



Elevate Health and Rehabilitation
Return to Mail Processing Center
P.O. Box 989728
West Sacramento, CA 95798-9728



Enrollment Code: [REDACTED]

Enrollment Deadline: October 31, 2026

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

July 31, 2026

Notice of Data Breach

Dear [REDACTED],

Elevate Health and Rehabilitation (“Elevate”) writes to let you know of an incident that occurred involving your personal information. Although the incident is contained and we have no reason to believe that any of your data that was involved in this incident will be used to perpetrate a theft of your identity, we are contacting you to explain the circumstances of this incident, and to provide information about the service we will provide to help you protect against the possible misuse of your data. We understand that you may have concerns about this incident, which arose from the compromise of two of our trusted third-party vendors. Protecting the privacy and security of your information remains a responsibility we take seriously, and we are committed to supporting you as described below.

What Happened

On June 1, 2026, Elevate discovered that records maintained by a trusted vendor, some of which contained personal information concerning Elevate residents, had been accessed and copied by an unauthorized person. Upon discovering the compromise, we took prompt action to remediate the incident and secure access to the files stored in our vendor’s system. We began an investigation, engaging a specialized cybersecurity vendor to assist. We also contacted the FBI.

Our investigation indicated that a bad actor had logged into our vendor’s systems, using credentials stolen from another trusted vendor, beginning on November 25, 2025, and ending on November 28, 2025. On June 1, 2026, we received an email that first alerted us to the problem. We worked without delay to ensure that there was no further compromise of your data and engaged experts to investigate the incident. In particular, we took prompt action to ensure that the compromised credentials were disabled and passwords were reset, as part of our effort to protect against any further compromise of our residents’ data that was maintained in this vendor’s systems.

Based on our investigation, which is ongoing, we have no reason to believe that the bad actor still has access to personal information concerning residents or to the vendor’s systems. We also were able to secure credible evidence that the bad actor did not publish your personal information and has permanently deleted all of the data that was taken.

What Information Was Involved

The personal information that may have been involved in this incident includes resident name, date of birth, home address, email address, driver's license, and Social Security number. Health information compromised in this incident may have included information related to resident care, such as diagnoses, lab results, medications, treatment information, and patient account numbers.

What We Are Doing

As detailed above, in response to this incident, we engaged and worked closely with cybersecurity experts and legal counsel, as well as taking prompt action to ensure that the compromised credentials were disabled and passwords were reset. Importantly, as noted above, we have received confirmation that the files were permanently deleted and will not be published. We have continued to conduct a review of the data accessed and of our systems and processes. As part of Elevate's ongoing commitment to protecting the privacy and security of your information, we are enhancing the safeguards that support our systems. Building on all of the security measures we already have in place, we are working to implement additional layers of safeguards designed to further strengthen how we protect your information. These additional measures reflect our continued dedication to data protection. Maintaining the confidentiality and integrity of your information remains one of our highest priorities.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include two years of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if you are concerned that your identity is compromised.

What You Can Do

We encourage you to contact IDX to enroll in the free identity protection services by calling 1-833-788-9712, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 31, 2026. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

While there is no evidence that your information has been misused, we take your privacy seriously and encourage you to take advantage of the credit monitoring service offering out of an abundance of caution.

For More Information

If you have questions about this incident or want to learn additional information, please contact our compliance office by calling this phone number, 833-266-7595, or by emailing contactus@suretycompliance.com.

Please call 1-833-788-9712 or go to <https://app.idx.us/account-creation/protect> for assistance with enrollment in identity protection services or for any additional questions you may have about those services.

Sincerely,

Dena Edwards, Privacy Officer
Elevate Health and Rehabilitation

(Enclosure)



Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-833-788-9712 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft, including fraud alerts and security freezes, from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

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, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov>, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

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