August 14, 2020

Via Email

Washington State Attorney General's Office
1125 Washington St SE
PO Box 40100
Olympia, WA 98504
Security.breach@atg.wa.gov

Orrick, Herrington & Sutcliffe LLP
701 Fifth Avenue
Suite 5600
Seattle, WA 98104-7097

+1 206 839 4300
orrick.com

Aravind Swaminathan

E aswaminathan@orrick.com
D +1 206 839 4340
F +1 206 839 4301

RE: Notification of Data Security Event / St. Joseph School

Dear Attorney General:

We are writing to let you know that Blackbaud, a St. Joseph School vendor that manages its donor databases, was recently the subject of a data security event. In July 2020, we learned that Blackbaud discovered and stopped a ransomware attack that occurred in May of this year. We understand that the cybercriminal removed a backup copy of donor information as part of a wide-reaching security event that involved data from multiple nonprofit organizations and other entities accepting donations. This backup copy contained the personal information of certain Washington residents.

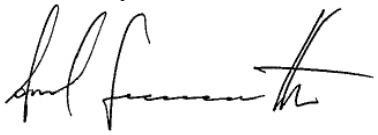
The affected file included donation information, such as names of donors, contact information, dates of birth, and donation dates and amounts. We have identified personal information—dates of birth—for 5,142 Washington residents. The cybercriminal did not access any credit card information, bank account information, or Social Security numbers, since we do not store this information in the database. Blackbaud also received confirmation that the copy of the data obtained by the cybercriminals was destroyed. We have no indication that these events resulted in any misuse of personal information.

We began notifying Washington State residents via letter and/or email on August 14, 2020, and due to lack of sufficient contact information, we are also providing substitute notice. We have attached a sample copy of the notification we are sending to individuals. We are offering one year of free credit monitoring services to those whose personal information was impacted. We have also been informed that Blackbaud has a number of safeguards in place and has already taken steps to enhance its systems to further protect against this kind of exploit. In particular,

Blackbaud has accelerated efforts to further harden its environment through enhancements to access management, network segmentation, deployment of additional endpoint monitoring, and network-based platforms.

If your office requires any further information in this matter, please contact me at (206) 839-4340 or aswaminathan@orrick.com.

Sincerely,



Aravind Swaminathan
Partner
Global Co-Chair Cyber, Privacy & Data Innovation

ST. JOSEPH SCHOOL
established 1907

August 14, 2020

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<MemberFirstName>> <<MemberLastName>>:

We are writing to let you know that Blackbaud, a St. Joseph School vendor that manages our donor database, was recently the subject of a data security event. Our records indicate that this may have impacted some of your personal information, **but not your credit card, bank account, or Social Security number**. This letter outlines what happened and provides you with some steps you can take to help protect yourself.

What Happened

In July 2020, Blackbaud notified St. Joseph School that it had discovered and stopped a ransomware attack that occurred in May of this year. This was a wide-reaching security event that involved data from multiple nonprofit organizations and other entities accepting donations. We understand the cybercriminal removed a backup copy of donor information that Blackbaud maintained for us. This backup copy may have contained some of your personal information. For more information about this data security event, Blackbaud released a public statement acknowledging this incident and describing its cybersecurity practices, located at www.blackbaud.com/securityincident.

What Information Was Involved

The affected file contained donation information, such as names of donors, contact information, dates of birth, and donation dates and amounts. The cybercriminal **did NOT access any credit card information, bank account information, or Social Security numbers,** since we do not store this information in our database.

Blackbaud also received confirmation that the copy of the data obtained by the cybercriminal was destroyed. We have no indication that these events resulted in any misuse of your personal information, but are notifying you so you can take certain precautions.

What We Are Doing

We are offering you free credit monitoring, provided by Experian. Please refer to the credit monitoring section of this letter, Attachment A, for more information about these credit monitoring services and how to sign up.

We take data security very seriously, especially as it relates to personal information. We deeply regret that this situation occurred. Once we were informed of the situation, we immediately reviewed our security protocols and procedures to reduce the risk of this situation arising again in the future. We then reviewed the files to determine who may have been impacted, to allow us to communicate clearly and accurately with those individuals and notify them of what happened. Blackbaud advised us that it implemented several changes to enhance the protection of personal information moving forward. In particular, Blackbaud has accelerated efforts to further harden its environment through enhancements to access management, network segmentation, deployment of additional endpoint monitoring, and network-based platforms.

What You Can Do

We encourage you to consider taking the following precautions:

- We urge you to remain vigilant against threats of identity theft or fraud. Regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity. Report any unauthorized activity on your credit or banking accounts to your credit or banking providers immediately.
- Be alert for “phishing” emails from someone who acts like they know you and requests sensitive information over email, such as passwords, Social Security numbers or bank account information.

- It is always a best practice to change your financial account passwords often.
- If you suspect you are the victim of identity theft or fraud, you have the right to file a report with the police or law enforcement.
- You may contact the FTC or the Washington State Attorney General to learn more about protecting yourself against identity theft. Attachment B, titled “Additional Information to Protect Yourself,” has more information about steps you can take to protect yourself against identity theft or fraud.

For More Information

For more information about this matter, or if you have additional questions or concerns, you may contact the call center set up by St. Joseph School at 1-844-915-2893 between the hours of 6:00 a.m. to 3:30 p.m. Pacific time, Monday through Friday. Again, we sincerely regret any concern this matter may cause.

Sincerely,

Patrick Fennessy
Head of School, St. Joseph School

Attachments

Attachment A

Credit Monitoring Services

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: <<b2b_text_1(EnrollmentDeadline)>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code: <<Member ID>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.288.8057 by **<<b2b_text_1(EnrollmentDeadline)>>**. Be prepared to provide engagement number **<<b2b_text_2(EngagementNumber)>>** as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your 12-MONTH EXPERIAN IDENTITYWORKS Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.288.8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Attachment B

Additional Information to Protect Yourself

To protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local law enforcement agency, your state's attorney general or the Federal Trade Commission. Please know that contacting us will not expedite any remediation of suspicious activity.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 726-1014.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

Consider contacting the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit-reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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, mortgages, employment, housing or other services.

A credit-reporting agency may not charge you to place, temporarily lift or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax:	Experian:	TransUnion:
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 105069	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
(888) 836-6351	(888) 397-3742	(800) 909-8872
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may obtain information about preventing identity theft at atg.wa.gov/identity-theftprivacy. You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes and how to protect yourself from identity theft. The FTC can be contacted at 600 Pennsylvania Ave. NW, Washington, DC 20580; telephone (202) 326-2222; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general or the FTC.