

NOTICE OF DATA BREACH

Pharmaca announced today that it has taken measures to investigate and address a data security incident involving payment information for some customers who made purchases at certain Pharmaca retail locations between July 19, 2018 and December 12, 2018. Pharmaca immediately responded and has since secured its systems.

Importantly, this incident does not include medical records, prescription information, Social Security numbers, driver's license numbers, passport numbers, government identification numbers, or other sensitive information about Pharmaca's customers. This incident did not affect online purchases.

What Happened? After receiving reports of fraud related to a small number of customers from payment card issuers, Pharmaca began an investigation, and on or around December 6, 2018, identified suspicious code on its point-of-sale systems. Pharmaca immediately began working with leading security experts to help determine what happened. Through this investigation, Pharmaca confirmed, on or about December 19, 2018, that malicious code may have captured customer credit and debit card information used for purchases at certain Pharmaca stores between July 19, 2018 and December 12, 2018.

What Information Was Involved? Payment card information, such as credit or debit card number, expiration date, and other card data, may have been acquired. Names may also have been captured for customers making swipe transactions.

What We Are Doing. Information privacy and security are among our highest priorities, and we take this incident seriously. Once discovered, we quickly took steps to determine how the information may have been accessed and took action to ensure our systems were secure. Pharmaca's systems do not store customer names and addresses for credit card transactions. Pharmaca is notifying potentially impacted individuals by way of this notice, as well as by providing notice to certain state media outlets.

What You Can Do. Please review the "Steps You Can Take to Prevent Identity Theft and Fraud," below.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance please call our dedicated information line at 866-904-6220 from 6am to 6pm PST, Monday through Friday, and 8am to 5pm PST Saturday through Sunday.

Pharmaca takes the privacy and security of the personal information in our care seriously. We regret any concern or inconvenience this may have caused you.

Steps You Can Take to Prevent Identity Theft and Fraud

Monitor Your Accounts.

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Customers should immediately report any unauthorized charges to their card issuer. The phone number to call is usually on the back of the credit or debit card.

Pharmaca- Website Notice

Fraud Alerts and Security Freezes. At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. You can obtain more information about security freezes and fraud alerts by contacting the consumer reporting agencies, below:

Experian PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-916-8800 www.transunion.com/credit-freeze	Equifax PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services
---	---	---

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. **For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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. You can to review your 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.