

To Our Valued Patient:

We use a third party company to electronically prescribe medications and communicate directly with our patients' pharmacy. We were informed by this company that they had a data breach. This is the information that we received from them:

Networking Technology, Inc. d/b/a RXNT ("RXNT") contracts with healthcare organizations to provide cloud-based, integrated software solutions for electronic prescribing, practice management, and electronic health record. We place the utmost of value on maintaining the privacy and security of the information we maintain for our customers. We are writing to inform you about a recent cybersecurity incident that involved some of your information, received in connection with the services RXNT provided for your healthcare provider. This letter explains the incident, outlines the measures we have taken in response, and steps you can take.

What Happened? On March 3, 2026, RXNT became aware of unauthorized activity in one of the RXNT solutions used by a portion of RXNT customers. RXNT conducted an internal investigation alongside cybersecurity experts and took steps to contain the activity and confirmed that the unauthorized actor had been eliminated from the environment. Additionally, they notified law enforcement. The investigation determined that, between March 1, 2026, and March 3, 2026, an unauthorized actor obtained certain data stored on RXNT's system. They conducted a comprehensive review of the affected data to identify what information was involved and the individuals and customers to whom it related. RXNT notified First Sight Family Vision on May 1, 2026.

What Information Was Involved? Our review determined that the affected data may have included the following: your name; date of birth; demographic information (such as address, contact information, and patient ID); and prescription data. The incident did involve your Social Security Number. The incident did not involve any payment card, bank account, or other financial information. At this time, we are not aware of any identity theft or fraud related to the use of any affected individual's information, including yours.

What We Are Doing. Data privacy and security are RXNT's highest priorities and we take this incident very seriously. After becoming aware of the incident, RXNT immediately took steps to contain it and, with the help of external cybersecurity experts, confirmed that the unauthorized actor was eliminated from the environment.

What You Can Do. Although we have no evidence that any of your information has been misused for identity theft or fraud, you should always remain vigilant by reviewing your account statements and credit reports for any unauthorized activity.

Sincerely,

Dr. Jason Egbert, OD

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing

your account statements and free credit reports for any 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 companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

Contact information for the Federal Trade Commission is as follows:

- Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes **Fraud Alerts:** There are two types of general 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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for prescreened credit card offers for two years, unless you ask them not to. **Credit or Security Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
- TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
- Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus. RXNT is located at 5540 Centerview Dr, Ste 204, PMB59595, Raleigh, NC 27606-8012, and can be reached at (800) 943-7968.

A Summary of Your Rights Under the Fair Credit Reporting Act:

The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.