New Century Ophthalmology, PC
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057

Jane A Smith Jr
123 Main St
Apt A
Test Adult, XX ABC12 DE34

Date

TEST

Draft

Dear Jane Smith,

We are writing to provide you with information regarding a data security incident (the "Incident") experienced by New Century Ophthalmology, PC ("NCO" or "we") that may have involved your personal information ("Information"). This letter provides you with information about this Incident, our response efforts, steps you can take, and if necessary, information on where to direct your questions. Additionally, although we are unaware of any fraudulent misuse of your Information in relation to the Incident, as a precaution we have also provided steps you can take to protect your Information.

What Happened?

On August 18, 2026, we became aware of unauthorized activity within certain systems of our practice. We immediately responded and took numerous steps to contain any suspicious activity, including changing passwords, terminating any unauthorized access, and enhancing the monitoring capabilities on each workstation within our offices. We also initiated an investigation with experienced data security and privacy professionals, which identified that the unauthorized activity included copying of certain data from our systems. Although our investigation could not rule out that files containing your Information were among the data acquired by the unauthorized actor, we have no evidence that your Information has been further disclosed or misused for identity theft or fraud in connection with this Incident. We are sending you this notice so that you can take the steps described below if you wish.

What Information Was Involved?

We determined that the following types of Information may have been impacted as a result of this Incident: name, address, date of birth, Social Security number, driver's license number, medical information including diagnosis and medications, and health insurance information. Note that this describes general categories of information that may be present within the impacted environment during the Incident and includes categories that may not be relevant to each individual whose Information may have been present.

What We Are Doing.

We take this Incident and the security of Information in our care seriously. Upon becoming aware of the Incident, we took immediate action to contain the situation and have worked closely with data security and privacy professionals to further strengthen our existing, significant safeguards. After determining unauthorized activity occurred, we began a thorough analysis of the information involved to identify those potentially affected and notify them. We have also notified federal law enforcement and the appropriate regulatory authority about this Incident. In response to the Incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for test from the date of enrollment when changes occur to your credit

Please Recycle Me!

file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What Can You Do?

To enroll in Cyber Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: ABC123DEF456 In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

It is always recommended that you remain vigilant, regularly monitor reports, review account statements, and report any suspicious activity to the relevant institutions. Please also review the "Additional Resources" section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have additional questions, you may call 1-800-658-5016 Monday through Friday from 8am through 8pm Eastern time (excluding U.S. holidays).

Sincerely,

New Century Ophthalmology

Encl.

Draft

Please Recycle Me!

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com/personal/credit-report-services, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com/help, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, https://www.transunion.com/data-breach-help, 1-833-395-6938

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. 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 Massachusetts 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 Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting Act ("FCRA").

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or 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 them 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 five years; and (5) any applicable incident report or complaint with a law enforcement agency or Department 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.

FTC 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 FTC and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid 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).

Please Recycle Me!

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, 1-800-952-5225. This notification was not delayed as a result of any law enforcement investigation.

For District of Columbia Residents: You can obtain information about steps to take to avoid identity theft from the FTC (contact information above) and the District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, https://oag.dc.gov/, 1-202-737-3400.

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

For Pennsylvania Residents: You may contact the Pennsylvania Office of the Attorney General, Bureau of Consumer Protection, 15th Floor, Strawberry Square, Harrisburg, PA 17120, www.attorneygeneral.gov, 1-800-441-2555.

Protecting Medical Information.

If you are concerned about protecting your medical information, 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.

Draft

Please Recycle Me!