OPN Healthcare, Inc.

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

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

<<b2b_text_1 (IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY / NOTICE OF DATA BREACH (CA Only))>>

Dear <<First_Name>> <<Last_Name>>:

I am writing with important information regarding a recent cybersecurity incident at OPN Healthcare, Inc. ("OPN") that involved some of your health information. OPN is a technology healthcare services company that partners with physicians and health insurance companies to coordinate oncology care to patients. We received your health information from <<b2b_text_2 (Data Owner)>> to help facilitate care with your doctor. The privacy and security of the personal information entrusted to OPN is of the utmost importance to us. As such, we wanted to provide you with information about the incident, and let you know that we continue to take significant measures to protect the information entrusted to us.

What Happened?

On or about June 3, 2026, OPN discovered unauthorized access to one (1) of our business email user accounts.

What We Are Doing.

Upon learning of the issue, we secured our network and commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals experienced in handling these types of incidents. The investigation determined that on or about June 3, 2026, an unauthorized party briefly accessed certain emails within the affected email account. We conducted a thorough review of the emails accessed by the unauthorized party and on September 25, 2026, determined that the accessed files contained some of your health information. We have further confirmed that no emails or attachments were downloaded during the incident. We notified <<b2b_text_2 (Data Owner)>> and worked with them to notify you.

What Information Was Involved?

The information that may have been impacted includes your full name, <<b2b_text_3 (Data Elements)>>. The emails did not contain any identifying information such as Social Security number or address.

What You Can Do.

We have no evidence that any of your information has been used to commit fraud or identity theft as a result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and inform you about other precautionary measures you can take to protect your personal information. You should always remain vigilant in reviewing your financial account statements, explanation of benefits, and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information on the following pages. Please see the "Other Important Information" provided in this letter for more information on these precautionary measures.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of the personal information entrusted to us.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at (844) 971-8657. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information. The response line is available Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time (except for holidays).

Sincerely,

OPN Healthcare, Inc.
550 N Brand Blvd., Suite 1000
Glendale, CA 91203

– OTHER IMPORTANT INFORMATION –

1. Protecting Your Medical Information.

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft:

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

2. Placing a Fraud Alert on Your Credit File.

A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft and, before they extend credit, they should use take extra steps to verify your identity. You can place a fraud alert on your credit report by contacting any one of the three nationwide credit bureaus using the information below. Once the fraud alert is added, the request will be shared with the other bureaus within 24 hours.

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit bureaus directly at:

Equifax	***Experian***	***TransUnion***
P.O. Box 740241	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19016-2000
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 680-7289

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain a free copy of your credit report and monitor it for any suspicious activity. You can obtain a free credit report once a week by visiting www.annualcreditreport.com or by calling 1-877-322-8228; TTY: 1-800-821-7232.

3. Placing a Security Freeze on Your Credit File.

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without your permission. A freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze.

Unlike a fraud alert, you must separately place a freeze on your credit file at each credit bureau. To place a freeze on your credit report, contact them online or by phone or mail and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a freeze for your spouse, this information must be provided for them as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; and (4) current address and any previous addresses for the past five years.

Below, please see relevant contact information for the three consumer reporting agencies:

Equifax	***Experian***	***TransUnion***
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348-5788	Allen, TX 75013	Woodlyn, PA 19094
www.equifax.com	www.experian.com	www.transunion.com
(800) 685-1111	(888) 397-3742	(888) 909-8872

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

* * * * *

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).

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 Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

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

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.