Dominik Cvitanovic
(504) 372-6698
Dominik.Cvitanovic@wilsonelser.com

March 2, 2026

Via Electronic Mail: DOJ-CBP@doj.nh.gov

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection Bureau
1 Granite Place South
Concord, NH 03301

Re: Data Event Involving High Point Treatment Center, Inc. – 16516.02595

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents High Point Treatment Center, Inc. ("High Point"), located at 72 Kilburn Street, New Bedford, MA 02740, with respect to a recent data event that was first discovered by High Point on or about July 6, 2025 (hereinafter, the "Event"). Please know that High Point takes the security and privacy of the information in its control very seriously.

This letter is an update to the notice submitted to your office on July 29, 2025. This letter will serve to inform you of the nature of the Event, the notifications provided to individuals potentially affected by the Event, and the steps that High Point has taken in response to the Event. By providing this notice, High Point does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

1. Nature of the Event

On or about July 6, 2025, High Point became aware of unusual activity in its network environment. Upon becoming aware, High Point promptly began an investigation into the scope and nature of the suspicious activity and retained legal counsel and third-party forensic specialists to investigate the unusual activity. That investigation revealed that certain information may have been copied by an unauthorized individual as part of the event. This activity occurred between June 17, 2025 and July 6, 2025. High Point then began a comprehensive review of the data set to determine what sensitive and/or personal information was impacted and to whom it related. On December 2, 2025, High Point's investigation discovered an additional data set impacted by this event, and High Point began reviewing that set. On February 24, 2026, High Point finished its review of the additional impacted information.

Although High Point is unaware of any actual or attempted misuse of information to perpetrate fraud, the data that may have been exposed as a result of this unauthorized activity included: name,

date of birth, health insurance identification number, health insurance group number, Social Security number, medical diagnosis information, medical treatment information, medical treatment location, doctor name, medical treatment dates, medical lab or test results.

2. Number of New Hampshire residents affected.

A total of thirty-four (34) New Hampshire residents were determined to be potentially impacted as a result of this event. Notification letters were mailed on July 29, 2025, to fifteen (15) New Hampshire residents via first class mail as part of the first wave of individual notices. The following types of information were potentially impacted: name, date of birth, health insurance identification number, health insurance group number, Social Security number, medical diagnosis information, medical treatment information, medical treatment location, doctor name, medical treatment dates, medical lab or test results. Notification letters were mailed on March 2, 2026, to an additional nineteen (19) New Hampshire residents as part of the second wave of individual notices. A sample copy of the notification letter is included with this letter under **Exhibit A.**

3. Steps taken in response to the Event.

High Point is committed to ensuring the security and privacy of all personal information in its control. Upon discovery of the Event, High Point moved quickly to investigate and respond to the Event. Specifically, High Point engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Event. Lastly, High Point informed its law firm and began identifying the affected individuals in preparation for notice.

High Point offered at least 12 months of complimentary credit monitoring and identity theft restoration services through Cyberscout, a TransUnion company, to all individuals to help protect their identity. Additionally, High Point provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, 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 free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

High Point remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Dominik.Cvitanovic@wilsonelser.com or (504) 372-6698.

Very truly yours,
Wilson Elser Moskowitz Edelman & Dicker LLP

Dominik Cvitanovic, Esq.

EXHIBIT A

High Point Treatment Center, Inc.
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

Via First-Class Mail

March 2, 2026

Notice of Data Event

Dear [redacted]:

High Point Treatment Center, Inc. ("High Point") writes to inform you of a recent event that may impact some of your personal information. While High Point is not aware of any actual or attempted misuse of your information to perpetrate fraud, out of an abundance of caution, we are providing you with an overview of the event, our response, and resources to help further protect your information, should you feel it necessary to do so.

What Happened?

On or about July 6, 2025, High Point became aware of unusual activity in its network environment. Upon becoming aware, High Point promptly began an investigation into the scope and nature of the suspicious activity and retained legal counsel and third-party forensic specialists to investigate the unusual activity. That investigation revealed that certain information may have been copied by an unauthorized individual as part of the event. This activity occurred between June 17, 2025 and July 6, 2025. High Point then began a comprehensive review of the data set to determine what sensitive and/or personal information was impacted and to whom it related. On February 24, 2026, High Point finished its review of the impacted information.

What Information Was Involved?

The impacted information varied by individual. Based on High Point's investigation, the following information may have been copied without authorization: [redacted].

What We Are Doing.

The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon becoming aware of the event, we moved promptly to investigate and respond to the event. As stated above, we are not aware of any actual or attempted misuse of your family member's information to perpetrate fraud but, out of an abundance of caution, we are notifying you so that you may take further steps to best protect your information, should you feel it is necessary to do so. As an added precaution, 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 12 months from the date of enrollment when changes occur to your credit 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 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. While High Point is covering the cost of these services, you will need to complete the activation process yourself.

What You Can Do

You can learn more about how to help protect you against potential information misuse in the enclosed *Steps You Can Take To Help Protect Personal Information*. There, you will find instructions on how to activate the complimentary credit monitoring. We also encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credits reports for suspicious activity, and to report any suspicious activity promptly to your bank, credit card company, or other applicable institution.

For More Information

We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the assistance line at 1-833-397-4692, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding major U.S. holidays. Please have this letter ready if you call.

Sincerely,

High Point Treatment Center, Inc.

Steps You Can Take To Help Protect Personal Information

Activate Monitoring Services

To enroll in Credit 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: [redacted]. Please note that the code is case-sensitive and will need to be entered as it appears.

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 and may not be available to minors under the age of 18 years of age. Once enrolled you will have 12 months of monitoring services. At the end of 12 months the services will be deactivated. 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877–322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/ credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at 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.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491. High Point is located at 72 Kilburn Street, New Bedford, Massachusetts 02740 and can be reached at 800-233-4478.

For New York residents, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 18 Rhode Island residents that may be impacted by this event.