



Relation Insurance Services

9225 Indian Creek Parkway, Suite 700, Overland Park, Kansas 66210

<<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>> <<middle_name>> <<last_name>> <<suffix>>,

Relation Insurance, Inc. ("Relation") is an insurance broker providing services to its business partners, including your health insurance carrier and writes to notify you of an incident that may affect the privacy of some of your personal and protected health information. Relation takes the protection of your information very seriously, and although we have no evidence of actual or attempted misuse of your information potentially affected by this incident, this letter provides details of the incident, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? On August 15, 2019, Relation became aware of unusual activity in an employee's email account. We immediately secured the employee's email account and launched an investigation, with the assistance of a third-party computer forensics expert, to determine what may have happened and what information may have been affected. Our investigation determined that an unknown individual had access to the email account between August 14th and August 15th of 2019. We then undertook a comprehensive review of emails that were present in the account at the time of the incident to identify what personal information was stored within the emails and to whom that information relates. On October 16, 2019, Relation confirmed personal information was present in the email account and began review of its files to determine which business partners and individuals were associated with this information. On December 13, 2019, Relation provided notice of this incident to your health insurance carrier. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notification out of an abundance of caution because your information was present in the email account.

What Information Was Involved? The information present in the email account at the time of the incident may have included your first and last name and the following identifiers: <<b2b_text_3(impacted data)>>.

What Are We Doing? Information privacy and security are among our highest priorities. Relation has strict security measures in place to protect information in our care. Upon discovering this incident, we immediately took steps to confirm the security of our systems, including our employee email accounts. We reviewed existing security policies and implemented additional measures to further protect information, including enhanced email security. We also reported this incident to law enforcement. In an abundance of caution, we are notifying potentially impacted individuals, including you, so that you may take steps to best protect your information, should you feel it is appropriate to do so. Although we are unaware of any actual or attempted misuse of information as a result of this incident, we arranged to have Kroll to provide identity monitoring for one (1) year, at no cost to you, as an added precaution.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You may review the information contained in the attached "Steps You Can Take to Help Protect Your Information." You may also activate the identity monitoring services we are making available to you. There is no charge to you for the cost of this service; however, you will need to activate this service.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-844-902-2034 (toll free), Monday through Friday, 9:00 a.m. to 6:30 p.m., ET.

We sincerely regret any inconvenience this incident may cause you. Protecting your information is important to us, and Relation remains committed to safeguarding the information in our care.

Sincerely,

A handwritten signature in black ink, appearing to read "Edward Nathan Page". The signature is fluid and cursive, written in a professional style.

Edward Nathan Page
President
Relation Insurance, Inc.

Steps You Can Take to Help Protect Your Information

Activate Your Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one (1) year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit enroll.idheadquarters.com to activate and take advantage of your identity monitoring services.

*You have until **May 4, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Monitor Accounts, Financial, and Medical Billing Statements

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, medical bills, explanation of benefits (EOBs), and credit reports for suspicious charges or claims. Under U.S. law you are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three (3) major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160

Woodlyn, PA 19094

1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000

Chester, PA 19106

1-800-680-7289

www.transunion.com/fraud-alerts

Equifax

P.O. Box 105069

Atlanta, GA 30348

1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For 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; and <https://ag.ny.gov/>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ 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'll have the option to call a Kroll fraud specialist, who can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ 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.