



**Via Electronic Mail**  
[securitybreach@atg.wa.gov](mailto:securitybreach@atg.wa.gov)

August 14, 2020

Attorney General Bob Ferguson  
Office of the Attorney General  
1125 Washington Street SE  
PO Box 40100  
Olympia, WA 98504-0100

Re: Notice of Security Incident

Dear Attorney General Ferguson:

We are writing you on behalf of our client The Greater Boston Food Bank (“GBFB”) to notify you of a recent security incident that affected the personal information of some Washington state residents. GBFB is a 501(c)(3) tax-exempt hunger-relief organization serving New England.

Please be aware that this was not the result of any security failure of GBFB. GBFB had previously contracted with Blackbaud, Inc. (“Blackbaud”) to provide customer relationship management systems and services. Although GBFB had terminated its agreement with Blackbaud in 2019, some of GBFB’s information remained in Blackbaud’s system. On July 16, 2020, Blackbaud informed all of its customers, including GBFB, that Blackbaud had been the victim of a ransomware attack that was, according to Blackbaud, stopped in May of 2020. According to Blackbaud, the cybercriminal was unsuccessful in blocking Blackbaud or customer access to the database, but apparently the cybercriminal was able to remove a copy of a subset of data, including that of GBFB’s donors. According to Blackbaud’s investigation, it believes that the cybercriminal first accessed the database on February 7, 2020 and Blackbaud says the incident was resolved by May 20, 2020. Again, GBFB did not receive notice from Blackbaud until July 16, 2020. Further information as provided by Blackbaud is in the Blackbaud statement regarding the security incident at <https://www.blackbaud.com/securityincident>.

GBFB began immediately to determine what donor information was stored in the Blackbaud database; given the information we received from Blackbaud, it is not possible to determine exactly which datasets may have been accessed by the cybercriminal. The personal information as defined in RCW 19.255.010 included name, address, and date of birth. GBFB does not collect sensitive information such as social security number, and no financial information or credit card information was included in the affected Blackbaud database. GBFB processes that information via a separate encrypted platform that was not involved in the Blackbaud cybersecurity incident.

It has been determined that the “personal information” of approximately 40 Washington state residents was in GBFB’s dataset. A copy of a notification letter being sent to these residents on or about August 14, 2020 is attached. GBFB continues to request additional information from Blackbaud, and has terminated its relationship with Blackbaud. Blackbaud has informed us that it has taken steps to strengthen its protection of personal information, including updating its network security controls and email system, and it will continue to closely monitor and take further steps as appropriate to safeguard such information. GBFB also continues to improve its own internal policies and vendor management.

If there are any questions, please contact the undersigned at [cjlarose@mintz.com](mailto:cjlarose@mintz.com).

Sincerely,

A handwritten signature in black ink, appearing to read "Cynthia J. Larose". The signature is written in a cursive style with a large initial "C".

Cynthia J. Larose



August 14, 2020

## NOTICE OF DATA INCIDENT

Dear <Name>,

We write to inform you that, as a result of a ransomware attack on the software company Blackbaud, Inc. (“Blackbaud”), certain personal information you may have provided to The Greater Boston Food Bank (“GBFB”) could have been compromised. This personal data may include: your name, email address, phone number, physical address, and date of birth. **No credit card or financial information was included in the affected GBFB database.** For your protection, GBFB collects that information on a separate encrypted platform that was not involved in the cybersecurity incident.

Based on our current review as described further below, we have no indication that your information has been used inappropriately. However, we want to provide you with information about the incident and with the attached additional information that you may find helpful.

**What Happened?** GBFB previously worked with Blackbaud, Inc. (“Blackbaud”), a large software company that provides customer relationship management systems for not-for-profit organizations and the higher education sector. On July 16, 2020, Blackbaud informed its customers, including GBFB, that Blackbaud had been the victim of a ransomware attack that culminated in May 2020. According to Blackbaud, the cybercriminal was unsuccessful in blocking access to the database, however, Blackbaud informed us that the cybercriminal was able to remove a copy of a subset of data, including that of GBFB. This incident involved many, many clients of Blackbaud and GBFB information was not targeted specifically. Blackbaud informed us that they undertook a complete forensics investigation and paid the cybercriminal’s demand with confirmation that the copy they removed had been destroyed. According to Blackbaud, based on “its research and the third-party investigation (including law enforcement), there is 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.”

**What Information Was Involved?** GBFB terminated active use of our Blackbaud systems in September 2019 and transitioned to a new customer relationship management system. However, personal information was still maintained in the system and may have been involved in the incident. This personal data may include: your name, email address, phone number, physical address, and date of birth. **No credit card or financial information was included in the affected GBFB database.**

**What We Are Doing.** As noted, GBFB has already transitioned to a new customer relationship management system. Our current contract with Blackbaud ends September 30, 2020. We have reached out to Blackbaud to request that any GBFB data they maintain must be deleted from their server on or before this date.

**What You Can Do.** Although we have not identified any suspicious activity pertaining to your files and have not received any reports of misuse of your information, it is always a good practice to be vigilant and closely review your accounts for any evidence of unusual activity, fraudulent charges, or signs of identity theft. Please review the attached “Additional Information” that may be helpful to you.

**For More Information.** For further information about the Blackbaud incident, please see <https://www.blackbaud.com/securityincident>. If you have any questions for GBFB, please contact Erin Lee, our Director of Revenue Operations, at [elee@gbfb.org](mailto:elee@gbfb.org) or 857-256-1750. Our hours are 8:30am – 4:30pm EST.

Sincerely,

Catherine D'Amato  
President & CEO

70 South Bay Avenue • Boston, MA 02118 • Tel: 617.427.5200 • Fax: 617.427.0146 • [GBFB.org](http://GBFB.org)



## ADDITIONAL INFORMATION

**Contact information for the three nationwide credit reporting companies is as follows:**

**Equifax**, P.O. Box 105788, Atlanta, Georgia 30348, 1-877-478-7625, [www.equifax.com](http://www.equifax.com)

**Experian**, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, [www.experian.com](http://www.experian.com)

**TransUnion**, P.O. Box 2000, Chester, PA 19016, 1-800-680-7289, [www.transunion.com](http://www.transunion.com)

The following information reflects recommendations from the Federal Trade Commission regarding identity theft protection.

**Free Credit Report.** It is always a good practice to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://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 from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, Georgia 30348-5281.

**Fraud Alert.** You may place a fraud alert on your credit file by calling one of the three nationwide credit reporting agencies above. 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. Pursuant to federal and state laws, you may place a fraud alert on your credit file free of charge.

**Security Freeze.** You have the right to put a security freeze on your credit file, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. If you place a security freeze on your credit file, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting agency.* Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze. The following information must be included when requesting a security freeze (note that if you are requesting a security freeze for your spouse, this information must be provided for your spouse 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 (5) 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.

**Federal Trade Commission and State Attorneys General Offices.** If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580, [www.ftc.gov/bcp/edu/microsites/idtheft](http://www.ftc.gov/bcp/edu/microsites/idtheft), 1-877-IDTHEFT (438-4338).

**Reporting of identity theft and obtaining a police report.** You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

70 South Bay Avenue • Boston, MA 02118 • Tel: 617.427.5200 • Fax: 617.427.0146 • [GBFB.org](http://GBFB.org)