On August 27, 2025, Clarity identified suspicious activity within its benefits platform. Upon becoming aware of the activity, Clarity engaged a leading third-party cybersecurity forensic specialist to investigate and determine the nature and scope of the activity. On September 18, 2025, the investigation confirmed that an unauthorized party accessed a small number of accounts. On September 23, 2025, Clarity completed a detailed review and identified that one (1) Maine resident may have been affected by this event. On September 26, 2025 Clarity provided notification to the data owners identified in the chart below and is now providing notification to individuals and regulators on the data owners' behalf. The type of information that could have been accessed included the individual's name and HSA Account number.

Data Owner Name	Number of Potentially Impacted Residents
Apis Services, Inc.	1

Clarity provided written notification to the potentially impacted Maine resident via First Class Mail on October 24, 2024, pursuant to Maine law. The notification letter includes details of the event and contact information for individuals to contact with inquiries. A copy of the notice letter is attached hereto as **Exhibit A**.

At Clarity Benefits Solutions
c/o Cyberscout
PO Box 245
Bellmawr, NJ 08099

Clarity | BENEFIT SOLUTIONS™
90 Woodbridge Center Drive, Suite 405
Woodbridge, NJ 07095
888.423.6359
claritybenefitsolutions.com

USBFS2093 T1 P1

[redacted]

Proof

0102000055

October 24, 2025

Dear <<FirstName>> <<LastName>>:

At Clarity Benefits Solutions ("Clarity"), protecting your information is a top priority. We are writing to inform you of an event that may affect your Clarity Health Savings Account (HSA) and the privacy of your information. While you may already be aware of this event, this letter serves as official notice regarding the disclosure, our response, and steps you can take to help protect your information, should you deem it appropriate to do so.

What Happened. On August 27, 2025, we identified suspicious activity within our benefits platform. Upon becoming aware of the activity, we engaged a leading third-party cybersecurity forensic specialist to investigate and determine the nature and scope of the activity. On September 18, 2025, the investigation confirmed that an unauthorized party accessed a small number of accounts. By September 23, 2025, we completed a detailed review to identify individuals who may have been affected. You are receiving this notice because your information may have been involved.

What Information Was Impacted. The data potentially impacted may include your name and HSA card number.

What Are We Doing. We acted quickly to secure our secure your account, our systems and launched a thorough investigation. We've also strengthened our safeguards to further protect your data and to prevent similar incidents from happening in the future. Additionally, we are offering you [redacted] months of complimentary credit monitoring and identity protection services, at no cost to you.

What You Can Do. We encourage you to stay vigilant for incidents of identity theft and fraud by regularly reviewing your credit reports and account statements for any unusual activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company.

Enclosed with this letter are detailed "**Steps You Can Take to Help Protect Your Information.**" Please review this section for more details on the steps you can take to help protect yourself against fraud and identity theft, including enrolling in the complimentary credit monitoring and identity protection services we are offering. Please note that you must enroll directly, as we cannot enroll you on your behalf.

For More Information. If you have any questions, please contact our designated call center at [redacted] between 8:00 AM and 8:00 PM ET Monday through Friday, excluding holidays.

Thank you for your attention to this matter and for trusting Clarity.

Sincerely,
Clarity Benefits Solutions

000055002001

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Identity Monitoring Services

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 [redacted] 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, a TransUnion company specializing in fraud assistance and remediation services.

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.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau. You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Proof

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

0102000055

0000550020001

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 1-202-727-3400, and www.oag.dc.gov/consumer-protection.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or www.ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this matter. There is 1 Rhode Island resident impacted by this matter.

Proof

0202000055

0000550020002