GODFREY & KAHN S.C.

833 EAST MICHIGAN STREET • SUITE 1800
MILWAUKEE, WISCONSIN 53202-5615

TEL • 414.273.3500 FAX • 414.273.5198

www • GKLAW.COM

Direct: 414-287-9450
**ssargent@gklaw.com**

October 30, 2020

**VIA ONLINE SUBMISSION**
**VIA OVERNIGHT MAIL**

Attorney General Aaron Frey
SECURITY BREACH NOTIFICATION
6 State House Station
Augusta, ME 04333

RE: Data Incident Notification

Dear Attorney General Frey:

Our firm represents Special Olympics Wisconsin, Inc. ("SOWI"), a nonprofit based in Madison, Wisconsin. SOWI hereby formally submits notification of a recent data incident involving its software provider, pursuant to Maine Rev. Stat. Tit. 10, Section 210-B-1346 et seq. SOWI reserves the right to supplement this notice with any significant details learned subsequent to this submission. By providing this notice, SOWI does not waive any rights or defenses regarding the applicability of Maine law, including the applicability of Maine Rev. Stat. Tit. 10, Section 210-B-1346 et seq., the applicability of any other laws of this or any other state, or the existence of personal jurisdiction over SOWI.

The relevant incident was a recent attempted ransomware attack targeting Blackbaud, Inc. ("Blackbaud")—not SOWI. Blackbaud is a cloud computing software company focused on serving nonprofits, including SOWI. Blackbaud recently informed SOWI that in May of 2020, Blackbaud discovered an unauthorized third party gained access to Blackbaud's systems in an attempt to install ransomware between February 7, 2020 and May 20, 2020. Blackbaud has described the incident in greater detail here: https://www.blackbaud.com/securityincident.

As relevant for purposes of this letter, Blackbaud has acknowledged that the attacker "removed a copy of a subset of data from [Blackbaud's] self-hosted environment." SOWI has since learned that its data was a part of the subset removed as a result of the attack on Blackbaud's system. SOWI determined that the data removed from Blackbaud's system may have contained individuals' names, driver's license numbers, and/or dates of birth. However, Blackbaud reports that it "paid the cybercriminal's demand" and received "confirmation that the copy they removed had been destroyed." Accordingly, Blackbaud 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." Based on Blackbaud's information and our investigation of this matter, we do not believe there is a significant risk of harm to the impacted individuals related to SOWI.

Out of an abundance of caution, however, SOWI has decided also to notify you (via this letter) and potentially affected residents of Maine on or about October 30, 2020, about the potential access to their personal information. SOWI will provide this notification to two (2) Maine residents. A sample notification letter is attached hereto as Exhibit A.

SOWI takes the security of personal information seriously, and SOWI will continue to monitor and engage in vendor due diligence with respect to Blackbaud and its handling of SOWI data. Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

GODFREY & KAHN, S.C.

Sarah A. Sargent

SAS

**EXHIBIT A**

**Sample Notification Letter**

Special Olympics Wisconsin

<<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>>,

We are writing to notify you, as a precautionary measure, of a recent security incident involving our service provider, Blackbaud, Inc. ("Blackbaud") that may have involved your personal information (the "Blackbaud Security Incident"). Blackbaud is a widely used provider of constituent relationship management software for engagement and fundraising offices of nonprofits, charities, and higher education institutions. To be clear, there was no intrusion into Special Olympics Wisconsin, Inc.'s ("SOWI") computer systems. Only Blackbaud's systems were impacted by the Blackbaud Security Incident. While we do not believe there is a significant risk of harm to your personal information, we wanted to inform you of this occurrence as a precautionary measure and share some steps that you can take to help protect yourself, as SOWI takes your privacy seriously.

**What Happened?**

On July 16, 2020, Blackbaud informed SOWI that an unauthorized third party gained accessed to Blackbaud's systems containing SOWI information. Upon learning of the Blackbaud Security Incident, SOWI retained counsel that specializes in data security incidents, and immediately began investigating to determine what information of SOWI was affected and to learn from Blackbaud additional details regarding the Blackbaud Security Incident. According to Blackbaud, the unauthorized third party gained access to Blackbaud's systems between February 7, 2020 and May 20, 2020, in an attempt to install ransomware. During that attempt, information from SOWI and many other Blackbaud customers was taken by the attacker. On August 20, 2020, SOWI determined what information was affected by this Blackbaud incident and began the process of assembling the information and resources necessary to provide notice to affected individuals.

