

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

June 30, 2022

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

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

Re: Modjeski and Masters, Inc. – Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents Modjeski and Masters, Inc. (“Modjeski”). I am writing to provide notification of an incident at Modjeski that may affect the security of personal information of two (“2”) Maryland residents. Modjeski’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, Modjeski does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Modjeski learned that an unauthorized individual may have obtained access to Modjeski’s network. Upon learning of the incident, Modjeski immediately commenced a prompt and thorough investigation. After an extensive forensic investigation and manual document review, Modjeski discovered on June 2, 2022 that certain files on its network containing personal information were potentially accessed and acquired between January 18, 2022 through March 21, 2022. The information contained within the compromised files may have included the residents’ full name and Social Security number.

Modjeski has no indication that any of the information has been misused. Nevertheless, out of an abundance of caution, Modjeski 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. Modjeski is providing the affected residents with written notification of this incident commencing on or about June 30, 2022 in substantially the same form as the letter attached hereto. Modjeski is offering the affected residents complimentary one-year membership with credit monitoring services. Modjeski will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Modjeski will 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.

June 30, 2022

Page 2

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

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

Sincerely,



James J. Giszczak

Encl.

Modjeski and Masters

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



[REDACTED]
[REDACTED]
[REDACTED]

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

June 30, 2022

[REDACTED]

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Modjeski and Masters. We are writing to provide you with information regarding a data security incident that involved your personal information. We want to provide you with information about the incident, advise you of the services we will be providing to you, and let you know that we continue to take significant measures to protect personal information.

What Happened?

Modjeski and Masters became aware of potential unauthorized access to its network that occurred between January 18, 2022 through March 21, 2022.

What We Are Doing.

Upon learning of the issue, we immediately commenced a prompt and thorough investigation to assess the extent and scope of the incident. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and internal document review, we discovered on June 2, 2022 that certain files containing your personal information were potentially acquired from our network.

What Information Was Involved?

Specifically, the personal information that may have been acquired included your full name and [REDACTED]

What You Can Do.

We have no forensic evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we wanted to make you aware of the incident.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit monitoring 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.

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 always

remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

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 personal information.

If you have any further questions regarding this incident, please call our toll-free response line at 1-800-939-4170. This response line is available Monday through Friday, 9 am to 9 pm ET.

Sincerely,

[REDACTED]
[REDACTED]

Modjeski and Masters
100 Sterling Parkway
Suite 302
Mechanicsburg, Pa 17050

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Enter your Activation Code: [REDACTED]

Enrollment Deadline: [REDACTED]

Website and Enrollment. 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.

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 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 105788
Atlanta, GA 30348
<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 LLC

P.O. Box 6790
Fullerton, PA 92834-6790
<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 sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

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

Experian Security Freeze

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

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016
<http://www.transunion.com/securityfreeze>
(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 monitoring 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.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

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.

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.

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: 1-888-743-0023.

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.