

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: 1.410.456.2741
Cell: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

February 6, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

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

Re: CohnReznick LLP –Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents CohnReznick LLP (“CohnReznick”) regarding a recent security incident. I am writing to provide notification of an incident at CohnReznick that may affect the personal information of two (2) Maryland residents. CohnReznick’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, CohnReznick does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about December 4, 2023, CohnReznick began detecting unusual network activity in its environment, and thereafter identified the “Play” ransomware variant on some of their systems. CohnReznick took immediate steps to secure its environment and engaged third party cybersecurity professionals to assist in a thorough investigation into the incident. CohnReznick reported the incident to law enforcement and appropriate regulatory bodies. CohnReznick is working diligently to gain a complete understanding of the incident and what data may have been impacted. However, CohnReznick discovered on January 8, 2024 that certain additional files may have been accessed or potentially removed from the network by an unauthorized party. CohnReznick determined that two (2) Maryland residents were potentially impacted. The information potentially impacted includes: name, financial account number, financial account routing number, and passport number. Not all information was impacted for each individual. CohnReznick provided written notice on February 6, 2024, to the two Maryland residents identified.

As stated above, upon learning of this issue, CohnReznick immediately commenced an internal investigation and promptly notified potentially affected individuals. CohnReznick has no indication that the information has been used to commit financial fraud or identity theft. CohnReznick wanted to inform you (and the affected residents) of the incident and to provide information to best protect the individuals’ personal information. CohnReznick advised the affected residents regarding precautionary measures to best protect their identity and financial accounts including: remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis; the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports; and contact information for the consumer reporting agencies and the Federal Trade Commission. The affected residents are also being

February 6, 2024

Page 2

provided with the contact information for the Maryland Attorney General. A sample of the notice letter is included herein for your reference.

At CohnReznick, protecting the privacy of personal information is a top priority. CohnReznick continues to evaluate and improve, where appropriate, its administrative and technical safeguards and tools to protect its network environment. If you have any additional questions, please contact me at (410) 456-2741 or spollock@mcdonaldhopkins.com.

Very truly yours,



Spencer S. Pollock

Encl.



**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

February 6, 2024

Dear [REDACTED]

The privacy and security of the personal information entrusted to us is of the utmost importance to CohnReznick LLP ("CohnReznick"). We are writing with important information regarding a recent security incident that impacted some of your information. Please read this notice carefully, as it provides information about the incident and the significant measures we take to protect your information.

What Happened?

On or about December 4, 2023, CohnReznick detected unusual activity on our network and we immediately took steps as detailed below.

What We Are Doing.

Upon learning of this issue, we immediately took steps to secure our network and mitigate against any additional harm. We also reported the incident to law enforcement and promptly commenced an investigation assisted by external cybersecurity professionals experienced in handling these types of incidents. Our efforts revealed on January 8, 2024 that certain files that contain personal information were accessed or potentially removed from our network by the unauthorized party. While cybersecurity threats continue to impact all of us, we are taking ever-increasing measures to protect the information entrusted to us. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of information entrusted to us. In response to this incident and through our continuing comprehensive review, we implemented additional security methodologies to further strengthen our network.

What Information Was Involved?

The information impacted contained some of your personal information, including your [REDACTED]

What You Can Do.

We have no evidence that any of your information has been used to commit financial fraud or identity theft as a result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. Please see the Other Important Information page which provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and 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.

If you have any further questions regarding this incident, please contact [REDACTED] at [REDACTED]. We apologize for any inconvenience or concern this may cause. We have taken this matter very seriously and will continue to take significant measures to protect the confidential and personal information in our possession.

Sincerely,
CohnReznick LLP
14 Sylvan Way 3rd Floor, Parsippany, NJ 07054

– OTHER IMPORTANT INFORMATION –

1. **Placing a Fraud Alert.**

We recommend that you place a 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 30348-5069
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(888) 378-4329

Experian

P.O. Box 9554
Allen, TX 75013
www.experian.com/fraud/center.html
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
www.transunion.com/fraud-alerts
(800) 680-7289

2. **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 cost. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/center.html
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
(888) 916-8800

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. 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 you do place a security freeze prior to enrolling in a credit monitoring service, 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.

3. **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.

4. **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.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General’s Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General’s Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.