18099

Company Logo

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.

Since then, St. Andrew's has worked with its insurer to engage outside counsel to further investigate the extent of the breach and its impact on our community. On September 29, 2020, St. Andrew's was notified that your social security number may also have been exposed as a result of this incident. St. Andrew's did <u>not</u> 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 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. It explains how you may access a credit monitoring service for two years at no cost. 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,
<Signature image>

Signature Image

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

Blackbaud Credit Monitoring Service

Blackbaud is 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/epiq263?ac=263HQ1737

If prompted, please provide the following unique code to gain access to services: **263HQ1737**

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 90 days from the date of this letter.

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, 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

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
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

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 *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) 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.

Company Logo

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,
<Signature image>

Signature Image

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, 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	**Rhode Island Office of the Attorney General**	**North Carolina Office of the Attorney General**	**Federal Trade Commission**
Consumer Protection Division	Consumer Protection	Consumer Protection Division	Consumer Response Center
200 St. Paul Place	150 South Main Street	9001 Mail Service Center	600 Pennsylvania Ave, NW
Baltimore, MD 21202	Providence RI 02903	Raleigh, NC 27699-9001	Washington, DC 20580
1-888-743-0023	1-401-274-4400	1-877-566-7226	1-877-IDTHEFT (438-4338)
www.oag.state.md.us	www.riag.ri.gov	www.ncdoj.com	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) 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	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
https://www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze	freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

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

Company Logo

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>>

To the Parent or Guardian of <<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 child's or ward's 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 child's or ward's 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 child's or ward's 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 child's or ward's credit file. Please continue to remain vigilant, and carefully monitor your child's or ward's 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 child's or ward's personal information. The protection of your child's or ward's 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,
<Signature image>

Signature Image

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, 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

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
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

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 *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) 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.