

RECEIVED

SEP 13 2018

CONSUMER PROTECTION

James J. Giszczak
Direct Dial: 248.220.1354
jgiszczak@mcdonaldhopkins.com

September 10, 2018

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Carpenters Benefit Funds of Philadelphia – Incident Notification

Dear Attorney General Delaney:

McDonald Hopkins PLC represents Carpenters Benefit Funds of Philadelphia (“Carpenters Benefit Funds”). I write to provide notification concerning an incident that may affect the security of personal information of two (2) New Hampshire residents. Carpenters Benefit Funds’ investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, Carpenters Benefit Funds does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Carpenters Benefit Funds learned of a potential issue involving a phishing scheme, which may have affected a limited number of employees’ email boxes. Upon learning of the issue, Carpenters Benefit Funds commenced a prompt and thorough investigation and took steps to mitigate any risk to its clients’ personal information. As part of its investigation, Carpenters Benefit Funds worked very closely with external cybersecurity professionals experienced in handling these types of incidents. The forensic investigation concluded that there was unauthorized access to two Carpenters Benefit Funds’ employees email boxes between April 23, 2018 and May 3, 2018.

An extensive manual document review, which concluded on July 18, 2018, confirmed that the incident may have affected the security of personal information of New Hampshire residents. The information that was potentially available included the impacted residents’ full names and Social Security numbers, and may have also included health insurance information.

While Carpenters Benefit Funds was not able to determine what, if any, personal information was accessed, out of an abundance of caution, Carpenters Benefit Funds wanted to make you (and the affected residents) aware of the incident and explain the steps it will be taking to help safeguard the residents against identity fraud. Carpenters Benefit Funds will provide the New Hampshire residents with written notice of this incident commencing on approximately

Attorney General Michael A. Delaney
Office of the Attorney General
September 10, 2018
Page 2

August 31, 2018, in substantially the same form as the letter attached hereto. Carpenters Benefit Funds will offer the impacted New Hampshire residents with a complimentary membership with a credit monitoring and identity theft protection service. Individuals with questions or concerns can contact a dedicated telephone number in the notice letter. Carpenters Benefit Funds will advise the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. Individuals whose health insurance information was impacted will be advised of steps they can take to protect their personal health information. Carpenters Benefit Funds will also advise the impacted residents about the process for placing a fraud alert and/or security freeze on their credit files, obtaining a free credit report and provide the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Carpenters Benefit Funds, protecting the privacy and security of personal information is a top priority. Carpenters Benefit Funds continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,



James J. Giszczak



CARPENTERS BENEFIT FUNDS
OF PHILADELPHIA
— WORK BENEFIT — ALL

[REDACTED]

**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

[REDACTED]

[REDACTED]

[REDACTED]:

I am writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Carpenters Benefit Funds of Philadelphia (“Carpenters”). As such, 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?

We learned that a limited number of Carpenters’ employees may have been the victims of an email phishing attack resulting in unauthorized access to the employees’ email boxes between April 23, 2018 and May 3, 2018.

What We Are Doing.

Upon learning of the issue, we 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 discovered on July 17, 2018 that the impacted email accounts that were accessed contained some of your personal and/or protected health information. We have no evidence that any of the 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 impacted email accounts that were accessed contained some of your personal and/or protected health information, including your full name and Social Security number, and may have included your health insurance information.

What You Can Do.

To protect you from potential misuse of your information, 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 identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

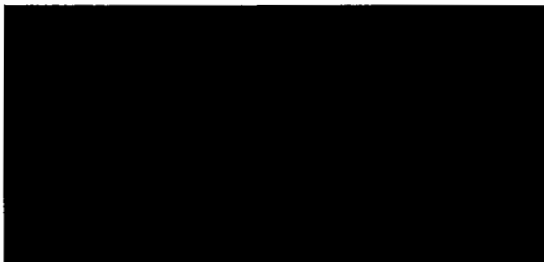
This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent it is helpful, we are also offering steps you can take to protect your health information on the following pages.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We have made extensive changes to our policies and we will continue to evaluate and modify our practices and internal controls to enhance the security and privacy of your 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 a.m. to 9 p.m. Eastern time.

Sincerely,



– OTHER IMPORTANT INFORMATION –

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

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: [REDACTED] (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**: [REDACTED]

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 [REDACTED] 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:

- **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, Equifax and Transunion files for indicators of 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.

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.

** 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.

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 90-day “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
1-800-525-6285

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC

P.O. Box 2000
Chester, PA 19016
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. 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

PO Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-349-9960

Experian Security Freeze

PO 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 monitoring 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.

Please note that there may be a charge associated with placing, temporarily lifting, or removing a security freeze with each of the above credit reporting companies. These fees vary by state, so please call or visit the credit reporting agencies’ websites to find out the specific costs applicable to the State in which you currently reside.

If you decide to place a Security Freeze on your credit file, *in order to do so without paying a fee*, you will need to send a copy of a valid identity theft report or police report, by mail, to each credit reporting company to show that you are a victim of identity theft and are eligible for free security freeze services. 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. After you sign up for the credit monitoring service, you may refreeze your credit file. We encourage you to wait to place a security freeze on your credit file until you have enrolled in the credit monitoring service to avoid paying additional fees related to placing an initial security freeze on your credit file, temporarily lifting or removing the security freeze and subsequently refreezing 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, 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.

6. Protecting Your Health Information.

We have no information to date indicating that your Protected Health Information (PHI) involved in this incident was or will be used for any unintended purposes. As a general matter, however, 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.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.