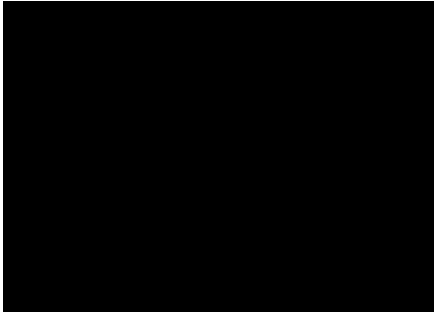


Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336



Dear [REDACTED]:



We are writing with important information regarding a recent data security incident at Phase II Systems d/b/a Public Agency Retirement Services (“PARS”). PARS designs, implements and administers retirement products designed for the unique needs of public agencies, including your current or former employer. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

As a result of a phishing incident, an unauthorized party obtained access to a PARS employee’s email account.

What We Are Doing.

Upon learning of the issue, we secured the account and commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an extensive forensic investigation and manual email review, we determined on November 28, 2021, that the impacted email account, which was accessed between March 31, 2021 and May 24, 2021, contained some of your personal information. We have no evidence that your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

The email account that was accessed contained some of your personal information, specifically your full name and:  
[REDACTED].

What You Can Do.

To protect you from potential misuse of your information, we are offering you a one-year membership in myTrueIdentity provided by TransUnion Interactive, a subsidiary of TransUnion. For more information on identity theft prevention and myTrueIdentity, including instructions on how to activate your one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

*For More Information.*

We regret any inconvenience that this may cause you. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to secure personal information.

**If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED].** This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, excluding U.S. holidays.

Sincerely,

Phase II Systems d/b/a Public Agency Retirement Services

– OTHER IMPORTANT INFORMATION –

**1. Enrolling in Complimentary 12-Month Credit Monitoring.**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at [REDACTED] and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code [REDACTED] and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at [REDACTED]. When prompted, enter the following 6-digit telephone pass code [REDACTED] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain 12 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *myTrueIdentity* online Credit Monitoring service anytime between now and [REDACTED]. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: [REDACTED], Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

**2. Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial one-year “Fraud Alert” on your credit files, *at no charge*. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

**Equifax**  
P.O. Box 105069  
Atlanta, GA 30348  
[www.equifax.com](http://www.equifax.com)  
1-800-525-6285

**Experian**  
P.O. Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742

**TransUnion LLC**  
P.O. Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
1-800-680-7289

### **3. Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

#### **Equifax Security Freeze**

P.O. Box 105788

Atlanta, GA 30348

<https://www.freeze.equifax.com>

1-800-349-9960

#### **Experian Security Freeze**

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

1-888-397-3742

#### **TransUnion Security Freeze**

P.O. Box 2000

Chester, PA 19016

<http://www.transunion.com/securityfreeze>

1-888-909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. 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 your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

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.

### **4. Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

### **5. Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them 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 on the web at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your payment card information and/or financial account information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

**6. Protecting Your Medical Diagnosis/Treatment and/or Health Insurance Information.**

If this notice letter states that your medical diagnosis/treatment information and/or health insurance information was impacted, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.