St. Vincent de Paul of Baltimore Provides Notice of a Data Privacy Event

St. Vincent de Paul of Baltimore ("SVDP") is providing notice of a data privacy event that may impact the privacy of certain personal information. At this time, SVDP has no indication of actual misuse of personal information relating to this incident, but is providing notice of this incident to potentially impacted individuals in an abundance of caution.

SVDP became aware of potential unauthorized access to an employee's email account and immediately launched an investigation to determine the nature and scope of the event. After further investigation, with assistance from outside IT specialists, SVDP determined there was unauthorized access to one employee email account. Since the investigation could not determine what information, if any, within the email account was accessed, SVDP conducted a thorough and lengthy review of the email account to determine what sensitive information could have been accessed without authorization. The investigation determined that personal information for certain individuals may have been subject to unauthorized access. The information potentially impacted by this event varied by individual but included first and last names and one or more of the following data elements: Social Security number, driver's license number, state identification card number, tax identification number, credit card or debit card information, health information, health insurance policy number, and username and password.

After determining those individuals potentially impacted by the incident, SVDP next worked to confirm whether valid address information for those individuals was available to which to mail written notice of the incident. On September 3, 2020, SVDP began mailing written notice of the incident to affected individuals for whom it was able to identify valid address information. The notice includes an offer of access to 12 months of credit monitoring and identity theft restoration services to individuals with Social Security number impacted at no cost to the individual.

SVDP takes this incident and the security of personal information in its care very seriously. Upon learning of this issue, SVDP removed any unauthorized rules from the account and implemented security measures to protect against similar incidents in the future, including the resetting of the impacted email account's credentials.

Please review the "Steps You Can Take to Help Protect Your Information" section below. We have also arranged for 12 months of complimentary credit monitoring and identity restoration services through Kroll for individual whose Social Security number was impacted. Instructions on how to enroll in these services is included in the enclosed "Steps You Can Take to Protect Your Information." We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and credit reports for suspicious activity.

We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please contact us by mail at 2305 North Charles Street, Suite 300, Baltimore, MD 21218, or our toll-free dedicated number at (888) 498-0917, Monday through Friday between 8:00 am and 5:30 pm CDT.

Steps You Can Take to Help Protect Your Information

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order

your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and, TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted by mail at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, by phone at 1-410-528-8662 or toll-free 1-888-743-0023, and online at www.marylandattorneygeneral.gov.