WHAT HAPPENED?

On April 9, 2026, AAWC became aware of unusual activity involving an employee VPN account. Upon discovery, we immediately began an investigation and worked with cybersecurity professionals to assist in determining the nature and scope of the incident.

The investigation determined that an unauthorized actor gained access to AAWC's network environment and accessed or acquired certain files. The unauthorized actor also provided a sample of files as part of an extortion communication. Although the investigation was able to confirm unauthorized access to certain files, it was not able to determine every specific file or record that may have been accessed or acquired. Therefore, AAWC is notifying individuals whose information was maintained in the affected environment.

AAWC worked to identify the individuals whose information may have been involved and to obtain available contact information needed to provide notice. That process was completed on or about June 5, 2026. AAWC then arranged to provide notice to potentially affected individuals.

WHAT INFORMATION WAS INVOLVED?

Based on the review of the potentially affected information, the information involved may have included some or all of the following: name, date of birth, Social Security number, driver's license number or other identification number, clinical or treatment information, lab results, prescription information, provider information, health insurance information, medical documents, ultrasound images, and copies of passports or identification documents.

Not all information was involved for all individuals.

WHAT WE ARE DOING

Upon discovering the incident, AAWC took steps to investigate and respond. These steps included working with cybersecurity professionals, securing the affected environment, resetting passwords, implementing additional security measures, and reviewing policies and procedures designed to protect personal information and protected health information. AAWC is also taking steps to reduce the likelihood of a similar incident occurring in the future.

WHAT YOU CAN DO

We encourage you to remain vigilant by reviewing account statements, credit reports, medical bills, and explanation of benefits statements for suspicious activity. If you see charges, claims, services, or accounts that you do not recognize, you should promptly contact the financial institution, health insurer, health care provider, or other appropriate organization.

You may also consider placing a fraud alert or security freeze on your credit file. Information about these steps is included below.

ADDITIONAL INFORMATION

AAWC has established a dedicated call center to answer questions about this incident. The call center is available Monday through Thursday from 8:00 a.m. to 4:00 p.m. Mountain Time and can be reached at 303-316-1134.

You may also contact AAWC at:

AAWC
799 E. Hampden Ave, Suite 430

Englewood, CO 80113
info@allaboutwomenscare.com
allaboutwomenscare.com

AAWC deeply regrets any inconvenience or concern this incident may cause.

Sincerely,

AAWC

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Account Statements and Explanation of Benefits Statements

As a precautionary measure, you should remain vigilant by reviewing financial account statements, credit reports, medical bills, and health insurance explanations of benefits statements for suspicious activity. If you detect suspicious activity, promptly contact the financial institution, health insurer, health care provider, or other organization involved.

Report Suspicious Activity

If you believe you are the victim of identity theft or fraud, you should report the incident to local law enforcement, your state Attorney General, and the Federal Trade Commission.

Federal Trade Commission
IdentityTheft.gov
1 877 438 4338
600 Pennsylvania Avenue NW
Washington, DC 20580

You may also obtain information about identity theft, fraud alerts, and security freezes from the Federal Trade Commission at IdentityTheft.gov.

Credit Reports

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every twelve months by visiting AnnualCreditReport.com, calling 1-877-322-8228, or mailing a completed Annual Credit Report Request Form to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348

You may also contact the three major credit reporting agencies directly:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1 800 525 6285
equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1 888 397 3742
experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1 800 916 8800
transunion.com

Fraud Alerts

You may place a fraud alert on your credit file. A fraud alert tells creditors to take additional steps to verify your identity before opening a new account. An initial fraud alert is free and lasts at least one year. You may place a fraud alert by contacting any one of the three major credit reporting agencies. The agency you contact is required to notify the other two.

Security Freezes

You have the right to place a security freeze on your credit file at no cost. A security freeze helps prevent new credit from being opened in your name without your consent. You must separately place a security freeze with each of the three major credit reporting agencies.

To place a security freeze, you may be asked to provide identifying information, such as your full name, Social Security number, date of birth, current and previous addresses, a copy of a government issued identification card, and a recent utility bill, bank statement, or insurance statement.

Fair Credit Reporting Act Rights

You have rights under the Fair Credit Reporting Act. These rights include the right to know what is in your credit file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information.

For more information about your rights under the Fair Credit Reporting Act, visit consumer.ftc.gov.

Medical Identity Theft

Because this incident may have involved health information, you should also review medical bills, health insurance statements, and explanation of benefits statements for services you did not receive. If you see suspicious medical activity, contact your health insurer or health care provider immediately. You may also request a copy of your medical records if you are concerned that inaccurate information has been added to your records.