



November 6, 2020

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

**Via Postal Mail Only**

**Attorney General Gordon J. MacDonald**  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03302

STATE OF NH  
DEPT OF JUSTICE  
2020 NOV 13 PM 3:03

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent St. Andrew’s School – Rhode Island (“St. Andrew’s”), located at 63 Federal Rd, Barrington, RI 02806, with respect to a data security incident described in more detail below. St. Andrew’s takes the security and privacy of donor and student information very seriously, and has taken steps to prevent a similar incident from occurring in the future.

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

St. Andrew’s is a nondenominational boarding and day school located in Rhode Island. On Thursday, July 16, 2020, St. Andrew’s received a notification from Blackbaud, Inc. (“Blackbaud”) that Blackbaud experienced a cybersecurity incident (ransomware attack) which resulted in the exposure of personal information maintained by hundreds of non-profit and educational institutions on multiple Blackbaud platforms. On September 29, 2020, St. Andrew’s received a second notification from Blackbaud indicating that additional St. Andrew’s personal information stored by Blackbaud was compromised. Blackbaud is a cloud computing provider that is used by St. Andrew’s and many other institutions to organize and store information related to members of their community. After an initial investigation, St. Andrew’s discovered the Blackbaud platforms they use, *Blackbaud Education Edge* and *Blackbaud Financial Edge NXT*, contained the name, home address, date of birth, and some health information of St. Andrew’s donors and former students. According to communication from Blackbaud, Blackbaud did not encrypt these platforms containing the backup datasets of St. Andrew’s data.

**2. Number of New Hampshire residents affected.**

A total of two (2) New Hampshire residents may have been potentially affected by this incident. A notification letter to these individuals will be mailed the week of November 9, 2020 by first class mail. A sample copy of the notification letters are included with this letter.

**3. Steps taken.**

St. Andrew’s takes the security and privacy of the information very seriously. Upon discovery of  
55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

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

**wilsonelser.com**



the incident, St. Andrew's immediately informed Wilson Elser Moskowitz Edelman & Dicker LLP to determine potential legal privacy obligations pursuant to Blackbaud's cybersecurity incident.

**4. Contact information.**

St. Andrew's 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](mailto:Anjali.Das@WilsonElser.com) or (312) 821-6164.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'Anjali C. Das'.

**Wilson Elser Moskowitz Edelman & Dicker LLP**

Anjali C. Das

Enclosure.

Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Dear <<Name 1>>

We are writing to inform you of a data security incident involving Blackbaud, Inc. ("Blackbaud"). St. Andrew's School ("St. Andrew's") 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 protect your information.

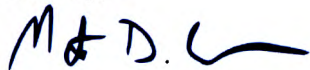
Blackbaud is a cloud computing provider that is used by St. Andrew's and many other institutions to organize and store information related to members of our community. St. Andrew's utilizes Blackbaud platforms known as *Blackbaud Education Edge* and *Blackbaud Financial Edge NXT*. In July 2020, Blackbaud notified hundreds of non-profit and educational institutions, including St. Andrew's, that Blackbaud experienced a cybersecurity incident (a ransomware attack) which resulted in the exposure of personal information maintained by non-profit and educational institutions on the Blackbaud platform. St. Andrew's subsequently learned that this information may have included your name, home address, and email address as well as limited health information. St. Andrew's did not use *Education Edge* or *Financial Edge NXT* to store any financial, banking, or credit card information.

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 St. Andrew's community has been misused as a result of this incident. However, for purposes of full disclosure, we feel it important to inform you that information related may have been viewed by unauthorized individuals as a result of this incident.

St. Andrew's is committed to ensuring the security of all personal information in our control. As a best practice, we recommend that you remain vigilant and report any suspicious activity or suspected identity theft to the proper law enforcement authorities. Please review the enclosed "Additional Important Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission ("FTC") regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. Please continue to remain vigilant, and carefully monitor your mail and credit reports for any suspect activity, and report any incident of identity theft to your local law enforcement, Attorney General, and the FTC.

As always, we recommend that you continue to join us in remaining vigilant to protect your personal 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 any questions, please do not hesitate to call (401) 246-1230, ext. 3036, Monday – Friday, 9:00am to 5:00pm.

Sincerely,

A handwritten signature in black ink, appearing to read "M. D. C." followed by a long horizontal flourish.

Matthew Cerullo  
Director of Business Services  
St. Andrew's School – Rhode Island



### Additional Important Information

**For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina:*** It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

---

**For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:***

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](http://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.

---

**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 laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

---

**For residents of *Maryland, Rhode Island, Illinois, and North Carolina:***

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](http://www.oag.state.md.us)

**Rhode Island Office of the  
Attorney General**

Consumer Protection  
150 South Main Street  
Providence RI 02903  
1-401-274-4400  
[www.riag.ri.gov](http://www.riag.ri.gov)

**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](http://www.ncdoj.com)

**Federal Trade Commission**

Consumer Response Center  
600 Pennsylvania Ave, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

---

**For residents of *Massachusetts:*** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

---

**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](https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf)) 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](http://www.experian.com/freeze)  
888-397-3742

**TransUnion (FVAD)**

P.O. Box 2000  
Chester, PA 19022  
[freeze.transunion.com](http://freeze.transunion.com)  
800-680-7289

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