

BakerHostetler

Baker&Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Sara M. Goldstein
direct dial: 215.564.1572
sgoldstein@bakerlaw.com

August 4, 2021

VIA EMAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Formella:

We are writing on behalf of our client, IAM National Pension Fund (“The Fund”), to notify you of a security incident.

The Fund determined that a phishing attack targeting one of its employees may have resulted in unauthorized access to some participant information. The Fund investigated after phishing emails were sent from an employee’s email account without their knowledge. Upon learning of this, The Fund immediately reset the password to the employee’s email account and launched an investigation. Through its investigation, The Fund determined that there was unauthorized access to the employee’s email account between the dates of September 28, 2020 and October 15, 2020. As part of its investigation, The Fund conducted a comprehensive review of the emails and attachments in the employee’s email account to determine whether they contained any information pertaining to The Fund participants. The investigation determined that some participant information was contained in emails or attachments in the email account, including participant names and Social Security numbers.

Beginning on August 4, 2021, The Fund will mail a notification letter via United States Postal Service First-Class mail to one New Hampshire resident in accordance with N.H. Rev. Stat. Ann. § 359-C:20. A copy of the notification letter is enclosed.¹ To help monitor for any potential misuse of personal information, The Fund is offering a complimentary one-year membership in

¹ This report is not, and does not constitute, a waiver of The Fund’s objection that New Hampshire lacks personal jurisdiction over The Fund regarding any claims related to the data security incident.

Attorney General John Formella

August 4, 2021

Page 2

credit monitoring and identity theft protection services through Experian to the resident involved in this incident. The Fund also established a dedicated toll-free incident response line to answer questions that members may have.

To help prevent something like this from happening again, The Fund has provided training to its employees regarding phishing emails and other cybersecurity issues.

Should you have any questions, please do not hesitate to contact me.

Sincerely,

A handwritten signature in cursive script that reads "Sara Goldstein". The signature is written in black ink and is positioned below the word "Sincerely,".

Sara M. Goldstein

Partner

Enclosure

IAM National Pension Fund
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



D-1

August 4, 2021

Dear [REDACTED]:

IAM National Pension Fund (“The Fund”) is committed to protecting the security and confidentiality of all the information we maintain. We are writing to inform you about a data security incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On February 9, 2021, we determined that a phishing attack that targeted one of The Fund’s employees may have resulted in unauthorized access to some participant information. The Fund investigated after phishing emails were sent from an employee’s email account without their knowledge. Upon learning of this, we immediately reset the password to the employee’s email account and launched an investigation.

Through our investigation, we determined there was unauthorized access to the employee’s email account between September 28, 2020 and October 15, 2020. Our investigation also indicated that the likely purpose of the unauthorized access to the employee’s email account was to send additional phishing emails, not to view or use any information in the account. However, we could not rule out the possibility that emails and attachments in the account may have been viewed or accessed during the incident.

Accordingly, as part of our investigation, we conducted a comprehensive review of the emails and attachments in the employee’s email account to determine whether they contained any information pertaining to The Fund’s participants. Our investigation determined that some of your information was contained in emails or attachments in the email account, including your name and Social Security number.

To date, we are unaware of any misuse of the information maintained in the employee’s email account. However, out of an abundance of caution, we wanted to let you know this happened and assure you we take this very seriously. We recommend you remain vigilant to the possibility of fraud by reviewing your financial account and payment card statements for any suspicious activity. Immediately report any suspicious activity to your financial institution. As a precaution, we have secured the services of Experian® to offer you a complimentary one-year membership of Experian’s IdentityWorksSM. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect yourself, please see the pages that follow this letter.**

We regret any inconvenience or concern this may cause you. To help prevent a similar incident from occurring in the future, we have provided training to our employees regarding phishing emails and other cybersecurity issues. If you have any questions, please call **1-888-527-9342** Monday through Friday, **8:00 a.m. to 5:00 p.m.**, Eastern Time.

Sincerely,

Raymond Goad

Raymond Goad
General Counsel

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **October 10, 2021** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: **XXXXXXX**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-288-8057**. Be prepared to provide engagement number **XXXXXX** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- A. Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- B. Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- C. Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- D. \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.

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. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **877-288-8057**.

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. Please refer to the actual policies for terms, conditions, and exclusions of coverage.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit. *How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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 bureau will provide you with 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. *How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.