[redacted]

[redacted]

From: Kim, Sue <Sue.Kim@wilsonelser.com>
Sent: Sunday, February 28, 2021 2:05 PM
To: DOJ: Consumer Protection Bureau <DOJ-CPB@doj.nh.gov>
Cc: Reed, Nanette <Nanette.Reed@wilsonelser.com>
Subject: Landmark Christian School - Blackbaud Ransomware Attack Notification

Dear Office of the Attorney General of New Hampshire,
This email is to notify you of a cyber breach that occurred as a result of a ransomware attack on Blackbaud which affected one (1) resident of New Hampshire. The initial attack occurred from February 20, 2020 to May 20, 2020, and Blackbaud paid the ransom demanded by the cybercriminals with the help of the FBI. The cyber criminals assured that any exfiltrated files were destroyed, and Blackbaud's 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 already implemented changes to their data security protocols to prevent a similar incident from occurring again.

As part of their continuing investigation, Blackbaud discovered when it merged data from previous versions of some of their solutions into current versions, there were hidden tables containing the older data (which included unencrypted Personal Information) merged into the new program which were not visible. Blackbaud notified the affected organizations, including Landmark Christian School, on September 29, 2020. Blackbaud did not provide the necessary information to notify affected individuals until December 8, 2020.

Landmark Christian School immediately contacted counsel and informed its constituents of the breach, notifying them by mail on February 24, 2021. Landmark Christian School took action to understand the potential exposure and scope of personal data. The personal information that was exposed to the one (1) New Hampshire resident included name, phone number, address, date of birth, and Social Security number.

A copy of the notification letter is attached for your reference.

Please do not hesitate to contact us with any questions.

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

LANDMARK CHRISTIAN SCHOOL
believe. belong. become.

<<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>>,

This shall 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 and entitles you to free credit monitoring and fraud assistance services.

What Happened? Blackbaud is an engagement and fundraising software service provider, providing multiple solutions to non-profit companies, schools and institutions across 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 2020 and May 20, 2020.

Once Blackbaud detected the intrusion, it was able to halt further system access. The cyber-criminal 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 cyber-criminal 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 already implemented changes to their data security protocols to prevent a similar incident from occurring again.

As part of their continuing investigation, Blackbaud discovered when it merged data from previous versions of some of their solutions into current versions, there were hidden tables containing the older data (which included unencrypted Personal Information) merged into the new program which were not visible. We were notified of this new exposure on September 29, 2020 and took action to verify and determine scope, which required the cooperation of Blackbaud in producing the hidden data files. According to Blackbaud, the information was exposed because the company failed to destroy or encrypt certain “legacy” files after a migration of our files to a new platform.

What PI Was Exposed? At this time, we are informed sensitive personal information including your name, phone number, address, date of birth, and Social Security number were exposed. This is older data from the prior legacy versions of the programs that were used prior to migration.

What You Can Do:

To help you guard against identity theft or other potential fraud as a result of this incident, Blackbaud is offering free credit monitoring and fraud assistance services for 24 months. Information about how to access these services accompanies this letter. Although services are available to you, it is important to remain vigilant and promptly report any suspected fraud to law enforcement. For information on avoiding identity theft, please visit www.ftc.gov/idtheft.

In addition, security experts suggest that you contact your financial institution and all major credit bureaus immediately to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file.

We encourage you to contact CyberScout to enroll in free CyberScout services by going to **https://www.cyberscouthq.com/** [redacted] and using the Enrollment Code provided above. Please note the deadline to enroll is April 15, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

Enclosed hereto you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

ELN-????

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call Kroll at 1-XXX-XXX-XXXX, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Kroll representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Landmark Christian School values the security of your personal data, and we apologize for any inconvenience that this incident has caused.

Sincerely,

Mary S. Mayfield

Mollie Mayfield
Chief Financial & Ops Officer

Additional Important Information

For residents of *Maryland*:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

---

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

Credit Monitoring Services

We are providing you with access to **Single Bureau Credit Monitoring*** services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

Proactive Fraud Assistance. For sensitive breaches focused on customer retention, reputation management, or escalation handling, CyberScout provides unlimited access during the service period to a fraud specialist who will work with enrolled notification recipients on a one-on-one basis, answering any questions or concerns that they may have. Proactive Fraud Assistance includes the following features:

- Fraud specialist-assisted placement of fraud alert, protective registration, or geographical equivalent, in situations where it is warranted.
- After placement of a Fraud Alert, a credit report from each of the three (3) credit bureaus is made available to the notification recipient (United States only).
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Answering any questions individuals may have about fraud.
- Provide individuals with the ability to receive electronic education and alerts through email. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Identity Theft and Fraud Resolution Services. Resolution services are provided for enrolled notification recipients who fall victim to an identity theft as a result of the applicable breach incident. ID Theft and Fraud Resolution includes, but is not limited to, the following features:

- Unlimited access during the service period to a personal fraud specialist via a toll-free number.
- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparation of all documents needed for credit grantor notification, and fraud information removal purposes.
- All phone calls needed for credit grantor notification, and fraud information removal purposes.
- Notification to any relevant government and private agencies.
- Assistance with filing a law enforcement report.
- Comprehensive case file creation for insurance and law enforcement.
- Assistance with enrollment in applicable Identity Theft Passport Programs in states where it is available and in situations where it is warranted (United States only).
- Assistance with placement of credit file freezes in states where it is available and in situations where it is warranted (United States only); this is limited to online-based credit freeze assistance.
- Customer service support for individuals when enrolling in monitoring products, if applicable.
- Assistance with review of credit reports for possible fraudulent activity.
- Unlimited access to educational fraud information and threat alerts. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Enrollment Instruction

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please navigate to: **https://www.cyberscouthq.com/** [redacted]

If prompted, please provide the following unique code to gain access to services: [redacted]

Once registered, you can access Monitoring Services by selecting the "Use Now" link to fully authenticate your identity and activate your services. **Please ensure you take this step to receive your alerts.**

In order for you to receive the monitoring services described above, you must enroll within 45 days from the date of this letter.