



Lauren Godfrey, Partner
Cybersecurity & Data Privacy Team
322 North Shore Drive
Building 1B, Suite 200
lgodfrey@constangy.com
Direct: 412.870.4129
Mobile: 973.462.9521

February 14, 2025

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Tel: 401-576-6491
Email: Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents The Pension Specialists, Ltd. ("TPS"), a company headquartered in Machesney Park, Illinois, in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident.

1. What Happened

On February 24, 2024, TPS experienced a network disruption and immediately initiated an investigation of the matter. TPS engaged independent cybersecurity experts to assist with the process. TPS determined that certain files may have been accessed or acquired without authorization between February 18, 2024 and February 23, 2024. TPS then conducted a comprehensive review of all potentially affected information to identify any personal information that could have possibly been involved. On December 16, 2024, TPS determined that personal information may have been involved in the incident. Since that time, TPS has been working to gather contact information for individuals and prepare notification to all affected individuals of this incident. Please note that TPS has no evidence of the misuse, or attempted misuse, of any potentially impacted information.

2. Number of Maryland Residents Notified and Type of Information

On February 14, 2025, TPS began notifying 276 Maryland residents of this data security incident via U.S. First-Class Mail. The data sets affected by this incident included individuals' names, Social Security numbers, and driver's license numbers. A sample copy of the notification letter sent to potentially impacted individuals known at this time is included with this correspondence.

3. Steps Taken Relating to the Incident

TPS has implemented additional security measures to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, TPS has offered notified individuals 12 months of complimentary services through Kroll, which includes credit

February 14, 2025

Page 2

monitoring, Fraud Consultation and Identity Theft Restoration.

4. Contact Information

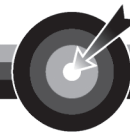
TPS remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please contact me.

Very truly yours,

Lauren D. Godfrey

Lauren Godfrey
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Subject: [Notice of Data Security Incident] / [Notice of Data Breach])>>

Dear <<first_name>> <<last_name>>:

We are writing to inform you of a data security incident that may have involved your personal information. If you are receiving this letter it is likely that you currently receive, or have received, retirement plan services from The Pension Specialists (“TPS”) through an employer, as TPS is a retirement plan administrator. TPS takes the privacy and security of all information within our possession very seriously. We are sending this correspondence to tell you what happened, what information was involved, what we have done, and what you can do to address this situation.

What Happened? On February 24, 2024, we experienced a network disruption and immediately initiated an investigation of the matter. We engaged independent cybersecurity experts to assist with the process. We determined that certain files may have been accessed or acquired without authorization between February 18, 2024 and February 20, 2024. We then conducted a comprehensive review of all potentially affected information to identify any personal information that could have possibly been involved. On December 16, 2024, we determined that your personal information may have been involved in the incident. Since that time, we have been working to gather contact information for individuals and prepare notification to all affected individuals of this incident. Please note that we have no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved? The information may have included your <<b2b_text_2(data elements)>>.

What We Are Doing. As soon as we discovered this incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. We are also offering you complimentary identity monitoring services through Kroll, a leader in consumer identity protection. Your identity monitoring services include <<Monitoring Term Length (Months)>> months of Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. The deadline to activate these services is <<b2b_text_6(activation deadline)>>.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also activate the complementary services offered to you through Kroll by following the instructions below.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call (866) 450-7766 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

A handwritten signature in black ink, appearing to read "Joel Radakovitz", with a large, stylized circular flourish at the beginning.

Joel Radakovitz, President & CEO
CPA®, QPA, CPC, MST, CFP®, ERPA, AIFA®
The Pension Specialists
10501 North 2nd Street
Machesney Park, IL 61115-1455

Steps You Can Take to Help Protect Your Personal 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 (the “FTC”).

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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 one year. 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: You have the right to put a security freeze on your credit file for up to one year at no cost. 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 credit reporting agency. 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
ag.ny.gov
800-771-7755

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.