ECKERT SEAMANS
ATTORNEYS AT LAW

Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

TEL: 412 566 6000
FAX: 412 566 6099

Matthew H. Meade, Esq.
(412) 566-6983
mmeade@eckertseamans.com

October 2, 2020

VIA FIRST CLASS MAIL

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, New Hampshire 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

I am writing to you on behalf of my client, St. Paul Center for Biblical Theology ("St. Paul Center"), a 501(c)(3) non-profit research and educational institute that promotes Scripture study and serves clergy, laity, students and scholars. By way of this letter, St. Paul Center is providing notice of a data security incident which may have resulted in the unauthorized acquisition of some personal information provided by individuals using St. Paul Center's website to make online purchases or donations. This information may have included the name, address, email address, telephone number, and payment card number, along with the accompanying CVV code, pin or expiration date, of thirty-five (35) New Hampshire residents. St. Paul Center will be providing written notice to the affected individuals later today, via U.S. mail. The notice includes general advice on how to protect one's identity as well as information on obtaining free credit reports and security freezes. A sample of the notice that will be provided is enclosed. Additional information on the incident is below.

On August 20, 2020, St. Paul Center received notice from a payment processing vendor that its website (http://www.stpaulcenter.com) was a common point of purchase for some unauthorized payment card transactions and that there may have been a possible compromise of the website. St. Paul Center conducted an investigation to find out what happened, to prevent something like this from happening again, and to provide notice to potentially affected individuals.

St. Paul Center determined that a cyber-criminal installed malware in software that St. Paul Center used to enhance its online purchasing. The malware permitted the unauthorized collection or "scraping" of certain payment card data provided through the website. St. Paul Center believes the incident only involved customers who made purchases or donations on the website between March 3, 2020 and August 9, 2020. On August 26, 2020, St. Paul Center determined that the incident may have involved the personal information of New Hampshire residents.

St. Paul Center's technical experts identified and corrected the issue, effectively closing the point of entry for the website malware. To help prevent a similar incident from occurring in the future, St. Paul Center conducted an extensive internal audit to all systems and has implemented more stringent, ongoing processes for identifying and eliminating vulnerabilities. In addition to providing notice to potentially affected individuals, St. Paul Center is providing notice of this incident to appropriate regulators, consistent with its compliance obligations and responsibilities.

Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,

/s/ Matthew H. Meade

MHM/
Enclosure

ST. PAUL CENTER
for BIBLICAL THEOLOGY
1468 Parkview Circle, Steubenville, OH 43952-1739

October 2, 2020

NOTICE OF DATA SECURITY INCIDENT

We are writing to tell you about a recent data security incident that may have resulted in the unauthorized acquisition of personal information you provided when using our website to make online purchases. We take this matter very seriously because we know how important your personal information is to you. We are providing this notice to you as a precautionary measure, to inform you and to explain steps that you can take to protect your information.

What Happened

On August 20, 2020, St. Paul Center received notice from a payment processing vendor that our website (http://www.stpaulcenter.com) was a common point of purchase for some unauthorized payment card transactions and that there may have been a possible compromise of our website. We investigated to find out what happened, to prevent something like this from happening again, and to provide notice to potentially affected individuals.

We determined that a cyber-criminal installed malware in software that we use to enhance our online purchasing. The malware permitted the unauthorized collection or "scraping" of certain payment card data provided through the website. We believe the incident only involved customers who made purchases or donations on the website between March 3, 2020 and August 9, 2020. On August 26, 2020, we determined that the incident may have involved your personal information because you made a payment card purchase or donation using our website during that time period.

What Information Was Involved

Once we determined that there may have been unauthorized acquisition of payment card information, we reviewed our purchase records to find out who may have been affected and where those people resided. The information may have included your name, address, email address, telephone number and payment card number, along with the accompanying CVV code, pin or expiration date.

What We Are Doing About It

When we discovered this incident, our technical experts identified and corrected the issue, effectively closing the point of entry for the website malware. To help prevent a similar incident from occurring in the future, we conducted an extensive internal audit to all systems and have implemented more stringent, ongoing processes for identifying and eliminating vulnerabilities. We are also providing notice of this incident to appropriate state regulators, consistent with our compliance obligations and responsibilities.

What You Can Do

We recommend that you remain vigilant to the possibility of fraud and identity theft by monitoring your account statements and free credit reports for any unauthorized activity. Report any incidents of suspected identity theft to your local law enforcement and state Attorney General.

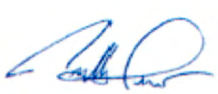
If you believe your payment card information may have been compromised, you should consider contacting your payment card company and/or financial institution and request that the card be cancelled. We strongly recommend that you review the information provided at the end of this letter, entitled "More Information about Identity Theft and Ways to Protect Yourself" and "State-Specific Information."

For More Information

If you have any questions or need more information, please call us, toll-free, at 1-888-487-2114, Monday through Friday, from 9:00 a.m. to 5:00 p.m. EST.

We know that this situation is frustrating to you, and we deeply regret this incident. Please know we take your support, and your trust, very seriously. We hope our actions moving forward will demonstrate this.

Very truly yours,



Anthony Puorro,
Chief Financial Officer

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

You also may request a security freeze be added to your credit report at Experian's online Freeze Center, www.experian.com/freeze/center.html, by phone at 1-888-EXPERIAN (1-888-397-3742), or by mail to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013. More information on a security freeze can be found below.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

For Georgia, Maryland, New Jersey, 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.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically, which can help spot and address problems 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 at the information provided above.

Fraud Alerts

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 new accounts in your name. To place a fraud alert on

your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. 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; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

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 you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

STATE SPECIFIC INFORMATION

DISTRICT OF COLUMBIA residents: You may also obtain information about preventing and avoiding identity theft from the D.C. Attorney General's Office. This office can be reached at:

Office of the Attorney General of the District of Columbia
Office of Consumer Protection
441 4th Street, NW
Washington, D.C. 20001
www.oag.dc.gov
1-202-727-3400

MARYLAND residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
Toll-free: 1-888-743-0023

NEW MEXICO residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may

not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

NEW YORK residents: You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State
Division of Consumer Protection
1-800-697-1220
http://www.dos.ny.gov/consumerprotection

New York Attorney General
1-800-771-7755
http://www.ag.ny.gov/home.html

NORTH CAROLINA residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
Toll-free: 1-877-566-7226

RHODE ISLAND residents: You have the right to file and obtain a copy of a police report concerning any fraud or identity theft committed using your personal information. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
Toll-free: 1-401-274-4400