WHITEFORD, TAYLOR & PRESTON L.L.P.

SPENCER S. POLLOCK
DIRECT LINE (410) 832-2002
DIRECT FAX (410) 339-4028
spollock@wtplaw.com

7 ST. PAUL STREET
BALTIMORE, MD 21202-1636
MAIN TELEPHONE (410) 832-2000
FACSIMILE (410) 832-2015

DELAWARE*
DISTRICT OF COLUMBIA
KENTUCKY
MARYLAND
NEW YORK
PENNSYLVANIA
VIRGINIA

WWW.WTPLAW.COM
(800) 987-8705

August 25, 2021

Privileged and Confidential
(SUBMITTED ONLY VIA THE ONLINE PORTAL AT https://appengine.egov.com/apps/me/maine/ag/reportingform)
Office of the Attorney General
Attorney General Aaron Frey

Re: Security Breach Notification

Dear Attorney General Frey,

We are writing on behalf of our client, San Andreas Regional Center ("SARC") (located at 6203 San Ignacio Ave #200, San Jose, CA 95119), to notify you of a data security incident involving four (4) Maine residents.[1]

Nature

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. 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 that the unauthorized individual potentially gained access to its network via an open remote desktop portal ("RDP") on July 3, 2021, which has since been secured.

Further, based on the investigative findings, 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, in an abundance of caution, and pursuant to its obligation under HIPAA, SARC is providing notification to all potentially impacted individuals, regardless of the information not being subject to unauthorized access and or acquisition. Finally, on August 20, 2021, after concluding a comprehensive search through a significant amount of data, SARC confirmed that the incident potentially included four (4) Maine residents.

[1] By providing this notice, SARC does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

The information potentially included first and last names, addresses, dates of birth, telephone numbers, social security numbers, driver's license numbers/passport numbers, email addresses, health plan beneficiary numbers, health insurance information, full-face photos and or comparable images, UCI numbers (unique identifying number or code), medical information, diagnosis, disability codes, and certificate/license numbers.

Notice and SARC's Response to the Event

On August 27, 2021, SARC will mail a written notification to the potentially affected Maine residents, pursuant to 45 CFR §§ 164.400-414 and 10 M.R.S.A. §§1346-1350-B, in a substantially similar form as the enclosed letter (attached as Exhibit A). Further, SARC is providing these potentially impacted individuals the following:

- Free access to credit monitoring services for one year through Kroll;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank.
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Further, SARC provided the notice to the three major credit reporting agencies and the applicable government regulators, officials, and other states Attorney Generals (as necessary).

Finally, SARC is implementing cybersecurity safeguards, enhancing its employee cybersecurity training, and improving its cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 832-8002 or email me at spollock@wtplaw.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

6203 San Ignacio Avenue
Suite 200
San Jose, CA 95119

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

At San Andreas Regional Center, we value transparency and respect the privacy of your information, which is why we are writing to let you know about a data breach that may involve some of your personal information, what we did in response, and steps you can take to help protect yourself against possible misuse of your personal information.

What Happened

On July 5, 2021, we discovered that we were the victim of a sophisticated ransomware attack that impacted our networks and servers. Ransomware incidents typically involve an unauthorized actor gaining access to an entity's network and deploying malware that encrypts the entity's files, making them inaccessible. The unauthorized actor then commonly demands a ransom payment in exchange for the key to decrypt the entity's files.

After discovering the incident, we quickly took steps to secure and safely restore our systems and operations. Further, we immediately engaged outside counsel 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. We concluded our initial investigation on August 2, 2021, and determined that an unauthorized individual encrypted some of our systems that contained your information. Further, the unauthorized individual acquired some of the information contained on our servers, but we cannot confirm if the information obtained by the unauthorized individual included your information.

However, as of now, we have no evidence indicating misuse of any of your information, but we wanted to notify you of this incident out of an abundance of caution.

What Information Was Involved

The types of information potentially involved are your first and last name, address, date of birth, telephone numbers, Social Security number, email address, health plan beneficiary number, health insurance information, full-face photos, and or comparable images, UCI (unique identifying number or code generated by us for you), medical information, diagnosis, disability codes, and other certificate/license numbers.

What We Are Doing

As explained above, we took immediate steps to secure our systems, filed a report with the FBI, and engaged third-party forensic experts to assist in the investigation. Further, in response to this incident, we are implementing cybersecurity safeguards, enhancing our employee cybersecurity training, and improving our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

What You Can Do

The security and privacy of the information contained within our systems is a top priority for us. Therefore, while we have no evidence indicating your information was misused, we strongly recommend you remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity to the institution that issued the record and law enforcement. Please see "***other important information***" on the following pages for guidance on how to best protect your identity.

Also, we are offering a complimentary one-year membership with Kroll. This product provides you with free credit monitoring, identity theft insurance, and identity theft restoration services.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **November 30, 2021** to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

Please see the information on the following page for additional details.

For More Information

We sincerely regret this incident occurred and for any concern, it may cause. We understand that you may have questions about it beyond what is covered in this letter. 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., Eastern Time (excluding some U.S. holidays).

Sincerely yours,

Javier Zaldivar, Executive Director

KROLL

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your 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, you 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 your credit report or general identified above inquiries.

Equifax	**Experian**	**TransUnion**
(888) 766-0008	**(888) 397-3742**	**(800) 680-7289**
P.O. Box 740256	P.O. Box 2104	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com

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. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. 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. In addition, in some states, the agency cannot charge you 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).

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	**Security Freeze & Fraud Victim**
Atlanta, GA 30348	Allen, TX 75013	**Assistance Dept.**
https://www.freeze.equifax.com	www.experian.com/freeze	P.O. Box 6790
		Fullerton, CA 92834
		https://freeze.transunion.com

Consider Placing a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your 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 Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you 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; 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.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you 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 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.

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. **Maryland residents** may wish to review the information the *Attorney General*, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us. **New Hampshire residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above. **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. **New York Residents**: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: *New York Attorney General's Office Bureau of Internet and Technology*, (212) 416-8433, https://ag.ny.gov/internet/resource-center and or NYS Department of State's Division of Consumer Protection, (800) 697-1220, https://www.dos.ny.gov/consumerprotection. **North Carolina residents** may wish to review the information provided by the North Carolina Attorney General at https:// ncdoj.gov/protecting-consumers/identity-theft/, or by contacting the Attorney General by calling *1-877-566-7226* or emailing or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office* 9001 Mail Service Center Raleigh, NC 27699. **Oregon Residents**: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: *Oregon Department of Justice*, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877- 9392, www.doj.state.or.us. **Rhode Island residents** have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the *Rhode Island Attorney General* at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.