SOWI further learned that during the Blackbaud Security Incident, the ransomware was not installed successfully, but the unauthorized third party removed a copy of Blackbaud's back-up files, which included your personal information. The unauthorized third party removed the information for the purpose of extorting money from Blackbaud. Subsequently, Blackbaud paid the unauthorized third party to delete the copy of the back-up files and received confirmation of the deletion. Based on the nature of the Blackbaud Security Incident, Blackbaud's research, SOWI's discussions with Blackbaud, and third-party investigations (including law enforcement), we have no reason to believe that any information taken in the Blackbaud Security Incident has been or will be misused at this time. Blackbaud has stated they took additional steps to ensure and received assurances that the attacker permanently deleted the back-up files. Nevertheless, SOWI is informing you of the Blackbaud Security Incident because we greatly value our relationship with you and take this matter seriously.

**What Information Was Involved?**

We have determined that the back-up files removed from Blackbaud's system may have contained your name, driver's license number, and/or date of birth, as well as information relating to your relationship with SOWI as a donor or volunteer. We have confirmed with Blackbaud that the unauthorized third party did not obtain any of your sensitive financial information or Social Security numbers that could be used for identity theft.

**What We Are Doing**

As one of many worldwide organizations that was impacted by Blackbaud's Security Incident and alleged security failures, we are disappointed and troubled by the Blackbaud Security Incident. We have therefore taken a number of steps to investigate the Blackbaud Security Incident because you and your privacy are important to us. We have had multiple conversations with Blackbaud and its counsel to understand what happened and obtain as many details as possible, and we have reviewed Blackbaud's extensive third-party forensic security report. We have also obtained assurances that Blackbaud has already taken steps to prevent something like this from happening in the future. Blackbaud informed us that its security team has fixed the vulnerability associated with the Blackbaud Security Incident, and this fix has been confirmed by third parties. In addition, Blackbaud hired a third-party team of experts to monitor the internet for any misuse of your information as a precautionary measure. Finally, we are providing you with this notice so that you understand what happened and get the opportunity to ask any questions you may have.

**For More Information**

We have included further information attached to this letter containing steps you can take to protect your personal information. SOWI sincerely apologizes for any inconvenience and concern this incident may cause you. We greatly appreciate your support of our organization and our cause. If you have additional questions, please contact Blackbaud at 1-855-907-2099, Monday through Friday, 9:00 a.m. to 9:00 p.m. EST or SOWI at donorsupport@specialolympicswisconsin.org.

Sincerely,

Special Olympics Wisconsin, Inc.
2310 Crossroads Drive Ste 1000
Madison, WI 53718

**Further Information Regarding Steps You Can Take**

Review Your 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 for the next 12 – 24 months. 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, including your state attorney general and the Federal Trade Commission (FTC). You have the right to obtain a police report if you are a victim of identity theft. You may need to give copies of the police report to creditors to clear up your records.

To file a complaint with the FTC, go to http://www.IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

For California Residents: You may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.

For Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: (410) 576-6491.

For New York Residents: You may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General at https://ag.ny.gov/ or by calling 1-800-771-7755; the New York State Police at http://troopers.ny.gov/ or by calling 1-518-457-6721; and/or the New York Department of State at https://www.dos.ny.gov or by calling 1-800-697-1220.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

For Rhode Island Residents: You have the right to file and obtain a copy of any police report. You also have the right to request a security freeze as described above. You may contact the Rhode Island Attorney General at https://www.riag.ri.gov, by calling 401-274-4400, or by writing to 150 South Main Street, Providence, RI 02903.

Obtain and Monitor Your Credit Report

We recommend that you 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. If you remain concerned, you can obtain a credit report from one of each of the three agencies/bureaus every four months (switching bureaus each time), to ensure you are actively monitoring your credit report. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Contact information for the three national credit reporting agencies is provided below:

| Equifax | Experian | TransUnion |
|---|---|---|
| (800) 685-1111 | (888) 397-3742 | (800) 888-4213 |
| www.equifax.com | www.experian.com | www.transunion.com |
| P.O. Box 740241 | P.O. Box 4500 | 2 Baldwin Place |
| Atlanta, GA 30374 | Allen, TX 75013 | P.O. Box 1000 |
| | | Chester, PA 19016 |

Consider Placing a Fraud Alert on Your Credit Report

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 1 year. 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. After you place an initial fraud alert, you can renew the alert for an additional 1 year period by calling any one of the agencies above.

Take Advantage of Additional Free Resources on Identity Theft

You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; http://www.IdentityTheft.gov; 1-877-ID THEFT (1-877-438-4338); and TTY: 1-866-653-4261. A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

Consider a Security Freeze on Your Credit File

You can request a "Security Freeze" on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies whose use is not exempt under law, will not be able to access your credit report without consent. Placing or removing a credit freeze is free. To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses or visit the URLs provided above.

The following information must be provided when requesting a security freeze: (1) Your name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.); (2) Your Social Security Number; (3) Your date of birth (month, day, and year); (4) Your complete address including proof of current address, such as a current utility bill, bank or insurance statement, or telephone bill; (5) If you have moved in the past 2 years, your previous addresses where you lived for the past 2 years; and (6) A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.).