc.edu](mailto:foundation@moore.sc.edu) or leave us a message at 803-576-8486, and include your full name, phone number, and your question(s), and we will respond with the information that we have at that time.

We apologize for any inconvenience this event may have caused you.

Sincerely,



Jean E. Duke  
President  
University of South Carolina – Business Partnership Foundation

## **STEPS YOU CAN TAKE**

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by 11/30/2020. (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: XXXXXXXX

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 by 11/30/2020. Be prepared to provide engagement number XXXXXXXX as proof of eligibility for the identity restoration services by Experian.

## **ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:**

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.890.9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

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

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

**Below are additional actions you may take, if you feel it is necessary.**

➤ **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Note that a security freeze generally does not apply to existing account relationships and when a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a security freeze. To place a security freeze on your credit report, contact each of the three major consumer reporting agencies using the contact information listed below:

### 3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES

**Equifax**

P.O. Box 105788  
Atlanta, GA 30348  
1-800-525-6285  
www.equifax.com

**Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
www.experian.com

**TransUnion**

P.O. Box 2000  
Chester, PA 19022  
1-800-680-7289  
www.transunion.com

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.), Social Security number, and date of birth;
- If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security

number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving the request to remove the freeze.

➤ **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is an alert lasting 7 years. Contact the credit reporting agencies listed above to activate an alert.

➤ **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS, & REPORT FRAUD.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity. Report suspicious or fraudulent charges to your insurance statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor and law enforcement. (For Oregon & Iowa residents: Report any suspected identity theft to law enforcement, Federal Trade Commission, and your State Attorney General.)

➤ **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 877-322-8228 to obtain one free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

➤ **POLICE REPORT:** You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it.

➤ **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM FTC / STATE ATTORNEY GENERAL.** Go to <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html>. The Federal Trade Commission also provides information at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft). The FTC can be reached by phone: 1 - 877-438-4338; TTY: 1-866-653-4261 or by writing: 600 Pennsylvania Ave., NW, Washington, D.C. 20580. Your State Attorney General also may provide information. For North Carolina residents: You may contact North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), 1-877-566-7226.

➤ **FILE YOUR TAXES QUICKLY AND SUBMIT IRS FORM 14039.** If you believe you are at risk for taxpayer refund fraud, the IRS suggests you file your income taxes quickly. Additionally, if you are an actual or potential victim of identity theft, the IRS suggests you give them notice by submitting IRS Form 14039 (Identity Theft Affidavit). This form will allow the IRS to flag your taxpayer account to alert them of any suspicious activity. Form 14039 may be found at <https://www.irs.gov/pub/irs-pdf/f14039.pdf>.

➤ **FAIR CREDIT REPORTING ACT:** You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit [www.ftc.gov/credit](http://www.ftc.gov/credit). The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Please note that identity theft victims and active duty military personnel may have additional rights under the FCRA.

➤ **PROTECT YOURSELF FROM PHISHING SCAMS.** Learn to recognize phishing emails. Do not open emails from unknown senders and be sure not to click on strange links or attachments. Never enter your username and password without verifying the legitimacy of the request by contacting the sender by telephone or other methods. Replying to the email is not a safe way to confirm. Visit <https://www.consumer.ftc.gov/articles/0003-phishing> for more information on these types of scams.

17474

**BAKER DONELSON**  
BEARMAN, CALDWELL & BERKOWITZ, PC

CHASE NORTH TOWER  
450 LAUREL STREET  
21ST FLOOR  
BATON ROUGE, LOUISIANA  
70801

PHONE: 225.381.7000  
FAX: 225.343.3612

www.bakerdonelson.com

RECEIVED

AUG 26 2020

LAYNA S. COOK RUSH, SHAREHOLDER  
Direct Dial: 225.381.7043  
Direct Fax: 225.382.0243  
E-Mail Address: lrush@bakerdonelson.com

OFFICE OF CONSUMER AFFAIRS

August 19, 2020

Attorney General Maura Healey  
Consumer Protection Division  
Attn: Data Breach Notification  
One Ashburton Place  
Boston, MA 02108

