

Standard Insurance Company
900 SW Fifth Avenue
Portland, OR 97204

May 26, 2023

Office of the Attorney General
ATTN: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Standard Insurance Company – Security Incident Notification

To whom it may concern,

Standard Insurance Company (The Standard) values the privacy and security of our customers' personal information. Regrettably, we are writing to notify you of an incident involving Maryland residents' personal information. This letter explains the incident and the measures we have taken in response.

What happened?

On April 25, 2023, The Standard's information security teams detected unauthorized access to several employee email accounts as a result of spear phishing. Our information security teams immediately reset the employees' credentials, terminated all active sessions and began an investigation, which determined the incident originated from a spear phishing email an employee received on April 20, 2023, from the legitimate email address of a former client. The Standard uses multi-factor authentication for email access; however, the unidentified third party utilized a method known as an "Attacker in The Middle Attack" to intercept the user's sign-in session, and skipped the authentication process. The unauthorized access to the email accounts occurred intermittently between April 20 and April 25, 2023. The Standard began a comprehensive review of emails and attachments within the accounts that were potentially subject to unauthorized access to identify the information involved and to whom it related.

On May 9, 2023, the investigation identified that Maryland residents' information was contained within an email or attachment.

What information was involved?

The potentially accessed information included name and Social Security number and may have included one or more of the following: sex, address, email address, date of birth, insurance carrier, salary information, member ID number, policyholder name, employer name and policy number. It is important to note that we have no indication that this information has been misused.

What we are doing:

Our information security teams successfully contained the incident. They have since implemented features that strengthen prevention controls and enhance detection capabilities. Remedial and additional training is planned for The Standard's employees.

The Standard is providing notification to the affected Maryland residents, and has secured the services of IDExperts to provide 24 months of credit monitoring and identity protection services at no cost to Maryland residents. A sample notification letter is enclosed below.

Who was affected?

Notification is being provided to **4** potentially affected Maryland residents.

For more information:

If you have questions, please contact me at (971) 321-2086.

Sincerely,

A handwritten signature in black ink that reads "Elizabeth A. Fouts". The signature is written in a cursive, flowing style.

Elizabeth A. Fouts

VP, Chief Legal Officer & Corporate Secretary
The Standard

(enclosure)



4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

To Enroll, Please Call:

1-800-939-4170

Or Visit:

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

Enrollment Code:

<<XXXXXXXX>>

<<First Name>> <<Last Name>>

<<Address1>> <<Address2>>

<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

The privacy and security of your data is vital to Standard Insurance Company (The Standard). Regrettably, we are writing to tell you about a recent phishing incident at The Standard that may have involved some of your personal information. This letter explains the incident, the measures we have taken and the steps you can take in response.

What Happened

On April 25, 2023, The Standard's information security teams detected unauthorized access to several employee email accounts as the result of a spear phishing campaign. Our information security teams immediately began an investigation and promptly contained the incident. The investigation revealed that the incident originated from a spear phishing email an employee received on April 20, 2023, from a trusted source.

What Information Was Involved

The potentially accessed information included your name and Social Security number and may have included one or more of the following: sex, address, email address, date of birth, insurance carrier, salary information, member ID number, policyholder name, employer name and policy number. It is important to note that we have no indication that this information has been misused.

What We Are Doing

The safety and security of our customers' information are among The Standard's top priorities. We have put additional controls in place to help prevent a future occurrence — including strengthened prevention, enhanced detection, and additional security measures.

In addition, we are offering identity theft protection services through IDX, a ZeroFox Company, a data breach and recovery services expert. IDX identity protection services include: 24 months of Tri-Bureau 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 contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 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 6 a.m.-6 p.m. Pacific Time. Please note the deadline to enroll is [Enrollment Deadline].

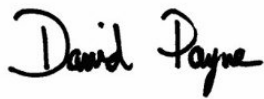
Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives are knowledgeable about the incident and can answer questions or concerns you may have regarding protection of your personal 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 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink that reads "David Payne". The signature is written in a cursive, flowing style.

David Payne | Vice President,
Employee Benefits
Standard Insurance Company

(Enclosure)



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 1-800-939-4170 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:

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 also encourages those who discover that their information has been misused to file a complaint with them.

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.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your 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 Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

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: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

Washington, D.C. Residents: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001, www.oag.dc.gov, Telephone: 202-347-8922.

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.