



A business advisory and advocacy law firm®

Spencer Pollock
Direct Dial: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

McDonald Hopkins LLC
1820 Lancaster Street
Suite 200
Baltimore, MD 21231

P 1.410.917.5189

June 26, 2026

Re: Aesto LLC Security Incident

To Whom it May Concern:

McDonald Hopkins PLC represents Aesto LLC. We are writing to provide information about a security incident impacting Aesto, which involved data owned by HIPAA Covered Entity Clients. By providing this information, Aesto does not waive any rights or defenses regarding the applicability of law or personal jurisdiction.

On or about December 18, 2025, Aesto experienced a network security incident that impacted a limited portion of their Amazon Web Services (“AWS”) infrastructure. Upon learning of the issue, Aesto commenced a prompt and thorough investigation. As part of Aesto’s investigation, Aesto worked very closely with external cybersecurity professionals experienced in handling these types of incidents.

After an extensive forensic investigation and manual document review, on May 26, 2026, Aesto confirmed that between on or about December 2, 2025, and December 18, 2025, a limited amount of sensitive information pertaining to Covered Entities, which was stored Aesto’s network, may have been accessed and/or acquired by an unauthorized actor. On June 26, 2026, Aesto notified Covered Entities with impacted information of the incident. Aesto has no evidence that any of the information has been misused.

Aesto is committed to maintaining the privacy of sensitive information in its possession and has taken many precautions to safeguard it. Please note, this incident was contained to a limited portion of Aesto’s AWS infrastructure and did not affect the systems of Covered Entities.

Should you have additional questions, please contact McDonald Hopkins at **AestoOptIn@mcdonaldhopkins.com**.

Very truly yours,

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

Spencer Pollock

Baltimore | Chicago | Cleveland | Columbus | Detroit | West Palm Beach
mcdonaldhopkins.com



Return Mail Processing
PO Box 6508
Carol Stream, IL 60197

+ 0000007371 0000001 2100000018377162 NN NN NN



SAMPLE A. SAMPLE
123 MAIN STREET
ANYTOWN US 12345-6789



August 7, 2026

[Extra1]

Dear Sample A. Sample:

Aesto, LLC (“Aesto”) provides healthcare data migration and archiving services for [Extra2] and writes with important information regarding a recent data security incident at Aesto involving some of your protected health information. The privacy and security of the information we maintain is of the utmost importance to Aesto and [Extra2]. 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 December 18, 2025, Aesto experienced a network security incident that impacted a limited portion of their Amazon Web Services infrastructure.

What We Are Doing. Upon learning of the issue, Aesto commenced a prompt and thorough investigation. As part of Aesto’s investigation, Aesto worked very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, on May 26, 2026, Aesto confirmed that between on or about December 2, 2025, and December 18, 2025, a limited amount of your protected health information pertaining to [Extra2], which was stored Aesto’s network, may have been accessed and/or acquired by an unauthorized actor. Aesto has no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved? The information potentially impacted includes your full name, as well as your [Extra3].

What You Can Do. Aesto has no evidence that any protected health information has been or will be misused for identity theft or financial fraud as a direct result of this incident. However, out of an abundance of caution, to help protect your identity, [Extra2] is offering a complimentary [Extra5] month membership of Experian IdentityWorks. For more information on identity theft prevention and Experian IdentityWorks, including instructions on how to activate the complimentary [Extra5]-month membership, 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. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information on the following pages.

For More Information. Please accept our apologies that this incident occurred. 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 your 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 833-918-8060.** 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. Be prepared to provide **your engagement number [B#####]**.

Sincerely,
Aesto LLC, on behalf of

[Extra2]

END OF LETTER PROVIDED BY AESTO LLC. FURTHER INFORMATION PROVIDED BY [Extra2]

Experian IdentityWorksSM Enrollment Information

To help protect your identity, My Doctor LLC is offering complimentary access to Experian IdentityWorksSM for [Extra5] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra5] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra5]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** December 31, 2026 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by December 31, 2026. Be prepared to provide engagement number [B#####] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra5]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.



Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov
888-743-0023

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212-416-8433

New York Attorney General
The Capitol
Albany, NY 12224
ag.ny.gov
800-771-7755

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.