Walgreens
104 Wilmot Road
MS #3213
Deerfield, IL 60015

September 10, 2025

[redacted]

Dear [redacted]:

Walgreens values your privacy. We recently became aware of an IT incident that may have involved information about you and are writing to inform you of the details and steps you can take.

WHAT HAPPENED

On July 14, 2025, data stored with a Walgreens vendor was inadvertently disclosed to an unauthorized third party. This issue was discovered on the same date it occurred. While Walgreens cannot confirm that your information was specifically disclosed, we believe it is important to make you aware of this incident and potential compromise.

WHAT INFORMATION WAS INVOLVED

We would like to assure you that our investigation has determined that your credit/debit card number, banking information, driver's license number, and Social Security Number were NOT compromised. The information of yours that may have been involved includes one or more of the following data elements:

- First and last name
- Gender
- Address
- Phone number
- Date of birth and/or age
- Medication name
- Email address

WHAT WE ARE DOING

Upon learning of the potential compromise of information, Walgreens implemented enhanced technical and administrative security protections. Walgreens regularly evaluates its safeguards and will continue to do so.

WHAT YOU CAN DO

As always, stay alert and avoid phishing scams, which may appear through emails, text messages, or phone calls. Official communications from Walgreens about your account will always come from trusted domains that contain @walgreens.com, and you can securely access your information through the Walgreens website or mobile app. Remember that phishing messages often include urgent language, fake "free" offers, unexpected links or files, or unfamiliar email addresses. Walgreens will never contact you and ask you to provide online account information such as your password or verification code. For additional guidance on protecting yourself from fraud and scams, you can visit www.walgreens.com/topic/fraud_information.jsp.

Walgreens also recommends that you monitor your prescription and medical records. As a general matter, we recommend the following actions as good practices our customers can take to protect themselves from medical identity theft:

- Review your "explanation of benefits statement" which you get from your health insurance company. Follow up with your insurance company or care provider for any items you don't recognize.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow-up with your insurance company or care provider for any items you don't recognize.

Additionally, even though your financial information was not involved, we have enclosed information on steps you can take to further protect your information, and how to obtain a free copy of your credit report from each of the three (3) major credit reporting agencies as a courtesy for your reference.

FOR MORE INFORMATION

For further information and assistance, please contact Walgreens' toll-free number 1(877) 924-4472. You can also contact us in writing at 108 Wilmot Road, MS 3213, Deerfield, Illinois 60015.

We appreciate and value the confidence that you place in Walgreens. We take our obligation to protect your information very seriously. Please know we will continue to work diligently to protect your personal information.

Sincerely,

Natalie LaPorta

Natalie LaPorta
Chief Privacy Officer
Walgreen Co.

Walgreens

Additional Ways You Can Protect Your Information

Review Your Account Statements. It is important that you remain vigilant in reviewing your account statements and monitoring credit reports closely. Even though no financial information was involved in this incident, any time you detect suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, or the Federal Trade Commission. In some states, you may also obtain a police report regarding this incident.

Obtain and Monitor Your Credit Report. You have the right to obtain a free copy of your credit report from each of the 3 major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 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 http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf. Or you can elect to purchase a copy of your credit report and optional remediation services by contacting one of the three national credit reporting agencies shown below:

Equifax	**Experian**	**TransUnion**
(800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	(888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	(800) 916-8800 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report. You may consider placing a fraud alert on your credit report. This fraud alert statement informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Other Important Information

Security Freeze. In some U.S. states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, cell phone, or any service that requires a credit check. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift, or remove the security freeze; however, this fee may be less in certain states (in MA, there shall be no charge). In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. You must separately place a security freeze on your credit file with each credit reporting agency referenced above.

To place a credit freeze on your credit file, you may send a written request by regular, certified, or overnight mail to the addresses below. You may also place a credit freeze through each of the consumer reporting agencies' websites or over the phone using the contact information below:

Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045
https://www.equifax.com/personal/credit-report-services/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
https://www.transunion.com/credit-freeze

Take Advantage of Additional Free Resources on Identity Theft. In addition to credit reporting agencies, you can also contact the Federal Trade Commission (FTC) about fraud alerts and security freezes, as well as how to avoid or prevent identity theft. The FTC identity theft hotline number is: 1-877-ID-THEFT (877-438-4338); TTY: 1-866653-4261. They also provide information on-line at www.ftc.gov/idtheft, and their mailing address is 600 Pennsylvania Avenue, NW, Washington, DC 20580. The FTC encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.