



330 WEST BROADWAY, SUITE 700
SAN DIEGO, CA 92101

State of California
DEPARTMENT OF JUSTICE



P.O. BOX 944255
SACRAMENTO, CA 94244-2550

DATE

Dear Sir/Madam,

This letter is to inform you of an incident that involved unauthorized access to your personal information.

In November 2011, hackers affiliated with the group Anonymous accessed and released private email accounts belonging to a retired agent from the Department of Justice who was a member of the Computer and Technology Crime High-Tech Response Team (CATCH). CATCH is a multi-agency task force that was formed to apprehend and prosecute all criminals who use technology to prey on the citizens of San Diego, Imperial Valley, and Riverside Counties. Some of the emails the hackers released included closed identity theft case files that contained some of your personal information including, but not limited to, your name, financial account information or credit card number, and possibly your Social Security number.

We have no reason to believe that your information was specifically targeted since Anonymous released the information as part of their ongoing protest against the U.S. Government and law enforcement agencies. Nevertheless, we wanted to inform you of this incident and provide you with some preventative measures you can take to protect yourself from becoming a possible victim of identity theft.

Because your Social Security number was involved, we recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days. Just call one of the three credit reporting agencies at a number below. This will let you automatically place an alert with all of the agencies. You will receive letters from all three, confirming the fraud alert and letting you know how to get a free copy of your credit report from each.

Experian 1-888-397-3742

Equifax 1-800-525-6285

TransUnion 1-800-680-7289

Once you place a fraud alert on your credit files, we recommend you follow the steps outlined in the enclosed *Privacy Protection Recommendations*. For more information on identity theft, you may also visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov.

In addition, although it appears that the identity theft case file in which your information was contained has been closed, you may want to confirm that your financial account has been closed. If it has not, we suggest that you immediately contact the financial institution and close your account. Tell them that your account may have been compromised, and ask that they report it as "closed at customer request." If you want to open a new account, ask them to give you a PIN or password. This will help control access to the account.

We sincerely regret any inconvenience or concern this event may have caused you, and we urge you to consider following the steps we have provided to help protect yourself from the possibility of identity theft. If you have any questions or concerns regarding this letter, you may call (916) 324-0349 or send an email to ecrimeunit@doj.ca.gov. You may also submit any inquiries to the eCrime Unit at P.O. Box 944255, Sacramento, CA 94244-2550.

Enclosure