Office of Consumer Affairs and Business Regulation  
501 Boylston Street, Suite 5100  
Boston, MA 02116

Re: *University of South Carolina - Business Partnership Foundation - Notice of Vendor Data Incident*

Dear Attorney General Healey and Others Whom It May Concern:

I serve as outside counsel to University of South Carolina - Business Partnership Foundation (the "Foundation"), a not-for-profit organization whose principal place of business is located at 1014 Greene Street, Columbia, South Carolina 29208. The Foundation was recently notified by Blackbaud, Inc., one of its vendors, of a vendor data incident. Blackbaud is a global market leader in third-party applications used by many charities, health, and educational organizations in the U.S. and abroad. The Foundation does not maintain any physical facilities in Massachusetts and the incident did not affect the Foundation's computer systems.<sup>1</sup>

On July 16, 2020, we were notified that Blackbaud discovered and stopped a ransomware attack of Blackbaud's self-hosted platform in May 2020. According to Blackbaud, this incident occurred at some point between February 7, 2020 and May 20, 2020.<sup>2</sup> Due to the risk that personally identifiable information ("PII") may have been accessed or acquired during the incident, in an abundance of caution, notification letters are being sent by my client via U.S. Mail

<sup>1</sup> By providing this notice, the Foundation does not waive any rights or defenses regarding the applicability of your State's law, the applicability of your State's data event notification statute, or personal jurisdiction.

<sup>2</sup> Blackbaud has stated that it reported the incident to law enforcement.

WP

August 19, 2020

Page 2

to 5 residents of your State on or about August 21, 2020, in accordance with M.G.L.A. 93H § 3. The PII that was potentially at risk included the first and last name and Social Security number. The notification letter includes instructions for activating two (2) years of credit monitoring services at no cost to the resident. A sample notification letter is enclosed for your reference and includes:

- A description of the security incident;
- Steps taken to investigate;
- Steps taken to mitigate any potential harm to consumers;
- Instructions for activation of 2 years of free identity theft protection services that include credit monitoring and a \$1 million insurance reimbursement policy to all consumers who received notification, in accordance with M.G.L.A. 93H § 3A;
- Instructions on how to place a security freeze on the recipient's consumer credit report; and
- Instructions regarding how to obtain more information about this event, etc.

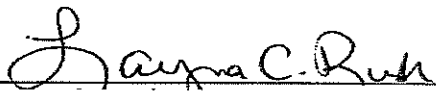
The Foundation is fully committed to protecting consumer privacy and the confidentiality of personal information. To that end, the Foundation has a written information security policy.

We will follow-up this correspondence with any forms or other documents that may need to be completed. Please contact me if you require any additional information regarding this incident.

Sincerely,

BAKER, DONELSON, BEARMAN,  
CALDWELL & BERKOWITZ, PC

By:

  
Layna C. Rush

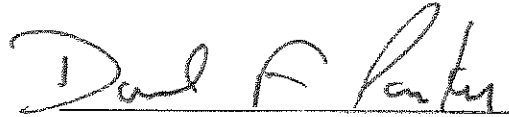
**Enclosure:**

Exhibit 1: Sample Notification Letter sent to 5 residents



**Certification of Compliance with M.G.L.A 93H, § 3A**

On behalf of the University of South Carolina -Business Partnership Foundation, I certify that the University of South Carolina - Business Partnership Foundation has contracted with Experian Consumer Services to offer the five (5) Massachusetts resident(s) whose Social Security number was potentially involved in this incident with two (2) years of credit monitoring services at no cost to the resident. The notification letter to the resident includes the instructions from Experian for enrolling in the credit monitoring services. The University of South Carolina - Business Partnership Foundation is not requiring that the resident waive his/her right to a private cause of action against the University of South Carolina - Business Partnership Foundation as a condition of the University of South Carolina - Business Partnership Foundation's offer of credit monitoring services.



**David F. Parker**

Vice President

USC - Business Partnership Foundation