
To the Office of the Attorney General,

By way of this email, and on behalf of our client Red Tortoise, LLC, I am providing the Office of Attorney General notification that Red Tortoise experienced a data security event that has impacted one Maryland resident. This email intrusion event of undetermined origin started on December 30, 2023, and was discovered and mitigated on January 26, 2024. Red Tortoise has undertaken and continues to undertake actions to address the breach, including the retention of a computer forensics expert, enhancements to its Microsoft 365 platform, and the planned addition of managed detection software on all Red Tortoise devices. Red Tortoise has also undertaken a review of its data security policies and procedures in order to augment and strengthen its security environment.

Finally, please see attached form of notice that will be sent to the affected individual.

If you have any questions about this event and related notice, please do not hesitate to reach out to me.

Regards,

Julie Engbloom

Partner

503-546-0675

1500 SW First Ave

Suite 1020

Portland, OR 97201

www.ttlawgroup.com





Date: [February __, 2024]

<<Name>>

<<Address>>

Dear [Name],

We are writing to inform you of a data security incident that may have involved your personal information. There is currently no definitive evidence that your personal information has been accessed or misused as a result of this incident. Out of an abundance of caution we are providing you with information about this event and the steps taken since discovering the incident. The privacy and security of your personal information is important to us and it is why we are informing you about this incident and providing you with information relating to steps you can take to help protect your information.

What Happened? On January 26th, Red Tortoise, LLC (“Red Tortoise”) became aware of unusual activity in one of our email accounts. As soon as we discovered this activity, we immediately initiated an investigation to determine what happened and what information may have been affected. With the assistance of computer forensics experts, Red Tortoise learned that its Microsoft 365 platform experienced an intrusion of unknown origin, which resulted in unauthorized use of two Red Tortoise email accounts from December 30, 2023, to January 26, 2024.

What Information Was Involved? Although to date, we are unaware of any actual or attempted misuse of your personally identifiable information, we are notifying you in an abundance of caution because your information may have been present in an impacted email account at the time of the incident.

We cannot confirm that your information was actually accessed by the unauthorized individual. However, our investigation indicates that your name, date of birth, social security numbers and/or financial account numbers may have been present in the impacted email accounts and/or files at the time of the incident.

To understand the scope of the breach, it may be helpful to understand that our Microsoft system is separate from the platforms associated with Charles Schwab, Fidelity, Interactive Brokers, Black Diamond (our portfolio accounting system), Right Capital (our financial planning system), and Red Tail (our contact management system). These each have distinct credentials. We have no reason to believe the threat actor has been able to access any of these separate systems.

What Are We Doing? As mentioned, we engaged a leading cybersecurity firm to determine the extent of the breach. We have already taken steps to strengthen our defenses and are seeking advice from cybersecurity experts to further protect our environment,

which includes enhancements to our Microsoft 365 platform and adding managed detection software to all Red Tortoise devices. Besides hardening our system, we are looking to reduce and compartmentalize the sensitive information we retain.

Information privacy and security are among our highest priorities. Red Tortoise has strict security measures in place to protect information in our care. Upon learning of this incident, we took steps to confirm the security of our systems, including our email accounts. Red Tortoise reset the passwords for all email and Microsoft accounts, implemented increased security protocols for account access, and implemented increased internal security measures. As a precautionary matter, law enforcement was also notified of this incident. We have also arranged for you to enroll, at no cost to you, in an online credit and ID monitoring service for 2 years provided by Kroll, a leader in risk solutions. Because we want you to feel secure, this offer includes triple credit bureau monitoring, a credit report, a service to watch for your data on the web, plus insurance. More information on how to enroll in this service is enclosed.

What You Can Do: You can follow the recommendations on the following pages to protect your personal information. We suggest using long and unique passwords for important accounts (and a password manager when possible), employing two-factor authentication, and pre-emptively freezing your credit and only unfreezing it when necessary. We also remind you to remain vigilant to guard against data security intrusion and identify theft by closely monitoring your financial records and statements and credit reports.

For More Information: We understand you may have questions about this incident that are not addressed in this letter. If you have questions about this incident, please contact us or call us toll-free at 833-666-1200 ext. 4, Monday through Friday, 9:00 a.m. to 5:00 pm. ET.

We take this matter very seriously and sincerely regret any worry or inconvenience that this may cause you.

Yours truly,

Rex Macey

Chief Executive Officer

How to Activate Your Identity Monitoring Services (via Kroll)

1. Visit **Enroll.krollmonitoring.com/redeem** to activate your identity monitoring services.
1. Provide Your Activation Code: <<XXXX>> and Your Verification ID: <<XXXX>>
2. Duration: 2 years
3. You must activate your identity monitoring services by <<Enter Activation Deadline>>. Your Activation Code will not work after this date.



We have secured the services of Kroll to provide identity monitoring at no cost to you two years. 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 services¹ include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services¹ from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$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 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.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge.

You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.