

EXHIBIT 1

We represent MedicareCompareUSA (“MCUSA”) located at 1407 North Forest Street, Bellingham, WA 98225, and we are writing to notify your Office of an incident that may affect the security of certain personal information relating to nine hundred twenty-two (922) Washington residents on behalf of Humana.

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MCUSA does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

In November 2024, MCUSA became aware of suspicious activity related to certain email accounts. MCUSA immediately took steps to secure its 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. MCUSA recently completed this review and, on March 18, 2025, MCUSA notified Humana that individuals related to Humana were potentially involved.

The information that could have been subject to unauthorized access includes name, date of birth, health insurance policy number, Medicare number, and Social Security number.

Notice to Washington Residents

On or about May 12, 2025, MCUSA began providing written notice of this incident to nine hundred twenty-two (922) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the suspicious activity, MCUSA moved quickly to investigate and respond to the incident, assess the security of MCUSA systems, and identify potentially affected individuals. MCUSA is also working to implement additional safeguards and training to its employees. MCUSA is providing access to credit monitoring services for one (1) year, through Transunion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, MCUSA is providing impacted individuals with guidance on how to better protect against identity theft and fraud. MCUSA is providing individuals with information on how to place a fraud alert and security freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

MCUSA is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A



May 12, 2025

Dear _____ :

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. 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, date of birth, health insurance policy number, and Medicaid number.

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 Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) 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 the 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. 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 1-833-998-8824 from 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding major U.S. holidays. If you have a speech or hearing impairment and use a TTY, call **1- 800- 833- 3301**.

Sincerely,

MedicareCompareUSA

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: **1D1742B2F310** 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

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 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 0 Rhode Island residents that may be impacted by this event.

EXHIBIT 1

We represent MedicareCompareUSA (“MCUSA”) located at 1407 North Forest Street, Bellingham, WA 98225, and we are writing to notify your Office of an incident that may affect the security of certain personal information relating to nine hundred twenty-two (922) Washington residents on behalf of Humana.

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MCUSA does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

In November 2024, MCUSA became aware of suspicious activity related to certain email accounts. MCUSA immediately took steps to secure its 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. MCUSA recently completed this review and, on March 18, 2025, MCUSA notified Humana that individuals related to Humana were potentially involved.

The information that could have been subject to unauthorized access includes name, date of birth, health insurance policy number, Medicare number, and Social Security number.

Notice to Washington Residents

On or about May 12, 2025, MCUSA began providing written notice of this incident to nine hundred twenty-two (922) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the suspicious activity, MCUSA moved quickly to investigate and respond to the incident, assess the security of MCUSA systems, and identify potentially affected individuals. MCUSA is also working to implement additional safeguards and training to its employees. MCUSA is providing access to credit monitoring services for one (1) year, through Transunion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, MCUSA is providing impacted individuals with guidance on how to better protect against identity theft and fraud. MCUSA is providing individuals with information on how to place a fraud alert and security freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

MCUSA is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A



May 12, 2025

Dear _____ :

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. 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, date of birth, health insurance policy number, and Medicaid number.

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 Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) 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 the 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. 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 1-833-998-8824 from 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding major U.S. holidays. If you have a speech or hearing impairment and use a TTY, call **1- 800- 833- 3301**.

Sincerely,

MedicareCompareUSA

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: **1D1742B2F310** 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

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 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 0 Rhode Island residents that may be impacted by this event.