



KAREN L. SMITH, MD, MPH
Director and State Public Health Officer

State of California—Health and Human Services Agency
California Department of Public Health



EDMUND G. BROWN JR.
Governor

May XX, 2018

Notice of Data Breach

We are writing to you because the California Department of Public Health (CDPH) experienced a privacy breach involving your personal information. We take patient privacy very seriously, and it is important to us that you are made fully aware of a recent event.

What Happened?

On March 12, 2018, a CDPH contractor who performs health facilities inspections on behalf of the department's vehicle was broken into and some documents and a laptop were stolen. The police were immediately notified and a report was taken and documented. Your personal and health information, which we obtained as part of health surveys/inspections, was stolen from the contractor's vehicle.

What Information Was Involved?

The information involved may have included your first and last name, date of birth, Social Security number, address, diagnoses and other health information, health insurance information, and demographic information.

What We Are Doing:

We take this incident very seriously and are taking the necessary precautions to protect all patient related information from theft and other criminal activity. We want to assure you that we are reviewing our procedures and practices and have provided additional training to our workforce to minimize the risk of recurrence.

What You Can Do:

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider or plan to serve as a baseline to ensure accuracy.

Because your Social Security number may have been involved, in order to protect yourself from the possibility of identity theft, we recommend that you place a *fraud alert* on your credit files and order copies of your credit reports by following the recommended privacy protection steps outlined in the enclosure. Check your credit



NAME
Page 2
Date

reports for any accounts that you do not recognize. If you find anything suspicious, follow the instructions found in number four under the *Social Security Number* section of the enclosure.

Since your health insurance information was also involved, we recommend that you regularly review the explanation of benefits statement that you receive from your health insurance provider. If you see any service that you believe you did not receive, please contact the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services in your name or under your plan number.

Other Important Information:

Enclosure "Breach Help –Consumer Tips from the California Attorney General"

For More Information:

For information about your privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection Unit at www.privacy.ca.gov.

Agency Contact:

Should you need any further information about this incident, please contact [name of the designated agency official or agency unit handling inquiries] at [toll-free phone number].

Sincerely,

[Signature of Entity Head or Delegate]
[Title]

Enclosure



Breach Help

Consumer Tips from the California Attorney General

Consumer Information Sheet 17 • October 2014

You get a letter from a company, a government agency, a university, a hospital or other organization. The letter says your personal information may have been involved in a data breach. Or maybe you learn about a breach from a news report or company web site. Either way, a breach notice does not mean that you are a victim of identity theft or other harm, but you could be at risk.

The breach notice should tell you what specific types of personal information were involved. It may also tell you what the organization is doing in response. There are steps you can take to protect yourself. What to do depends on the type of personal information involved in the breach.

Note that credit monitoring, which is often offered by breached companies, alerts you *after* someone has applied for or opened new credit in your name. Credit monitoring can be helpful in the case of a Social Security number breach. It does not alert you to fraudulent activity on your existing credit or debit card account.

Credit or Debit Card Number

The breach notice should tell you when and where the breach occurred. If you used your credit or debit card at the location during the given time, you can take steps to protect yourself.

Credit Card

1. Monitor your credit card account for suspicious transactions and report any to the card-issuing bank (or American Express or Discover). Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.
2. Consider cancelling your credit card if you see fraudulent transactions on it following the breach. You can dispute fraudulent

transactions on your credit card statement, and deduct them from the total due. Your liability for fraudulent transactions is limited to \$50 when you report them, and most banks have a zero-liability policy.¹

3. If you do cancel your credit card, remember to contact any companies to which you make automatic payments on the card. Give them your new account number if you wish to transfer the payments.

Debit Card

1. Monitor your debit card account for suspicious transactions and report any to the card issuer. Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.

2. Report any unauthorized transactions to your bank immediately to avoid liability. Your liability for fraudulent transactions is limited to \$50 if you report them within two days. Your bank may have a zero liability policy. But as time passes, your liability increases, up to the full amount of the transaction if you fail to report it within 60 days of its appearance on your bank statement.²
3. Consider cancelling your debit card. The card is connected to your bank account. Cancelling it is the safest way to protect yourself from the possibility of a stolen account number being used to withdraw money from your bank account. Even though it would likely be restored, you would not have access to the stolen money until after your bank has completed an investigation.

Social Security Number

Here's what to do if the breach notice letter says your Social Security number was involved.

1. Contact the three credit bureaus. You can report the potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus. You will also be sent instructions on how to get a free copy of your report from each of the credit bureaus.

