CONIFER
HEALTH SOLUTIONS®
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Middle Name>> <<Last Name>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

December 18, 2025

Notice of Data Breach

Dear <<First Name>> <<Middle Name>> <<Last Name>> <<Suffix>>:

Conifer Value-Based Care, LLC ("Conifer" or "we") is writing to inform you about a recent data security incident that may have affected your personal information. We provide certain administrative services to healthcare providers and plans. Our providers and plans include <<Variable Text: Client>>, from where you may have received services or paid for another person's services. We are committed to protecting your information. This commitment includes notifying you if we believe that an incident may have involved your personal information. This letter provides information about the incident and resources available to you.

What happened?

On August 28, 2025, we learned that an unauthorized third party gained access to an employee's Microsoft Office 365-hosted business email account. Upon discovery, we took immediate steps to contain the threat and launched an investigation. Conifer has determined that an unauthorized third party was able to access the business email account on August 28, 2025 and August 29, 2025. This email account is separate from Conifer's internal network and systems, which were not affected by this incident.

Conifer performed a comprehensive review to identify individuals affected by the incident and the organization to which they belong. This review was completed on November 10, 2025, and we notified your provider or health plan of the incident on November 14, 2025. We have since worked with your provider or health plan to locate and verify addresses for potentially affected individuals, where possible, which was completed on December 5, 2025.

What information may have been involved?

The personal information involved may have included one or more of the following elements: <<Variable Text: Data Elements>> Please note that not all data elements were involved for each individual. ***Your Social Security number, driver's license or state ID number, credit and debit card information, financial account information, and account passwords were not involved in this incident.***

Additionally, some of this information may relate to guarantors. A guarantor is a person who agrees to pay the bill for health care services but is not the patient.

What we are doing.

Conifer takes privacy and security very seriously. As soon as we discovered the incident, we immediately took action to mitigate and remediate the incident and to help prevent further unauthorized activity. We continue to enhance our security controls and monitoring practices as appropriate to minimize the risk of any similar incident in the future.

What you can do.

While we are not aware of any misuse of individuals' information as a result of this incident to date, the enclosed Reference Guide includes steps you can take to monitor and help protect your personal information. We encourage you to carefully review statements sent from healthcare providers and insurance companies to ensure that all account activity is valid. Any questionable charges should be promptly reported to the provider or company with which the account is maintained.

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/VBCevent2025, or call toll-free 1-833-781-8318. This call center is open from 6 am – 6 pm Pacific Time, Monday through Friday, except holidays.

We deeply regret any concern this incident may cause and want to assure you that we take this matter seriously.

Sincerely,

Conifer Privacy Officer

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 provider or 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 to 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, 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 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 following contact information: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); 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, GA 30348	1-888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

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	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	www.transunion.com

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 5 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.

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.

Oregon

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us.

CONIFER
HEALTH SOLUTIONS®
P.O. Box 989728
West Sacramento, CA 95798-9728

Parent or Legal Guardian of
<<First Name>> <<Middle Name>> <<Last Name>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

December 18, 2025

Notice of Data Breach

Dear Parent or Legal Guardian of <<First Name>> <<Middle Name>> <<Last Name>> <<Suffix>>:

Conifer Value-Based Care, LLC ("Conifer" or "we") is writing to inform you about a recent data security incident that may have affected your child's personal information. We provide certain administrative services to healthcare providers and plans. Our providers and plans include <<Variable Text: Client>>, from where your child may have received services. We are committed to protecting your child's information. This commitment includes notifying you if we believe that an incident may have involved your child's personal information. This letter provides information about the incident and resources available to you.

What happened?

On August 28, 2025, we learned that an unauthorized third party gained access to an employee's Microsoft Office 365-hosted business email account. Upon discovery, we took immediate steps to contain the threat and launched an investigation. Conifer has determined that an unauthorized third party was able to access the business email account on August 28, 2025 and August 29, 2025. This email account is separate from Conifer's internal network and systems, which were not affected by this incident.

Conifer performed a comprehensive review to identify individuals affected by the incident and the organization to which they belong. This review was completed on November 10, 2025, and we notified your child's provider or health plan of the incident on November 14, 2025. We have since worked with your child's provider or health plan to locate and verify addresses for potentially affected individuals, where possible, which was completed on December 5, 2025.

What information may have been involved?

The personal information involved may have included one or more of the following elements: <<Variable Text: Data Elements>> Please note that not all data elements were involved for each individual. ***Your child's Social Security number, driver's license or state ID number, credit and debit card information, financial account information, and account passwords were not involved in this incident.***

Additionally, some of this information may relate to guarantors. A guarantor is a person who agrees to pay the bill for health care services but is not the patient.

What we are doing.

Conifer takes privacy and security very seriously. As soon as we discovered the incident, we immediately took action to mitigate and remediate the incident and to help prevent further unauthorized activity. We continue to enhance our security controls and monitoring practices as appropriate to minimize the risk of any similar incident in the future.

What you can do.

While we are not aware of any misuse of individuals' information as a result of this incident to date, the enclosed Reference Guide includes steps you can take to monitor and help protect your child's personal information. We encourage you to carefully review statements sent from healthcare providers and insurance companies to ensure that all account activity is valid. Any questionable charges should be promptly reported to the provider or company with which the account is maintained.

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/VBCevent2025, or call toll-free 1-833-781-8318. This call center is open from 6 am – 6 pm Pacific Time, Monday through Friday, except holidays.

We deeply regret any concern this incident may cause and want to assure you that we take this matter seriously.

Sincerely,

Conifer Privacy Officer

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 provider or 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 to 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, 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 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 following contact information: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); 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, GA 30348	1-888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

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	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	www.transunion.com

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 5 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.