

Clover Health

{RecipientFirstName} {RecipientMiddleName} {RecipientLastName}
{RecipientMailingAddressLine1}
{RecipientMailingAddressLine2}

Re: Notice of Data Security Event

Dear {First Last Name}:

Clover Health Investments Corp. (“Clover Health” or the “Company”) is writing to notify you about a cybersecurity incident that may have involved some of your personal information. While we are unaware of any attempted or actual misuse of any personal information since the incident occurred, we are providing you with information about the incident and steps you can take to protect your personal information.

What Happened? On July 4, 2026, Clover Health determined that it had experienced a cybersecurity incident involving unauthorized access to certain Company applications and data. We immediately initiated an investigation, activated our incident response procedures, engaged leading third-party cybersecurity experts, took steps to contain the activity, and notified law enforcement.

The investigation determined that, between July 3, 2026, and July 4, 2026, an unauthorized party gained access to access credentials belonging to three non-managerial Company employees and then used those credentials to access certain Company applications and data. Clover detected the incident on July 4, 2026, and was able to terminate the unauthorized access within hours of discovery.

The investigation determined that certain data was subject to unauthorized access and acquisition. A third-party e-discovery expert was retained to conduct a review of the data and identify any personal information that had been accessed or acquired. On August 28, 2026, after a comprehensive review, it was determined that some personal information pertaining to you was subject to unauthorized access and acquisition.

What Information Was Involved? The investigation determined that the following types of information pertaining to you were involved: {DATA}.

What We Are Doing. Please know that protecting your personal information is something that we take very seriously. When we detected the incident, we took immediate action and, as a result, the unauthorized access was terminated within hours of detection. We engaged leading third-party cybersecurity experts and notified law enforcement. We also took steps to reduce the likelihood of a similar incident occurring in the future, and we continue to make additional improvements that strengthen our cybersecurity posture.

What You Can Do. We encourage you to closely review the information about how to help protect yourself against any possible identity theft or fraud in the ***Additional Important Information*** section below.

Remain Vigilant. We recommend that you remain alert to signs of possible fraud or identity theft by reviewing your account statements and monitoring your free credit reports for any unauthorized activity.

Report Suspicious Activity. If you notice any unauthorized activity, report it immediately to your financial institution and, if appropriate, file a report with your local police department and the Federal Trade Commission. The FTC can be reached at 1-877-438-4338 or www.identitytheft.gov and provides additional information on steps you can take to protect against identity theft.

For More Information. We take our responsibility to safeguard your personal information seriously and deeply regret any inconvenience this incident might cause. For further information and assistance, please call 1-888-619-4930 from 9 am to 5 pm Eastern Time, Monday through Friday, excluding major U.S. holidays.

Sincerely,
Clover Health

cloverhealth.com

Clover Health is a PPO and HMO organization with a Medicare contract. Enrollment in Clover Health depends on contract renewal.

Y0129_26MX131_C

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring 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 should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes, and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-IDTHEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by 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 can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. As the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies below to find out more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

This notice was not delayed at the request of law enforcement.

If account credentials were involved in this incident described in the “What Information Was Involved?” section above, you should promptly change your credentials and security questions as appropriate. If you use these credentials with other accounts, you should take similar steps to secure those accounts as well.

Additional information for residents of the following states:

District of Columbia Residents: You may obtain information about steps you can take to avoid identity theft from the Federal Trade Commission and from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, DC 20001, (202) 727-3400, <https://oag.dc.gov>.

Maryland Residents: You may obtain information about steps you can take to avoid identity theft from the Federal Trade Commission and from the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / (410) 576-6300, www.marylandattorneygeneral.gov.

North Carolina Residents: You may obtain information about preventing identity theft from the Federal Trade Commission and from the North Carolina Attorney General’s Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 (toll-free in North Carolina) or (919) 716-6000, www.ncdoj.gov. You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

New York Residents: You may obtain information regarding security breach response and identity theft prevention and protection from the Federal Trade Commission and from the following New York State agencies: (1) the New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>; and (2) the New York Department of State, Division of Consumer Protection, 99 Washington Avenue, Albany, NY 12231, 1-800-697-1220, www.dos.ny.gov/consumerprotection.

Iowa Residents: You are advised to report any suspected identity theft to local law enforcement or to the Iowa Attorney General. The Office of the Attorney General of Iowa, Consumer Protection Division, is located at the Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, 515-281-5926 or 888-777-4590 (outside the Des Moines metro area), www.iowaattorneygeneral.gov.

Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General. The Oregon Department of Justice is located at 1162 Court Street NE, Salem, OR 97301-4096, 1-877-877-9392 or 503-378-4400, www.doj.state.or.us.

Massachusetts Residents: You have the right to obtain a police report if you are the victim of identity theft. You also have the right to request a security freeze on your credit report at no charge; to request a freeze, contact each of the three nationwide consumer reporting agencies using the information provided above. There is no fee to place, temporarily lift, or remove a security freeze.