

June 2, 2023

<<First Name Last Name>>

<<Address>>

<<City, State Zip Code>>

Re: Notice of Breach of Protected Health Information

Dear <<First Name>>,

EyeMed Vision Care, LLC ("EyeMed") manages the vision benefits for T. Rowe Price Group, Inc. ("we" and "our") as part of our flexible benefits plan. You had, and still may have, vision benefits through our flexible benefits plan. In 2020, you were notified by EyeMed about a data security incident that involved some of your Protected Health Information ("PHI") maintained by EyeMed.

On April 5th, 2023, EyeMed informed us that in connection with the 2020 data security incident, EyeMed had hired a law firm, Orrick, Herrington & Sutcliffe, LLP ("Orrick"), to assist it with responding to the incident. As part of this communication, EyeMed also informed us that Orrick recently experienced a data security incident that has resulted in a breach of your PHI. We regret that this incident occurred and are working with EyeMed to ensure appropriate actions are taken to safeguard PHI.

Accordingly, we are providing you this letter in accordance with federal law (45 CFR § 164.404) in order to explain the data security incident at Orrick, the measures that are being taken, and steps you can take in response.

What happened?

Orrick has stated that on March 13th, 2023, it detected that an unauthorized third party gained remote access to a portion of its network, including an area it used to store certain client files. Upon detection, Orrick took steps to block the unauthorized access, launch an investigation with the assistance of outside cybersecurity specialists, and inform law enforcement. Orrick determined that on March 7th, 2023, the unauthorized third party had obtained files of its client, EyeMed, which included your PHI. Orrick informed EyeMed on April 3rd and EyeMed informed us on April 5th.

What information was involved?

The PHI obtained as part of Orrick's data security incident included your name, <<variable data elements>>.

What is being done in response?

Orrick is offering persons whose PHI was affected two years of complimentary credit monitoring and identity restoration services through Kroll ("Kroll"). To take advantage of these free credit monitoring and identity theft protection services, please follow the instructions in the "Identity Monitoring Services" section of this letter. You must enroll by August 21st, 2023 to receive these services.

Orrick also has reported that it deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network. We are working with EyeMed to better understand its protocols and oversight of its sub-contractors which have access to PHI, including Orrick.

What can you do?

Orrick has reported that it is not aware of any misuse of your information. However, we want to let you know of steps you may want to take to guard against potential identity theft or fraud. We encourage you to remain vigilant by regularly reviewing your financial statements, credit reports, and Explanations of Benefits (EOBs) from your health insurers for any unauthorized activity. If you identify services that you did not receive or accounts, charges, or withdrawals that you did not authorize, you should immediately contact and report to the involved company and to credit reporting agencies.

Please also review the "Additional Resources" section included with this letter. It describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

More Information:

If you have questions, please call us at 1-877 HR SERVE (1-877-477-3783), Monday through Friday from 8:00 a.m. to 5:00 p.m. Eastern Time.

Sincerely,

T. Rowe Price

Identity Monitoring Services

Orrick has secured the services of Kroll to provide identity monitoring at no cost to you for 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 services* include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

You must activate your identity monitoring services by August 21, 2023.

1. Visit [Enroll.krollmonitoring.com/redeem](https://enroll.krollmonitoring.com/redeem) to activate your identity monitoring services.
2. Provide Your Activation Code: <<Enter Activation Code>> and Your Verification ID: <<Verification ID>>

Take Advantage of Your Identity Monitoring Services

You've 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'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.

* 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

The Federal Trade Commission (FTC) recommends that you remain vigilant by checking your credit reports periodically. Checking your credit reports can help you spot problems and address them quickly. You can also order free copies of your annual reports through www.annualcreditreport.com. You should monitor your financial accounts for any suspicious activity. For more information about steps you can take to reduce the likelihood of identity theft or fraud, call 1-877-IDTHEFT or 1-877-438-4338, visit the FTC's website at www.ftc.gov/bcp/edu/microsites/idtheft/ or write to: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. However, if you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency, your state's attorney general, or the FTC.

Contact Information for Consumer Reporting Agencies and Information on Credit Report Fraud Alerts

In addition to enrolling for credit monitoring, you may also choose to place a fraud alert on your credit file, which is free of charge to you and can be done with any **one** of the companies listed below (i.e., if you place a fraud alert with one company, they will automatically notify the others). A fraud alert tells creditors to contact you **before** they open any new accounts or change your existing accounts.

	Experian	Equifax	TransUnion
Phone	1-888-397-3742	1-800-525-6285 or 1-888-766-0008	1-800-680-7289
Address	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	Equifax Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Credit Report Fraud Alert Form	www.experian.com/fraud/center.html	www.equifax.com/personal/credit-report-services	www.transunion.com/fraud-alerts

Information on Security Freezes

In addition to a fraud alert, you may place a security freeze on your credit file. A security freeze **will block** a credit bureau from releasing information from your credit report **without your prior written authorization**. Please be aware that it may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. There is no cost to place, lift or remove a security freeze.

To place a security freeze on your credit report, you may send a written request to **each** of the major consumer reporting agencies by regular, certified, or overnight mail. You can also place security freezes online by visiting **each** consumer reporting agency online. Please provide the information requested, which varies by consumer reporting agency, but typically includes: full name, address, Social Security Number, date of birth, proof of identity and proof of address.

	Experian	Equifax	TransUnion
Address	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	www.experian.com/freeze/center.html	www.equifax.com/personal/credit-report-services	www.transunion.com/credit-freeze

You may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, <http://www.ncdoj.gov>, 1-877-5667226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.