

May 26, 2023

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

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

Re: Wagner Duys & Wood – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents Wagner Duys & Wood (“Wagner”). I am writing to provide notification of an incident at Wagner that may affect the security of personal information of approximately one hundred and sixty-two (162) Maryland residents. Wagner’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, Wagner does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Wagner discovered that unauthorized access to an employee email account and through that their accounting system on or about March 21, 2023. Upon learning of this issue, Wagner immediately contained and secured the threat and commenced a prompt and thorough investigation. As part of the investigation, Wagner engaged external cybersecurity professionals experienced in handling these types of incidents to determine the extent of any compromise of the information on the Wagner network. Based on the comprehensive investigation, Wagner concluded that certain client documents and records were accessed and/or obtained in connection with this incident. Following the extensive manual document review, Wagner determined on May 23, 2023 that certain personal information was present in those documents and records. The impacted data includes full name in combination with Social Security number, taxpayer ID number, date of birth, driver’s license number and/or state identification number, account number, account type, routing number, institution name, worker’s compensation information, IRS PIN, and health insurance information. Not all data elements were impacted for every Maryland resident.

To date, Wagner has been made aware of several reports of identity fraud, or incidents of financial fraud as a result of this incident as several impacted individuals had fraudulent tax returns filed upon their behalf. As a result of this and out of an abundance of caution, Wagner is providing notice to the affected clients commencing on May 26, 2023 in substantially the same form as the document attached hereto. All notified individuals will receive complimentary credit

May 26, 2023

Page 2

monitoring services. Additionally, Wagner will advise the affected residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Wagner will further advise 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.

Protecting the privacy of personal information is a top priority for Wagner. Wagner remains fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. Wagner continually evaluates and modifies practices to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



James J. Giszczak

Encl.

Exhibit A



4145 SW Watson Avenue
Suite 400
Beaverton, OR 97005

To Enroll, Please Call:
[REDACTED]
Or Visit:
[REDACTED]
[REDACTED]
Enrollment Code: [REDACTED]

**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

May 26, 2023

Dear [REDACTED]

I am writing with important information regarding a recent data security incident that Wagner Duys & Wood (“Wagner”) experienced. The privacy and security of the protected personal information belonging to our clients is of the utmost importance to Wagner. As such, 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 information.

What Happened?

We recently learned that we experienced a security incident on April 7, 2023 where an unauthorized actor was able to access and take certain client files via a phishing email.

What We Are Doing.

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an investigation and manual review of the impacted data, we discovered on May 23, 2023 that the client files that were downloaded by the unauthorized actor contained some of your protected personal information. We want to make you aware of the incident and provide you with steps you can take to protect your information further. Additionally, Wagner is reviewing its existing policies and training protocols relating to data protection while enhancing security measures and monitoring tools to mitigate risk and to better prevent similar incidents in the future.

What Information Was Involved?

The data that was downloaded by the unauthorized actor contained some of your protected personal information, including [REDACTED]

What You Can Do.

We want to make you aware of the incident. To protect you from potential misuse of your information, we are offering **complimentary** identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

For more information on complimentary services offered, please see the additional information provided in this letter. 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.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling [REDACTED] or going to [REDACTED] and using the Enrollment Code provided above. IDX representatives are available [REDACTED]. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter. Please note the deadline to enroll is [REDACTED].

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the proper handling, protection and privacy of protected 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 protected 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 help protect against potential misuse of your information.

Sincerely,



Brad H. Wagner
CPA
Wagner Duys & Wood

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring.

Website. 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.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day “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. 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
<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.

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. 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.

You may also reach out to the Social Security Administration to notify them of the impact on your Social Security Number. They may be reached via the telephone by contacting the National 800 Number at 1-800-772-1213 between 8:00 a.m. – 7:00 p.m., Monday through Friday. If you are deaf or hard of hearing and use TTY equipment, you can call the TTY number at 1-800-325-0778.

6. State Specific Information.

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.oag.state.md.us/Consumer, 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 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.