Notice of Cybersecurity Incident

Palomar
INSURANCE

20595

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<last_name>>,

Out of an abundance of caution, we are writing to inform you of a recent cybersecurity incident which affected Palomar Insurance Agency ("Palomar"). The cybersecurity incident may have resulted in the potential compromise of some of your data. This letter contains information about the incident and information about how to protect your personal information going forward. Palomar considers the protection of sensitive information a top priority, and sincerely apologizes for any inconvenience as a result of the incident.

What Happened

Palomar has been providing effective, tailored insurance programs to companies and individuals since its founding in 1954. Unfortunately, on or about November 6, 2020, an unauthorized individual gained access to a Palomar employee's business email account. Upon detecting the unauthorized individual on or about November 18, 2020, Palomar immediately terminated the individual's access and initiated an investigation to determine the nature and scope of the Incident.

Shortly thereafter, Palomar engaged a specialized cybersecurity firm to conduct an investigation to determine the nature and scope of the Incident. This investigation concluded on or about December 9, 2020. Palomar then engaged a data mining vendor to examine the contents of the inbox and to compile the results in the form of a data file. We received this notice list on or about April 9, 2021. Based on this list, Palomar procured credit monitoring for affected individuals, and drafted notices to individuals, consumer credit reporting agencies, and state regulators as appropriate.

What Information Was Involved

While we have no reason to believe that your information has been misused as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the unauthorized individual may have had access to one or more of the following data elements: name, contact information, date of birth, Social Security number, driver's license number, payment card information, and/or financial account information. Please note that not every data element was present for every individual. While we appreciate that the incident may be concerning, please note that Palomar is not aware of any instances of misuse of sensitive data.

What We Are Doing

Palomar engaged a specialized cybersecurity firm to conduct an investigation of the incident. Since the incident, Palomar has greatly enhanced its security, including by changing passwords, implementing multi-factor authentication, and disabling less secure email protocols to ensure that such an incident does not happen again. Additionally, we have also obtained complimentary credit monitoring for all affected individuals. We encourage you to take advantage of the complimentary credit monitoring services.

What You Can Do

We recommend that you continue to remain vigilant in monitoring your personal information. The easiest way to do this is to take advantage of the complimentary identity monitoring services we are offering to you. Details regarding these services are included in a separate attachment to this letter.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **September 5, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

There are additional steps you can take to protect yourself which are contained in the supplement to this letter titled "*Additional Important Information.*"

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause. If you have any questions, please do not hesitate to call 334-409-3227 Monday through Friday, between 8:00 AM and 5:00 PM Central time.

Sincerely,

Sonya Dalrymple Berryman, CISR
Senior Vice President, Insurance Services
Palomar Insurance

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fair Credit Reporting Act: You are also advised that you may have additional rights under the federal Fair Credit Reporting Act.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
(800)-525-6285
https://www.equifax.com/personal/credit-report-services/credit-freeze/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
(888)-397-3742
www.experian.com/freeze

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
(800)-680-7289
freeze.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.