Regence | 1111 Lake Washington Blvd N, Suite 900
Renton, WA 98056

May 6, 2025

Attorney General Nick Brown
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

RE: Notification of Breach of Washington Residents' Information

Dear Attorney General Brown,

I am reporting a data breach experienced by MedicareCompare (MCUSA). Regence contracts with MCUSA as our business associate to serve as a broker of Regence products. MCUSA's breach impacted multiple MCUSA customers and we have confirmed that the breach impacted 706 Washington residents who have policies with Regence. Below are the details and the steps taken in response to the incident

On Nov. 19, 2024, MCUSA discovered suspicious activity in some email accounts within their email tenant. MCUSA immediately took steps to secure their environment and engaged a third-party forensic specialist to investigate. Immediately upon learning of the suspicious activity, MCUSA proceeded to conduct password resets for the impacted accounts. To further mitigate the event and secure the accounts, MCUSA implemented Multi-Factor Authentication for all licensed accounts. MCUSA has confirmed there is currently no evidence of identity theft or fraud related to this incident.

The investigation determined that through a successful phishing attack, an unauthorized actor accessed some MCUSA email accounts between Nov. 5, 2024, and Nov. 21, 2024, and that certain emails were viewed by the unauthorized actor. On Jan. 20, 2025, MCUSA received an impacted member data file from the third-party vendor and undertook efforts to validate the results of the data mining and match individuals back to the covered entity with whom they are affiliated. This process was completed on Mar. 6, 2025. On Mar. 27 our Privacy Office received a notification from MCUSA confirming that our member data was impacted, and we received the impacted member file on Apr. 3, 2025. On Apr.9, 2025, our data team validated that from the files provided by MCUSA, 706 Washington residents were impacted.

The affected information was primarily contained in commission statements that were sent internally within MCUSA as part of the procedure for processing

Regence | 1111 Lake Washington Blvd N, Suite 900
Renton, WA 98056

commission payments to agents. The affected information included member names and ID numbers. Some of the affected information also included dates of birth, Social Security numbers (SSN), medical history information, and Medicare beneficiary numbers.

MCUSA initially notified the United States Department of Health and Human Services Office for Civil Rights (OCR) on Mar. 21, 2025, and will be amending the report to include Regence as an impacted covered entity. Additionally, MCUSA submitted media notification in the State of Washington via PR Newswire submission on Mar. 21, 2025. MCUSA is also notifying all affected members on Regence's behalf with an offer of one year of complimentary credit monitoring and identity theft protection services. Lastly, MCUSA has set up a dedicated line for affected members to call with any questions.

If you have any questions, please contact me at (503) 225-4962.

Sincerely,

Valerie Berg
Privacy Officer, Director

[COMPANY LOGO]

<<Return Mail Address>>

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>> <<Date>>
<<City>>, <<State>> <<Zip>>
<<Country>>

[NOTICE OF DATA BREACH]

Dear <<Name 1>> <<Name 2>>:

MedicareCompareUSA ("MCUSA") is writing to make you aware of an event that may involve your information. MCUSA has your information because we helped you purchase a health insurance policy from [DATA OWNER]. MCUSA is providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? In November 2024, MCUSA became aware of suspicious activity related to certain email accounts. We immediately took steps to secure our environment and launched an investigation to determine the nature and scope of the activity. The investigation determined there was unauthorized access to certain accounts between November 5, 2024 and November 21, 2024. As a result, MCUSA began an extensive review of the accounts to determine if any sensitive information could be affected and to whom it relates. We recently completed this review and are providing this notice in an abundance of caution.

What Information Was Involved? The investigation determined that the following types of information were included in the files involved: your name, [DATA ELEMENTS].

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon becoming aware of this event, we immediately took steps to confirm the security of our email tenant and to determine what information was potentially impacted. We implemented additional cybersecurity measures and reviewed existing security policies to further protect against similar events moving forward.

As an added precaution, we are offering you immediate access to credit monitoring and identity theft protection services for [DURATION] months at no cost to you, through [VENDOR]. You can find more information on how to enroll in these services in the enclosed additional information section. We encourage you to enroll in these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. We encourage you to enroll in the complimentary credit monitoring services as we are not able to do so on your behalf. Please also review the information contained in the enclosed additional information section.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call [TELEPHONE NUMBER] from X:00 a.m. [TIMEZONE] to X:00 p.m. [TIMEZONE], Monday through Friday, excluding major U.S. holidays.

Sincerely,

MedicareCompareUSA

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

[Enrollment Instructions]

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to

file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. MCUSA Holding, Inc. is located at 1407 North Forest Street, Bellingham, WA 98225.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. We encourage consumers to review their 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.

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 https://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 reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [#] Rhode Island residents that may be impacted by this event.