

## GRANITE WELLNESS CENTERS

### NOTICE OF DATA BREACH

January 28, 2021

Granite Wellness Centers recently discovered a security incident that affected the personal information of our clients. While we are not aware of any actual misuse of personal information as a result of this incident, we take the privacy of our clients very seriously, and want to make sure that you are aware of this incident so that you can take appropriate precautions to protect your personal information. We are providing information on identity protection resources at the end of this notice.

#### **What Happened?**

On January 5, 2021, we discovered that some of the data stored on our computer servers had become encrypted due to a “ransomware” attack by an unknown actor. The incident was in process at the time we discovered it. We immediately took the affected systems offline, reported the incident to law enforcement, and began to assess the incident, to eliminate the ransomware, and to take measures to restore our systems and prevent further attacks. We are able to fully restore our systems from back-up files, and the care of our clients has not been compromised. This notification has not been delayed as a result of a law enforcement investigation.

#### **What Information Was Involved?**

The following types of personal information relating to some of our clients were present in the affected system: full name, date of birth, dates of care, treatment/health information, treatment provider, health insurer.

#### **What We Are Doing**

We take this incident and the security of your personal information seriously. As part of our ongoing commitment to the privacy of personal information in our care, we are taking steps to rebuild the affected systems, and implementing additional safeguards to further secure the information in our systems. We will also be notifying state and federal regulators, as required.

#### **What You Can Do**

You can find out more about how to protect against potential identity theft and fraud in the attached “Steps You Can Take to Help Protect Your Information.” We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanations of benefits, and to monitor your credit reports for suspicious activity.

#### **For More Information**

Please review the *Steps You Can Take to Protect Your Information* below. We sincerely apologize that this incident occurred and regret any concern or inconvenience this may cause you. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please contact Eric Smith, Privacy Officer, at [helpdesk@corr.us](mailto:helpdesk@corr.us) or 855-467-3496.

Sincerely,  
Eric Smith Compliance  
Director/Privacy Officer  
Granite Wellness Centers

## STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

**Monitor Your Account Statements.** We encourage you to remain vigilant against incidents of identity theft and fraud, and to review your credit and bank account statements for suspicious activity. You should promptly report suspected identity theft to appropriate authorities.

**Request Your Credit Reports.** You are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit <http://annualcreditreport.com> or call toll-free at 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. When you receive your credit reports, read them carefully. Look for accounts you don't recognize. Look in the inquiries section for names of creditors from whom you haven't requested credit. If you find anything you don't understand, call the credit bureau at the telephone number listed on the report.

**Consider Placing a Fraud Alert on Your Credit File.** You can place an initial or extended "fraud alert" on you file at no cost. An initial fraud alert is a 1-year alert that is placed on your credit file. Upon seeing a fraud alert display on your credit file, a business is required to take steps to verify your identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

<b>Experian</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/fraud/center.html">www.experian.com/fraud/center.html</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19016 1-888-909-8872 <a href="http://www.transunion.com">www.transunion.com</a>	<b>Equifax</b> P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 <a href="http://www.alerts.equifax.com">www.alerts.equifax.com</a>
---	---	---

**Consider Placing a Security Freeze on Your Credit File.** You also have the right to place a "security freeze" on your credit file, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make for a new loan or extension of credit. You cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed above, or use these links:

Experian: [www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

TransUnion: [www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

Equifax: [www.alerts.equifax.com](http://www.alerts.equifax.com)

**For More Information** - You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338). The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be promptly reported to law enforcement and your state Attorney General. Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.