



C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE



NAME

ADDRESS1

ADDRESS2

CSZ



SEQ
CODE 2D
Ver1GC

BREAK

To Enroll, Please Call:

(833) 967-1095

Or Visit:

<https://ide.myidcare.com/cvrc-protect>

Enrollment Code: <<XXXXXXXXXX>>

October 18, 2019

Subject: Notice of Data Security Breach

Dear: <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident that may have involved your personal information. The privacy and security of the personal information of the individuals we serve is extremely important to Central Valley Regional Center (“CVRC”). That is why we are writing to inform you about this incident, offer you complimentary identity protection services, and provide you with information relating to steps that can be taken to help protect your information.

What Happened? On July 29, 2019, CVRC learned that an unauthorized third party may have gained access to an employee’s email account. Once discovered, CVRC disabled access to the account, immediately began an investigation, and engaged a computer forensics firm to determine the scope of the incident. Based on the results of the investigation and the computer forensic firm’s findings, it was determined that CVRC employee email accounts were subject to unauthorized access on July 25–August 2, 2019. On August 12, 2019, the investigation first revealed that data containing individuals’ personal information within one or more email accounts may have also been affected.

As part of our investigation, we completed a thorough review of the affected accounts to determine whose personal information may have been affected. While we have no evidence that any personal information has been misused, we are informing you of the incident and providing you with access to complimentary identity protection services from ID Experts.

What Information Was Involved? The types of information that may have been impacted include: individuals’ names, addresses and contact information, dates of birth, driver’s license information, state identification card or other government identification numbers, Medi-Cal numbers, UCI numbers, and/or medical or health information or health insurance information. For a limited number of individuals, Taxpayer Identification numbers, PINs or other access codes, account passwords, usernames, email addresses or electronic identifiers and the means to access the related accounts, and/or IRS PINs may have also been affected.

What Are We Doing? As soon as CVRC discovered the incident, we took the steps described above. We have also taken measures to further enhance the security of personal information in our possession and to prevent similar incidents from happening in the future. In addition, we have notified the Federal Bureau of Investigation (“FBI”) about this incident, and we will work with and provide assistance to law enforcement to hold the perpetrators accountable.

We are also providing you with information about steps that you can take to help protect your personal information and, as an added precaution, we are offering complimentary identity protection services for one year through ID Experts’ MyIDCare™.

ID Experts is a data breach and recovery services expert and has extensive experience helping individuals who have had an unintentional exposure of personal information. The MyIDCare services include: CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

To receive these services by mail instead of online, please call (833) 967-1095. Please note that you must enroll in the services no later than **January 11, 2020**.

What You Can Do: You can follow the recommendations on the following page to protect your personal information.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions concerning this incident, please contact (833) 967-1095, Monday through Friday, 6:00 a.m. to 6:00 p.m. Pacific Time.

We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Ed Araim", written in a cursive style.

Ed Araim
Director of Administration

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the “FTC”).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major 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 also contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
www.annualcreditreport.com

Fraud Alert: 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 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or your Attorney General. Further recommended privacy protection steps are outlined in the Breach Help – Consumer Tips from the California Attorney General, and can be found at: <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf>.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies 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>.

