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

March 11, 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 Norwich University (hereinafter "Norwich"), 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 Norwich. On July 16, 2020, Norwich was notified by Blackbaud that it had discovered and stopped a ransomware attack that occurred in May 2020. According to the notification received by Norwich, Blackbaud's systems that were affected by the attack included a database containing limited information about Norwich's community, including individuals' contact information, as well as a history of their relationship with Norwich. Further, Blackbaud 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. Immediately upon receiving notification from Blackbaud, Norwich worked to provide general notification of this incident to its community based on the information provided by Blackbaud.

Blackbaud 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. However, instead of relying on the representations made by Blackbaud, and in order to independently verify Blackbaud's investigation, Norwich requested a backup file of their Blackbaud database. Once received, Norwich immediately began working to review the data to determine whether sensitive information was contained within the database. However, due to the complexity of the database file provided by Blackbaud, this took significant time and effort with the assistance of third-party

forensic experts. At this time, Norwich had no reason to believe that personal information of any resident of New Hampshire was impacted.

On February 8, 2021, Norwich learned of all individuals contained within the Blackbaud database, as well as the potentially impacted information. Based on this information, Norwich discovered that the personal information of approximately seven (7) residents of New Hampshire was potentially impacted as a result of this incident. The personal information potentially impacted as it relates to these seven (7) individuals includes one or more of the following data types: Social Security number, financial account number, credit card number, and treatment/diagnosis information.

Norwich worked to provide formal notification to affected individuals, including complimentary credit monitoring services for two (2) years, which was mailed on March 10, 2021, with the expected receipt by the affected individuals within the next several days. Norwich is taking steps to comply with all applicable notification obligations. Notably, our investigation is currently ongoing and therefore, we will supplement this notification should we learn whether additional New Hampshire residents are impacted.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: John Loyal
John Loyal

NORWICH UNIVERSITY
1819
Expect Challenge. Achieve Distinction.

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

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: <<NOTICE OF DATA BREACH/Important Security Notification>>. Please read this entire letter.

Dear <<Name 1>>:

Norwich University is writing to inform you of a data security incident experienced by Blackbaud, Inc. ("Blackbaud"), a provider of cloud-based database management services to Norwich, 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 compromise, it is crucial that we be as supportive and transparent as possible. That is why we are proactively writing to inform you of this incident, to offer information about steps that can be taken to help protect your information, and to let you know about complimentary credit monitoring services that are being offered to you.

What Happened:

On July 16, 2020, we were notified by Blackbaud that it had discovered and terminated 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 Norwich. 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. Nevertheless, out of an abundance of caution, we wanted to advise you of this incident and provide you with resources to protect your personal information.

Blackbaud's initial notification contained minimal information regarding the scope of impacted information as it relates to Norwich and our community. Upon discovery, we immediately undertook an in-depth investigation, with the assistance of independent forensic experts, into the impacted data. Due to the complex nature of the data provided by Blackbaud, this process took significant 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. Despite these assurances, we immediately informed our community of this incident on July 24, 2020, and provided the information available to us at this time. Additionally, instead of relying on the representations made by Blackbaud, and in order to independently verify Blackbaud's investigation, Norwich requested a backup file of the Blackbaud database. On February 8, 2021, after significant investigation, Norwich discovered that the potentially impacted information includes your name, along with one or more of the following data elements: date of birth; social security number; financial account number; credit card number; and/or diagnosis information.

What Is Being Done:

Blackbaud has indicated that they are taking 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 is provided below.

Credit Montoring:

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies for 24 months. Due to privacy laws, we cannot register you directly. Additional information regarding how to enroll in the complimentary credit 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 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 855-435-0531 Monday through Friday, 9 am to 9 pm (excluding US holidays). The security of our community's personal information is of the utmost importance to us and we deeply regret this incident.

We remain committed to ensuring your trust in us and continue to be thankful for your support. Please accept our sincere regret for any concern or inconvenience that this Blackbaud incident may cause you.

Sincerely,

Reed Curry
Assistant Vice President of Development
Norwich University

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

TransUnion® *my*TrueIdentity provides you with the following key features:

- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- 24 months of unlimited access to your TransUnion® credit report and credit score.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible.[1]

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

➢ PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE

An **initial 1-year security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

TransUnion
Fraud Victim Assistance Dept.
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

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

Equifax
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

➢ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. In order to request a security freeze,you will need to provide some or all of the following informationto the credit reporting agency, depending on whether you do so online, by phone, or by mail: 1. Your full name (including middle initial as well

[1] (Policy limitations and exclusions may apply.)

as Jr., Sr., II, III, etc.); 2. Social Security Number; 3. Date of birth; 4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years; 5. Proof of current address,suchas a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); 7. Social Security Card, pay stub, or W2; 8. 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.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit www.annualcreditreport.com or call 1-877-322-8228. 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.

- **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

- **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements.
Be proactive and create alerts on credit cards and bank accounts to notify you of activity.
If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)**

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: (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 your employees; (v) you may limit "prescreened" offers of credit an insurance you get based on information in your credit report; (vi) and you may seek damages from a violator. 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, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at http://www.annualcreditreport.com. Under Rhode Island and Massachusetts law, you have the right to obtain any police report filed in regard to this incident.

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.

- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.

- **For District of Columbia residents**, the Attorney General can be contacted at 400 6th Street, NW, Washington, DC 20001, 1-202-442-9828, https://oag.dc.gov/consumer-protection.

- **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

- **For New York residents,** 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/consumerprotectionl; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

- **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

- **For Rhode Island Residents,** the Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov or 401-274-4400.