

July 13, 2022

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Email Only:

Attorney General Brian Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Cybersecurity Incident Involving The de Paul School

Dear Attorney General Frosh:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents The de Paul School (“de Paul”), a public school offering programs from kindergarten to eighth grade students, located at 1925 Duker Avenue, Louisville, KY 40205, with respect to a cybersecurity incident described in more detail below. De Paul takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of residents being notified, and the steps that de Paul has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

Blackbaud is a cloud computing provider that is used by de Paul and many other institutions to organize and store information related to members of our community. In July 2020, Blackbaud notified hundreds of non-profit and educational institutions, including de Paul, that Blackbaud experienced a cybersecurity incident which resulted in the exposure of personal information maintained by non-profit and educational institutions on the Blackbaud platform (hereinafter, the “Incident”). De Paul was first notified of this Incident by Blackbaud on July 16, 2020. Since then de Paul has been working with legal counsel familiar with Blackbaud’s incident as well as conducting significant work to identify potentially impacted individuals.

On May 20, 2021, de Paul notified potentially impacted individuals of this Incident. However, after the initial notice, Blackbaud informed de Paul of another broad subset of data potentially impacted by the underlying Incident. Due to the nature and complexity of the information stored on Blackbaud’s systems, and the vague notice, it took time for de Paul to identify the potentially

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Los Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

impacted data affected by the cybersecurity incident. Once the affected data was identified, from June 2021 to April 29, 2022, de Paul engaged a data mining vendor to conduct an automated term searching and manual document review exercise in order to identify the specific individuals affected by the Incident. From May to June, 2022, de Paul engaged a mailing vendor to provide the mailing services, call center, and credit monitoring services for the impacted individuals. Based on the investigations, it appears that some personal information was compromised, specifically individuals' names, addresses, Social Security numbers, and limited health information.

With any such event, it takes time to gather the relevant information, identify the affected individuals, hold the necessary internal discussions, and make the appropriate decisions to line-up the assistance services that are being offered. De Paul has been diligent with the investigation to ensure the appropriate protection services would be provided.

2. Number of Maryland residents affected.

A total of one (1) Maryland resident may have been potentially affected by this incident. A notification letter to this individual was mailed on July 13, 2022, by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

De Paul mailed a notification letter to one (1) Maryland resident on May 20, 2021.

3. Steps taken in response to the Incident.

De Paul is committed to ensuring the security of all personal information in our control, and we are taking steps to prevent a similar event from occurring in the future. Blackbaud has indicated that it has taken (or plans to take) the following steps to strengthen its cybersecurity post-attack: hardening Blackbaud's environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms; steps to improve to the granularity of reporting at both the host and network level to ensure intrusion detection capabilities; accelerating efforts to add multi-factor authentication to all of Blackbaud's self-hosted solutions; ensuring all users reset their passwords regularly; requiring stronger user passwords for certain customers; increasing efforts to migrate customers to Cloud environments (including Microsoft Azure and Amazon Web Services).

Although de Paul is not aware of any actual or attempted misuse of the affected personal information, de Paul is also providing potentially impacted individuals with identity theft protection and credit monitoring services for a period of twelve (12) months at no cost through Kroll. Additionally, de Paul provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

De Paul remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

EXHIBIT A



<<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 inform you of a cybersecurity incident involving Blackbaud, Inc. (“Blackbaud”), a third party vendor utilized by the de Paul School (“de Paul”) that may have impacted your information. De Paul takes the security of your information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident and steps you can take to help protect your information.

What Happened?

Blackbaud is a cloud computing provider that is used by de Paul and many other institutions to organize and store information related to members of our community. In July 2020, Blackbaud notified hundreds of non-profit and educational institutions, including de Paul, that Blackbaud experienced a cybersecurity incident which resulted in the exposure of personal information maintained by non-profit and educational institutions on the Blackbaud platform (the “Incident”). De Paul was first notified of this Incident by Blackbaud on July 16, 2020. Since then we have been working with legal counsel familiar with Blackbaud’s incident as well as conducting significant work to identify potentially impacted donors.

On May 20, 2021, de Paul notified potentially impacted individuals of this Incident. However, after the initial notice, Blackbaud informed de Paul of another subset of data potentially impacted by the underlying Incident. Due to the nature and complexity of the information stored on Blackbaud’s systems, it took time to parse the relevant data affected by the cybersecurity incident. Once the affected data was secured, from June 2021 to April 29, 2022, de Paul engaged a data mining vendor to conduct an automated term searching and manual document review exercise in order to identify the specific individuals affected by the Incident. From May to June, 2022, de Paul engaged a vendor to provide the mailing services, call center, and identity monitoring services for the impacted individuals. With all required due diligence completed, we are now able to share this communication with you.

With any such event, it takes time to gather the relevant information, identify the affected individuals, hold the necessary internal discussions, and make the appropriate decisions to line-up the assistance services that are being offered. De Paul has been diligent with the investigation to ensure the appropriate services would be provided.

What Information Was Involved?

At this time, based on the information we have received from Blackbaud, we have no reason to believe that any personal information of members of the de Paul community has been misused as a result of this incident. However, for purposes of full disclosure, we feel it important to inform you that limited information may have been accessible by unauthorized individuals as a result of this incident.

Specifically, de Paul utilized Blackbaud’s platform known as *Financial Edge NXT* and *Raiser’s Edge NXT* to store information related to our donors and students. We feel it is important to inform you that we use this platform to store the following information which we believe may have been exposed as a result of this incident: name; home address;
<<b2b_text_1 (data elements)>>.

What We Are Doing

De Paul is committed to ensuring the security of all personal information in our control, and we are taking steps to prevent a similar event from occurring in the future. As always, we recommend that you continue to join us in remaining vigilant to protect your personal information. Once de Paul became aware of this incident, we contacted Blackbaud for more details, including steps taken by Blackbaud to mitigate the risk of similar occurrences in the future. Blackbaud engaged cybersecurity experts to follow up on this incident. Based on the nature of the incident, their research, and third party (including law enforcement) investigation, Blackbaud has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly. Blackbaud has also hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do

We encourage you to activate Kroll's identity monitoring services, to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to help protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to help protect against the possibility of information misuse.

Other Important Information

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause you and your family. If you have questions, please call 1-???-???-???, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

Leslie Johnson
Chief Financial Officer



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'll 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.

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.

Steps You Can Take to Help Protect Your Information

Credit Reports: 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.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. 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.

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-alerts

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You 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:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade

Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

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 Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004; 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203; 1-720-508-6000; www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov