

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

November 30, 2023

VIA E-MAIL (idtheft@oag.state.md.us)

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

Re: Jefferson Area Board for Aging – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents Jefferson Area Board for Aging (“JABA”) regarding a recent security incident, located at 674 Hillsdale Dr. Suite 9, Charlottesville, Virginia 22901. I am writing to provide notification of an incident at JABA that may affect the security of personal information of approximately eleven (11) Maryland residents. JABA 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, JABA does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about April 4, 2023, JABA detected unauthorized access to their network as a result of a ransomware incident. JABA contained the threat by disabling access to the network, restored encrypted data, commenced a prompt investigation, and engaged external cybersecurity professionals. Although the forensic investigation did not observe evidence indicating that data was removed from the network environment, the ability to determine whether data was removed was limited by available evidence. Out of an abundance of caution, JABA conducted a detailed and thorough manual review of all potentially impacted data. On November 1, 2023, JABA discovered that personal information was potentially impacted as a result of the incident. JABA proceeded to promptly notify all potentially impacted individuals as expeditiously as possible and is providing written notice on or about December 1, 2023. The potentially impacted data includes full name, Health Insurance Member ID / Group Number, Medicare number, clinical or treatment information, and Social Security number. Not all data elements were impacted for each individual. JABA has also provided notice of this incident to credit monitoring agencies. On November 28, 2023, JABA located the most recent contact information for the impacted individuals.

As stated above, upon learning of this issue, JABA immediately commenced an internal investigation and promptly proceeded to notify potentially affected individuals. JABA has no indication that the information has been used to commit financial fraud or identity theft.

Nevertheless, JABA 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. JABA is offering residents with Social Security numbers impacted complimentary one-year membership with a credit monitoring service. JABA will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. JABA 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. A sample of the provide notice letter is included herein for your reference.

At JABA, protecting the privacy of personal information is a top priority. JABA is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. In response to this incident, JABA deployed Teamview and Malwarebytes. In addition, users are now required to utilize multifactor authentication to access all systems and password credential requirements have been strengthened. Moreover, servers are encrypted at rest and VPN is only accessible via multifactor authentication. JABA continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

JABA 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 (410) 456-2741 or spollock@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Spencer S. Pollock".

Spencer S. Pollock

[REDACTED]



[REDACTED]

December 1, 2023

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]

We are writing to provide you with information regarding a recent incident that involves the security of some of your personal information that was maintained on our servers. The privacy and security of the information entrusted to us is of the utmost importance to JABA. 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

On or about April 4, 2023, JABA detected access to our network as a result of a cybersecurity incident that resulted in the potential exposure of some data we maintain. The information that may have been accessed contained some of your personal information, including your [REDACTED].

What We Are Doing.

Upon learning of this issue, we contained the threat by disabling all access to our network. We then restored all encrypted data, and immediately conducted a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. The forensic investigation revealed that the unauthorized actor may have been able to view, or potentially acquired, some of the information contained on the impacted servers. We followed up with a thorough and extensive manual review of the data potentially contained on the impacted servers and, on November 1, 2023, determined that some of your personal information may have been impacted as a result of this incident.

What You Can Do.

We have no evidence that any of your information has been used to commit financial or identity fraud. Nevertheless, out of an **abundance of caution**, we wanted to make you aware of the incident and provide complimentary credit monitoring services as a precaution. In response to the incident, 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 twelve 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.

As an addendum to this letter, you will find 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.

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 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 for 90 days from the date of this letter, between the hours of 8:00 a.m. to 8:00 p.m. Eastern Standard Time, Monday through Friday, excluding holidays. Please supply the representative with the unique code listed above.

In this world of constant announcements of cyber attacks, we want to extend our sincerest apologies that this incident impacted your information. We are sorry for any worry or concerns this has caused and we have implemented numerous security protocols to our data systems to help prevent intruders from gaining access to our systems in the future. 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 all information. We hope that you will continue to trust JABA.

Sincerely,

JABA
674 Hillsdale Drive, Suite 9
Charlottesville, VA 22901

– 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.

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; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

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