Experian	1-888-397-3742
Equifax	1-800-525-6285
TransUnion	1-800-680-7289
2. What it means to put a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that there may be fraud on the account. This

alerts the merchant to take steps to verify the identity of the applicant. A fraud alert lasts 90 days and can be renewed. For information on a stronger protection, a security freeze, see *How to Freeze Your Credit Files* at www.oag.ca.gov/privacy/info-sheets.

3. Review your credit reports. Look through each one carefully. Look for accounts you don't recognize, especially accounts opened recently. Look in the inquiries section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. You may find some inquiries identified as "promotional." These occur when a company has obtained your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (You are automatically removed from lists to receive unsolicited offers of this kind when you place a fraud alert.) Also, as a general precaution, look in the personal information section for any address listed for you where you've never lived.
4. If you find items you don't understand on your report, call the credit bureau at the number on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to contact the creditors involved and report the crime to your local police or sheriff's office.

Password and User ID

In the case of an online account password breach, you may receive a notice by email or when you go to the log-on page for your account. Here are steps to take if you learn that your password and user ID or email address, or perhaps your security question and answer, were compromised.

1. Change your password for the affected account. If you find that you are locked out of your account, contact the company's customer service or security department.
2. If you use the same password for other accounts, change them too.
3. If a security question and answer was involved, change it. Don't use questions based on information that is publicly available, such as your mother's maiden name, your pet's name or the name of your high school.
4. Use different passwords for your online accounts. This is especially important for accounts that contain sensitive information, such as your medical or financial information. Consider accounts at online merchants where you may have your credit card number stored in the account.
5. Create strong passwords. Longer is better—at least ten characters long and a mix of uppercase and lowercase letters, numerals, punctuation marks, and symbols. Don't use words found in a dictionary. You can base passwords on a phrase, song or book title.

Example: "I love tropical sunsets" becomes
1luv1rop1calSuns3ts!

6. A password manager or password "safe" can help you create and manage many strong passwords. These software programs can run on your computer, your phone and other portable devices. You only have to remember one password (or passphrase) to open the safe. The Electronic Frontier Foundation (www.eff.org) lists some free versions and computer magazines offer product reviews.

Bank Information

If the breach notice says your checking account number, on a check for example, was breached, here's what to do.

1. Call the bank, tell them about the breach and tell them you want to close your account. Find out what checks are outstanding. You may want to wait until they have cleared before closing the account. (Or you could write to each recipient, tell them about the breach, ask them not to process the old check and enclose a new check on your new account.)
2. Open a new bank account. Tell the bank you want to use a new password for access to your new account. Do not use your mother's maiden name or the last four digits of your Social Security number. Ask your bank to notify the check verification company it uses that the old account was closed.

Driver's License Number

If the breach notice says your driver's license or California identification card number was involved, and you suspect that you are a victim of identity theft, contact DMV's Driver License Fraud and Analysis Unit (DLFAU) by telephone at 1 866-658-5758 or by email at dlfraud@dmv.ca.gov. Do not include personal information on your e-mail.

Medical or Health Insurance Information

If the breach notice says your health insurance or health plan number was involved, here's what you can do to protect yourself against possible medical identity theft. A breach that involves other medical information, but not your insurance or plan number, does not generally pose a risk of medical identity theft.

1. If the letter says your Social Security number was involved, see section on Social Security number breaches. Also contact your insurer or health plan, as in number 2 below.
2. If the letter says your health insurance or health plan number was involved, contact

your insurer or plan. Tell them about the breach and ask them to note the breach in their records and to flag your account number.

3. Closely watch the Explanation of Benefits statements for any questionable items. An Explanation of Benefits statement comes in the mail, often marked "This is not a bill." It lists the medical services received by you or anyone covered by your plan. If you see a service that you did not receive, follow

up on it with your insurer or plan. For more on medical identity theft, see *First Aid for Medical Identity Theft: Tips for Consumers*, at www.oag.ca.gov/privacy/info-sheets.

For more details on what to do if you suspect that your information is being used to commit identity theft, see the *Identity Theft Victim Checklist* at www.oag.ca.gov/idtheft/information-sheets.

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice on a particular case, you should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the California Department of Justice, and (3) all copies are distributed free of charge.

NOTES

¹ Truth in Lending Act, 14 U.S. Code sec. 1601 and following.

² Electronic Funds Transfer Act, 15 U.S. Code sec. 1693 and following.