Identity Theft

California Legislature
Assembly

DAVE COGDILL

ASSEMBLYMAN, 25TH DISTRICT

Dear Friend,

Many of you know people who have become victims of identity theft. You've heard heartbreaking stories about how financially and emotionally devastating this crime can be.

This booklet describes the crime of identity theft. It contains important information on how to safeguard your privacy and gives tips on how to protect yourself from becoming a victim.

It also describes what steps to take if someone steals your identity.

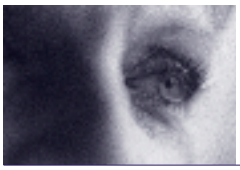
Take the time to read this booklet and to follow some very simple steps to protect yourself and your family.

Special thanks to Turlock Police Detective Kipp Loving, assigned to the Sacramento Valley Hi-Tech Crimes Identity Theft Task Force, and Turlock Police Services in working to make this brochure a possibility. (Revised 10/05)

Capitol Office: P.O. Box 942849 • Sacramento, CA 94249-0025 (916) 319-2025 Phone • (916) 319-2125 Fax

District Office: 1912 Standiford Avenue, Ste 4 • Modesto, CA 95350 • (209) 576-6425 Phone • (209) 576-6426 Fax

table of contents



Identity Theft

what is identity theft?

PC 530.5: Unauthorized Use of Personal Identifying Information

(a) Every person who willfully obtains personal identifying information, as defined in subdivision (b), of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services or medical information in the name of the other person, without the consent of that person, is guilty of a public offense.

(a) "Personal identifying information," means the name, address, phone number, driver's license, social security number, place of employment, employee ID number, mother's maiden name, demand deposit account number, savings account number, or credit card number of an individual person.

In short, identity theft occurs when someone appropriates your personal information without your knowledge to commit fraud or theft. It can happen when the identity theft involves acquiring key pieces of someone's identifying information, (i.e., name and social security number) in order to impersonate them.

Unlike your fingerprints, which are unique to you and cannot be given to someone else for their use, your personal data, especially your social security number, your bank account or credit card number, your telephone calling card number, and other valuable identifying data can be used, if they fall into the wrong hands, to personally profit at your expense.

For victims, this guide will assist you in dealing with the clearing of your name.

If you are not a victim, this guide will help you secure your information better and allow you to spot irregularities of your personal information sooner. Whether or not you are a victim, take the ID theft test on the back resource page to evaluate your vulnerability.

what is California doing about it?

The California Legislature has taken action to prevent identity theft by passing laws that punish the criminals and help victims clear their names.

Following are a few of the laws recently passed by the California Legislature.

- Credit card companies must notify card holders of their right to prohibit disclosure of their personal information.
- Identity theft victims have the right to receive copies of any fraudulent credit, financial or other applications submitted using their identifying information.
- Credit reporting agencies are required to accept "security alerts" from consumers.
- Creditors can't sell a consumer debt to a debt collector if they have reason to believe the consumer is a victim of identity theft.
- The Office of Privacy Protection is created within the Department of Consumer Affairs.
- Social security numbers cannot be printed on material mailed to a person unless required by state or federal law.
- Consumers have the right to request and receive a record of all inquiries made to credit-reporting agencies for the past year.
- Consumers can have their names removed from credit card solicitation mailing lists for a minimum of two years.

How crooks get personal information

- They go through your trash can looking for straight cut or unshredded papers.

  Solution: Always shred pre-approved credit applications, credit card receipts, bills and other financial information you don't want before throwing into the trash.

- They steal your mail.

  Solution: Quickly remove mail from your mailbox or use a P.O. box. Deposit outgoing mail at the post office or in another secure receptacle.

- They listen in on conversations you have in public.

  Solution: Always be aware of your surroundings.

- They buy the information either on the Internet or from someone who might have stolen it.

  Solution: Regularly check your credit report for unauthorized accounts.

- They steal it from a loan or credit application form you filled out or from files at a hospital, bank, school, car lot or business that you deal with. They may have obtained it from dumpsters outside of such companies.

  Solution: Ask questions of businesses you deal with as to how your information will be used and disposed of once no longer needed. Be aware of Assembly Bill 2246 (2000), which requires all banks and businesses to destroy paperwork containing customer's personal and financial information. The business must destroy it by 1) shredding 2) erasing 3) or modifying it in such a manner that it is unreadable or undecipherable. Customers can initiate civil action against the bank or business if they are the victim of identity theft or fraud as a result of them not destroying paperwork properly.

- They get it from your computer, especially those without firewalls.

  Solution: Always use a firewall and virus protection on your computer if connected to the Internet. Keep all programs updated, including your operating system (i.e., Windows 98, XP, etc.)

- They may be a friend or relative or someone who works for or with you who has access to your information.

  Solution: Do not allow anyone you don't fully trust access to your computer or personal information.

Secure your social security number

- Your social security number (SSN) is the key to your credit and banking accounts and is the prime target of criminals. Protect your SSN. Release it only when absolutely necessary (i.e., tax forms, employment records, most banking, stock and property transactions). Do not carry your SSN in your purse or wallet.
- Do not have your SSN printed on your checks. Don't let merchants write it onto your checks because of the risk of fraud.
- Order your Social Security Earnings and Benefits Statement once a year to check for fraud.

Protect your personal information

- Do not carry your Social Security card or number, birth certificate, passport, passwords, or extra credit cards in your purse of wallet.
- Lock your home mailbox, use a mail slot instead of a mailbox, or use a U.S. Post Office box.
- When you pay bills, mail them at a U.S. Post Office. Do not leave them at your home mailbox, your work place's out box, or even your neighborhood Postal Service mailbox. Neighborhood mail boxes can be burglarized.
- Instruct the post office not to process address change requests unless you personally deliver the

request and show identification and proof of residence.

