



# ST. SEBASTIAN'S SCHOOL

<<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>>,

I am writing to inform you that Blackbaud, Inc., a leading provider of cloud-based accounting and fundraising software used by St. Sebastian's School and thousands of other schools and organizations, recently provided us with information regarding a data security incident that affected some of your personal information.

## What Happened?

Last July, St. Sebastian's School was notified that Blackbaud discovered and stopped a ransomware attack of its self-hosted platform that had occurred in May 2020.

According to Blackbaud, prior to being locked out, the cybercriminal removed a copy of a subset of data from its self-hosted environment, which data contained information related to individuals affiliated with multiple schools and other organizations, including St. Sebastian's. Blackbaud said that it paid the cybercriminal's demand and received confirmation that the copy of the data removed has been destroyed. According to Blackbaud, this incident occurred at some point between February 7, 2020 and May 20, 2020; it was discovered in May of 2020.

In its original notice to us, Blackbaud reported that no credit card information, bank information, or Social Security Number of any St. Sebastian's constituent has been accessed or compromised. On September 29th, however, Blackbaud provided an updated notice letting us know that a limited number of Social Security numbers had been included in the copied data.

## What Type of Information Was Compromised?

Based on review of our records, we determined that the copied data included your name, address, email address, employment information and Social Security number. Other information relating to your association with St. Sebastian's might also have been included in the copied data.

As a result, on August 11th we emailed those individuals who we believed may have been affected a notification of the Blackbaud security incident and the types of information that may have been compromised, making it clear that we had been assured by Blackbaud that Social Security numbers and credit card information had not been compromised.

After sending that notice, we engaged an independent consultant to review records affected by the reported security incident. Based on our own review, we asked Blackbaud for additional information to help us fully understand the scope of the reported security incident.

On September 29th, when Blackbaud informed St. Sebastian's that a limited number of Social Security numbers may have been accessible in the copied data files, we promptly requested from Blackbaud access to the affected files and our third-party consultant continued its examination of affected records.

Based on the nature of the incident, Blackbaud's research, and third-party investigation, including investigation by law enforcement, Blackbaud has stated that it 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 reports it has hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

## What steps are we undertaking to secure your data?

Because we understand how unsettling it can be to learn that your personal data has been compromised – notwithstanding Blackbaud's assurances that misuse is not anticipated - we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. 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, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

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

You have until **February 2, 2021** to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing the services that are available to you is included with this letter.

Additionally, we are continuing to review relevant Blackbaud practices – even as Blackbaud has stated that it quickly identified the vulnerability associated with this incident and took swift action to fix it; and even as Blackbaud has confirmed through testing by multiple third parties that its fix should withstand all known attack tactics; and finally, even as Blackbaud has asserted that it is further hardening its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.

## What Can You Do?

While Blackbaud has stated that it 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, we still recommend that you take precautions and activate the free identity monitoring. Also, we have included information on some additional steps that you can take to help protect yourself, as you deem appropriate.

Whether or not you activate Kroll's services, it is always a good idea to watch for signs that your personal information is being misused and to report any suspicious activity to local law enforcement authorities. We have enclosed information explaining other steps that you can take to help protect your identity.

## For More Information About This Incident

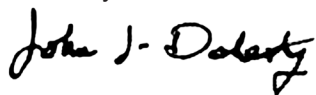
If you have questions, please call 1-???-???-???, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. Please have your membership number ready.

You can also consult the Blackbaud website at <https://www.blackbaud.com/securityincident>.

If you have further questions, please email me at [jack\\_dougherty@stsebs.org](mailto:jack_dougherty@stsebs.org) or leave me a message at 781-247-0111 or Ed Donovan, our Director of Technology, at [ed\\_donovan@stsebs.org](mailto:ed_donovan@stsebs.org) or leave him a message at 781-247-0133, and we will do our best to get back to you quickly.

Please know how terribly sorry we are about this most unfortunate incident.

Sincerely,



Jack Doherty '62  
Business Manager

## **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 will 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.

### **Web Watcher**

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

### **Public Persona**

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

### **Quick Cash Scan**

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

### **\$1 Million Identity Fraud Loss Reimbursement**

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

### **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.

## Other Steps You Can Take to Protect Your Identity

**St. Sebastian's School encourages you to enroll in Kroll's identity monitoring services. There are, however, other steps you may wish to take to protect your identity.**

### **REVIEW YOUR ACCOUNTS AND CREDIT REPORTS**

**Regularly review statements from your accounts and periodically obtain your credit report** from one or more of the national credit reporting companies. You should examine the reports carefully to see if there has been theft or unauthorized use of your credit or there is other incorrect information contained in the reports. The federal Fair Credit Reporting Act (FCRA) regulates how credit reporting agencies use, store, and disclose your information. FCRA provides you with various rights, including the right to require the credit reporting agencies to correct errors in the data that they maintain about you.

