Notice of Data Security Incident

As previously disclosed on September 26, 2025:

Superior Vision, a subsidiary of Versant Health ("we", "our", or "us"), mailed notice of the following incident directly to potentially impacted individuals at their last known mailing address via a letter dated September 26, 2025.

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?

The 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. In the notices mailed in September 2025, we offered potentially impacted individuals the opportunity to enroll in credit monitoring services at no additional cost.

We continue to treat the protection of our customers' information as a top priority.

We have established a toll-free call center to answer questions about the incident and address related concerns. Call center representatives are available Monday through Friday between 8 am – 9 pm (EST/EDT) and Saturday 9 am – 4 pm (EST/EDT) at 866-344-1414. We deeply regret any inconvenience that may have been caused by this incident.

WHAT YOU CAN DO

We are providing the following information to help those wanting to know more about steps they can take to protect themselves and their information:

Copy of Your Credit Report

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, call 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 below by regular, certified, or overnight mail at the addresses listed.

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.

Review Your Account Statements for Unauthorized Activity.

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