

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

<<Name 1>> <<Name 2>>
<<Address 1>> <<Address 2>>
<<City>><<State>><<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

December 30, 2024

NOTICE OF DATA BREACH

Dear <<Name 1>> <<Name 2>>:

Assurity Life Insurance Company (“Assurity”) values our customer relationships and the trust you place in us. We take seriously the obligation to safeguard our customers’ sensitive personal information. Unfortunately, Assurity recently experienced a cybersecurity incident that impacts some of our customers’ personally identifiable information (“PII”). The purpose of this letter is to tell you what happened, what information was involved, what we are doing in response to this incident, and steps you can take to protect your information against possible misuse.

What Happened

On November 18, 2024 Assurity suffered a cybersecurity incident when a single employee’s email account was accessed as the result of a phishing attack. We immediately began an investigation and conducted a review to determine what information was potentially exposed. Our investigation confirmed unauthorized access by an attacker to a single employee’s email account between approximately November 18, 2024 and November 19, 2024, which provided the attacker access to information in the account. It is not possible to determine which emails or attachments were viewed by the attacker. It is important to note that this incident was very limited in scope and did not affect Assurity’s internal systems or our ability to operate.

What Information was Involved

The emails to which the attacker had access were manually reviewed, and the review determined that information in these emails included your PII in an attachment to an email, such as in a spreadsheet or a PDF file. Information that may have been accessed includes full name, demographic information (such as address and date of birth), and Social Security number.

What We Are Doing

After learning of the attack, Assurity took important steps to prevent a similar incident from occurring in the future. Those steps include access protocol auditing enhanced monitoring, and new alert protocols.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance

reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to remain vigilant and review your credit reports and financial statements, and promptly report any suspicious activity. Please know you can contact local law enforcement to report any fraudulent activity you may discover.

We also encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling (833) 903-3648 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is March 30, 2025.

Again, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call (833) 903-3648 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

We apologize for this incident and any inconvenience or concern it may have caused. We take seriously the obligation to safeguard our customers' sensitive personal information and strive continually to improve our defenses against attackers.

Sincerely,

Susan L. Keisler-Munro

Susan L. Keisler-Munro
President / Chief Executive Officer
Assurity



Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies.

The Federal Trade Commission: Encourages those who discover that their information has been misused to file a complaint with them at www.identitytheft.gov or at 1-877-ID-THEFT (1-877-438- 4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Also visit the FTC's website at www.ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide "Identity Theft - A Recovery Plan".

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Missouri Residents: Consumers should report suspected incidents of identity theft to local law enforcement or the Missouri Attorney General at the Office of the Attorney General of Missouri, Supreme Court Building 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, <https://ago.mo.gov/>, Telephone: 573-751-3321. All recipients of this letter should remain vigilant by reviewing account statements and monitoring free credit reports.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.