

## Appendix

On July 16, 2020, Fort Hays State University Foundation (“FHSUF”) was notified by Blackbaud of a ransomware attack on Blackbaud’s network that the company discovered in May of 2020. Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits. Blackbaud reported that it conducted an investigation, determined that backup files containing information from some of its clients had been taken from its network, and an attempt was made to encrypt files to convince Blackbaud to pay a ransom. Blackbaud paid a ransom and obtained confirmation that the files that had been removed had been destroyed. Blackbaud also reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, FHSUF conducted its own investigation of the Blackbaud services used by FHSUF and the information provided by Blackbaud to determine what information was involved in the incident. On August 26, 2020, FHSUF determined that the backup files contained certain information pertaining to one Maine resident, including the resident’s name and Social Security number.

Beginning today, October 13, 2020, FHSUF is providing written notice to the Maine resident by mailing a letter via United States Postal Service First-Class mail.<sup>1</sup> FHSUF is offering the Maine resident a complimentary, one-year membership to credit monitoring and identity theft prevention services through Experian. FHSUF is recommending that the affected individuals remain vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. FHSUF has also established a dedicated phone number where the individuals may obtain more information regarding the incident.

Blackbaud has informed FHSUF that they identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect data from any subsequent incidents, and are undertaking additional efforts to improve the security of its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based monitoring tools.

---

<sup>1</sup> This report does not waive FHSUF’s objection that Maine lacks personal jurisdiction over it related to any claims that may arise from this incident.



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

You have trusted the FHSU Foundation with your philanthropy and advocacy and our goal is to continue to earn that trust. For this reason, we write to inform you that the FHSU Foundation, along with many other institutions, was recently notified by Blackbaud of a security incident. Blackbaud is the system that the FHSU Foundation uses to record and store information related to alumni and philanthropic giving to the institution. This notice explains the incident and the various measures taken in response.

#### *What Happened*

Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits. On July 16, 2020, Blackbaud notified the FHSU Foundation that it had discovered a ransomware attack on Blackbaud's network in May 2020. Blackbaud reported that it conducted an investigation, determined that backup files containing information from its clients had been removed from its network, and an attempt was made to encrypt files to convince Blackbaud to pay a ransom. Blackbaud paid a ransom and obtained confirmation that the removed files were destroyed. Blackbaud reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, we conducted our own investigation of Blackbaud services and used the information provided by Blackbaud to determine what information was involved in the incident. On August 26, 2020, we determined that our backup files contained certain information pertaining to you.

#### *What Information Was Involved*

The backup file involved contained your Name and Social Security number. Blackbaud has assured us that the backup file has been destroyed by the unauthorized individual and there is no reason to believe any data was or will be misused or will be disseminated or otherwise made available publicly.

#### *What You Can Do*

Even though we have no evidence that your personal information has been misused, we wanted to let you know this happened and assure you we take it very seriously. As a precaution, we are offering you a complimentary membership of Experian's® IdentityWorks<sup>SM</sup>. 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.

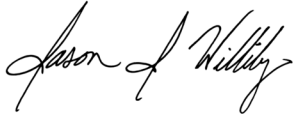
### *What Steps We Are Taking*

We are notifying you of this incident and sharing the steps that we, and Blackbaud, are taking in response. Blackbaud has informed us that they identified and fixed the vulnerability associated with this incident and have implemented several changes that will better protect your data from any subsequent incidents. Blackbaud is undertaking additional efforts to improve the security of its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based monitoring tools.

### *For More Information*

Your continued trust in our organization is of utmost importance and we regret that this occurred and apologize for any inconvenience. Should you have any questions or concerns regarding this matter, please contact FHSU Foundation staff, Travis Scoby at 785-628-4584 or Darci Cain at 785-628-5719.

Sincerely,

A handwritten signature in black ink that reads "Jason J. Williby". The signature is written in a cursive, flowing style.

Jason J. Williby, CFRE  
President & CEO  
FHSU Foundation

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

### Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b\_text\_1(EnrollmentDeadline)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<Member ID>>

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 <<b2b\_text\_2(EngagementNumber)>> 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 <https://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](http://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.

### Additional information for residents of the following states:

**New Mexico: A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.

- 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.
- You may seek damages from violators.

Identity theft victims and active duty military personnel have additional rights.

**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](http://www.ncdoj.gov)

\* 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.