THE BOARD OF PENSIONS
OF THE PRESBYTERIAN CHURCH (U.S.A.)

December 11, 2017

Name
Address
City, State Zip

Re: Notice of Unauthorized Access of Pensioner Information

Dear Name:

This letter is a follow-up to the telephone call you received from the Board of Pensions during the week of December 4 about an incident involving some of your personal information. We understand the importance of protecting the privacy and security of your personal information, and we take our obligations seriously. We apologize for any inconvenience this incident may cause you.

This letter provides additional information about what happened, what information was involved, what we are doing about it, and what you can do to protect your information. At the end of this letter is a phone number where you can contact us.

WHAT HAPPENED? On December 1, 2017, The Board of Pensions of the Presbyterian Church (U.S.A.) learned that unauthorized Benefits Connect logons had been established for certain pensioners who had not previously registered for Benefits Connect, and that contact and bank account information for those pensioners had been altered without pensioner authorization. In 11 instances, direct deposit routing information was changed and the Board's December 1 direct deposit was remitted to the altered account. If your December 1 pension payment was diverted, you have been advised and you have been sent a replacement check by mail. For the other pensioners impacted by this fraudulent activity, the information was changed after the Board's December 1 pension process. For those accounts, the fraudulent activity was detected and stopped before any future payments were sent.

WHAT INFORMATION WAS INVOLVED? The pensioner information that ***may*** have been accessed as a result of this incident includes names and dates of birth of pensioners, spouses, and dependents enrolled for Benefits Plan medical benefits; retiree mailing addresses; telephone numbers; email addresses; and bank account information. If an impacted retiree has designated a beneficiary for death benefits who was not a spouse or dependent child, the beneficiary's name, address, and Social Security number were also accessible.

WHAT WE ARE DOING. Once the Board became aware of the incident, we immediately launched a comprehensive investigation to determine the nature and the scope of the incident, which of our pensioners were involved in the incident, and how to restore the security of any personal information that was potentially impacted. We have notified law enforcement of the incident and we are assisting in the criminal investigation. We have also implemented additional controls to avert any future fraudulent activity.

WHAT YOU CAN DO. We encourage you to review the enclosed information on how to ensure the security of your information with us, as well as how to protect yourself against identity theft or fraud.

As an added precaution, AllClear ID identity protection services are being made available to you for 12 months at no cost to you. The following identity protection services start on the date of this notice, and you can use them at any time during the next 12 months.

> AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, call 877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit, and make sure your identity is returned to its proper condition.
>
> AllClear Credit Monitoring: This service offers additional layers of protection, including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or call 877-676-0379 using the following redemption code: XXXXXXXXX.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options. If you need enrollment assistance, please contact us at Member Services, 800-773-7752 (800-PRESPLAN).

There are other companies that offer similar protection programs, and a description of those programs and other steps you can take to protect yourself is enclosed.

FOR MORE INFORMATION. The security of the personal information that our members entrust into our care is one of our highest priorities. Should you have any questions about the content of this notification letter, or if you would like to learn more about ways that you can protect yourself against fraud and identity theft, please call us at Member Services, 800-773-7752 (800-PRESPLAN).

Sincerely,

Susan Reimann

Susan Reimann
Executive Vice President and Chief Operating Officer

ADDITIONAL STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

You may take action directly to further protect against possible identity theft or other financial loss. We encourage you to be vigilant against incidents of identity theft by reviewing your account statements regularly and monitoring your 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 bureaus. To order your free credit report, visit annualcreditreport.com or call, toll-free, 877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a *fraud alert* on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax Information Services LLC	Experian	TransUnion Fraud Victim Assistance
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
866-349-5191	888-397-3742	888-909-8872
equifax.com	experian.com	transunion.com

In addition to a fraud alert, consumers may place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place the freeze on all of your credit files.

To find out more on how to place a security freeze, you can contact the credit reporting agencies using the information below:

Equifax Information Services LLC	Experian Security Freeze	TransUnion LLC
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013	Chester, PA 19016
800-685-1111	888-397-3742	888-909-8872
www.freeze.equifax.com	experian.com	freeze.transunion.com

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission (FTC) or your state Attorney General. The FTC can be reached at: 600 Pennsylvania Ave. NW, Washington, DC 20580, ftc.gov/idtheft, 877-ID-THEFT (877-438-4338); TTY: 866-653-4261. The FTC also encourages those who discover that their information has been misused to file a complaint with the FTC. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement, including your state Attorney General.

For Iowa residents, the Attorney General can be contacted at Hoover State Office Building, 1305 E. Walnut St., Des Moines, IA 50319, 888-777-4590, iowaattorneygeneral.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.marylandattorneygeneral.gov.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699, 919-716-6400, ncdoj.gov.

For Oregon residents, the Attorney General can be contacted at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301, 877-877-9392, doj.state.or.us.

For Rhode Island residents, the Attorney General can be contacted at Office of the Attorney General, 150 S. Main St., Providence, RI 02903, 401-274-4400, riag.ri.gov.

For all other residents, information on how to contact your state attorney general may be found at naag.org/naag/attorneys-general/whos-my-ag.php.