Saint Luke's
FOUNDATION

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

We value and respect the privacy of your information, which is why, as a precautionary measure, we are writing on behalf of Saint Luke's Foundation ("SLF") to inform you of a recent security incident involving one of our third-party vendors that may have affected some of your information and share some steps that you can take to help protect yourself. SLF is a non-profit organization and affiliated foundation of Saint Luke's Health System ("SLHS").

WHAT HAPPENED?

On July 16, 2020, we were notified by one of our third-party vendors, Blackbaud, that it had experienced a security incident potentially involving certain limited information it obtained from SLF. Blackbaud is a widely used constituent relationship management software provider for engagement and fundraising offices in higher education and nonprofits. Blackbaud informed us that it discovered and stopped a ransomware attack, but not before some information may have been compromised. According to information provided to us by Blackbaud, the cybercriminal removed a copy of our backup file for the purpose of extorting funds from Blackbaud. Blackbaud stated that the ransomware attack and data compromise occurred at some point between February 7, 2020 and May 20, 2020.

Based on the nature of the incident, their research, and third-party (including law enforcement) investigation, Blackbaud has assured us that it has no reason to believe that any data went beyond this cybercriminal or was disseminated or otherwise made available publicly. Blackbaud further stated that they have taken additional steps to ensure that the backup file was permanently deleted.

WHAT INFORMATION WAS INVOLVED?

Blackbaud has informed us that the cybercriminal did not access credit card information, bank account information or social security numbers, as this information was encrypted and stored in a separate backup system from what was compromised. Blackbaud has also informed us that the compromised backup file may have contained some of your patient demographic and guarantor information, such as name, mailing address, and telephone number as well as your email address and date of birth, and possibly limited medical information about you, such as date of service and department of care.

WHAT WE ARE DOING

As part of its ongoing efforts to help avoid an event like this from happening in the future, Blackbaud has affirmed to SLF that it has already implemented changes to help protect its system from any subsequent incidents. Since learning of the issue, Blackbaud identified the vulnerability associated with this incident, including the tactics used by the cybercriminal, and has taken actions to fix it. Additionally, Blackbaud is accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint, and network-based platforms. As an additional precautionary measure, Blackbaud has indicated that it has hired a third-party team of experts to monitor the dark web for any further misuse of the data.

WHAT YOU CAN DO

Please review the enclosed “Other Important Information” document included with this letter for further steps you can take to protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. Although no Social Security numbers or financial account information were involved, as best practice, we recommend you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit reports for unauthorized activity.

FOR MORE INFORMATION

If you have any further questions or concerns regarding this matter, please do not hesitate to contact us at [redacted] between 8 a.m. – 8 p.m. Central Time, Monday through Friday. Additional information about this incident can be found at https://www.blackbaud.com/securityincident.

Sincerely,

Michael VanDerhoef
President and Chief Executive Officer, Saint Luke’s Foundation

OTHER IMPORTANT INFORMATION

Contact information for the three nationwide credit reporting agencies:

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 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. 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.

Fraud Alert. You have the right to place an initial or extended "fraud alert" on your file at no cost by contacting any of the three nationwide credit reporting agencies identified above. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert, which lasts for 7 years, on your credit file.

Security Freeze. You have the right 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. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or up to 3 business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the 3 credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to remove the security freeze.

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 FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (438-4338).

- **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. There are 16 Rhode Island residents potentially impacted by this incident.