ALL SAINTS' EPISCOPAL SCHOOL

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

To Enroll, Please Call:
1-833-791-1661
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>

November 6, 2020

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident experienced by one of our vendors, Blackbaud, that involved your personal information. At All Saints' Episcopal School ("All Saints'"), we take the privacy and security of our students, alumni, and employees' information very seriously. This is why I am explaining what happened, measures we and Blackbaud have taken, and informing you about steps you can take to help protect your personal information.

What Happened? On September 29, 2020, All Saints' was notified by Blackbaud, a large provider of cloud-based data management services to All Saints' and thousands of other schools, hospitals and not-for-profit organizations, that it had discovered and stopped a ransomware attack on Blackbaud's network that occurred in May 2020. Blackbaud, working with independent forensics experts and law enforcement, successfully prevented the cybercriminals from blocking system access and fully encrypting clients' data, including All Saints' files, and ultimately expelled the criminals from Blackbaud's system. However, prior to locking the cybercriminals out, the cybercriminals removed a copy of some of All Saints' data regarding students and other contacts located in a legacy version of the Blackbaud platform. Blackbaud informed All Saints' that this legacy platform had not been encrypted at the time of the incident.

What Information Was Involved? The information involved in this incident includes names and Social Security numbers.

What Are We Doing? As soon as we discovered the incident, All Saints' performed its own investigation to determine what information was stored in the legacy Blackbaud software and determined that your personal information may have been viewable to the unauthorized person. We have secured the services of IDX to assist us and, we are offering you credit monitoring and identity monitoring services for <<Membership Offering Length>> at no cost.

What You Can Do: Even though we have no evidence that your personal information has been misused, we want to encourage you to follow the recommendations included with this letter to protect your personal information. We strongly encourage you to enroll in the credit monitoring 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 1-833-791-1661 and provide the enrollment code found 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 your services is included with this letter. Please note you must enroll by February 5, 2021. If you have questions or need assistance, please call IDX at 1-833-791-1661.

For More Information: If you have any questions about this letter, please call 1-833-791-1661, Monday through Friday from 8 a.m. to 8 p.m. Central Time. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Rebecca Grimmer
CFO
All Saints' Episcopal School

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.