

# CONIFER

HEALTH SOLUTIONS®

P.O Box 989728  
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zipcode>>

September 30, 2022

Su información personal puede haber estado involucrada en un incidente de datos. Si desea recibir una versión de esta carta en español, por favor llame 1-833-764-0238.

## **Notice of Data Breach**

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident that occurred at Conifer Revenue Cycle Solutions, LLC (“we” or “Conifer”) and may have affected your personal information. Conifer provides revenue cycle management and other administrative services to healthcare providers, including Keck Medicine of USC.

### **What happened?**

On April 14, 2022, we learned that an unauthorized third party gained access to a Microsoft Office 365-hosted business email account. Upon discovery, we immediately began an investigation and engaged a leading security firm.

In the course of the investigation, we learned that the unauthorized party was able to access the business email account at Conifer on January 20, 2022. This email account is separate from Conifer’s internal network and systems, which were not affected by this incident. Based on the investigation and a detailed review that was performed and ultimately completed on August 3, 2022, it was determined that your personal information associated with the healthcare provider listed above was in the impacted business email account. We notified your healthcare provider of this incident on August 12, 2022 and since then have worked with them to provide you this notice.

### **What information may have been involved?**

Even though Conifer conducted a thorough investigation, it was not possible to conclusively determine whether personal information was actually accessed by the unauthorized party. To date, we are not aware of any misuse of your data. The personal information in the impacted business email account may have included one or more of the following elements for you: (1) information to identify you (such as full name, date of birth, and address); (2) medical and/or treatment information (such as medical record number, provider name, diagnosis or symptom information, and prescription/medication); (3) health insurance information (such as payor name and subscriber/Medicare/Medicaid number); and (4) billing and claims information. Please note that not all data elements were present for all individuals. Your Social Security number, driver’s license number, and financial account information were not identified in the impacted business email account.

### **What we are doing.**

Conifer takes privacy and security very seriously. In response to this incident, we immediately took action to block malicious IP addresses and URLs. In addition, the password for the impacted account was reset shortly after the unauthorized access. We have enhanced and continue to enhance our security controls and monitoring practices as appropriate to minimize the risk of any similar incident in the future, and we accelerated our implementation of multi-factor authentication for business email accounts within the environment.

**What you can do.**

The enclosed Reference Guide includes information on general steps you can take to monitor and protect your personal information. Although we are unaware of any actual or attempted misuse of patient information as a result of this incident, we encourage you to carefully review credit reports and statements sent from providers as well as your insurance company to ensure that all account activity is valid. Any questionable charges should be promptly reported to the company with which you maintain the account.

**For more information**

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit <https://response.idx.us/crcs-information> or call toll-free 1-833-764-0238. This call center is open from 6 am – 6 pm Pacific Time, Monday through Friday, except holidays.

We sincerely regret that this incident occurred and apologize for any inconvenience this incident may have caused you.

Sincerely,

A handwritten signature in black ink, appearing to read "D Kellner". The signature is written in a cursive, slightly slanted style.

Dustin Kellner  
Conifer Privacy Office

## **Reference Guide**

### **Review Your Account Statements**

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the company with which you maintain the account.

### **Provide Any Updated Personal Information to Your Health Care Provider**

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

### **Order Your Free Credit Report**

To order your free annual credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at [www.ftc.gov](http://www.ftc.gov) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

### **Contact the U.S. Federal Trade Commission**

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/)

### **Place a Fraud Alert on Your Credit File**

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can

place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	1- 888-766-0008	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	P.O. Box 9554 Allen, Texas 75013	1-888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

### **Security Freezes**

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. 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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111	<a href="http://www.equifax.com">www.equifax.com</a>
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	<a href="http://www.transunion.com">www.transunion.com</a>

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

### **For Residents of North Carolina**

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, [www.ncdoj.gov](http://www.ncdoj.gov).

### **For Residents of Massachusetts**

You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.