July 28, 2021

Notice of Data Security Incident

On May 3, 2021, our management company, Neff Pharmacy Management, Inc. ("Neff"), became aware of a data security incident involving a Neff email account. On June 11, 2021, Neff learned that the incident may have exposed some personal health information of our current or former patients to unauthorized access. Please note that our computer systems and network were not involved in the incident.

On July 28, 2021, Neff mailed notifications to individuals whose personal health information could have been accessed without authorization as a result of the incident. Unfortunately, we did not have sufficient contact information to provide written notice to some individuals. With regard to those individuals for whom we did not have sufficient contact information, we are providing the following information concerning the incident, including a toll-free call center telephone number below. That number can be called to determine whether an individual's personal information was included in the email box that was impacted by this incident.

At this time, we have no indication that any of this data has been inappropriately used by anyone. We are providing this notice as a precautionary measure to inform potentially affected individuals of the incident and of protective steps that can be taken. We recommend that you closely review the information provided below for some steps that you may take to protect yourself against potential misuse of your information.

What Happened

On May 3, 2021, Neff learned that an unauthorized person had gained access to a Neff email account. As soon as Neff learned this, Neff immediately launched an investigation to understand what happened and, more importantly, prevent something like this from happening again. Neff also engaged legal counsel with an expertise in data privacy, who then hired a cybersecurity firm to assist with the investigation.

The investigation revealed that there had been unauthorized access to one Neff employee's email account beginning in January of 2021 through May 3, 2021. Based upon the results of the investigation, Neff determined that it was possible for the unauthorized individual to have accessed the contents of individual emails and email attachments within the account. Although no specific evidence was found that such access occurred, it could not be ruled out.

Because Neff could not determine whether actual access to emails occurred or what, if any, specific information may have been accessed, Neff reviewed the entire contents of the compromised email box in order to find out what information was in each email, who may have been affected, and, when possible, where those people resided in order to provide notification to potentially affected individuals. On June 11, 2021, Neff learned that the compromised email account contained personal health information.

What Information Was Involved

The affected data varied but, based upon the investigation, it may have included your personal health information such as name, address, date of birth, provider name, insurance or medical record number, diagnosis, and treatment or prescription information.

What We Are Doing About It

When Neff discovered this incident, Neff immediately disabled the affected email account and reset the password. To further enhance our security and help prevent similar occurrences in the future, Neff has taken or will be taking the following steps:

1. Closely monitoring and restricting outside access to its systems;
2. Increasing the complexity of passwords and the frequency of its password reset policy;
3. Adding two factor authentication to access its network;
4. Migrating all employee email accounts to a secure, self-hosted server;
5. Strengthening its firewalls and spam filtering to help block dangerous emails;
6. Updating its response procedures to more quickly and effectively respond to incidents; and
7. Providing additional cyber training to staff in order to increase cyber awareness.

In addition, consistent with our compliance obligations and responsibilities, notice of this incident is being provided to appropriate state and federal regulators.

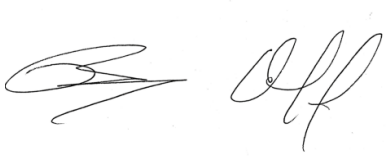
What Can You Do

Although we are not aware of any inappropriate use of your personal information, we recommend that you remain vigilant to the possibility of fraud and identity theft by monitoring your account statements and free credit reports for any unauthorized or suspicious activity. You should report any incidents of suspected identity theft to your local law enforcement, state Attorney General and the major credit bureaus.

If you did not receive written notice regarding this incident, but think that your information, or your relative's information, may have been included in the breach, please call our toll free hotline number 888-707-1586, Monday through Friday, from 8:00 a.m. to 4:30 pm EST. The hotline will be available through October 26, 2021.

We are very sorry this incident happened and for any inconvenience you may have experienced. The privacy and security of your information is very important to us and we remain committed to doing everything we can to maintain the confidentiality of your information.

Sincerely,



Barry Neff,
President

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

You also may request a security freeze be added to your credit report at Experian's online Freeze Center, www.experian.com/freeze/center.html, by phone at 1-888-EXPERIAN (1-888-397-3742), or by mail to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013. More information on a security freeze can be found below.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically, which can help spot and address problems quickly.

Fraud Alerts

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 new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place, you will need it if you choose to lift the freeze. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Helpful Information

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report with your local law enforcement agency and contact your Attorney General. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC at the information provided above.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.