Superior Vision Services, Inc.
500 Jordan Road
Troy, NY 12180

September 26, 2025

VIA EMAIL

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Breach

Dear Attorney General Formella:

Superior Vision Services, Inc., a subsidiary of Versant Health, Inc. ("we", "our", or "us"), is writing to notify you of a data security incident. This letter will serve to inform you of the nature of the incident, what information may have been compromised, the number of New Hampshire residents being notified, and the steps that Superior Vision has taken in response to the incident. We have also enclosed hereto a sample of the notification made to the impacted New Hampshire residents, which includes an offer of free credit monitoring services.

1. **Nature of the Incident**

On July 9, 2025, a Superior Vision employee was the victim of a sophisticated phishing attack. On July 11, 2025, the threat actor may have downloaded emails from the email account of the affected employee that contained customer personal information. The information that may have been accessed without authorization varies by resident but could include some combination of: full name, physical address, phone number, email address, date of birth, gender, Social Security number, vision coverage election information, and employment information related to enrollment.

2. **Number of New Hampshire residents affected**

A total of 10 New Hampshire residents were affected by this incident. Notification letters to these individuals will be mailed no later than September 26, 2025.

3. **Steps taken in response to the Incident**

After discovering this breach on July 11, 2025, Versant Health disabled the impacted email account and secured its systems rapidly to prevent further unauthorized access. Versant Health also performed a review to understand what data, if any, was impacted.

We implemented additional measures to further enhance our security. We also notified law enforcement.

We are offering all New Hampshire residents complimentary three-bureau credit monitoring for one year. The service is provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting companies.

Additionally, we are providing impacted residents with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on their credit file, information on protecting against fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports. We informed residents to contact the Federal Trade Commission, the state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

4. Contact Information

Should you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,

Superior Vision Services, Inc.
Lorena Jelks
Email: Lorena.Jelks@versanthealth.com
Phone: 210-245-2154

Enclosure: Consumer Notification Letter

Superior Vision
500 Jordan Road
Troy, NY 12180

[Insert Recipient's Name]
Insert Street Address
Insert City, State, and Zip

September 26, 2025

Re: Data Breach Notification

Dear Name:

Superior Vision, a subsidiary of Versant Health ("we", "our", or "us"), is writing to inform you of a recent data security incident that may have involved some of your personal information. We take the privacy and security of your information seriously.

WHAT HAPPENED

On July 9, 2025, a Superior Vision employee was the victim of a sophisticated phishing attack. On July 11, 2025, the threat actor may have downloaded emails from the email account of the affected employee that contained customer personal information. After discovering this breach on July 11, 2025, Versant Health disabled the impacted email account and secured its systems rapidly to prevent further unauthorized access. Versant Health also performed a review to understand what data, if any, was impacted.

WHAT PERSONAL INFORMATION WAS INVOLVED?

Your information that may have been accessed without authorization varies by individual but could include some combination of: full name, physical address, phone number, email address, date of birth, gender, Social Security number, vision coverage election information, and employment information related to enrollment.

WHAT WE ARE DOING

We implemented additional measures to further enhance our security. We also notified law enforcement. This notification was not delayed due to a law enforcement investigation. We continue to treat the protection of our customers' information as a top priority.

We have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service *(myTrueIdentity)* for one year. The service is provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting companies.

WHAT YOU CAN DO

Privacy laws do not allow us to register you directly to the monitoring service. To enroll in this service, go to the *myTrueIdentity* website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code: **[REDACTED]** and follow the three steps to receive access to the credit monitoring service online within minutes.

If you do not have access to the Internet, you may enroll in a similar offline paper-based credit

monitoring service via U.S. mail delivery, by calling the TransUnion Fraud Response Service's toll-free hotline at **1-855-288-5422,** and when prompted, enter this code: **[REDACTED]** and follow the steps to enroll in the offline credit monitoring service.

