

18532



Annunciation Orthodox School
3600 Yoakum Blvd, Houston, TX 77006
(713) 470-5600

<<Date>>

<< First Name>><< Last Name>>

<<Address 1>>

<<Address 2>>

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

Dear << First Name>><< Last Name>>, or Parent or Guardian:

Out of an abundance of caution, we are writing to inform you of a data security incident that involved one of our vendors, Blackbaud, Inc. ("Blackbaud"). The Blackbaud cybersecurity incident may have resulted in the potential compromise of some of your or your child's data. Annunciation Orthodox School of Texas ("Annunciation") 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 Annunciation and many other institutions to organize and store information related to members of our community, including students, their parents or guardians, and our vendors. In July 2020, as you may already be aware, Blackbaud notified hundreds of educational institutions, including Annunciation, that Blackbaud experienced a cybersecurity which resulted in the exposure of some information maintained by educational institutions on the Blackbaud platform. Blackbaud's notice stated that a ransomware attack, designed to extort funds from Blackbaud by making their service unusable, was apparent in the incident. However, Blackbaud's notice also stated that any sensitive personal information was securely encrypted within its platform.

Annunciation uses Blackbaud's Raiser's Edge, Financial Edge, and Learning Management product to maintain and protect information from members of its community. Notably, Annunciation routinely updates its software to ensure that its security protections are up to date. However, Blackbaud maintained backups of its older products and customer data in the event that a Blackbaud customer, such as Annunciation, would need to restore to a prior version. Notably, these backups and the data that they contain are not accessible to customers like Annunciation. Based on the most recent information provided by Blackbaud, it was these backups that Blackbaud maintained that were inaccessible to Annunciation that was compromised in the course of Blackbaud's data incident.

As we mentioned, Blackbaud's initial notice of its data incident in July 2020 stated that any sensitive information, such as social security number or bank account numbers stored in the Blackbaud platform were securely encrypted throughout its applications.

Later, Blackbaud notified us on September 29, 2020 that it discovered that some information for some of its customers was not securely encrypted, contrary to what it previously reported. Blackbaud explained that sensitive information that Blackbaud held that was not accessible to or viewable by Annunciation was not encrypted, and could have been exposed in the course of its data incident. Since the information that Blackbaud referenced was not accessible to or viewable by Annunciation, we requested details of the data that Blackbaud maintained. On October 05, Blackbaud preliminarily determined the individuals' whose information was potentially exposed during the course of the incident. We conducted our own due diligence to investigate the information that was stored in various Blackbaud systems, and determined the individuals whose information was potentially exposed. Thereafter, we worked to determine the data elements that were

potentially exposed for certain individuals. We also worked with a third-party vendor to send letters to affected individuals and set up a call center to field the questions that you may have. Furthermore, we worked with Blackbaud to obtain credit monitoring services for those that could be affected by the Blackbaud data incident.

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 Annunciation community has been misused as a result of this incident. However, based on the updated information from Blackbaud, we now have reason to believe that some personal information of students, their parent or guardian, and some of our vendors may have been made available to the attacker. Specifically, the information that may have been made available included [[VARIABLE TEXT]]. Blackbaud has assured us that they acted expeditiously to block the attacker, restore access, and ensure that the data has not gone beyond the attacker.

Annunciation Orthodox School is committed to ensuring the security of all student personal information in our control, and we are working with Blackbaud to ensure that student data is secure going forward. Blackbaud has promised to encrypt sensitive data fields, and delete unsecured backups of sensitive information by the end of the year. However, as always, we recommend that you continue to join us in remaining vigilant to protect your information.

While we have no reason to believe that any information has been, or will be misused, out of an abundance of caution, we ask that you join us in continuing to remain vigilant in monitoring your personal information. We are working with Blackbaud and CyberScoutHQ to provide you or your child with complimentary identity monitoring services. Information about the services being provided, along with additional information about how to protect yourself or your child, is included in the materials attached to this letter:

There are additional steps you can take to protect you identity. For instance, you can obtain information from the Federal Trade Commission about fraud alerts and security freezes. You can also request a security freeze from the credit bureaus. Additional information is provided in the insert that came with this letter.

The protection of your and your child's information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause your family. If you have any questions, please do not hesitate to call <<PHONE NUMBER>> Monday through Friday, between <<TIME AND TIME>>, <<TIME ZONE>>.

Sincerely,
Bryant Richardson, CFO
Annunciation Orthodox School
3600 Yoakum Blvd, Houston, TX 77006
(713) 470-5600

Credit Monitoring Services from CyberScout

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 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=263HQ1099>

If prompted, please provide the following unique code to gain access to services: **263HQ1099**

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, New York, 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.ncdol.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338)

www.ftc.gov/idtheft

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>

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); TransUnion (<https://www.transunion.com/fraud-alerts>); 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 listed above.