McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
1820 Lancaster St.
Suite 200
Baltimore, MD 21231

Spencer S. Pollock
Direct Dial: (410) 917-5189
E-mail: spollock@mcdonaldhopkins.com

June 26, 2026

VIA MAIL

Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: MCBS, LLC – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents MCBS, LLC ("MCBS") regarding a recent security incident. We are writing to notify you of an incident at MCBS that may have impacted the security of personal information of 135 New Hampshire residents. MCBS is a business associate providing this notice on behalf of its impacted covered entities. By providing this notice, MCBS does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On or about September 25, 2025, MCBS became aware of unauthorized access to its network. Upon detecting the unauthorized activity, MCBS immediately contained the incident and commenced a prompt and thorough investigation. After a thorough and detailed forensic investigation and extensive manual document review, MCBS discovered on or about May 28, 2026 that personal information attributable to certain individuals potentially may have been accessed or acquired between September 22, 2025 and September 26, 2025. On June 16, 2026, MCBS confirmed the most recent addresses of the impacted individuals.

The impacted information may include full name, Social Security number, date of birth, health plan beneficiary number, health insurance policy number or subscriber identification number, other health insurance information, medical history, mental or physical condition, medical treatment information, and diagnosis information. MCBS proceeded to promptly notify all potentially impacted individuals as expeditiously as possible and is providing written notice on or about June 26, 206.

To date, MCBS has no evidence of any identity theft or financial fraud related to this incident. Nevertheless, out of an abundance of caution, MCBS wanted to inform your office (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the personal information in its care.

MCBS is providing the affected residents with written notification of this incident in substantially the same form as the letter attached hereto. MCBS will advise the affected

individuals to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. The affected individuals will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission. Those whose Social Security numbers may have been impacted will be offered a 12-month complimentary credit monitoring service.

At MCBS, protecting the privacy of personal information is a top priority. MCBS is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. MCBS 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) 917-5189 or spollock@mcdonaldhopkins.com.

Very truly yours,

Spencer S. Pollock

Encl.

MCBS, LLC
[redacted]

[redacted]

[redacted]

[redacted]

Dear [redacted]:

MCBS, LLC ("MCBS") is writing to notify you on behalf of covered entity of an incident that may have impacted your personal information. MCBS obtained your information from covered entity to provide medical billing services. We take this incident seriously and want to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?
On or about September 25, 2025, we learned that an unauthorized individual may have gained access to our network.

What We Are Doing
Upon learning of this issue, we immediately 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. After an extensive forensic investigation and comprehensive document review, we discovered on or about May 28, 2026, that certain files containing your personal information may have been subject to unauthorized acquisition between approximately September 22, 2025 and September 26, 2025.

What Information Was Involved?
The information potentially impacted includes [redacted].

What You Can Do
At this time, we are not aware of any misuse of or fraudulent activity relating to anyone's personal or health information as a result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the occurrence and provide some general practices for reference that can help deter, detect, and protect you from medical identity theft. These practices include protecting documents that contain medical information, reviewing your medical records and Explanation of Benefits statements for errors or services not received, and reporting any errors or suspicious activity to your health care provider. For more information about these practices, please visit *consumer.ftc.gov/articles/what-know-about-medical-identity-theft*. We also wanted to provide you complimentary access to identity protection services through [redacted] for [redacted] as a precaution.

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

[redacted]

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 potential misuse of your information. The response line is available [redacted].

Sincerely,

MCBS, LLC
1125 Troupe St
Augusta, GA 30904

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [redacted]-Month Credit Monitoring.
[redacted]

2. Obtain and Monitor Your Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies. You can obtain a free copy of your credit report by calling **1-877-322-8228,** visiting **www.annualcreditreport.com,** or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/index.action. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below.

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

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.

3. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. 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. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/.

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

4. Placing a Security Freeze on Your Credit File.

Following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below). 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

[redacted]

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. 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 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. If you do place a security freeze *prior* to enrolling in any 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.

5. Protecting Medical Information.

As a general matter, the following practices can help deter, detect, and protect from medical identity theft. For more information visit consumer.ftc.gov/articles/what-know-about-medical-identity-theft. Only share health insurance cards with health care providers and other family members who are covered under the insurance plan or who help with medical care. Review the "explanation of benefits statement" which is provided by the health insurance company. Follow up with the insurance company or care provider for any items not recognized. 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 the insurance company for a current year-to-date report of all services paid for the impacted individual as a beneficiary. Follow up with the insurance company or the care provider for any items not recognized.

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 under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/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 may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400. There were [redacted] Rhode Island residents impacted by this incident.

[redacted]

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.

[redacted]