Premise Health

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

November 6, 2026

Q5975-L03-0000003 P001 T00001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L03 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Notice of Data Breach

Dear Sample A. Sample:

We are writing to let you know about a data security incident that affected some of your personal information. We take the protection of your information very seriously and are contacting you to explain the circumstances of this situation, including the steps we have taken, and continue to take, in response, and the resources we are making available to you.

What Happened?

On September 18, 2026, Premise Health Holding Corp. ("Premise Health") discovered that an employee had violated company information security policies and misappropriated certain company data beginning on or about March 26, 2026. Upon discovery, we took immediate action to revoke the employee's credentials and system access, validate our security controls, and investigate the incident. On October 14, 2026, we received a preliminary analysis of the relevant data. Following further analysis and validation of the results, we are now reaching out to you to let you know that the incident involved some of your personal information.

What Information Was Involved?

Relevant personal information included, in part or whole, your name, address, date of birth, government identification number such as Social Security number, health insurance information, diagnostic or other treatment information and other information provided to us in connection with your eligibility for services with or relationship with Premise Health. We are not aware of any misuse of your personal information.

What We Are Doing.

As mentioned above, upon discovery, we took prompt steps to revoke the employee's credentials and system access, validate our security controls, and investigate the matter. The employee has been terminated. We have also reported the incident to law enforcement. We continue to monitor our systems and have introduced additional measures to further enhance our security defenses.

ENGAGE#A, ENGAGE#M

Premise Health

What You Can Do.

You can remain vigilant by reviewing your personal records and monitoring free credit reports, which is described later in this letter. In addition, we are sharing with you common steps you may take to guard against potential identity theft or fraud. Please review the enclosed "Important Identity Theft Information" for information about what you can do.

To help protect your, or your minor dependent's (if they are the recipient of this letter), identity, we are offering complimentary access to Experian IdentityWorks℠ for ## months.

If you believe there was fraudulent use of your, or your minor dependent's (if they are the recipient of this letter), information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your, or your minor dependent's (if they are the recipient of this letter), personal information, please follow the steps below:

Ensure that you enroll by February 26, 2027, at 11:59 p.m. UTC. (Your activation code will not work after this date.) Determine the appropriate enrollment option:

If the recipient is a minor under the age of 18:

- Visit: **https://www.experianidworks.com/minorplus**
- Activation Code: **MINOR_CODE**

If the recipient is an adult age 18 or older (including adult dependents):

- Visit: **https://www.experianidworks.com/1Bcredit**
- Activation Code: **ADULT_CODE**

Important: If you are enrolling a minor, you will be prompted to provide the minor's information during the enrollment process.

ENGAGE#A, ENGAGE#M

5500 Maryland Way #120
Brentwood, TN 37027
P: 844.407-7557
premisehealth.com

Premise Health

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by February 26, 2027, at ###-###-#### Monday – Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide engagement number, ENGAGE#M for minors and ENGAGE#A for adults, as proof of eligibility for the Identity Restoration services by Experian.

Si necesita asistencia o tiene preguntas sobre este aviso en otro idioma, incluido el español, puede comunicarse con nuestro centro de atención telefónica al ###-###-####. Estamos disponibles de lunes a viernes, de 8:00 a. m. a 8:00 p. m. (hora del centro), excepto los días principales festivos de EE. UU.

Additional Details Regarding Your ##-Month Experian IdentityWorks Membership

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

If a dependent minor is the recipient of this letter:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.

If an adult 18 or older is the recipient of this letter:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*

If a dependent minor or an adult 18 or older is the recipient of this letter:

- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information.

If you have questions, please call ###-###-####, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays. Please have your engagement number, ENGAGE#M for minors and ENGAGE#A for adults, ready.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ENGAGE#A, ENGAGE#M

5500 Maryland Way #120
Brentwood, TN 37027
P: 844.407-7557
premisehealth.com

Premise Health

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity.

Reviewing Your Accounts and Credit Reports

Federal regulators recommend that you be especially vigilant for the next 12 to 24 months and that you promptly report incidents of suspected identity theft to your financial institution. As part of staying vigilant, you should regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are also available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report. If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge. If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting agency. The credit reporting companies do not notify each other about security freezes.

ENGAGE#A, ENGAGE#M

Premise Health

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you with a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze, and should be careful to record it somewhere secure.

For loved ones who may have recently passed away, individuals may also place a "deceased – do not issue credit" flag on the loved one's credit file. You need only notify one of the consumer reporting bureaus, which will take steps to notify the other two major credit reporting companies. More information on this process is available at the below websites:

Equifax: https://www.equifax.com/personal/help/article-list/-/h/a/relative-death-contact-credit-bureaus
Experian: https://www.experian.com/blogs/ask-experian/reporting-death-of-relative/
TransUnion: https://www.transunion.com/blog/credit-advice/reporting-a-death-to-tu

Suggestions if You Are a Victim of Identity Theft
If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the police report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877- IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, DC 20580.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; dispute incomplete or inaccurate information; and have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-march-2026.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

5500 Maryland Way #120
Brentwood, TN 37027
P: 844.407-7557
premisehealth.com

Premise Health

Special Information for Residents of the District of Columbia, Iowa, Maryland, Massachusetts, New Mexico, New York, North Carolina, Oregon, Rhode Island, and Vermont.

District of Columbia residents can learn more about preventing identity theft from the District of Columbia Office of the Attorney General, by visiting the website at https://oag.dc.gov/, calling 1-202-727-3400, or requesting more information via email at oag@dc.gov or mail at 400 6th Street, N.W., Washington, DC 20001.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling 1-515-281-5164, or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting the website at https://oag.maryland.gov/i-need-to/Pages/identity-theft-information.aspx, calling the Identity Theft Unit at 1-410-576-6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting company with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to the credit reporting company honoring your request.

New Mexico residents have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the credit reporting companies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. In addition to those listed above, we encourage consumers to review their 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 to the Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, DC 20580.

New York residents may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the New York State Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; telephone: 1-800-771-7755.

ENGAGE#A, ENGAGE#M

5500 Maryland Way #120
Brentwood, TN 37027
P: 844.407-7557
premisehealth.com

Premise Health

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their website at https://ncdoj.gov/protecting-consumers/protecting-your-identity/, calling 1-919-716-6400, or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling 1-503-378-4400, or requesting more information from the Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1-401-274-4400, through their website at https://riag.ri.gov/, or by mail at 150 South Main Street, Providence, RI 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at https://ago.vermont.gov/.

5500 Maryland Way #120
Brentwood, TN 37027
P: 844.407-7557
premisehealth.com