McDonald Hopkins
A business advisory and advocacy law firm®

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

1820 Lancaster Street
Suites 208 & 209
Baltimore, MD 21231

P: 1.410.917.5189

June 25, 2026

VIA U.S. Mail

The Hon. John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Operation PAR, Inc., Boley Centers, Inc., and PEMHS dba Eleos – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Operation PAR, Inc ("Operation PAR") located at 6655 66th Street N Pinellas Park, Florida 33781, Boley Centers, Inc. ("Boley") located at 445 31st Street N St. Petersburg, Florida 33713, and PEMHS dba Eleos ("Eleos") located at 11254 58th Street N Pinellas Park, Florida 33782. Operation PAR, Boley, and Eleos is providing notification of the incident that may affect the security of personal and health information of sixty-five (65) New Hampshire residents. By providing this notice, Operation PAR, Boley, and Eleos does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Operation PAR, Boley, and Eleos discovered that an unauthorized actor may have gained access to its network environment. Upon learning of this issue, Operation PAR, Boley, and Eleos immediately worked to contain the threat and secure its internal environment. Operation PAR, Boley, and Eleos commenced a prompt and thorough investigation into the incident and worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any personal or sensitive data had been compromised as a result of this incident. After an extensive forensic investigation and manual document review, Operation PAR, Boley, and Eleos discovered on June 10, 2026, that the impacted systems, which may have been accessed and/or acquired between June 6, 2025 and June 10, 2025, contained some personal and/or health information for New Hampshire residents. The personal information may include the individual's full name, date of birth, medical information, driver's license number, health insurance information, and Social Security number. The information impacted varied by individual.

To date, Operation PAR, Boley, and Eleos 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, Operation PAR, Boley, and Eleos 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. Operation PAR, Boley, and Eleos is providing the affected residents with written notification of this incident commencing on or about June 25, 2026 in substantially the same form as the letter attached hereto. Operation PAR, Boley, and Eleos is offering the affected residents whose Social Security numbers were impacted complimentary one-year memberships with a credit monitoring service. Operation PAR, Boley, and Eleos 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 Operation PAR, Boley, and Eleos, protecting the privacy of personal information is a top priority. Operation PAR, Boley, and Eleos is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Operation PAR, Boley, and Eleos continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

If you have any additional questions, please contact me at (410) 917-5189 or spollock@mcdonaldhopkins.com.

Very truly yours,

Spencer Pollock

Encl.



Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line

[redacted]

[redacted]

[redacted]

Dear [redacted]

The privacy and security of the personal information we maintain is of the utmost importance to Operation PAR, Inc, Boley Centers, Inc. and PEMHS dba Eleos ("Operation PAR, Boley, and Eleos"). We are writing to provide you with information regarding a recent cybersecurity incident that potentially involved your personal information. You are receiving this letter as you may have been a patient or employee at one or more of the above-named facilities. Please read this notice carefully, as it provides information about the incident, the complimentary identity monitoring services we are making available to you, and precautionary measures you can take to protect your information.

What Happened?
On or about June 10, 2025, Operation PAR, Boley, and Eleos detected unauthorized access to our network as a result of a cybersecurity incident.

What We Are Doing.
Upon learning of the issue, we secured our network and commenced 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. Following the completion of our investigation, it was determined that some of our files may have been accessed or removed by the unauthorized individual(s) between June 6, 2025 and June 10, 2025. We conducted a thorough review of the potentially impacted data and on June 10, 2026, we determined that the impacted files may have contained your personal information.

While cybersecurity threats continue to impact all of us, we are taking ever-increasing measures to protect the information entrusted to us. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. In response to this incident and through our continuing comprehensive review, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts.

What Information Was Involved?
The information that may have been accessed contained some of your personal information, including your first and last name and [redacted]

What You Can Do.

To date, we do not have evidence that your information has been used to commit financial fraud or identity theft. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and provide complimentary credit monitoring services as a precaution. We are providing you with access to Epiq credit monitoring.

This letter provides more information about the complimentary services, enrollment instructions, and 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.

If you have questions, please contact our dedicated and confidential call center at 866-659-7103. The response line is available for 90 days from the date of this letter, between the hours of 8:00 a.m. and 8:00 p.m. Central Time, Monday through Friday, excluding holidays. We apologize for any inconvenience or concern this may cause. We have taken this matter very seriously and will continue to take significant measures to protect the personal information in our possession.

Sincerely,

Operation PAR, Inc.
6655 66th Street N
Pinellas Park, Florida 33781

Boley Centers, Inc.
445 31st Street N.
St. Petersburg, Florida 33713

PEMHS dba Eleos
11254 58th Street N
Pinellas Park, Florida 33782

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring.

Activation Code: [redacted]
Enrollment Deadline: [redacted]
Coverage Length: [redacted] Months

Epiq - Privacy Solutions ID
1B Credit Monitoring - Basic

How To Enroll:

1) Visit www.privacysolutionsid.com and click "Activate Account"
2) Enter the following activation code, [redacted] and complete the enrollment form
3) Complete the identity verification process
4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5) Enter your log-in credentials
6) You will be directed to your dashboard and activation is complete!

Product Features:

1-Bureau Credit Monitoring with Alerts
Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

Dark Web Monitoring (Basic)
Monitors one email address, phone, name, DOB, and SSN on the dark web. Includes retrospective report as well as ongoing monitoring.

Credit Protection
3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Change of Address Monitoring
Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Identity Restoration & Lost Wallet Assistance
Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 1B Credit Monitoring - Basic, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

2. 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
Equifax Information Services LLC
P.O. Box 105069, Atlanta, GA 30348-5069
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
1-888-EQUIFAX (1-888-378-4329)

Experian
P.O. Box 9532, Allen, TX 75013
www.experian.com/fraud
1-888-EXPERIAN (1-888-397-3742)

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000, Chester, PA 19016
www.transunion.com/fraud-alerts
800-916-8800; 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
Equifax Information Services LLC
P.O. Box 105788, Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-888-EQUIFAX (1-888-378-4329)

Experian Security Freeze
P.O. Box 9554, Allen, TX 75013
www.experian.com/freeze
1-888-EXPERIAN (1-888-397-3742)

TransUnion Security Freeze
P.O. Box 160, Woodlyn, PA 19094
www.transunion.com/credit-freeze
800-916-8800; 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 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.

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.

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.

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.

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.marylandattorneygeneral.gov, 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 Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit. In addition, you have the right to obtain a security freeze (as explained above) or submit a declaration of removal. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act. For more information about the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

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.

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.

Rhode Island Residents: You have the right to obtain a police report if one was filed, or alternatively, you can file a police report. Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. There were <<RI Count>> of Rhode Island residents impacted.

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.