LEWIS BRISBOIS BISGAARD & SMITH LLP

Kamran Salour
650 Town Center Drive, Suite 1400
Costa Mesa, California 92626
Kamran.Salour@lewisbrisbois.com
Direct: 714.966.3145

December 9. 2020

File No. 213.1735

VIA ELECTRONIC MAIL ONLY

Attorney General Gordon MacDonald
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301
E-Mail: DOJ-CPB@doj.nh.gov

Re: **Notice of Data Security Incident**

Dear Attorney General MacDonald:

We represent Gleaners Community Food Bank of Southeastern Michigan ("Gleaners") in connection with the recent data security incident experienced by Blackbaud, Inc. ("Blackbaud"), one of the largest providers of fundraising and financial management software for non-profit organizations, including Gleaners. The incident did not involve Gleaners' network or systems.

I. Nature of the Security Incident

On July 16, 2020, Blackbaud reported that it experienced a data security incident that may have involved information pertaining to Gleaners' donors. Upon learning of the incident, Gleaners immediately launched an investigation to determine what happened and whether any personal information was impacted. According to Blackbaud, between February 7, 2020 and June 4, 2020, an unauthorized party had access to backup files related to the Blackbaud fundraising and donor management software used by Gleaners.

Upon learning this information, Gleaners retained outside cybersecurity experts to conduct an investigation. During the course of the investigation, Gleaners determined that personal information for its donors was contained in the backup files. On August 3, 2020, Gleaners notified its donors via email or mail, depending on the address Gleaners had for each donor, and informed them of the incident.

On November 4, 2020, Gleaners was able to identify the donors whose regulated datasets were contained in the backup files. Accordingly, on December 9, 2020, Gleaners provided individual notification letters to these constituents and provided them with steps they can take to protect their personal information.

II. Type of Information and Number of New Hampshire Residents Involved

The incident involved personal information for two New Hampshire residents. The information involved in the incident may differ depending on the individual but may include name, address, phone number, email address, date of birth, gender, giving information, and publicly-available donor analytics data. For a small subset of donors, the information involved may also include financial account information or credit/debit card information.

III. Steps Taken Relating to the Incident

As soon as Gleaners learned of the incident, it launched an investigation. It also worked with Blackbaud to obtain additional information regarding the incident and to confirm that the company was taking steps to ensure that the information at issue was not being misused, and that it was taking steps to further protect Gleaners information going forward. Blackbaud has represented that they are monitoring the dark web for any exchange of personal information related to this incident, but have found no indication that the information is available on the dark web. Blackbaud also stated that they have reported the incident to the Federal Bureau of Investigation ("FBI"). Gleaners will provide the FBI and law enforcement whatever assistance is needed.

In addition, Gleaners has notified the affected individuals and provided them with steps they can take to protect their personal information. For donors whose financial account information or credit/debit card information was involved in the incident, Gleaners is providing 12 months of complimentary identity monitoring services, fully managed identity theft recovery services, and $1,000,000 of coverage of reimbursement of any out of pocket identity recovery expenses through IDX.

IV. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at Kamran.Salour@lewisbrisbois.com or 714.966.3145.

Sincerely,

Kamran Salour of
LEWIS BRISBOIS BISGAARD & SMITH LLP

KS

Enclosure: Notification Letter Templates

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 9, 2020

Re: Notice of Data Security Incident

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

In August we sent you a notification alerting you to a data security incident experienced by Blackbaud, Inc., a third-party service provider for Gleaners that involved your personal information. We are commited to protecting your personal information to every degree possible and to keeping you informed about what occurred. This letter contains additional information that we have learned since our email and mail notice. Also included are suggested steps you can take to protect your personal information.

What Happened: On July 16, 2020, Blackbaud informed Gleaners that it had experienced a data security incident that involved information pertaining to our donors. We learned at that time that between February 7, 2020, and May 20, 2020, an unauthorized third party gained access to Blackbaud's servers where backup files for our fundraising and donor relationship management software were stored. Blackbaud informed us that they have no reason to believe that any information in the files has been or will be misused or will otherwise be made available publicly.

