Aesto, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

June 26, 2026

PNNUW00020004200042010 2L0400

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear Compliance Officer:

We are writing to let you know that Aesto, LLC ("Aesto") experienced a cyber incident that involved information your organization entrusted to us. We take this matter seriously and want to provide you with a clear account of what happened, what we've done in response, and what steps are available to you.

What Happened?
On or about December 18, 2025, Aesto experienced a network security incident that impacted a limited portion of our Amazon Web Services ("AWS") infrastructure. Our core data platform, where your live archive resides, was not compromised. Upon learning of the issue, we immediately launched a thorough investigation with experienced external cybersecurity professionals to determine whether sensitive information had been accessed and/or acquired. On May 26, 2026, we confirmed that between on or about December 2, 2025, and December 18, 2025, a limited amount of information stored in our network may have been accessed and/or acquired by an unauthorized actor through forensic analysis. However, your organization's information was not amongst the impacted data contained on the threat actor's list.

What Information Was Involved?
The affected information includes protected health information of certain individuals affiliated with your organization, consisting of full names, dates of birth, medical information, driver's license numbers, financial account numbers only, health insurance information, individual taxpayer identification numbers, other government ID numbers, and Social Security numbers. Not all individuals had Social Security numbers impacted. The list of affected individuals and specific data elements involved for each person will be provided to your organization upon request (*see Next Steps below*).

What We Are Doing.
As part of our investigation, we worked with cybersecurity professionals to secure our network. We have reset credentials, enhanced our security measures and monitoring tools, and are reviewing our existing policies and training protocols to help prevent similar incidents in the future. This was an isolated incident, and we are taking all necessary actions to address the situation and reduce risk going forward. **We are providing an attestation from our cybersecurity professionals detailing the root cause of the incident, the steps we took to remediate and harden our network, and confirmation that no further unauthorized activity has been observed.**

Next Steps and Services We are Offering:

1. **Obtain Your Data File of Affected Individuals**

Please send an email to **AestoDataReq@transunion.com** by **July 17, 2026**, and we will make arrangements to securely transfer a data file with the list of individuals related to your organization whose protected health information may have been affected by this incident. As the data owner, your organization can then review the files and determine which, if any, individuals should be notified of the incident.

2. **Individual Notifications**

Upon review of your data file, you may determine legal notification obligations are required. Unfortunately, Aesto is unable to issue individual notifications on your behalf. However, we are providing a notification package for you to assist with any notification obligations you identify. For individual notifications, the package will include Cover Letters with Aesto's letterhead that may be used for individual notifications. The package includes multiple Cover Letter versions to assist with various types of individuals who may need to be notified. The Cover Letters also include a call center for individuals who may have questions. The notification package includes a sample of the FAQs the call center will utilize. **Please note, other than the variable fields, these Cover Letters may not be altered in any way.**

Aesto does not represent that these Cover Letters will fulfill your legal notification obligations. You should seek counsel to determine your legal notification obligations and ensure the notifications you send fulfill all applicable laws. While Aesto has provided a Cover Letter, legal notification obligations typically include additional information such as:

- How to place a fraud alert or a security freeze.
- How to obtain a free credit report.
- Credit monitoring instructions.
- How to protect sensitive information.
- Additional helpful resources.
- Contact information for law enforcement and regulatory bodies.

You may download the notification package using this link:
https://ezshield.sharefile.com/d-s07fa1677a75b466f9ceb7fe5782b7ddf. Do not share this link outside of your response team.

3. **Health and Human Services Office of Civil Rights (HHS OCR) Notification**

We are offering to notify HHS OCR on your behalf if you choose to **OPT-IN by July 17, 2026.** If you would like to **OPT-IN** HHS OCR notification, you may do so by sending an email to **AestoOptIn@mcdonaldhopkins.com** with the following information by **July 17, 2026**:

a. **Name of your organization.**
b. **Organization's full address.**
c. **Point of contact for your organization (name, email, phone number).**
d. **Type of covered entity: health plan, healthcare clearing house, or healthcare provider.**
e. **Number of impacted individuals.**
f. **Estimated mailing date of your individual notice.**
g. **Whether you plan to use the cover letter as your notification letter. If not, you must provide a sample of your notice letter.**

To **OPT-IN**, you must provide all of the above information by **July 17, 2026** by sending an email to **AestoOptIn@mcdonaldhopkins.com**. Incomplete information *will not* be reported to HHS OCR.