You may also add an initial fraud alert to your credit file or speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime within the next **90 days**. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion®, Experian® or Equifax®, or an address in the United States or its territories, and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® or Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

FOR MORE INFORMATION

If you have any questions about this situation, please call us Monday through Friday between 8am – 9pm (EST/EDT) and Saturday 9am – 4pm (EST/EDT) at 866-344-1414. We deeply regret any inconvenience that may have been caused by this incident.

Sincerely,

Superior Vision Privacy Office

SuperiorVision

OTHER IMPORTANT INFORMATION

Under federal law, you are also entitled to one free credit report once every 12 months from each of the three major nationwide credit reporting companies. To receive yours, c all 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

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. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission at www.ftc.gov/idtheft or at 1-877-ID-THEFT (1-877- 438-4338). Your complaint will be added to the Federal Trade Commission's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Also visit the Federal Trade Commission's website at www.ftc.gov/idtheft to review the comprehensive information available in the "*Taking Charge: What to Do if Your Identity is Stolen*" step-by-step guide. You may also call 1-877-438-4338 to request a free copy.

Security Freeze

Consumers are also allowed to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. A credit reporting agency may not charge you to place, lift, or remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies listed above by regular, certified, or overnight mail at the addresses above.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number

(PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

You may contact any of the above-listed credit reporting agencies or the FTC to obtain information concerning security freezes.

Fraud Alerts

You should also consider placing a "fraud alert" or "security alert" on your credit file. An alert helps warn creditors checking your file that recent fraudulent activity may have occurred or may occur in the future. A potential creditor would then know to contact you before opening any new accounts. To place a fraud alert, contact the credit reporting agencies directly:

Equifax ® PO Box 105851 Atlanta, GA 30348 888-766-0008 www.equifax.com	**Experian** ® PO Box 9532 Allen, TX 75013 888-397-3742 www.experian.com	**TransUnion** ® PO Box 1000 Chester, PA 19016 800-680-7289 www.transunion.com

When you place any type of fraud alert on your credit file, the credit reporting agencies will send you a free copy of your credit report. Look for accounts that are not yours, debts you do not owe, or any other inaccuracies (e.g., wrong social security number or home address). If you find an error, contact the credit reporting agency directly. By law, that credit reporting agency must investigate and respond. You should also monitor your financial statements for unauthorized activity. To learn more about identity theft, visit the Federal Trade Commission's "Your National Resource about Identity Theft" guidance materials at www.ftc.gov/idtheft or write to 600 Pennsylvania Avenue, NW, Washington, DC 20580. You should remain vigilant by reviewing account statements and monitoring free credit reports.

Finally, you should also monitor your financial statements for unauthorized activity.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

For Iowa Residents: State law advises you to report any suspected identity theft to local law enforcement or the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General and FTC about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us. You can contact the FTC at its Consumer Response Center at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, 877-ID-THEFT, www.ftc.gov/idtheft.

For Massachusetts Residents: You also have the right to obtain a police report.

For New Mexico Residents: You have rights under the federal Fair Credit Reporting Act ("FCRA").

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office Bureau of Internet and Technology (212) 416-8433 https://ag.ny.gov/internet/resource-center	NYS Department of State's Division of Consumer Protection (800) 697-1220 https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General and FTC about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: North Carolina Attorney General's Office, Consumer Protection Division, 90001 Mail Service Center, Raleigh, NC 27699-9001, 877-566-7226 (Toll-free within North Carolina), 919-716-6000, www.ncdoj.gov. You can contact the FTC at its Consumer Response Center at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, 877-ID-THEFT, www.ftc.gov/idtheft.

For Oregon Residents: State law advises you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903; (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.

Washington, D.C. Residents: You can obtain information about avoiding identify theft from the Office of Attorney General for the District of Columbia. You can contact the Office of Attorney General for the District of Columbia at: 400 6th Street NW, Washington, D.C. 20001; 1-202-727-3400; https://oag.dc.gov.