

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

December 4, 2023

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: Troutman Pepper Hamilton Sanders LLP – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents Troutman Pepper Hamilton Sanders LLP (“Troutman Pepper”), located at 600 Peachtree Street N.E. Suite 3000, Atlanta, Georgia 30308. I am writing to provide notification of an incident at Troutman Pepper that may affect the security of personal information of approximately two hundred and twenty-six (226) Maryland residents. Troutman Pepper’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, Troutman Pepper does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about February 8, 2023, Troutman Pepper detected unauthorized access to its network as a result of a ransomware cybersecurity incident. Upon learning of the issue, Troutman Pepper immediately took steps to secure its network and mitigate against any additional harm, as well as reported the incident to the Federal Bureau of Investigation. Troutman Pepper promptly launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine whether any sensitive data had been compromised as a result of the incident. The investigatory team learned on March 22, 2023, that the unauthorized individual(s) removed certain files and folders from limited portions of the network on or about February 8, 2023. On November 15, 2023, following an extensive review and analysis of the data at issue, Troutman Pepper determined that certain files and folders that may have been accessed or acquired contained identifiable personal and/or protected health information pertaining to certain individuals. Information potentially impacted for residents includes Social Security number, financial account number, routing number, driver’s license or state identification, medical information, and/or health insurance information. Not all information was impacted for all individuals. On December 1, 2023, Troutman Pepper located the most recent address of the impacted individuals and promptly proceeded to supply notice to the potentially impacted individuals as expeditiously as possible, to be effectuated on or about

December 4, 2023

Page 2

December 4, 2023. Troutman Pepper also provided notice of the incident to the major credit reporting agencies including Experian, Equifax, and TransUnion.

As stated above, upon learning of this issue, Troutman Pepper immediately commenced an internal investigation and promptly notified potentially affected individuals. Troutman Pepper has no indication that the information has been used to commit financial fraud or identity theft. Troutman Pepper wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Troutman Pepper is offering the residents whose Social Security number was potentially impacted with complimentary memberships with a credit monitoring service. Troutman Pepper is advising the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity. Troutman Pepper also is advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies, and the Federal Trade Commission. A sample of the notice letter is included herein for your reference.

Troutman Pepper is committed to maintaining the privacy of personal information and is taking ever-increasing measures to safeguard the information entrusted to Troutman Pepper. In response to this incident, Troutman Pepper has strengthened the network and made additional security improvements recommended by third-party cyber security experts. These include resetting account passwords, strengthening password security policies and endpoint detection software, integrating a 24/7 third-party security monitoring service, enhancing records management practices, and implementing additional training related to network security and threat detection. Troutman Pepper 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) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Thank you for your cooperation.

Sincerely,



Dominic A. Paluzzi

Encl.

December 4, 2023

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear 

The privacy and security of the personal information we maintain is of the utmost importance to Troutman Pepper. We are writing regarding a cybersecurity incident that involved your personal information. Please read this notice carefully, as it provides information about the incident, the complimentary identity monitoring services we are making available to you, and the significant measures we take to protect your information.

What Happened

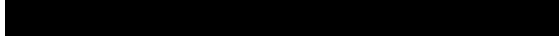
On or about February 8, 2023, Troutman Pepper detected unauthorized access to our network as a result of a cybersecurity incident (ransomware attack) that resulted in the exposure of the data we maintain.

What We Are Doing

Upon learning of the incident, we immediately took steps to secure our network and mitigate against any additional harm. We also reported the incident to law enforcement. We promptly launched an investigation assisted by outside cybersecurity experts to determine whether any sensitive data had been compromised as a result of the incident. Our investigatory team learned in late March that the unauthorized individual(s) removed certain files from a limited portion of our network on or about February 8, 2023. After several months of extensive efforts to obtain, review, and analyze the impacted data, on November 15, 2023, we determined that the impacted files contained identifiable personal and/or protected health information pertaining to certain individuals.

While cybersecurity threats continue to impact all of us, Troutman Pepper is taking ever-increasing measures to protect the data entrusted to us. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. In response to this incident and through our continuing comprehensive review, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts.

What Information Was Involved

The impacted files contained some of your personal information including your 


What You Can Do

To date, we are not aware of any reports of identity fraud or improper use of your personal information as a result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and provide resources you can use to protect yourself from the possibility of identity theft. We are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes

place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

This letter also provides other 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 remain vigilant and regularly monitor your financial account statements and credit reports for fraudulent or irregular activity that you did not initiate or authorize.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information

If you have questions, please contact our dedicated and confidential call center at [REDACTED] (toll free). The response line is available for 90 days from the date of this letter, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

We apologize for any inconvenience or concern this may cause. Troutman Pepper is committed to maintaining the confidentiality and privacy of personal information in our possession and will continue to take precautions to safeguard it.

Sincerely,
Troutman Pepper Hamilton Sanders LLP

600 Peachtree Street, N.E. Suite 3000
Atlanta, Georgia 30308

- 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. **Protecting Your Medical Information.**

If this notice letter indicates that your medical information was impacted, we have no information to date indicating that your medical information 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.

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.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

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.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit. In addition, you have the right to obtain a security freeze (as explained above) or submit a declaration of removal. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act. For more information about the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

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.

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, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392.

Rhode Island Residents: You have the right to obtain a police report if one was filed, or alternatively, you can file a police report. Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above. In order to request a security freeze, you may need to provide the following information: your full name (including middle initial as well as Jr., Sr., II, III, etc.); Social Security number; date of birth; complete address; prior addresses; proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.); and if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. When you place a security freeze on your credit report, within five (5) business days you will be provided with a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following: (1) the unique personal identification number or password provided by the consumer reporting agency; (2) proper identification to verify your identity; and (3) the proper information regarding the period of time for which the report shall be available to users of the credit report. There were 4 of Rhode Island residents impacted.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

December 20, 2023

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: Troutman Pepper Hamilton Sanders LLP – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents Troutman Pepper Hamilton Sanders LLP (“Troutman Pepper”), located at 600 Peachtree Street N.E. Suite 3000, Atlanta, Georgia 30308. I am writing to provide supplemental information to the previously provided incident notification submitted on December 4, 2023, regarding an incident at Troutman Pepper that may affect the security of personal information of approximately four (4) additional Maryland residents. Troutman Pepper is reporting on behalf of certain of the law firm’s clients. Troutman Pepper’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, Troutman Pepper does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

In addition to the information previously provided, on or about November 30, 2023, Troutman Pepper provided notice to appropriate data owners. Following notice thereafter, Troutman Pepper either received confirmation from the data owner for Troutman Pepper to provide notice on its behalf, or determined that the data owner entity is no longer in operation. Despite not maintaining ownership of the data, Troutman Pepper will proceed to notify the individuals directly to ensure notice is provided. Troutman Pepper confirmed the individuals’ most up to date address information on or about December 16, 2023. Troutman Pepper wanted to inform you (and the affected individuals) of the incident and to explain the steps that it is taking to help safeguard the affected individuals against identity fraud. Troutman Pepper is providing the affected individuals with written notification of this incident on or about December 20, 2023, in substantially similar form as the letter previously submitted. Troutman Pepper is offering the residents with complimentary membership with a credit monitoring service. Troutman Pepper will advise the affected individuals to always 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. The affected individuals are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,



Dominic A. Paluzzi