



## NOTIFICATION OF A DATA BREACH

**San Jose, CA** — Working with the California Department of Developmental Services, San Andreas Regional Center (“SARC”) provides advocacy, services, and support for individuals with developmental disabilities. SARC announced today that it experienced a data breach that may involve the personal and protected health information of some individuals it serves. As such, SARC sent notification of this incident to potentially impacted individuals and is providing resources to assist them.

On July 5, 2021, SARC discovered that they were the victim of a sophisticated ransomware attack and encryption event. After discovering the incident, SARC quickly took steps to secure and safely restore its systems and operations via viable backups. Further, SARC immediately engaged our firm and third-party forensic experts to conduct a thorough investigation of the incident's nature and scope, assist in the remediation efforts, and contacted and filed a report with the FBI.

On August 2, 2021, SARC concluded its initial investigation and determined the incident involved personal and protected health information. SARC believes that the vast majority of impacted individual’s personal information was not obtained. However, SARC’s investigation could not confirm the specific information potentially obtained and or accessed. Therefore, SARC, out of an abundance of caution, SARC is providing notification to all potentially impacted individuals, regardless of the information not being subject to unauthorized access and or acquisition. ***However, presently, SARC has no evidence indicating misuse of this information.***

Further, after reviewing the potentially impacted information, SARC determined that it could include first and last names, addresses, dates of birth, telephone numbers, social security numbers, email addresses, health plan beneficiary numbers, health insurance information, full-face photos, and or comparable images, UCI numbers (unique identifying number or code generated by us for you), medical information, diagnosis, disability codes, and certificate/license numbers.

The notification letter to the potentially impacted individuals includes steps that they can take to protect their information and offer them access to complimentary identity monitoring and protection services. SARC recommends that individuals enroll in the services provided and follow the recommendations contained within the notification letter to ensure their information is protected. Also, in addition to notifying the FBI, SARC reported the incident to certain regulatory authorities, as required.

“The security and privacy of the information contained within our systems is a top priority for us, and we were shocked to learn that we were one of the thousands of victims of this type of cyberattack,” said Executive Director Javier Zaldivar. “We are fully committed to protecting the information on our systems and sincerely regret the worry caused by this incident. We thank the community, our employees, patients, and partners for their support during this event.”

California residents may wish to review the recommended privacy protection steps outlined in the Breach Help-Consumer Tips from the California Attorney General, which can be found at: <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf>.

Please see “other important information” below for additional resources and tips to prevent identity theft.

For individuals seeking more information or questions, please call SARC’s dedicated toll-free helpline at If you have additional questions, please call our toll-free helpline response line at (855) 651-2669 on Mondays through Fridays between at 9:00 a.m. to 6:30 p.m. (EST). In addition, individuals seeking to contact SARC directly may write to 6203 San Ignacio Avenue, Suite 200, San Jose, CA 95119.

## Other Important Information

**Obtain and Monitor Credit Report.** SARC recommends that individuals obtain a free copy of their credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>

Alternatively, individuals can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of their credit report or general identified above inquiries.

<b>Equifax</b> <b>(888) 766-0008</b> P.O. Box 740256 Atlanta, GA 30348 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> <b>(888) 397-3742</b> P.O. Box 2104 Allen, TX 75013 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> <b>(800) 680-7289</b> P.O. Box 6790 Fullerton, CA 92834 <a href="http://www.transunion.com">www.transunion.com</a>
---	--	--

**Security Freeze (also known as a Credit Freeze).** Following is general information about how to request a security freeze from the three credit reporting agencies. 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 a credit report may delay, interfere with, or prevent the timely approval of any requests regarding for new loans, credit mortgages, employment, housing, or other services. In addition, in some states, the agency cannot charge individuals to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided above).

<b>Equifax Security Freeze</b> P.O. Box 105788 Atlanta, GA 30348 <a href="https://www.freeze.equifax.com">https://www.freeze.equifax.com</a>	<b>Experian Security Freeze</b> P.O. Box 9554 Allen, TX 75013 <a href="http://www.experian.com/freeze">www.experian.com/freeze</a>	<b>TransUnion Security Freeze &amp; Fraud Victim Assistance Dept.</b> P.O. Box 6790 Fullerton, CA 92834 <a href="https://freeze.transunion.com">https://freeze.transunion.com</a>
---	---	--

**Consider Placing a Fraud Alert on Credit Reports.** Individuals may want to consider placing a fraud alert on their credit report. An initial fraud alert is free and will stay on a credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within a report and requests that the creditor contact individuals before establishing any accounts in an individual's name. To place a fraud alert on a credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

**Remain Vigilant, Review Account Statements and Notify Law Enforcement of Suspicious Activity.**

As a precautionary measure, SARC recommends that individuals remain vigilant by closely reviewing their account statements and credit reports. If an individual detects any suspicious activity on an account, SARC strongly advise that they promptly notify the financial institution or company that maintains the account. Further, individuals should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including their state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, individuals can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to [IdentityTheft.gov/databreach](http://IdentityTheft.gov/databreach); or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

**Certain rights under the Fair Credit Reporting Act (FCRA):** These rights include knowing what is in an individual's file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies to correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

**Take Advantage of Additional Free Resources on Identity Theft.** SARC recommends that individuals review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>. For more information, please visit [IdentityTheft.gov](https://www.identitytheft.gov) or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at [https://www.consumer.ftc.gov/articles/pdf/0009\\_identitytheft\\_a\\_recovery\\_plan.pdf](https://www.consumer.ftc.gov/articles/pdf/0009_identitytheft_a_recovery_plan.pdf).