

STATE OF NH  
DEPT OF JUSTICE

2021 JAN 13 AM 10:13

**BakerHostetler**

**Baker&Hostetler LLP**

Key Tower  
127 Public Square, Suite 2000  
Cleveland, OH 44114-1214

T 216.621.0200  
F 216.696.0740  
www.bakerlaw.com

David E. Kitchen  
direct dial: 216.861.7060  
dkitchen@bakerlaw.com

January 12, 2021

**VIA OVERNIGHT MAIL**

New Hampshire Attorney General  
Gordon MacDonald  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

*Re: Incident Notification*

Dear Mr. MacDonald:

We are writing on behalf of our client, New Hampshire Public Radio, to notify you of a security incident involving New Hampshire residents. New Hampshire Public Radio is the National Public Radio member station serving the state of New Hampshire.

On July 16, 2020, New Hampshire Public Radio was notified by Blackbaud of a ransomware attack on Blackbaud's network that Blackbaud 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 that an attempt had been made to encrypt files to convince Blackbaud to pay a ransom. Blackbaud paid a ransom and obtained confirmation that the stolen files had been destroyed. Blackbaud also reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, New Hampshire Public Radio conducted its own investigation of the Blackbaud services used by New Hampshire Public Radio and the information provided by Blackbaud to determine what information was involved in the incident. On July 24, 2020, New Hampshire Public Radio voluntarily provided information about the incident on its website. On December 2, 2020, New Hampshire Public Radio determined that the backup files contained certain information pertaining to 11 New Hampshire residents, including the residents' names and financial account numbers or payment card numbers.

January 12, 2021

Page 2

Beginning today, January 12, 2021, New Hampshire Public Radio is providing written notice to the New Hampshire residents by mailing letters via United States Postal Service First-Class mail. A sample copy of the notification letter is enclosed. New Hampshire Public Radio is recommending that the individuals remain vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. New Hampshire Public Radio has also established a dedicated phone number where the individuals may obtain more information regarding the incident.

Blackbaud has informed New Hampshire Public Radio that it identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect data 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 platforms.

Please do not hesitate to contact me if you have any questions regarding this incident.

Sincerely,

A handwritten signature in blue ink that reads "David E. Kitchen". The signature is written in a cursive style and is positioned above the printed name.

David E. Kitchen  
Partner

Enclosure



2 PILLSBURY ST  
SIXTH FLOOR  
CONCORD NH 03301

[NAME 1]  
ADDRESS OF [NAME 1]  
CITY, STATE, ZIP

January 12<sup>th</sup>, 2021

Dear [NAME 1]:

New Hampshire Public Radio (“NHPR”) is writing to notify you of a data security incident that occurred with one of our vendors, Blackbaud, Inc. (“Blackbaud”). This notice explains the incident and 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 NHPR and many other institutions that it had discovered an attempted 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 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. The time period of unauthorized access was between February 7 to May 20, 2020. Blackbaud reported that it has been working with law enforcement. Upon learning of the incident from Blackbaud, we conducted our own investigation of the Blackbaud services we use and the information provided by Blackbaud to determine what information was involved in the incident. On December 2, 2020, we determined that the backup files contained certain information pertaining to you.

*What Information Was Involved*

The backup file involved contained your name and financial account number ending in -XXXX. In its July 16<sup>th</sup> notification, Blackbaud assured NHPR that the backup file was destroyed by the unauthorized individual and that it has 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. We encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements for any unauthorized activity. For more information, including 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. Blackbaud has informed us that it identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect your data from any subsequent incidents, and are undertaking additional efforts to improve security through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.

*For More Information*

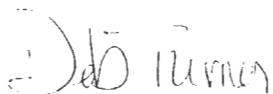
We regret that this occurred and apologize for any inconvenience. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact NHPR’s Member Service department at (800) 639-4131 weekdays between the hours of 8 am and 5 pm.

**NEW HAMPSHIRE PUBLIC RADIO**

**603.228.8910 | NHPR.ORG**

107.1 BERLIN 90.3 COLEBROOK 89.1 CONCORD/MANCHESTER 104.3 DOVER 91.3 HANOVER 96.5 HOLDERNESS  
99.5 JACKSON 90.7 KEENE 91.9 LITTLETON 88.3 NASHUA 97.3 PLYMOUTH 103.9 PORTSMOUTH

Sincerely,

A handwritten signature in black ink that reads "Deborah Turner". The signature is written in a cursive style with a large, stylized "D" at the beginning.

Deborah Turner  
Vice President of Development

## 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](http://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](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://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](http://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](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://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.

**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.