CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JOHN LOYAL
jloyal@c-wlaw.com

JASON MICHAEL GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

April 6, 2021

Via Mail
Office of Attorney General
33 Capitol Street
Concord, New Hampshire 03302

RE: Security Incident Notification

To Whom It May Concern:

I serve as counsel for the Chadron State Foundation (hereinafter "CSF"), and provide this notification to you of a recent data security incident suffered by Blackbaud. Blackbaud is one of the world's largest providers of customer relationship management systems, serving more than 35,000 clients around the world in the nonprofit and education sectors, including CSF. On July 16, 2020, CSF was notified by Blackbaud that it had discovered and stopped a ransomware attack that occurred in May 2020. According to the notification received by CSF, Blackbaud's systems that were affected by the attack included a database containing certain information about CSF's community. Blackbaud's notification stated that the attacker(s) may have acquired an unknown amount of data maintained within Blackbaud's database. Blackbaud informed us that it paid a ransom to the attacker and obtained confirmation that the compromised information had been destroyed and is no longer in the possession of the attacker(s). According to Blackbaud, and as far as we know, there is no indication that any of the compromised information has been subject to misuse or to further disclosure. Based on the information available at the time, CSF immediately notified its community of the incident by email, as well as through a posting within CSF's magazine.

Blackbaud has made numerous assurances that bank account information, usernames, passwords, and Social Security numbers that may have been contained in the affected systems were encrypted and the decryption keys were not compromised. On January 11, 2021, despite Blackbaud's assurances, CSF discovered that individuals' Social Security number may be contained within the affected Blackbaud database. CSF immediately investigated and worked to confirm whether this information was present and encrypted. On March 9, 2021, our investigation confirmed that individuals' Social Security numbers were included within the database and was not encrypted. CSF immediately worked to obtain current address information for affected individuals in order to provide notification.

On March 19, 2021, after a thorough review process, CSF confirmed that six (6) residents of New Hampshire were potentially impacted as a result of this incident, as their Social Security number was found within the Blackbaud database. CSF is taking steps to remove this information from their database.

CSF is working to provide notification, including complimentary credit monitoring services for one (1) year, to affected individuals as soon as possible which will be mailed on April 6, 2021. A copy of the drafted letter is attached. CSF is taking steps to comply with all applicable notification obligations.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: John Loyal
John Loyal

CHADRON STATE ALUMNI

Chadron State Alumni and Foundation
1000 Main Street
Chadron NE 69337

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

The Chadron State Foundation is writing to inform you of a data security incident experienced by Blackbaud, Inc. ("Blackbaud") that was described in an email distributed on, as well as a posting within our most recent issue of the Chadron State Magazine. Blackbaud is a provider of cloud-based database management services to the Foundation, as well as many other not-for-profit organizations, schools, colleges and universities worldwide.

We take the privacy and security of all information very seriously. While we have no evidence to suggest that any of the impacted information was viewed or misused during this incident, it is crucial that we be as supportive and transparent as possible.

What Happened:

On July 16, 2020, we were notified by Blackbaud that it had discovered and stopped a ransomware attack that occurred between February 7, 2020 and May 20, 2020. Blackbaud's systems that were affected by the attack included a database containing certain data related to the Foundation. According to the notification provided by Blackbaud, the attacker(s) may have acquired an unknown amount of data maintained within Blackbaud's database. Blackbaud informed us that it paid a demand to the attacker and obtained confirmation that the compromised information had been destroyed and is no longer in the possession of the attacker(s). According to Blackbaud, and as far as we know, there is no indication that any of the compromised information has been subject to misuse or to further disclosure. Blackbaud has also assured us that they are enhancing their safeguards to mitigate the risk of future attacks.

Blackbaud's initial notification contained minimal information regarding the scope of impacted information as it relates to the Foundation and our community. Upon discovery, we immediately notified our community based on the information available to us at the time.

What Information Was Involved:

According to Blackbaud's initial notification, as well as several separate assurances, bank account information, usernames, passwords, and Social Security numbers that may have been entered into the affected systems were encrypted and the decryption keys were not compromised. On January 11, 2021, the Foundation discovered that your Social Security number may be contained within the affected Blackbaud database. The Foundation immediately investigated and worked to confirm whether this information was present and encrypted. On March 9, 2021, our investigation confirmed that your Social Security number was included within the database and was not encrypted.

What We Are Doing:

Blackbaud has indicated that they have taken efforts to further secure their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms. Additionally, we are offering complimentary credit monitoring services to protect the security of your personal information. Information regarding the credit monitoring services being offered are provided below.

Identity Monitoring:

As a safeguard, we have arranged for you to activate identity monitoring services for 12 months provided by Kroll, a global leader in risk mitigation and response, at no cost to you. Your monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Due to privacy laws, we cannot activate these services on your behalf. Additional information regarding how to activate the complimentary identity monitoring service is enclosed.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

For More Information:

Should you have questions or concerns regarding this matter, please do not hesitate to contact 1-XXX-XXX-XXXX, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. The security of our community's personal information is of the utmost importance to us and we deeply regret this incident.

We stay committed to protecting your trust in us and continue to be thankful for your support of the Foundation. Please accept our regret for any worry or inconvenience that this Blackbaud incident may cause you.

Sincerely,

Ben Watson
Chief Executive Officer
Chadron State Foundation

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

You have until **July 1, 2021** to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/ account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit 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 credit freeze 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or

your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Chadron State Foundation may be contacted at 1000 Main St., Chadron, NE 69337.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection. Chadron State Foundation may be contacted at 1000 Main St., Chadron, NE 69337.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.