15073

The US Oncology Network

«NAME»
«PRIMARY_ADDRESS»
«CITY», «STATE_» «ZIP»

«GreetingLine»

US Oncology, Inc. ("U.S. Oncology") takes protection of the privacy and security of your information very seriously. We are writing to inform you of a recent potential disclosure of your personal information.

Specifically, Information Security and Risk Management for U.S. Oncology, as the business manager for physician practices within the U.S. Oncology Network (the "Network"), learned of a spear phishing attempt on or about June 7, 2018 to one individual's email account at a practice within the Network (the "Incident"). An email from an unknown third party, disguised as a legitimate business communication, was sent to and opened by an individual at a practice within the Network. The individual mistakenly clicked on the phishing attachment and link, and then provided email user id and password information. Upon discovery of and in response to this Incident, we promptly took the following corrective actions: the phishing URL was blocked, the user's password was reset, and the phishing e-mail was purged from the mailbox.

In order to understand if Protected Health Information ("PHI") or Personally Identifiable Information ("PII") was contained in the affected e-mail box, the practice engaged outside counsel to review the email account. On March 27, 2019, we were informed that the practice's counsel had located an email with an attachment containing PII within the mailbox. The email attachment contained a report generated by the 401k plan administrator, Fidelity, which included names of Network practice employees who participated in the retirement plan, as well as corresponding social security numbers, and 401K balances.

Although both Information Security and Risk Management for the Network and a third-party forensic firm thoroughly investigated the attack, we have no knowledge or evidence that the PII was accessed, viewed or misused as a result of this Incident. Out of an abundance of caution, we have contracted with Experian to provide you with credit monitoring services. Please note that the credit monitoring services are available for you to activate for one-year from the date of this letter. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

If you believe there has been fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that additional identity restoration support is needed, then an Experian Identity Restoration agent will work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

We also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft.

To start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: «ENROLLMENT_DATE» (Your code will not work after this date)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: «ACTIVATION_CODE»
- If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by «ENROLLMENT_DATE». Be prepared to provide engagement number «ENGAGEMENT_NO_» as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 24-MONTH EXPERIAN IDENTITYWORKS Membership:

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- Credit Monitoring: Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARE™: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information:

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

- Call the toll-free numbers of any of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening accounts in your name. You only need to contact one of the credit bureaus. As soon as that credit

bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.
    - Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241.
    - Experian: 1-888-EXPERIAN (1-888-397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013.
    - TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.
- Review your credit reports. By establishing a fraud alert, the credit bureaus will send you a free credit report. When you receive a credit report, you should examine it closely and look for signs of fraud, such as credit accounts that are not yours.
- Continue to monitor your credit reports and other accounts. Even though a fraud alert has been placed on your credit report, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information. You should also closely monitor your financial and other account statements, and if you notice any unauthorized activity, promptly contact the creditor.
- Contact law enforcement if you find suspicious activity. If you find suspicious activity on your credit reports or other account information, contact your local police department and file a report of identity theft. Keep copies of such reports for your records, as you may need to give them to creditors.
- Other resources. For more information about steps you can take to avoid identity theft, you may contact the Federal Trade Commission, by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington DC, 20580, via the Internet at www.ftc.gov/idtheft or by phone at 1-877-ID-THEFT (1-877-438-4338).

We apologize to you and deeply regret that this incident occurred. If you have any further questions or concerns, please contact us at 866-703-9557.

Sincerely,

US Oncology, Inc

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.