



200 Wilmot Road
MS #9000
Deerfield, IL 60015

July 24, 2020

Name

Address

City, State Zip

Engagement Number: DB21435

Dear First Name Last Name:

We recently learned of a potential compromise of certain information about you located at a Walgreens store. We are contacting you to provide you with information about the incident and also with information about steps you can take to protect yourself.

WHAT HAPPENED

Sometime between May 26 and June 5, 2020, various groups of individuals broke into multiple Walgreens stores and forced entry into the secured pharmacy at select locations, including your preferred Walgreens. Among the many items stolen were certain items containing health-related information —such as filled prescriptions waiting for customer pick up and paper records.

Between May 26 and June 5, Walgreens discovered customer information was impacted. We later determined that one or more of the items described above may have contained your information. We wanted to alert you to this fact.

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 included one or more of the following data elements (where applicable):

- First and last name
- Address
- Phone number
- Date of birth and/or age
- Clinical information such as medication name, strength, quantity, and description
- Prescription number
- Prescriber name
- Health plan name and group number
- Vaccination information including eligibility information
- Email Address
- Balance Rewards Number

WHAT WE ARE DOING

Upon learning of the potential compromise of information, Walgreens promptly took steps to close out and re-enter impacted prescriptions in our system to prevent potential fraud regarding the original prescription. Insurance claims were also reversed for any stolen filled prescriptions that had already been billed to health



plans. Walgreens is coordinating with local law enforcement where appropriate. Further, Walgreens regularly evaluates its safeguards and will continue to do so.

WHAT YOU CAN DO

Walgreens recommends that you monitor your prescription and medical records. Further, 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 the 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 (866) 918-7267 (M-F 6 a.m. – 8 p.m. PDT & Sat/Sun 8 a.m. – 5 p.m. PDT). You can also contact us in writing at 200 Wilmot Road, MS 9000, Deerfield, Illinois 60015.

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

Sincerely,

A handwritten signature in black ink that reads "Rina Shah".

Rina Shah, PharmD
Vice President, Pharmacy Operations
Walgreen Co.



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:

<u>Equifax</u> (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	<u>Experian</u> (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	<u>TransUnion</u> (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.

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.

For North Carolina Residents: In addition to the FTC, you can also obtain information about preventing identity theft from your Attorney General by referring to the contact information resources below:

North Carolina Consumer Protection Division

Consumer Protection Division

Attorney General's Office

Mail Service Center 9001

Raleigh, NC 27699-9001

Toll-free within North Carolina 1-877-5-NO-SCAM

From outside North Carolina: (919) 716-6000

En Espanol: (919) 716-0058