**You may obtain a free copy of your credit report** online, once every 12 months, at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov) and at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to:  
Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**You may also obtain a copy of your credit report** by contacting one or more of the three national credit reporting agencies listed below. Depending on the agency and service chosen, your state of residence, or other factors, the agency may charge fees. If you reside in any of the following jurisdictions, you are likely eligible for a free or discounted report and should request the price set by that jurisdiction: *CA, CO, CT, GA, ME, MD, MA, MN, MI, MS, MT, NJ, PR, VT, and VI.*

- Equifax (unless subject to state discount or waived, \$15.95 per single report or subscription).  
P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111.  
Online link: [www.equifax.com/personal/products/credit/report-and-score/](http://www.equifax.com/personal/products/credit/report-and-score/)
- Experian (options include free monthly report or additional services for variable fees).  
P.O. Box 9532, Allen, TX 75013, 1-888-397-3742.  
Online link: [www.experian.com/consumer-products/compare-credit-report-and-score-products.html](http://www.experian.com/consumer-products/compare-credit-report-and-score-products.html)
- TransUnion (unless subject to state discount or waived, \$11.50 for single report or subscription).  
P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-888-4213  
Online link: [disclosure.transunion.com/dc/disclosure/disclosure.jsp](http://disclosure.transunion.com/dc/disclosure/disclosure.jsp)

### **CONSIDER A FRAUD ALERT**

**Consider contacting the three major credit reporting agencies to request that a "fraud alert" be placed on your file.** A fraud alert notifies potential lenders to verify your identification before extending credit in your name. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies

- Equifax: Request alert by calling 800-525-6285  
Or online at: [www.alerts.equifax.com/AutoFraud\\_Online/jsp/fraudAlert.jsp](http://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp)
- Experian: Request alert by calling 800-397-3742 or 888-397-3742 (outside the U.S.)  
Or online at <https://www.experian.com/fraud/center.html>
- TransUnion: Request alert by calling 800-680-7289  
Or online at [www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

### **SECURITY FREEZE FOR CREDIT REPORTING AGENCIES**

**Consider contacting the three major credit reporting agencies to request that each place a "security freeze" on your individual credit file.** A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, it is important to understand that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit cards, mortgages, employment, housing or other services. Under most states' laws, if you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, state law limits to between \$5 and \$12 per transaction the prices that a credit reporting agency can charge to place, temporarily lift, or permanently remove a security freeze. For a summary of states' pricing limits, visit: [www.creditcards.com/credit-card-news/credit-freeze-laws-50-states.php](http://www.creditcards.com/credit-card-news/credit-freeze-laws-50-states.php).

To place a security freeze on your credit file you must submit a request to the credit agency that holds that file (whether it is Equifax, Experian or TransUnion). The following provides contact information, including online portals, mailing addresses and telephone numbers through which you can initiate requests for security freezes to the three major credit reporting agencies:

<u>Equifax Security Freeze</u>	<u>Experian Security Freeze</u>	<u>TransUnion Security Freeze</u>
<p><b><u>By mail:</u></b>  <b>Equifax Security Freeze</b>  <b>P.O. Box 105788</b>  <b>Atlanta, Georgia 30348</b></p> <p><b><u>By Telephone:</u></b>  <b>800-685-1111, except for</b>  <b>(New York residents, who may</b>  <b>instead call 800-349-9960).</b></p> <p><b><u>Online:</u></b>  <b><a href="http://www.freeze.equifax.com">www.freeze.equifax.com</a></b></p>	<p><b><u>By mail:</u></b>  <b>Experian Security Freeze</b>  <b>P.O. Box 9554</b>  <b>Allen, TX 75013</b></p> <p><b><u>By Telephone:</u></b>  <b>800-397-3742</b></p> <p><b><u>Online:</u></b>  <b><a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a></b></p>	<p><b><u>By mail:</u></b>  <b>TransUnion</b>  <b>Fraud Victim Assistance Dept.</b>  <b>P.O. Box 2000,</b>  <b>Chester PA 19016</b></p> <p><b><u>By Telephone:</u></b>  <b>888-909-8872</b></p> <p><b><u>Online:</u></b>  <b><a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a></b></p>

If you decide to request a security freeze, you will need to have the following information available when submitting your request:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. Complete home address information for the last two to five years (depending on your current state of residence)
5. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
6. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
7. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make your request to the credit reporting agencies by phone, mail, or if an agency provided it, by logging on to your online account. You will have to verify your identity by providing proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. You also will have to identify those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make your request to the credit reporting agencies by phone, mail, or if an agency provided it, by logging on to your online account. You will have to verify your identity by providing proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

#### **HELPFUL SUGGESTIONS IF YOU ARE A VICTIM OF IDENTITY THEFT**

- **File a police report.** Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- **Contact the U.S. Federal Trade Commission (FTC).** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); by mail, Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington DC 20580; or online at: [www.identitytheft.gov](http://www.identitytheft.gov).

- **Contact the attorney general or other consumer regulator for your state or territory.** In most states and territories within the U.S., the attorneys general or other consumer regulators administer identity theft protection laws and assist residents who are victims of such thefts. *Contact information for many of these state agencies is provided in a table at the end of this document.*
- **Keep a record of your contacts.** Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

## **OTHER INFORMATION**

**You can obtain further information about fraud alerts, security freezes, and steps you can take to avoid identify theft from the consumer reporting agencies identified above, and the FTC.** The FTC's identity theft website is located at [www.identitytheft.gov](http://www.identitytheft.gov); their toll free phone number is 1-877-ID-THEFT (1-877-438-4338); or you can write to: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

**For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), 1-877-566-7226.

**For New York residents:** The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**For Connecticut residents:** You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag).

**For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html).

### **Reporting of identity theft and obtaining a police report.**

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.