



Lawyers since 1897

Ryan, Swanson & Cleveland, PLLC
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3034
www.ryanswansonlaw.com

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

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

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a data security incident experienced by Ryan, Swanson & Cleveland, PLLC (“RSC”) that may have affected your personal information. At RSC, we take the privacy and security of personal information very seriously. This letter contains information about the incident and steps you can take to protect your personal information.

What Happened? On or around January 21, 2021, RSC learned of unusual activity within our email system. Upon learning of this activity, we took steps to secure our digital environment and began an investigation to determine what happened. In so doing, RSC engaged independent cyber experts to determine what happened and whether personal information may have been accessed or acquired without authorization. The investigation revealed that one RSC email account had been accessed without authorization. On March 18, 2021, RSC learned that messages and attachments contained within the accessed email account included some of your personal information. Though RSC has no evidence that anyone’s information has been misused as a result of this incident, we are providing you notification and information about steps you can take to protect your personal information out of an abundance of caution.

What Information Was Involved? Based on our investigation, the potentially impacted information may include your <<b2b_text_1(DataElements)>>.

What We Are Doing. As soon as we discovered the incident, we took the steps discussed above. In addition, we have taken affirmative steps to minimize the likelihood of a similar incident occurring in the future. This includes working with leading cybersecurity experts to enhance the security of our digital environment. Additionally, in an abundance of caution, we have arranged for you to activate, at no cost to you, in an identity monitoring service for one year provided by Kroll. Instructions to activate the complimentary One-Year Identity Monitoring Service are included here.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

*You have until **July 15, 2021** to activate your identity monitoring services.*

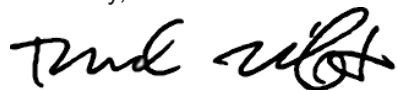
Membership Number: <<Member ID>>

What You Can Do. 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. You can also follow the recommendations included on the following pages to help protect your personal information.

For More Information: If you have questions, please call 1-855-930-6223, Monday through Friday from 6:00 a.m. – 3:30 p.m. Pacific Standard Time. Kroll representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

We remain committed to protecting your personal information and apologize for any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "David L. Tift". The signature is fluid and cursive, with the first name "David" and last name "Tift" clearly distinguishable.

David L. Tift
Member and Managing Director
Ryan, Swanson & Cleveland, PLLC

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



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.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.