



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Security Incident

Dear <<Name 1>>,

We are writing to inform you of a recent data security incident that may have involved your personal information. At Direct Scripts, we take the privacy and security of all of our customers' information very seriously and sincerely apologize for any inconvenience this incident may cause you. This letter contains information about steps you can take to protect your information and resources being made available to help you.

What Happened? On January 30, 2019, we learned that we had been the victim of a ransomware attack that affected our patient records. Ransomware is a type of malicious software that is used by cybercriminals to encrypt or lock up files on computers or servers and demand a ransom payment in order to restore access to the locked information. This ransomware attack locked the server that stored some of our patient information.

Immediately upon detecting the incident, we launched an investigation and engaged an independent forensics firm to assist in determining what happened and whether any individuals' protected health information ("PHI") had been accessed or acquired without authorization. While there is no evidence that any sensitive or personal information has been misused, we are notifying you out of an abundance of caution.

What Information Was Involved? The information potentially involved may include patient names, addresses, and prescription information. The impacted server did not and does not store patient Social Security numbers or credit card information.

What We Are Doing. As soon as we learned about the incident, we took the steps described above. In addition, we are providing you with information about steps you can take to help protect your information.

What You Can Do. While we do not believe any patient personal information was at risk, you can follow the recommendations included with this letter to protect your personal information. In addition, we are providing you with Automatic Identity Protection that includes \$25,000 of identity insurance and unlimited access to Identity Fraud, Inc. fraud resolution specialists to help resolve any type of identity theft or fraud.

For More Information. We remain committed to protecting your information. If you have questions or need assistance, please visit www.identityfraud.com/idprotect and/or call our dedicated call center toll-free at 1-866-443-3728, 8:00 a.m. to 5:00 p.m. Pacific, Monday through Friday.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause you.

Sincerely,

David Presper
Direct Scripts | President

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any 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, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three 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 this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion

P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Experian

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

Equifax

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

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert 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>.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

**North Carolina Attorney
General**

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island

Attorney General
150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your 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 the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.