

Fact Sheet

How To Protect Yourself From Identity Theft After A Data Breach

On May 3, the names, Social Security numbers and birth dates of every living veteran from 1975 to the present – more than 26.5 million U.S. veterans in all – were stolen by thieves who took a laptop computer containing the data from the Maryland home of a Department of Veterans Affairs employee. *All 26.5 million veterans whose data was stolen are now at risk for identity theft, because Social Security numbers were involved.*

What is Identity Theft?

Identity theft happens when someone steals your name, your Social Security number, and other personal information and uses that information to get loans, credit cards, cell phone services and more while pretending to be you. Studies show it takes an identity theft victim an average of 330 hours and \$2,671 in out-of-pocket expenses and lost wages to clean up their name and get their life back to normal.

Fortunately, Californians enjoy stronger legal protections against identity theft than people in any other state in the nation. You can dramatically lower your risk of becoming an identity theft victim by knowing your rights and following the steps below.

What Are My Rights?

The California Legislature has passed several laws designed to prevent identity theft:

Right To Keep Your Social Security Number Confidential Social Security numbers are the key to identity theft. Until recently, health plans printed Social Security numbers on medical cards, colleges posted grades by Social Security number, and credit unions and banks made the Social Security number double as checking and savings account numbers. That has all changed now with new California laws banning state government and businesses in California from using Social Security numbers as public identifiers [SB 168 (Bowen), Statutes of 2001; SB 25 (Bowen), Statutes of 2003]. *Unfortunately, these laws do not apply to federal agencies, such as the U.S. Department of Veterans Affairs, which still uses the Social Security number as the primary military identification number.*

Right To Early Warning About Breaches In recent years, hundreds of millions of Americans have been exposed to identity theft because of computer hacking incidents, stolen laptops and other security breaches at corporations and government agencies. In California, you have the right to know when your Social Security number, credit card number or driver's license number is

stolen from a business or government computer [SB 1386 (Peace), AB 700 (Simitian), Statutes of 2002].

With early warning, you can take steps to protect yourself before any damage is done. *In acknowledging the breach, U.S. Department of Veterans Affairs Secretary Jim Nicholson announced a letter would be sent to each U.S. veteran notifying them of the breach.*

Right To Put The "Freeze" On Identity Thieves Every Californian has the right to freeze access to their credit reports – the only truly effective way to foil identity thieves [SB 168 (Bowen), Statutes of 2001]. Once you freeze your credit reports, even if a criminal has your Social Security number, your risk of becoming an identity theft victim drops significantly, because banks can't pull the credit report or even see a credit score. That means the identity thief is denied credit and effectively foiled – no matter where they are in the U.S. and no matter how many different times they apply for loans, credit cards, cell phone service, or anything else in your name.

To find out how to freeze your credit reports, call the California Office of Privacy Protection's hotline at (866) 785-9663 or visit the office's website at <http://www.privacy.ca.gov/sheets/cis10securityfreeze.htm> .

What Steps Should I Take To Protect Myself & Avoid Becoming An Identity Theft Victim?

Monitor your bank and credit card accounts. Check carefully for charges or withdrawals you didn't make and report them to your bank immediately.

Check your credit reports regularly. You can order one free copy of your credit report every year from each of the three national credit reporting agencies, Experian, Equifax, and TransUnion. To make the best use of these, request one of the three reports every four months and check it for signs of identity theft, such as a change of address or a credit card you don't have. Call (877) 322-8288 or visit <http://www.annualcreditreport.com>.

Consider freezing your credit reports to stop identity thieves from getting approved for new loans and credit cards in your name. To find out how to freeze your credit reports, call (866) 785-9663 or visit <http://www.privacy.ca.gov/sheets/cis10securityfreeze.htm> .

What Should I Do If I Become A Victim?

Take these steps immediately if you find out you're a victim of identity theft:

File a police report with your local police department. Be sure to get a copy of your police report, because you will need to give copies of it to banks and credit reporting agencies to clear your name. For more information, visit the Identity Theft Resource Center at www.idtheftcenter.org/vg106.shtml .

