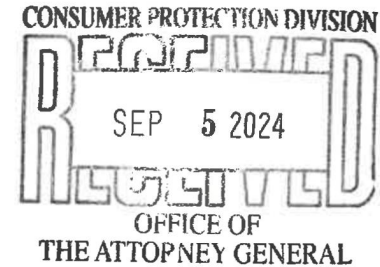


Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: 1.410.456.2741
Cell: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

August 29, 2024

VIA U.S. MAIL and Email (Idtheft@oag.state.md.us)

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



Re: Weinberg, Wheeler, Hudgins, Gunn & Dial, LLC – Incident Notification

To Whom it May Concern:

McDonald Hopkins PLC represents Weinberg, Wheeler, Hudgins, Gunn & Dial, LLC (“Weinberg”). I am writing to provide notification of an incident at Weinberg that may affect the security of personal information of approximately forty nine (49) Maryland residents. By providing this notice, Weinberg does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Weinberg recently became aware of unauthorized access to its network environment. Upon learning of the issue, Weinberg launched an investigation, contained and secured the network, eradicated the threat and alerted law enforcement. As part of the investigation, Weinberg has been working very closely with third-party cybersecurity professionals experienced in handling these types of incidents. The investigation aimed to determine the nature and scope of the incident and whether any sensitive data, including personal and/or health information, was accessed and/or acquired by the unauthorized party. After a thorough and detailed forensic investigation, Weinberg discovered on May 30, 2024 that the unauthorized actor accessed the network and removed certain files containing personal information from its network environment. On July 2, 2024, Weinberg began notifying the entities Weinberg received personal information from regarding the incident and offered to notify impacted individuals and regulators on these entities’ behalf. The information included residents’ full names and Social Security numbers.

To date, Weinberg is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Weinberg 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. Weinberg is providing the newly identified affected residents with written notification of this incident commencing on or about August 29, 2024 in substantially the same form as the letter attached hereto. Weinberg is advising the affected residents about the process for placing fraud alerts and/or security freezes 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.

At Weinberg, protecting the privacy of personal information is a top priority. Weinberg is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Weinberg 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 (410) 456-2741 or spollock@mcdonaldhopkins.com. Thank you for your cooperation.

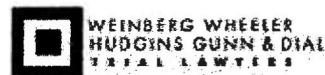
Sincerely,

A handwritten signature in black ink, appearing to read 'Spencer Pollock', with a stylized, cursive script.

Spencer Pollock

Encl.

Wheeler, Hudgins, Gunn & Dial, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED] :

Weinberg Wheeler Hudgins Gunn & Dial ("Weinberg") writes to inform you of a potential data security incident that may involve some of your individual personal information. Weinberg is a full service law firm operating throughout the United States. We provide legal services to a variety of businesses and received information about you from one of these businesses to facilitate legal services. 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 personal information.

What Happened?

Weinberg became aware of a cybersecurity incident that involved unauthorized access to certain systems within our network.

What We Are Doing.

Upon detecting the incident, we commenced an immediate and thorough investigation, contained and secured the network, eradicated the threat, and alerted law enforcement. As part of the investigation, we engaged external cybersecurity professionals to identify the extent of the incident and determine what, if any, sensitive data, including personal information may have been accessed and/or acquired by the unauthorized party.

After a thorough forensic investigation and comprehensive manual review of all data stored within the impacted systems, we determined the data involved contains some of your personal information and may have been accessed or acquired by an unauthorized party on September 11, 2023. On July 3, 2024, we notified the entity Weinberg received your information from and worked with them to notify you of this incident.

What Information Was Involved?

The information potentially involved includes your [REDACTED]

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 direct result of this incident. Nevertheless, out of an abundance of caution, we are providing you with access to **Single Bureau Credit Monitoring** services at no charge. These services provide you with alerts for [REDACTED] 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. In addition, 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, a TransUnion company specializing in fraud assistance and remediation services. **Please see enrollment instructions on the next page.**

000010103G0500

P

This letter also 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. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information in the "Other Important Information" section.

For More Information.

Weinberg values your privacy and deeply regrets 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 continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. Since detecting the incident, we have reviewed and revised our information security practices, and implemented additional security measures to mitigate the chance of a similar event in the future.

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, 8am - 8pm. Eastern Time, excluding holidays.

Sincerely,

Weinberg Wheeler Hudgins Gunn & Dial

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary Credit Monitoring.

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.



2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 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.

00001020380000

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

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

TransUnion

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

P

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, at no charge. 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

P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
1-800-349-9960

Experian

Security Freeze
P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
1-888-909-8872

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. 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 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 service. After you sign up for the credit monitoring service, you may refreeze 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. Protecting Your Medical Information.

The following practices can provide additional safeguards to protect against 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.

6. 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.

Connecticut Residents: You may contact and obtain information from your attorney general at:

Connecticut Attorney General’s Office, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

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, <https://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; <https://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.

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, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.



00001030300000

P