December 11, 2025

PLEASE READ THIS LETTER. IT INCLUDES IMPORTANT INFORMATION.

Re: Notice of Data Breach

Dear [Name]:

We are writing to let you know about a recent incident that took place with a third-party vendor for Cigna Healthcare®, for payment integrity services. It may have involved some of your personal information, which the vendor had due to the services that it provides to Cigna Healthcare. Cigna Healthcare is the administrator for the Massachusetts Mutual Life Insurance Company benefit plans.

The third-party vendor is unaware of any attempted or actual misuse of any information due to this incident. We are providing you with information about it and steps you can take to protect yourself, if you feel it is needed.

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.

What happened? On January 15, 2025, Cigna Healthcare was notified by one of our third-party vendors of an incident involving unauthorized access to their systems. But, the vendor did not confirm Cigna Healthcare data was impacted until September 3, 2025.

Your data was identified as part of the impacted data, between September 23-29, 2025. Through its investigation, the vendor determined that the incident occurred between October 21, 2024, and January 13, 2025. The data affected includes claim overpayment and recovery files managed by the Payment Integrity business unit.

Once discovered, the vendor safely restored its systems and operations and notified law enforcement.

What information was potentially disclosed? The information viewed/accessed varies by individual but included names, health care ID, date of service, treatment cost and claim numbers.

For some individuals, the information also included their Social Security numbers. Presently, there's no evidence or indication of actual or attempted misuse of your personal information.

What are we doing? Cigna Healthcare takes the privacy of those we serve seriously and works hard to protect our customers' information. We also adhere to regulatory requirements each and every day.

Since the incident, several services have been transitioned to other vendors, reducing this vendors role in Cigna Healthcare's operations. Cigna Healthcare continues to review its

relationship with this vendor through our third-party vendor oversight activities. This includes periodic security assessments and ensuring appropriate privacy and security controls. This is in alignment with expectations from State and Federal regulatory bodies.

We're also notifying you in case you decide to take further steps to protect your information if you feel it appropriate to do so**.**

In addition, we are providing you with access to 24 months of credit monitoring and identity restoration services through Equifax at no charge to you. You must enroll by February 28, 2026.

Please review the next page for more information on the Equifax credit monitoring offering and how to enroll.

If you have any questions, please call 800.548.3980.

We sincerely regret any issue this incident may have caused you.

Sincerely,
Cigna Healthcare

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. 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 may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

If you believe you are the victim of identity theft or any of your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps to avoid identity theft and to place fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. You should obtain a copy of the police report in case you are asked to provide it to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center**,** 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

Credit Freeze: Under the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018 (Public Law No. 115-174), as of September 21, 2018, you have the right to put a credit freeze on your credit file free of charge. A credit freeze is designed to prevent a credit reporting company from releasing your credit report without your consent. If you place a credit freeze on your credit file, no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate the freeze. In addition, potential creditors and other third parties will not be able to provide access to your credit report unless you lift the freeze. Therefore, 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 agency. You can obtain more information about fraud alerts and credit freezes by contacting the Federal Trade Commission or one of the national credit reporting agencies listed above.

If you are a resident of the District of Columbia, and you either believe you are the victim of identity theft or need to obtain information on the steps to take to avoid identify theft, you should immediately contact the District of Columbia Attorney General at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov, and www.oag.dc.gov.

If you are a resident of Iowa, you are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General. Iowa Office of the Attorney General, Consumer

Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, 1-888-777-4590, consumer@ag.iowa.gov.

If you are a resident of Maryland, and you either believe you are the victim of identity theft or need to obtain information on the steps to take to avoid identify theft, you should immediately contact the Maryland Attorney General at Office of Attorney, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

If you are a resident of New Mexico, you have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

If you are a resident of New York, the Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-(800)-771-7755; or www.ag.ny.gov.

If you are a resident of North Carolina, and you either believe you are the victim of identity theft or need to obtain information on the steps to take to avoid identify theft, you may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400.

If you are a resident of Oregon, you are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Office of the Attorney General: Oregon Office of the Attorney General, Consumer Protection Division, 1162 Court St. NE, Salem, OR 97301-4096, 1-877-877-9392, www.doj.state.or.us.

If you are a resident of West Virginia, you also have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is as follows:

Equifax, PO Box 740256, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-680-7289

As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft/.

You may also obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a

security freeze on your credit report pursuant to West Virginia law. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique personal identification number ("PIN") or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

(1) The unique personal identification number ("PIN") or password provided by the consumer reporting agency;
(2) Proper identification to verify your identity; and
(3) The period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request.

A security freeze does not apply to circumstances in which you have an existing account relationship, and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit.