14572

SEI Private Trust Company
1 Freedom Valley Drive
P.O. Box 1100
Oaks, PA 19456
T 610 676 1000
seic.com

14572

February 15, 2019

RE: NOTICE OF DATA BREACH

Dear _____:

SEI Private Trust Company (or, "SEI") acts as the custodian for your retirement account sponsored by Stanadyne LLC ("Stanadyne") under our agreement with Stanadyne. We are sending you this notice to explain a recent privacy breach resulting from a technical system issue we experienced with a web-based reporting tool we make available to our retirement plan customers.

What Happened:

This web-based reporting tool allows our customers, including Stanadyne, to generate reports containing participant-level information necessary to administer their retirement plans. As a result of a system update we made on September 22, 2018, in very limited circumstances, an authorized person of one plan sponsor could generate a report that included participant-level information for both that plan's participants and unrelated plans' participants.

What We Are Doing:

We disabled the reporting functionality on November 29, 2018 when we discovered the issue and conducted an internal review to ascertain the scope of the problem and take steps to prevent a reoccurrence. Based on this review, we have determined that eleven authorized individuals working with our retirement plan customers generated reports that included your personal information along with their plan participants' data. We have contacted each of our customers whose authorized system users may have run a report that inadvertently included your personal information. Each of these customers has certified to us in writing that personnel who generated or accessed these reports did not copy, distribute or otherwise misuse any data listed in the reports and have since destroyed all copies of them.

On January 29, 2019, Stanadyne received notice of the breach and worked with us to notify you of the breach.

What Information Was Involved:

The affected reports generally included names, Social Security numbers, plan account numbers, and distribution amounts.

What You Can Do:

While SEI takes all privacy-related incidents very seriously, we believe this incident presents a very low risk of harm to you. This was not the result of a malicious attack by external parties but was caused by an internal software coding issue that we have since addressed. The reporting functionality in question is password-protected and limited to use by individuals that routinely handle sensitive employee information.

Although we believe the incident presents a very low risk of harm, if you are interested in credit monitoring services, we are offering a complimentary two-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. If you would like to start monitoring your personal information, simply follow the steps below.

- URL to activate the membership is: https://www.experianidworks.com/3bcredit
- Your engagement number is: _____

- Activation Code:_____
- Toll-free number for enrollments/questions is: 877-890-9332
- Enrollment end date: 4/30/2019

We have also enclosed some general information about steps you can take to guard against identity theft and fraud.

For More Information:

We sincerely apologize for this issue and hope that this information will provide reassurance that SEI takes this matter seriously. If you have additional questions, please contact SEI Benefit Payment Services by email at Pay_Svcs@SEIC.com, by phone at 888-734-8922 or Richard Cosgrove from Stanadyne at 860-525-0821 ext. 2258.

Reference Guide

Monitor Account Statements. Remember to look at your account statements regularly to be sure they are correct.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open and bills you do not recognize. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

If you find items you don't understand on your report, call the relevant credit bureau at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission. If you detect any unauthorized transactions in your financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft (including information about fraud alerts and security freezes):

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For a summary of your rights under the federal Fair Credit Reporting Act, please visit: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Place a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus. [*The table below contains the contact information relevant to fraud alerts.*]

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Place a "Security Freeze" on Your Credit File (for Non-Massachusetts Residents). You also may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. There is no longer a fee for placing, lifting, and/or removing a security freeze. Unlike a fraud alert, you must place a security freeze on your credit file at each credit bureau individually. Since the instructions for establishing a security freeze differ from state to state, please contact the three national credit bureaus to find out more information. [*The table below contains the contact information relevant to security freezes.*]

Equifax	P.O. Box 105788 Atlanta, Georgia 30348	877-478-7625	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Attn: Security Freeze P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

The credit bureaus may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth

- Your complete address including proof of current address, such as current utility bill or telephone bill
- If you have moved in the past two (2) years, give your previous addresses where you have lived for the past two years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

Additional Information for Maryland Residents.

You can also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office:

Office of the Maryland Attorney General
Identity Theft Unit
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
1-888-743-0023
idtheft@oag.state.md.us
http://www.marylandattorneygeneral.gov

Additional Information for North Carolina Residents.

You can also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

Additional Information for Rhode Island Residents.

Under Rhode Island law, you have the right to file a police report regarding this incident and obtain a copy of it.

You can contact the Rhode Island Attorney General to learn more about how to protect yourself from becoming a victim of identity theft:

Office of the Rhode Island Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
consumers@riag.ri.gov
http://www.riag.ri.gov

Additional Information for Massachusetts Residents.

Under Massachusetts law, you have the right to obtain any police report filed 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.

Massachusetts law also allows consumers to 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 written authorization. However, please be aware 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. There is no longer a fee for placing, lifting, and/or removing a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348

Experian Security Freeze P.O. Box 9554 Allen, TX 75013

Trans Union Security Freeze Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19022-2000

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.)

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Please find below Stanadyne's responses to the below questions on the Massachusetts Office of Consumer Affairs and Business Regulation's Online Data Breach Notification Form.

Please give a detailed explanation of how the data breach occurred.*

On January 29, 2019, SEI Private Trust Company ("SEI"), the custodian of Stanadyne's retirement plan, notified Stanadyne that it had experienced a technical system issue first arising on September 22, 2018, due to a system update performed by SEI, which affected a web-based reporting tool available to SEI's retirement plan customers. This web-based reporting tool allows SEI's customers to generate reports containing participant-level information necessary to administer their retirement plans. SEI further informed Stanadyne that, as a result of this system update SEI made on September 22, 2018, authorized persons of retirement plan customers generated a certain type of report that included participant-level information for both that plan's participants and unrelated plans' participants.

Please note that no Stanadyne system or service, and no data maintained by Stanadyne, was involved in this security breach. SEI has a primary place of business at 1 Freedom Valley Drive, Oaks, Pennsylvania 19456, and Stanadyne considers Jim Winz, who may be contacted at (610) 676-3579 or JWinz@seic.com, to be its primary contact at SEI.

Based upon its investigation of the breach, SEI determined that the affected reports generally included names, Social Security numbers, plan account numbers, and distribution amounts.

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring.*

SEI informed Stanadyne that it discovered the issue on November 29, 2018 and promptly disabled the reporting functionality on that same day. Also upon discovery, SEI conducted an internal review to ascertain the scope of the problem and take steps to prevent a reoccurrence. Based on this review, SEI determined that eleven authorized individuals working with SEI's retirement plan customers had generated reports that included the personal information of unrelated plans' participants, along with their plan participants' data. SEI informed Stanadyne that it contacted each of its retirement plan customers whose authorized system users may have run a report that included the personal information of unrelated plans' participants and that SEI has received a written certification from each of these customers providing that the personnel who generated or accessed these reports did not copy, distribute or otherwise misuse any data listed in the reports and have since destroyed all copies of them.

Upon Stanadyne's request dated February 4, 2019, SEI has agreed to provide notice to all impacted individuals on Stanadyne's behalf. Also upon Stanadyne's request dated February 4, 2019, SEI has agreed to offer each such individual, at no cost, two (2) years of Experian's® ProtectMyID® Alert. Stanadyne is also notifying other state regulatory agencies as applicable.