



Baker & Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Joseph L. Bruemmer
direct dial: 513.929.3410
jbruemmer@bakerlaw.com

July 18, 2024

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Carnegie Institute of Washington (“Carnegie Science”), to provide notice to your office concerning a security incident involving three Maryland residents. Carnegie Science is located at 5241 Broad Branch Road, Washington, D.C. 20015.

Carnegie Science recently completed an investigation into a data security incident that involved unauthorized activity on certain devices in its network. Upon identifying the activity, Carnegie Science immediately implemented its incident response protocols, took measures to contain the activity, and launched an investigation. A third-party cybersecurity firm that has assisted other companies with similar situations also was engaged.

The evidence showed that an unauthorized actor accessed certain devices in Carnegie Science’s network. Between April 9, 2024 and April 11, 2024, the unauthorized actor may have attempted to collect usernames and passwords for online accounts that were stored in the internet browsers of the Carnegie Science workstations that the unauthorized actor accessed, including the workstations of three Maryland residents.

While the investigation was ongoing, Carnegie informed the Maryland residents of the unauthorized activity and recommended that they change the passwords for any online accounts they accessed from their Carnegie workstations. Carnegie also offered the residents a complimentary, one-year membership to credit monitoring and identity theft protection services. On July 17, 2024, Carnegie mailed a notification letter via First Class mail to the involved Maryland residents in accordance with Md. Code Ann., Com. Law. § 14-3504. A sample copy of the notification letter is enclosed. The letter explains what happened, what Carnegie has done in

July 18, 2024

Page 2

response, and what the residents can do. It also provides points of contact at Carnegie Science that the residents can call or email with questions.

To help prevent something like this from happening again, Carnegie Science has taken steps to enhance its existing security measures.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in blue ink, appearing to read "Joseph L. Bruemmer", with a large, stylized initial "J" and a long horizontal flourish extending to the right.

Joseph L. Bruemmer
Partner

Attachment



July 17, 2024

NAME
Address
CSZ

Dear FN,

Carnegie Science understands the importance of protecting information. We are writing to inform you that we have completed our investigation of the incident we previously brought to your attention and have determined that it may have involved some of your information. This notice explains what happened, what we have done in response, and what you can do.

What Happened?

We previously informed you that we identified and were addressing a data security incident that involved unauthorized activity on certain devices in our network. Upon identifying the activity, we immediately implemented our incident response protocols, took measures to contain the activity, and launched an investigation. A third-party cybersecurity firm that has assisted other companies with similar situations also was engaged.

The forensic investigation is now complete. The evidence showed that an unauthorized actor accessed certain devices in Carnegie Science's network. Between April 9, 2024 and April 11, 2024, the unauthorized actor may have attempted to collect usernames and passwords for online accounts that were stored in the internet browsers of the Carnegie Science workstations that the unauthorized actor accessed, including your workstation.

What Information Was Involved?

The evidence did not show whether the unauthorized actor accessed information on your Carnegie Science workstation. If you saved usernames and passwords for online accounts in the internet web browser on your Carnegie Science workstation, however, it is possible the unauthorized actor may have accessed those usernames and passwords.

What We Are Doing.

We wanted to notify you of this incident and to assure you that we take it seriously. To help prevent something like this from happening again, we have taken steps to enhance our existing security measures.

What You Can Do.

As we previously advised, if you used your Carnegie Science device to log into any online accounts, including any personal online accounts, you should change the account passwords for those accounts and all other online accounts that use the same username and password. Additionally, we previously arranged for you to receive one year of complimentary credit monitoring. You can still enroll in that service if you have not yet done so. The instructions for enrolling in the complimentary credit monitoring service were included in an email we previously sent to you. For additional information concerning steps you can take in response, please review the pages that follow this letter.

For More Information.

We regret that this occurred and apologize for any inconvenience. If you have additional questions, you may contact Anthony DiGiorgio, Director of Information Technology & Security, at adigiorgio@carnegiescience.edu or 202-352-4311, or the Carnegie Science Office of General Counsel at ogc@carnegiescience.edu.

Sincerely,

Carnegie Science

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, 1-800-378-4329
- *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.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

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 is because most creditors need to see your credit report before they approve a new account. If they cannot 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:

- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com
- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com

You will 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.

Carnegie Institute of Washington is located at 5241 Broad Branch Road, Washington, D.C. 20015 and can be reached at 1-202-387-6400.

Additional information for residents of the following jurisdiction:

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, <https://www.marylandattorneygeneral.gov/>