

Nicholas A. Kurk
Direct Dial: 312-642-6738
E-mail: nkurk@mcdonaldhopkins.com

December 19, 2023

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

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

Re: Broening, Oberg, Woods & Wilson, PC – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Broening, Oberg, Woods & Wilson, PC (“Broening Oberg”). I am writing to provide notification of an incident at Broening Oberg that may affect the security of personal information of Maryland residents. By providing this notice, Broening Oberg does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

In April 2023, Broening Oberg became aware of suspicious activity involving an employee email account. Upon identifying the activity, Broening Oberg acted quickly to contain the threat, investigate, and ensure the security of its systems with the assistance of third-party forensic specialists. The investigation revealed that an unauthorized actor gained access to one Broening Oberg employee’s email account between March 29, 2023 to May 23, 2023. On December 1, 2023, after an extensive forensic investigation and review, Broening Oberg discovered that certain personal information of two (2) Maryland residents was included within the mailbox data that was subject to unauthorized access or acquisition as a result of the incident. Further, on December 12, 2023, Broening Oberg located the most recent contact information for these individuals.

The personal information contained within the impacted data included first and last name and Social Security number.

Broening Oberg has no evidence of financial fraud or identity theft related to this data. Nevertheless, out of an abundance of caution, Broening Oberg 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. Broening Oberg is providing the affected residents with notification of this incident, commencing on or about December 20, 2023. The notice will be in substantially the same form as the letter attached hereto. Broening Oberg is also offering the affected residents whose Social Security number was potentially impacted by the incident with complimentary one-year membership with a credit monitoring service. Broening Oberg is advising

the affected residents to always remain vigilant in reviewing financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis. Broening Oberg is also 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. Additionally, the affected residents are being provided with the contact information for the Maryland Attorney General's Office, consumer reporting agencies and the Federal Trade Commission.

At Broening Oberg, protecting the privacy of personal information is a top priority. Broening Oberg is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Broening Oberg continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (312) 642-6738 or nkurk@mcdonaldhopkins.com.

Very truly yours,



Nicholas A. Kurk

Encl.



BROENING OBERG
WOODS + WILSON

Enrollment Code: [REDACTED]

To Enroll, Scan the QR Code Below:



Or Visit:



Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to Broening Oberg Woods & Wilson PC. ("Broening Oberg"). We're writing with important information regarding a recent data security incident that involved some of your information. We want to provide you with information about the incident, let you know about the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently learned that an unauthorized individual obtained access to one Broening Oberg employee email account.

What We Are Doing.

Upon learning of this issue, we immediately began efforts to remediate the incident and commenced a prompt and thorough investigation. As part of our investigation, we have been working closely with external cyber security professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on December 1, 2023, that the impacted email account that was accessed between March 29, 2023 to May 23, 2023 contained some of your personal information. None of our firm's systems or servers were impacted by this incident beyond the one email account.

We currently have no evidence indicating that any personal information has been used for identity theft or financial fraud as a result of the incident, however, out of an abundance of caution, we wanted to notify you of the incident and provide you with information on steps you can take to help protect your information.

What Information Was Involved.

The impacted email account contained some of your personal information, specifically your name, [REDACTED]

What You Can Do.

While we have no evidence of financial fraud or identity theft related to this data, we want to make you aware of the incident. To protect you and your information, we are providing you with [REDACTED] months of free credit monitoring and identity theft protection services through IDX, A Zero Fox Company. This service helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This service is completely free to you and enrolling in this program will not hurt your credit score. For more information, contact IDX with any questions and to enroll in free identity protection services go to [REDACTED], or scan the QR image and use the Enrollment Code provided above. Please note the deadline to enroll is March 15, 2024.

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 have also provided information on protecting your medical information on the following pages.

For More Information.

Please accept our apologies that this incident occurred. We remain fully 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 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, 9am to 9pm Eastern.

Sincerely,

Broening Oberg Woods & Wilson PC
2800 N Central Ave, Suite 1600
Phoenix, AZ 85004
[REDACTED]

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary Credit Monitoring.**

Website and Enrollment. Scan the QR image or go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at [REDACTED] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. **Placing a Fraud Alert on Your Credit File.**

We recommend that you place an initial one (1) 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
<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

3. **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 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888) 298-0045

Experian Security Freeze

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

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(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 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.

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.

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.

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.

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.

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.

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.