

STATE OF NH  
DEPT OF JUSTICE

2021 FEB 24 PM 12:06

**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

February 22, 2021

**VIA UPS OVERNIGHT DELIVERY**

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

*Re: Incident Notification*

Dear Attorney General MacDonald:

We are writing on behalf of our client, San Francisco University High School ("SFUHS"), to notify you of a security incident involving a New Hampshire resident. San Francisco University High School is a private college preparatory high school located in San Francisco, California.

On July 16, 2020, SFUHS 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 stolen files had been destroyed. Blackbaud also reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, SFUHS conducted its own investigation of the Blackbaud services used by SFUHS and the information provided by Blackbaud to determine what information was involved in the incident. SFUHS subsequently determined that the backup files contained certain information pertaining to one New Hampshire resident, including the resident's name and Social Security number.

February 22, 2021

Page 2

Beginning today, February 22, 2021, SFUHS is providing written notice to the New Hampshire resident by mailing a letter via United States Postal Service First-Class mail.<sup>1</sup> A sample copy of the notification letter is enclosed. SFUHS is offering the New Hampshire resident a complimentary, one-year membership to credit monitoring and identity theft prevention services through Kroll. SFUHS is recommending that the individual remain vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. SFUHS has also established a dedicated phone number where the individual may obtain more information regarding the incident.

Blackbaud has informed SFUHS that they 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,



David E. Kitchen  
Partner

Enclosure

---

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



SAN FRANCISCO  
UNIVERSITY  
HIGH SCHOOL

3065 Jackson Street  
San Francisco, CA 94115

Phone (415) 447-3100  
Fax (415) 447-5801  
www.sfuhs.org

<<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>>,

We are writing to notify you that we and many other institutions were notified by Blackbaud that it experienced a security incident. 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 us 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 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 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. We subsequently determined that the unencrypted Blackbaud backup file contained some of your information.

#### *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 have also secured the services of Kroll to provide identity monitoring at no cost to you for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on your complimentary one-year membership, please see the additional information provided in the pages that follow this letter.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

#### *What We Are Doing*

We are notifying you of this incident and sharing the steps that Blackbaud is taking in response. Blackbaud has informed us that they 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 harden their environment 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 us at [1-800-877-8339](tel:1-800-877-8339), Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

A handwritten signature in black ink, appearing to read "M. Novak".

Michael Novak  
CFOO

## **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

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

### **Triple Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—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.

## **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.