Franciscan HEALTH
FOUNDATION

November 13, 2020

Name
Address
Address

Subject: Notice of Data Security Incident

Dear Name,

We take the proper handling of your personal information very seriously. For this reason, we are contacting you directly to explain the circumstances of a data security incident that involved your personal information.

What Happened?
On July 16, 2020, Franciscan Health Foundation (the "Foundation") was notified by Blackbaud, a nationwide vendor that provides numerous nonprofit organizations with software and support for their fundraising donor management systems, that Blackbaud experienced a data security incident involving your personal information. Upon receiving this notice, we took immediate steps to begin our own investigation to determine what, if any, Foundation data was impacted. Please note that this attack did not occur within the information systems of Franciscan Health Foundation or any affiliated Ministry. We are contacting you to explain the incident and provide you with steps you can take to protect yourself. While we have no information at this time that would indicate that your personal information has been misused, please find details below about the incident and additional steps you can take to protect your information.

Blackbaud informed us that their organization was a target of a ransomware event that occurred between February 7, 2020 and May 20, 2020. As a result of the data security incident, cybercriminals obtained some personal information about Blackbaud customers' donor data, which included Franciscan Health Foundation donors. After discovering the event, Blackbaud's Cyber Security team collaborated with independent forensics experts and law enforcement to evaluate the impact of the event. Blackbaud stated that they had confirmation that the cybercriminals deleted all copies of the back-up files containing personal information in exchange for a paid ransom. More details about Blackbaud's data security incident can be found at: https://www.blackbaud.com/securityincident.

While data security incidents and ransomware attacks have increased in frequency, this is not something the Foundation ever wants to happen to our valued supporters. The privacy of our donors is of utmost importance to us.

What Information Was Involved in This Data Security Incident?
Your information involved in the Blackbaud incident included: names, addresses, telephone numbers, and images of checks or financial account numbers. It also may have included email addresses, dates of birth, and mailing addresses; and a history of donor relationships with our organization, such as donation dates, donation amounts, and other information in our donor profiles.

To protect personal customer data, Blackbaud paid the cybercriminal's demand with confirmation that the removed data had been destroyed. Based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, Blackbaud does not believe any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly, and Blackbaud has hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

What Are We Doing to Protect You?
We continue to work with Blackbaud to monitor the situation for any new details about the incident and are re-evaluating how we collect and store information to further protect the information of our donors.

What You Can Do

We want to emphasize again that based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, 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. To help relieve concerns and restore confidence following this incident, we have secured the services of First Watch to provide identity theft protection, upon enrollment, at no cost to you for one year. The identity theft protection services being offered to protect you include credit monitoring, identity theft consultation and restoration, and identity theft protection insurance of up to $1 million dollars to protect you against identity theft. First Watch's team has extensive experience helping people whose records have been involved in data security incidents. As a best practice, we recommend that donors remain vigilant by reviewing their account statements and credit reports closely and reporting any suspicious activities.

- If you receive unsolicited requests for donations from us or other nonprofits, then call the number on the organization's website to confirm the legitimacy of the solicitation.

- You can 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 completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. The three nationwide credit reporting agencies are:

  Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
  Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
  TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

- Also, you have the ability to place a security freeze on your credit report, free of charge, through the three credit reporting agencies listed above. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent.

- If you detect any suspicious activity, then promptly notify the financial institution or company where the account is maintained. You also should report any fraudulent activity or suspected incidence of identity theft to law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

- To file a complaint with the Federal Trade Commission, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). The Federal Trade Commission offers tips on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

For More Information

We have established a hotline to answer your questions about the data security incident. If you have further questions, or if you would like to enroll with First Watch to provide identity theft protection, please contact the hotline at (833) 295-7812. Please have this letter available when you call.

We deeply regret that this incident occurred. Blackbaud has apologized to Franciscan Health Foundation and, on behalf of them and us, we sincerely apologize for any inconvenience this incident may cause you.

We know that every gift made to Franciscan Health Foundation is a choice. Thank you for your continued support of our healthcare ministry. Your generosity brings hope to the communities we are privileged to serve.

Sincerely,

Caitlin A. Leahy, Senior Vice President
Franciscan Health Foundation

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

To order your annual free credit report please visit **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) 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).

Fraud Alert. You may place a fraud alert in your 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.

Security Freeze. You have the ability to place a security freeze on your credit report, free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her 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 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 Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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, 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, 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; https://ag.ny.gov/; 1-800-771-7755.
For **Connecticut residents**: You may contact the Connecticut Office of the Attorney General, 55 Elm Street, Hartford, CT 06106; www.ct.gov/ag; 1-860-808-5318.
For **Massachusetts residents**: You may contact the Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108; www.mass.gov/ago/contact-us.html; 1-617-727-8400.

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.