17721

Southern Adventist University
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

SOUTHERN
ADVENTIST UNIVERSITY

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

Dear [redacted]:

We regret to inform you about a data security incident at a third-party vendor that Southern Adventist University has used for many years with no issues. The third-party vendor is a software and service provider that is widely used for fundraising and alumni or donor engagement efforts at thousands of non-profits and universities around the world, including Southern Adventist University ("Southern").

Southern takes the protection and proper use of your information very seriously. We follow best practices and confidentiality is a high priority. We are therefore contacting you out of an abundance of caution to explain the incident and provide you with timely information that the third-party vendor has provided its customers.

We recently learned that a limited amount of your personal information may have been disclosed to an unauthorized individual following an incident at our third-party vendor. This information may have included your [redacted]. **Your Social Security number was not exposed, as it was encrypted.**

According to the third-party vendor, there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Our vendor indicates that it has hired a third-party team of experts, including a team of forensic accountants, to continue monitoring for any such activity. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. This letter provides precautionary measures that you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis and report any suspicious activity to the proper authorities.

We sincerely apologize for this incident and regret any inconvenience it may cause you. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. The third-party vendor has assured us that they closed the vulnerability that allowed the incident and that they are enhancing their security controls and conducting ongoing efforts against incidents like this in the future. We continually evaluate and modify our practices, and those of our third-party service providers, to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free line set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The person you speak with will not have access to your sensitive information. The response line is available Monday through Friday, 8:00 a.m. to 5:00 p.m. Eastern Time.

Sincerely,

[redacted]
Southern Adventist University

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

You may place an initial one (1) year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

2. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-349-9960

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

5. **Obtaining a Police Report.**

Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.