[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

From: Kim, Sue <Sue.Kim@wilsonelser.com>
Sent: Thursday, September 17, 2020 4:18 PM
To: DOJ: Attorney General <attorneygeneral@doj.nh.gov>
Cc: [redacted]
Subject: Shady Hill School - Blackbaud Cyber Security Incident

EXTERNAL: Do not open attachments or click on links unless you recognize and trust the sender.

Dear Office of the Attorney General of New Hampshire,
Our office represents Shady Hill School in a matter that requires reporting to your office.

Blackbaud is an engagement and fundraising software service provider, providing multiple solutions to non-profit companies, schools and institutions across the United States. Blackbaud was the subject of a ransomware attack and the cyber-criminal may have had access to specific personal information identified below between February and May 20, 2020. Blackbaud paid a ransom to ensure that all information exfiltrated was destroyed. The FBI was involved in the internal forensic investigation and Blackbaud's system was fully restored after the ransom payment. Blackbaud has already implemented changes to their data security protocols to prevent a similar incident from occurring again.

On July 16, 2020, our client was notified of the incident, including information on the specific Blackbaud Solution back-ups exposed. Shady Hill School immediately took action to understand the potential exposure and scope of personal data and retained counsel to assist and advise. Shady Hill engaged an outside forensic investigation as well, as there were contradictions in the information provided by Blackbaud as to encrypted data fields, and Shady Hill discovered that the majority of the unencrypted sensitive PII related to data entries on a prior version of the Blackbaud system prior to 2012. Shady Hill is taking steps to have all this newly discovered unencrypted data deleted.

Between Sept.15-Sept.20th, my client sent out letters to 823 affected individuals notifying them of the breach. Of the 823 individuals, three (3) were residents of New Hampshire. Of the three, one individual was notified of the breach because that individual's social security number was exposed. The two other individuals were not notified as the personal information exposed were credit card numbers without exposure of a required security code. The resident whose social security number was exposed was offered 12 months of free credit monitoring. Attached is the sample notification letter.

Please contact partner Nanette Reed for further inquiries regarding the matter. She is copied on this email and can be reached at 213-330-8838.

Sue Kim
Attorney at Law
Wilson Elser Moskowitz Edelman & Dicker LLP
555 S. Flower Street - Suite 2900
Los Angeles, CA 90071-2407
213.330.8798 (Direct)
213.443.5100 (Main)
213.443.5101 (Fax)
sue.kim@wilsonelser.com

For further information about Wilson, Elser, Moskowitz, Edelman & Dicker LLP, please see our website at www.wilsonelser.com or refer to any of our offices.

Thank you.

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

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

Dear Friend of Shady Hill School,

We are writing to notify you that one of our third-party vendors, Blackbaud, suffered a cyber incident which may have allowed access to some of your personal information. At Shady Hill, we deeply value our ongoing relationships and the trust you place in us as an institution. Please know that the privacy of our community's data is of critical importance.

What Happened? Blackbaud is an engagement and fundraising software service provider to many non-profit companies, schools, and other institutions across the United States. Blackbaud was the subject of a ransomware attack and the cybercriminal may have had access to specific personal information identified below between February and May 20, 2020.

Once Blackbaud detected the intrusion, it halted further system access. The cybercriminal only gained access to certain back-up files in specific Blackbaud Solutions. Blackbaud, in conjunction with the FBI, investigated the incident and ultimately paid a ransom to the cybercriminal under the assurance that any exfiltrated files would be destroyed, and their system was fully restored after ransom payment. Through vigilant monitoring post-incident, Blackbaud reports that there has been no evidence of improper use of any of the data files that may have been exposed. Blackbaud has implemented changes to their data security protocols to prevent a similar incident from occurring again.

What Personal Identifying Information (PII) Was Exposed? Shady Hill received notice of this incident on July 16, 2020, including information on the specific Blackbaud Solution back-ups that were exposed. We immediately took action and retained our own forensic cyber investigators to thoroughly research our database for any possible exposure. As a result of the ransomware attack, we have determined that there was exposure of your first and last names, physical and email addresses, date of birth, your giving history with the School (all non-PII) and your Social Security number (PII). Our investigation revealed that the exposure of Social Security numbers was likely the result of data entry prior to 2012 on earlier versions of Blackbaud's Raiser's Edge and Financial Edge programs.

What You Can Do? We advise you to remain vigilant in reviewing your account statements and monitoring your free credit reports. There are several ways you can obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

1. Visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.
2. Mail a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-free-credit-reports) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

3. Contact one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion
PO Box 105851	PO Box 9532	PO Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Free Credit Report Monitoring: In addition, we have arranged with Kroll to provide you with identity monitoring services for 12 months, at no cost to you. This "Essential Monitoring" package provides you with the following benefits:

- One Bureau Credit Monitoring
- Web Watcher, Public Persona, Quick Cash Scan
- Up to $1M Identify Fraud Loss Reimbursement

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

You have until **December 22, 2020** to activate your identity monitoring services.

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

Attorney General Information: You may wish to review information provided by Rhode Island's Attorney General to obtain more information about preventing identity theft. To contact the Attorney General, call (401) 274-4400, write to the Office of the Attorney General, 150 South Main Street, Providence, RI, or visit www.riag.ri.gov.

If you require additional information, please contact our dedicated call center at 1-844-945-3745 Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

Thank you again for your trust and goodwill. We regret any inconvenience this incident at Blackbaud may have caused you.

Sincerely,

Pam Dickinson
Director of External Relations

Cindy Dobe
Chief Information Officer

Kroll | A Division of DUFF&PHELPS

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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.