

18751



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

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

Re: Important Notice Regarding Your Personal Information

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

On August 12, 2020, we notified you that we learned from Blackbaud, a large provider of cloud-based data management services to The Lamplighter School, and many other educational institutions, hospitals, and other not-for-profit organizations around the world, that a ransomware attack, which it had discovered and stopped in May 2020, had impacted a database containing certain information concerning members of our community. Blackbaud has recently discovered that the compromised data also included additional information, which we detail more specifically below. Unfortunately, some of your information was included in this discovery.

What Happened

As stated in our notification letter of August 12, 2020, Blackbaud informed us that following the attack, it paid a ransom to the attacker and obtained confirmation that the compromised information was destroyed. According to Blackbaud, and as far as we know, there is no indication that any of the compromised information is subject to further disclosure or misuse. Blackbaud has also assured us that they are enhancing their safeguards to mitigate the risk of future attacks and are taking ongoing steps to monitor the dark web for any evidence that the information was further compromised.

What Information Was Involved

Blackbaud had initially informed us that the compromised information included certain information about you, but *did not* include your social security number. Unfortunately, on September 29, 2020, Blackbaud notified us that the compromised information *did* include unencrypted social security numbers, including yours and the following other identifiers: your name, contact information (mailing address and phone numbers), date of birth, and school relationships. We have no indication that any of your personal information has been misused, but we wanted to make you aware of the incident, our efforts to safeguard your personal information, and resources you may use to protect yourself.

What Lamplighter is Doing

We have attached instructions to this letter for how you may access two years of credit monitoring services at no cost to you. We have also been in contact with legal counsel and are reviewing our relationship with Blackbaud in response to this update. We have also been in contact with our peer schools who were affected in this incident as well, and we will remain in close contact with Blackbaud regarding this matter.


What You Can Do

As always, we recommend that you remain vigilant and review your account statements and credit reports regularly; and report any concerning or suspect transactions to your financial services provider. To assist you in protecting yourself against risks related to this incident, Blackbaud has engaged CyberScout to provide you with its credit monitoring services for two years at no cost to you. Enclosed with this letter is information regarding these services and instructions for enrollment, as well as an insert providing additional useful information regarding steps you can take to protect yourself from identify theft. If you have any questions regarding this incident, please contact Marynell Murphy, Chief Operations Officer, at mmurphy@thelamplighterschool.org or 214-369-9201, x343 from 8:00 a.m. – 4:00 p.m., Monday through

Friday, Central Time, and to enroll in the credit services we are offering at no cost to you, please contact CyberScout by following the instructions attached to this letter by March 27, 2021.

We sincerely apologize for any inconvenience or concern this situation may cause. Again, we want to reassure you that we have taken steps to improve the security of personal information entrusted to us.

Sincerely,



Joan Buchanan Hill, Ed.D.

Catherine M. Rose Head of School



Marynell Murphy

Chief Operations Officer

How to Access Your 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 by March 27, 2021.**

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 By March 27, 2021

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please navigate to: **<https://www.cyberscouthq.com/epiq263?ac=263HQ1832>**

If prompted, please provide the following unique code to gain access to services: **263HQ1832**

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 by March 27, 2021.

Additional Information and U.S. State Notification Requirements

There are a number of steps you should consider to guard against identity theft.

Review Your Account Statements and Credit Report: It is recommended that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports. Report any fraudulent transactions to the creditor or credit reporting agency from whom you received the statement or report. You may obtain a free copy of your credit report from each credit reporting agency once every 12 months, whether or not you suspect any unauthorized activity on your account, by visiting <https://www.annualcreditreport.com> ~~www.annualcreditreport.com~~<http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form available at that website and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report at any time by contacting any one or more of the national credit reporting agencies listed below.

Equifax

P.O. Box 740241
Atlanta, Georgia 30374
www.equifax.com
1-800-685-1111 Credit Reports
1-888-766-0008 Fraud Alert
1-800-685-1111 Security Freeze

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742 Credit Reports
1-888-397-3742 Fraud Alert
1-888-397-3742 Security Freeze

TransUnion (FVAD)

P.O. Box 105281
Atlanta, GA 30348-5281
www.transunion.com
1-800-888-4213 Credit Reports
1-800-680-7289 Fraud Alert
1-800-680-7289 Security Freeze

Federal Trade Commission and State Resources: General guidance on protecting yourself from identify theft is available from the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. NW, Washington D.C. 20580, by phone at 877-ID-THEFT (438-4338), and/or from the FTC website at <http://www.ftc.gov/bcp/edu/microsites/idtheft>. In many states, additional information is also available from your state's Attorney General's Office.

Fraud Alerts and Security Freezes: You may obtain information about fraud alerts and security freezes (also referred to as credit freezes), including how to place a fraud alert or security freeze, from the Federal Trade Commission or credit reporting agencies at the contact information provided above. However, be aware that a fraud alert or security freeze may interfere with or delay legitimate requests for credit approval.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State law advises you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Maryland and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General about steps you can take to avoid 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

North Carolina Office of the Attorney General

Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699- 9001
1-877-566-7226
www.ncdoj.com