Place a fraud alert on your credit reports. You can do this with one phone call. Pick any one of the toll-free numbers below and use the automated system to report your case to the three major credit reporting agencies and place fraud alerts on your credit reports. The other two agencies will be notified automatically. The fraud alert lasts 90 days and warns lenders to take extra measures to verify identity. Experian 1-888-397-3742. Equifax 1-800-525-6285. Trans Union 1-800-680-7289.

Order your credit reports and review them carefully. Once you place the fraud alerts (Step #2), you'll get a letter in the mail from each agency to confirm your fraud alert and tell you how to order a free copy of your credit report, which you're entitled to as a victim. Review your reports carefully for more signs of fraud. Each credit report will have a phone number you can use to talk directly to a live person in the agency's fraud department, so you can report any fraudulent items on your report.

Fill out an Identity Theft Affidavit. The Federal Trade Commission's affidavit form is accepted by most financial institutions and can be found on the FTC's website at: www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf. Send a copy of the affidavit to every bank or business where you have an account that has been compromised or a new account fraudulently opened in your name by an identity thief. You can also file a complaint of identity theft with the FTC at www.consumer.gov/idtheft. The FTC keeps a database of identity theft cases that is used by many law enforcement agencies.

Close all accounts that have been compromised or opened fraudulently. Call and ask to speak with someone in the security or fraud department. Document the date of your phone call, and follow up your call with a letter, including copies of your ID Theft Affidavit (Step #4), your police report (Step #1), and any other supporting documentation. Under California law, you have a right to request account information on fraudulent accounts to help you and the police track down the identity thief.

Send letters to each of the three credit reporting agencies. Itemize each account that has been compromised or opened fraudulently, and remind the agency that they're required by law to block or remove any information on your credit report you identify as fraudulent. Include copies of your police report (Step #1) and your affidavit (Step #4). Send your letters by certified mail, return receipt requested, and keep a copy of each letter.

Equifax P.O Box 740241 Atlanta, GA 30374-0241	Experian P.O. Box 9530 Allen, TX 75013	Trans Union P.O. Box 6790 Fullerton, CA 92834
--	---	--

Instead of mailing a letter, you can also dispute items on your credit report online at: www.equifax.com, www.experian.com, and www.transunion.com/index.jsp .

Consider freezing your credit reports. Remember, fraud alerts only send a warning to creditors, and won't stop an identity thief from being approved for a new loan or service in your name. If you freeze your credit reports, banks can't pull the report or even see a credit score and will not approve new loans and credit cards in your name. To find out how to freeze your credit reports, call (866) 785-9663 or visit <http://www.privacy.ca.gov/sheets/cis10securityfreeze.htm> .

If your driver's license or ID is stolen, contact your local Department of Motor Vehicles (DMV) office to report it stolen and make an appointment to get a replacement. Ask for a fraud alert to be placed on your license. Once you've received your replacement, contact the DMV Fraud Hotline at 866-658-5758 to report your case. For more information, visit the DMV at www.dmv.ca.gov/pubs/brochures/fast_facts/ffd124.htm .

If you are wrongly accused of a crime committed by an identity thief, register with the California Identity Theft Registry at <http://caag.state.ca.us/idtheft/general.htm> and see the Office of Privacy Protection's Information Sheet 8: "How to Use the California Identity Theft Registry - A Guide for Victims of 'Criminal' Identity Theft," available at <http://www.privacy.ca.gov/cover/identitytheft.htm> .

If someone uses your Social Security number to get a job or claim unemployment benefits, contact the California Employment Development Department's toll-free Fraud Hotline at 800-229-6297. For more information, see their web site

at www.edd.ca.gov. Also, contact the federal Social Security Administration's Fraud Hotline at 1-800-269-0271.

Where Can I Get More Information?

This fact sheet is based on information from the following sources:

California Office of Privacy Protection

www.privacy.ca.gov

Toll free: (866) 785-9663

California Department of Justice

<http://www.ag.ca.gov>

Federal Trade Commission

www.consumer.gov/idtheft

Identity Theft Resource Center

www.idtheftcenter.org

Privacy Rights Clearinghouse

www.privacyrights.org.