BenefitsCal

March 26, 2024

Notice of Data Breach

Dear <first_name> <last_name>,

BenefitsCal is contacting you to inform you of a data security incident that may have impacted some of your personal information. Please review this letter carefully, as it contains important information about the incident and resources you may use to protect your information.

What Happened:

On February 9, 2024, BenefitsCal discovered that someone, that was not allowed, may have logged into accounts of some users of the BenefitsCal website using reused passwords taken from other websites. Your account may have been one of those accessed. BenefitsCal took immediate steps to protect you by temporarily inactivating your account. Someone that was not allowed may have accessed your account between March 1, 2023 and February 13, 2024. In reviewing your account use during that time, your personal information may have been accessed.

What Information Was Involved:

Your potentially accessed personal information may have included your name, address, date of birth, full or last four digits of Social Security Number, email address, phone number, EBT card number, case number, Medi-Cal ID number and information about your program eligibility and benefits.

BenefitsCal takes our commitment to the privacy and security of your information very seriously. BenefitsCal is providing you this letter about this incident, our response, and what you can do to further protect your information.

What We Are Doing:

In addition to temporarily inactivating your account, BenefitsCal took additional steps to further secure your account prior to using it again, including requiring you to provide not just your password but confirm that you are the one asking to access the account through either your email or your phone number when logging in. We also reissued your EBT card if you have one. BenefitsCal has also added other security changes to reduce the risk of a someone potentially accessing information that is not allowed.

What You Can Do:

BenefitsCal recommends that you review the suggestions included with this letter about how to protect your information.

For More Information:

Should you have questions or concerns about this matter, please contact us at <incident_contact_email> or call the dedicated security help line at <incident_phone_number>.

Steps You Can Take To Protect Your Personal Information

Best practices for account security:

To prevent your account from being accessed using passwords that others who are not allowed may have, you should take these additional steps:

- Change the passwords used on your online accounts.
- Use a unique password for each online account.
- Activate multi-factor authentication whenever possible.
- Be wary of emails or phone calls asking you for personal information, especially passwords or one time passcodes.
- Regularly check your accounts for to see if there may be activities that are not yours. If you see something that doesn't look right, call your county office.
- Regularly review and update the security settings on your email and phone accounts.

Monitor Your Accounts

We encourage you to watch out for incidents of identity theft and fraud by regularly reviewing your credit reports for activity that doesn't look right. Where you can get help to protect your credit information:

1) **Free Credit Report**
   Under United States law, you have the right to request a free credit report from each of the three major credit reporting bureaus each year. Review your credit report for any activity that does not look right, including accounts you did not open or requests from creditors that you did not approve. If you have questions about the information in your report, or think there is wrong information in your report, contact the credit reporting bureau. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228.
2) **Credit Freeze**
   You have the right to place a credit freeze on your credit file with each of the three credit bureaus at no cost to yourself. This stops the credit bureau from sharing information in the credit report without your approval. This credit freeze is intended to prevent credit accounts, loans, or other services from being approved without your permission. Be aware that using a credit freeze may delay or prohibit timely approval of credit applications you make, including for loans, mortgages, credit accounts, or other types of credit. To place a credit freeze on your credit file, contact the three major credit reporting bureaus listed below.
3) **Fraud Alert**
   In addition to a credit freeze, you can also place a fraud alert on your credit file. A fraud alert requires a business to take additional steps to confirm your identity before extending new credit. An initial fraud alert lasts for one year. If someone stole your identity, you may request an alert for seven years. To place a fraud alert on your credit file, contact the three major credit reporting bureaus listed below.

Credit Bureau Contact Information:

Equifax 1-888-298-0045 www.equifax.com	Experian 1-888-397-3742 www.experian.com	TransUnion 1-800-680-7289 www.transunion.com

Identity Theft

For additional information on identity theft and resources you can use to protect yourself, you may contact the credit reporting bureaus, the California State Attorney General, and the Federal Trade Commission. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

The California Attorney General provides additional information on identity theft online at https://oag.ca.gov/idtheft.