PenServ
PLAN SERVICES

March 31, 2017

[Name]
[Address]
[Address]
[City], [State] [Zip]

Re: Notice of Data Breach

Dear [Name]:

We are writing to tell you about a data security incident that may have exposed some of your personal information. While we are unaware of any actual or attempted misuse of your personal information, we take the protection and proper use of your information very seriously. Accordingly, we are contacting you directly to explain the circumstances of the incident.

What Happened?

As you may know, PenServ Plan Services, Inc. is a third-party administrator for Security Finance's 401(k) Profit-Sharing Savings Plan. In connection with its services as plan administrator, PenServ recently sent plan participants an email notifying them of their various plan options and benefits guides. Unfortunately, this email inadvertently included a spreadsheet containing plan participants' personal information to some of its recipients. The date of this email notice ranged from February 26, 2017 to March 1, 2017. The error was discovered on March 1, 2017, and we have since reached out to all recipients of this email and instructed them to permanently delete this email and all of its attachments. This notice was not delayed as a result of a law enforcement investigation. We have also worked with Security Finance to delete all versions of this email and its attachments from its email servers. None of our systems were breached, and no other information was accessed or obtained.

What Information Was Involved?

The personal information at issue included your name, Social Security number, age, date of birth, compensation, and financial plan information.

What We Are Doing About This Issue

PenServ values the security and privacy of your information and takes this matter very seriously. Although PenServ has policies and procedures that should have avoided this type of data security event, we are conducting a thorough review of the events surrounding this incident in order to prevent any future occurrences, including the implementation of additional protocols for sending information electronically. Additionally, we will be

Penserv Plan Services, Inc.
102 Trade Zone Drive
West Columbia, South Carolina 29170
Tel +1 803.822.1820
www.penserv.com

working with outside subject matter experts in this investigation to avoid any similar incidents and to provide training to our staff.

To help protect your confidential information, PenServ is offering you twelve (12) months of free identity protection services through Experian. Please see the enclosed document titled "How To Access Your Free Identity Protection Services" to learn how to enroll and take advantage of your free identity monitoring services.

What You Can Do

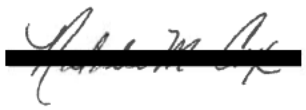
In addition to enrolling in the free identity protections services referenced above, there are additional actions you can take to mitigate the chances of fraud or identity theft. We encourage you to monitor your credit reports and other financial records for fraudulent transactions as well as review the information included in the attachment to this letter titled "Steps You Can Take to Further Protect Your Information," which has further information on steps you can take to protect your information.

For More Information

We understand that you may have questions relating to this even that are not answered in this letter. If you have any questions, or if PenServ can be of further assistance, please contact Natalie Cox at 877-206-6497 (M-F 9:00 a.m. to 5:00 p.m. ET) or via email at natalie.cox@penserv.com.

Again, we take the privacy of your information very seriously and sincerely regret and apologize for any inconvenience or concern this may have caused. We are available to answer your questions and to help you find solutions to any problems that arise.

Sincerely,



Natalie Cox

Enclosures: How To Access Your Free Identity Protection Services
Steps You Can Take to Further Protect Your Information

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file a report with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Reports filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	TransUnion (800) 680-7289 www.transunion.com P.O. Box 2000 Chester, PA 19016

Fraud Alert

We recommend 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 accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each of credit reporting agencies listed above. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee to place, lift or remove the security freeze, which may vary by state. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Complaint Form with the FTC, there may be no charge to place the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

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 Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

Federal Trade Commission: You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at www.ftc.gov/bcp/edu/microsites/idtheft/.

For North Carolina residents: North Carolina residents may wish to review information provided by the North Carolina Attorney General, Consumer Protection Division at www.ncdoj.gov, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

For California residents: California residents may wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.

Reporting of identity theft and obtaining a policy report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Taxes

Some of the information affected by this incident could be used to file a fraudulent tax return. If you believe you are the victim of tax fraud or that somebody has filed or accessed your tax information, you should immediately contact the IRS or state tax agency as appropriate.

For Federal Taxes: The IRS requires that each individual report the problem to them. The IRS will not financially penalize you even if they paid a fraudulent refund. Accordingly, as an additional measure of precaution, we recommend you (and, if applicable, your spouse or domestic partner) complete IRS Form 14039 and then mail or fax that form to the IRS. A copy of that form can be obtained by going to https://www.irs.gov/pub/irs-pdf/f14039.pdf. You may also call the IRS at 800-908-4490 (Identity Theft Hotline) to learn whether you are a victim of this fraudulent scheme. For additional information from the IRS about identity theft, you may visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

For State Taxes: There may be similar resources and forms for each state, so we recommend that you contact your state department of revenue directly for more information. Additional information on how to contact your state department of revenue may be found by going to http://www.taxadmin.org/state-tax-agencies.

HOW TO ACCESS YOUR FREE IDENTITY PROTECTION SERVICES

As an added precaution and **if you choose to enroll**, we are offering you twelve (12) free months of credit monitoring and identity theft and litigation services which will help prevent and detect misuse of your personal information. To take advantage of this offer, please call our toll free number at 877-206-6497 to obtain your activation code. Once you receive your activation code, please follow the instructions below.

To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **July 31, 2017** (You will not be able to obtain a code after this date).
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/creditone
- Provide your **activation code**.
- Provide your **Engagement #** [redacted]

The Terms and Conditions for this offer are located at: www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

As an added benefit if you choose to enroll, Identity Restoration assistance is available to you. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.

- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.

- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions