LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Allen E. Sattler
650 Town Center Drive, Suite 1400
Costa Mesa, California 92626
Allen.Sattler@lewisbrisbois.com
Direct: 714.668.5572

January 22, 2021

VIA EMAIL
Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent Landon School ("Landon") in connection with a data security incident which is described in greater detail below. Landon takes the protection of all sensitive information within its possession very seriously.

1. **Nature of the security incident.**

In July 2020, Landon was initially notified by Blackbaud, a large provider of cloud-based data management services to Landon and many other not-for-profit organizations, that it had discovered and stopped a ransomware attack that occurred in or about May 2020. Blackbaud stated that, working with independent forensics experts and law enforcement, it successfully prevented the cybercriminals from blocking system access, including to Landon's files, and ultimately expelled the criminals from Blackbaud's system. However, prior to being locked out, the cybercriminals removed a copy of some of Landon's data regarding donors and other contacts located in a legacy version of the Blackbaud platform. On September 29, 2020, Blackbaud informed Landon that this legacy platform contained certain unencrypted personal information at the time of the incident. In response to this notice, Landon reviewed the data stored in the legacy Blackbaud software and immediately took steps to identify and notify these individuals.

2. Number of New Hampshire residents affected.

Landon mailed notification letters to the two (2) New Hampshire residents regarding this data security incident on January 22, 2021. A sample copy of the notification letter sent to the affected individuals is enclosed with this letter.

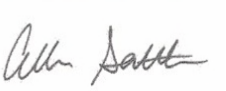
3. Steps taken relating to the incident.

Landon has taken steps outlined above in response to this incident. Additionally, we provided impacted individuals with information about steps they can take to help protect their personal information. Further, while there is no evidence of misuse or disclosure of these individuals' personal information, we are offering credit monitoring and identity protection services through IDX, which will help individuals resolve issues if their identity is compromised due to this incident.

4. Contact information.

Landon remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (714) 668-5572 or via email at Allen.Sattler@lewisbrisbois.com.

Regards,



Allen E. Sattler of
LEWIS BRISBOIS BISGAARD & SMITH LLP

AES:rmp

Enclosures: Sample consumer notification letter variations

Landon

C/O IDX
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-754-1795
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [XXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January 22, 2021

Re: Notice of Data Security Incident

Dear <<First Name>>,

We are writing to you to provide additional information regarding the data security incident impacting Landon School ("Landon"), of which you may have received prior notice in July 2020. At Landon, we take the privacy and security of our students', alumni, and employees' information very seriously, and we treated this situation accordingly. This follow-up notice is to provide you with updated information about the incident, offer credit and identity monitoring services, and inform you about steps you can take to help protect your personal information.

What Happened? As indicated in our prior correspondence, Landon was notified in July 2020 by Blackbaud, a large provider of cloud-based data management services used by Landon and other schools and not-for-profit organizations, that it had discovered and stopped a ransomware attack that occurred in or around May 2020. Working with independent forensics experts and law enforcement, Blackbaud successfully prevented the cybercriminals from blocking its system access and ultimately expelled the cybercriminals from Blackbaud's systems. At that time, Blackbaud believed that none of the information potentially disclosed as a result of the incident contained unencrypted personal information of Landon's constituents, and Blackbaud further stated that none of the information had been misused.

In September 2020, we received a follow up notification from Blackbaud informing us that, based on its additional investigation into the incident, prior to being locked out of its network, the cybercriminals removed a copy of older data regarding donors and other contacts of longer term Blackbaud clients, including Landon. This data was retained by Blackbaud as part of a legacy version of its platform. Blackbaud informed Landon that the legacy platform contained certain unencrypted personal information at the time of the incident, which Blackbaud previously believed to be encrypted. Upon receipt of this notice, Landon obtained copies of the data stored in the legacy software to assess what and whose information may have been impacted in the incident.

Based on this review, Landon determined that your personal information may have been impacted in the incident. While Blackbaud has no reason to believe that your personal information has been misused, out of an abundance of caution and transparency, we are providing you with this new information and offering you credit and identity monitoring services at no charge.

What Information Was Involved? <<Variable Data 1>>.

What Are We Doing? As soon as we received Blackbaud's follow up notification in late September, we took the steps described above to investigate the extent of the incident and any additional associated risk. In addition, we are providing you with the information below outlining steps you can take to protect your personal information. We are also offering you free credit and identity monitoring and recovery services for <<12/24 months>> through IDX as described below.

What is Blackbaud Doing? Blackbaud shared that, in response to the incident, it identified the vulnerability associated with the incident, including the tactics used by the cybercriminal, and took action to close that vulnerability. It subsequently

confirmed through testing by multiple third parties, including relevant platform vendors, that their vulnerability closure could withstand all currently known attack tactics. Additionally, Blackbaud accelerated other efforts to enhance its systems and harden its environment to protect its clients from a similar incident in the future.

What You Can Do: While there is no evidence of misuse of any impacted information, out of an abundance of caution, we suggest you read and follow the recommendations included at the end of this letter. We also strongly encourage you to enroll in the credit and identity monitoring services we are offering through IDX to protect your personal information. To enroll, please visit https://app.idx.us/account-creation/protect or call 1-833-754-1795 and provide the enrollment code provided above.

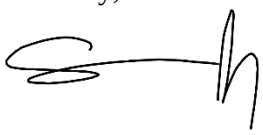
To receive credit services, you must be over the age of 18, and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Additional information describing these services is included with this letter.

Please note you must enroll by April 22, 2021. If you have questions or need assistance, please call IDX at 1-833-754-1795.

For More Information: If you have any questions about this letter, please call 1-833-754-1795, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.

As stated above, we take the privacy and security of your personal information very seriously, and we will continue to work diligently to ensure our partners and the school itself do what is necessary to appropriately safeguard and/or limit any data that the school retains as part of its operations. Please accept our sincerest apologies. We deeply regret any worry or inconvenience that this may cause you, and we hope the information and resources offered here might be of assistance.

Sincerely,



Stephen B. King
Interim CFO / COO
Landon School Corporation

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-866-349-5191	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.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 90 days. 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: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.