4. State Regulatory Notifications

Aesto is unable notify regulators on your behalf. However, to aid in any regulatory notification obligations you may determine are necessary, the notification package includes a **regulatory letter** detailing the incident including contacts for more information that may be attached to any state regulatory reports.

5. Website and Media Notification

Aesto has posted website notice and provided nation-wide media notices. An example of the media notification is included in the notification package. The media notification includes call center information and a live link to a list of Covered Entities who choose to be named to satisfy their substitute notice obligations. **If you want to add your organization's name to a live link on Aesto's website, please send an email to AestoOptIn@mcdonaldhopkins.com indicating the full name of your organization and your consent to be added to the list.**

Please note, you should seek your own counsel to ensure that Aesto's website and media notice satisfy your substitute notice legal obligations. Aesto does not guarantee that these notices fulfill your legal obligations.

We sincerely regret that this incident occurred. We are committed to maintaining the privacy of information in our possession and continually evaluate and strengthen our practices and internal controls. Since this incident, we have reset passwords and worked with an external cybersecurity firm to further harden our network security. If you have questions, please contact our dedicated and confidential toll-free response line at **833-918-8060.** The response line is staffed with professionals familiar with this incident and is available Monday through Friday, 8 am - 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide **your engagement number B167548.** Thank you for your cooperation and your continued trust.

Sincerely,

Aesto, LLC
1800 International Park Drive, Suite 110
Birmingham, AL 35243

PNNUW00020004200042020202D0000

McDonald Hopkins
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,



Spencer Pollock

Attestation of Security Investigation

January 23, 2026

On December 18, 2025, McDonald Hopkins as Legal Counsel (“Counsel”) on behalf of Aesto Health (“Aesto”) engaged GuidePoint Security, LLC (“GuidePoint”) to perform Incident Response services. GuidePoint utilized Aesto’s existing security tools and data sources and deployed supplemental tools to establish broad environmental visibility as outlined below. GuidePoint leveraged industry standard Incident Response techniques and tools to the best extent possible to identify the intrusion vector, signs of data theft, and other threat actor related activity. GuidePoint has made every effort to perform a thorough and comprehensive analysis and to provide appropriate recommendations. GuidePoint is bound by defined scope, allocated time, therefore this investigation is the result of a point-in-time assessment based on the state of the Aesto’s environment at the conclusion of the investigation.

REMEDIATION SUMMARY

Based on the available data, GuidePoint was able to determine that Aesto was the victim of a cyber incident with an earliest known date of December 2, 2025.

GuidePoint has been able to identify how the threat actor breached the network, the accounts that the threat actor managed to compromise, the changes the threat actor made to existing AWS Lambda functions, and other threat actor actions taken during the dwell time on the network. Based on these findings and other best practices, Aesto has taken numerous security steps to remediate this incident and to harden their defense posture moving forward. Some of these steps include:

1. Closed the security gaps exploited by the threat actor to gain access to the network.
2. Deleted the impacted Lambda functions.
3. Rotated all impacted AWS secrets.
4. Deleted unauthorized files uploaded by the threat actor.

Based on these steps and the continuing monitoring of the network, GuidePoint has not observed any threat actor activity on the network since December 18, 2025.

Copyright © 2025
(877) 889-0132 dfir.team@guidepointsecurity.com

P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name >
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>
<<Country>>

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: December 30, 2026

To Enroll, Scan the QR Code Below:

[redacted]
SCAN ME

Or Visit:
[redacted]

[redacted]

<<IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY // NOTICE OF DATA BREACH>>

Dear <<First Name>> <<Last Name>>:

Aesto, LLC ("Aesto") provides healthcare data migration and archiving services for <<Covered Entity>> 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 <<Covered Entity>>. 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 <<Covered Entity>>, 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 <<Variable Text 2>>.

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, <<Covered Entity>> is offering a complimentary <<12/24>> month membership of IDX identity protection services. IDX identity protection services include: credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. We encourage you to contact IDX to enroll in the free identity protection services by calling [redacted], going to [redacted] or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 AM - 8 PM Central Standard Time (excluding major U.S. holidays). Please note the deadline to enroll is December 30, 2026.

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** [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 minor's information. The response line is available Monday through Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide **your engagement number** [redacted]

Sincerely,
Aesto LLC, *on behalf of*
<<Signature>>
<Signer Name>>
<<Covered Entity>>



Recommended Steps to Help Protect Your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, https://oag.maryland.gov, Telephone: 1-888-743-0023.

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 reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.