What Information Was Involved: On November 4, 2020, our investigation determined that some of your personal information was contained in the backup files. The incident involved the following information: name, address, phone number, email address, date of birth, gender, giving information, and publicly available donor analytics data. For a small subsect of our supporters, the information involved may have also included bank account and/or credit/debit card information – provided that you gave us such information. Please be assured that your Social Security number was **not** involved in the incident as we do not collect that information.

What We Are Doing: As soon as we learned of the incident, we engaged our own cybersecurity experts and launched an investigation. We also worked with Blackbaud to obtain additional information regarding the incident, to confirm that information about our donors was not misused, and to ensure that it took steps to further protect this information going forward. We also confirmed that the incident was reported to the Federal Bureau of Investigation. Now, we are providing you with more information on the incident and steps you can take to protect your personal information.

What You Can Do: Though Blackbaud has no reason to believe that any information in the files has been or will be misused or will otherwise be made available publicly, we are offering <<12 months/24 months>> of complementary identity monitoring services, fully-managed identity theft recovery services, and $1,000,000 of coverage for reimbursement of any out-of-pocket identity recovery expenses through IDX. In addition, you can follow the recommendations in the attached document to further protect your personal information.

For More Information: If you have any questions about this letter, please call (800) 939-4170 between 9 a.m. and 9 p.m. Eastern Time. You may also consult the resources included on the following page, which provides information about how to protect your personal information.

This incident with Blackbaud affected thousands of charities across the country that rely on its fundraising and donor management platforms. The security of your information is a top priority for Gleaners. We are committed to safeguarding your data and privacy, and we regret any concern that this incident may cause.

Sincerely,

Gerald F. Brisson
President & CEO

Steps You Can Take to Further Protect Your 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. 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 9532	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	1-800-525-6285	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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their attorneys general using the contact information below.

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 the right 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. 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.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 9, 2020

Re: Notice of Data Security Incident

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

In August we sent you a notification alerting you to a data security incident experienced by Blackbaud, Inc., a third-party service provider for Gleaners that involved your personal information. We are commited to protecting your personal information to every degree possible and to keeping you informed about what occurred. This letter contains additional information that we have learned since our email and mail notice. Also included are suggested steps you can take to protect your personal information.

What Happened: On July 16, 2020, Blackbaud informed Gleaners that it had experienced a data security incident that involved information pertaining to our donors. We learned at that time that between February 7, 2020, and May 20, 2020, an unauthorized third party gained access to Blackbaud's servers where backup files for our fundraising and donor relationship management software were stored. Blackbaud informed us that they have no reason to believe that any information in the files has been or will be misused or will otherwise be made available publicly.

What Information Was Involved: On November 4, 2020, our investigation determined that some of your personal information was contained in the backup files. The incident involved the following information: name, address, phone number, email address, date of birth, gender, giving information, and publicly available donor analytics data. Please be assured that your Social Security number was **not** involved in the incident as we do not collect that information. The incident also did **not** involve your bank account information or your credit/debit card information.

What We Are Doing: As soon as we learned of the incident, we engaged our own cybersecurity experts and launched an investigation. We also worked with Blackbaud to obtain additional information regarding the incident, to confirm that information about our donors was not misused, and to ensure that it took steps to further protect this information going forward. We also confirmed that the incident was reported to the Federal Bureau of Investigation. Now, we are providing you with more information on the incident and steps you can take to protect your personal information.

What You Can Do: You can follow the recommendations in the attached document to further protect your personal information.

For More Information: If you have any questions about this letter, please call (800) 939-4170 between 9 a.m. and 9 p.m. Eastern Time. You may also consult the resources included on the following page, which provides information about how to protect your personal information.

This incident with Blackbaud affected thousands of charities across the country that rely on its fundraising and donor management platforms. The security of your information is a top priority for Gleaners. We are committed to safeguarding your data and privacy, and we regret any concern that this incident may cause.

Sincerely,

Gerald F. Brisson
President & CEO

Steps You Can Take to Further Protect Your 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. 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 9532	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	1-800-525-6285	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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their attorneys general using the contact information below.

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 the right 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. 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.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.