- Before you reveal any personal identifying information to a business, find out how it will be used and whether it will be shared. Ask if you can have your personal information kept confidential.
- Be careful sending personal information over internet chat lines, email or postings.

Credit cards

- Check to see if your ATM/Debit Bank Card has a MC/VISA logo. If so, make a request to disable this feature. An ATM Card requires a pin code to use. However; using the MC/VISA feature allows someone to make purchases without having to use a pin code. Additionally, this money comes directly out of your checking account (and savings account if you have overdraft protection). Suggestion: Use a real Credit Card (Master Card/Visa/American Express). You then have the opportunity to review all charges prior to paying. In fact, reduce the number of credit cards you actively use to a bare minimum. Carry only one or two of them in your wallet. Cancel all unused accounts. Even though you do not use them, their account numbers are recorded in your credit report which is full of data that can be used by identity thieves.
- Keep a list or photocopy of all your credit cards, the account numbers, expiration dates, and telephone numbers of the customer service and fraud departments in a secure place (not your wallet or purse) so you can quickly contact your creditors in case your cards have been stolen. Do the same with your bank accounts.
- Never give out your credit card number or other personal information over the phone unless you have a trusted business relationship with the company and **you** initiated the call.
- Always take credit card receipts with you. Never toss them in a public trash container.

Protect your passwords and PINs

- When creating passwords and PINs (personal identification numbers), do not use the last four digits of your social security number, your birth date, middle name, pet's name, consecutive numbers, or anything else that could easily be discovered by thieves.
- Memorize all your passwords. Don't record them on anything in your wallet or purse.
- Shield your hand when using a bank ATM machine or making long distance phone calls with your phone card. "Shoulder surfers" may be nearby.

Responsible information handling

- Carefully review your credit card statements and phone bills, including cellular phone bills, for unauthorized use.
- Store your canceled checks in a safe place. In the wrong hands, they could reveal a lot of information about you, including the account number, your phone number and driver's license number. Never permit your credit card number to be written onto your checks. It's a violation of California law (California Civil Code 1725) and puts you at risk of fraud.

Internet and On-Line Services

- Use caution when disclosing checking account numbers, credit card numbers or other personal financial data at any web site or on-line service location unless you receive a secured authentication key from your provider.
- When you subscribe to an on-line service, you may be asked to give credit card information. When you enter any interactive service site, beware of con artists who may ask you to "confirm" your enrollment service by disclosing passwords or the credit card account number used to subscribe. Don't give them out!

What is Phishing and Pharming?

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use "spoofed" e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers.

Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crime ware onto PCs to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.

The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically. While online banking and e-commerce is very safe, as a general rule you should be careful about giving out your personal financial information over the Internet. Suggestions on how to avoid becoming a victim of these scams include:

- Be suspicious of any email with urgent requests for personal financial information.
- Don't use the links in an email to get to any web page, if you suspect the message might not be authentic.
- Avoid filling out forms in email messages that ask for personal financial information.
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser.
- Regularly log into your online accounts.
- Regularly check your bank and credit card statements to ensure that all transactions are legitimate.
- Ensure that your browser is up to date and security patches applied.

If you become a victim

- Keep a log of all your contacts and make copies of all documents.
- Contact all creditors, by phone and in writing, to inform them of the problem.
- Contact each of the three credit bureaus' fraud units to report identity theft. Ask to have a "Fraud Alert/Victim Impact" statement placed in your credit file asking that creditors call you before opening any new accounts.
- Request that a copy of your credit report be sent to you.
- If you have been charged with a crime committed by another person using your stolen identity, or if your identity has been mistakenly associated with a record of criminal conviction, you can register to enter your name into California's ID Theft Database. www.caag.state.ca.us/idtheft/general.htm.

Sample Dispute Letter — Credit Bureau

Date

Your Name, Address, City, State, Zip Code

Institution Name, Address, City, State, Zip Code

Ref: (account number if known)

To Whom It May Concern:

I am writing to dispute a fraudulent charge (or debit) attributed to my account in the amount of $_____. I am a victim of identity theft, and I did not make this charge (or debit). I am requesting the charge be removed (or the debit reinstated), that any finance or other charges related to the fraudulent amount be credited as well, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as a police report) supporting my position. Please investigate this matter and correct the fraudulent charge (or debit) as soon as possible.

Sincerely,

Credit bureaus

- **Trans Union:** 800-888-4213, www.tuc.com (fraud div. 800-680-7289)
- **Experian:** 888-EXPERIAN, www.experian.com (fraud div. 888-397-3742)
- **Equifax:** 800-685-1111, www.equifax.com (fraud div. 800-525-6285) TDD 800-255-0056
- Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. Request a free copy of your credit report every few months so you can monitor any new fraudulent activity.
- Alert your banks to flag your accounts and contact you to confirm any unusual activity. Request a change of PIN and a new password.
- If you have any checks stolen or bank accounts set up fraudulently, report it to the following companies:

SCAN – 800-262-7771

TeleCheck – 800-710-9898 or 800-927-0188

Crosscheck – 707-586-0551

Equifax Check Systems – 800-437-5120

International Check Services – 800-526-5380

Social Security Administration's Fraud Hotline – 1-800-269-0271

- Contact the DMV to see if another license was issued in your name. If so, fill out a DMV complaint form to request a new license number and to begin the fraud investigation process.
- Obtain a description of the suspect (if known).
- Obtain witness information.
- What is the financial loss to you? Attach all supporting documents.
- Make note of this case number in your detailed history folder and reference it when you have contact with any business or law enforcement agency concerning this report. Depending upon the location (jurisdiction) of where the crime occurred (goods or services obtained or delivered), an investigator may or may not be assigned to this case.
- If there are workable leads, such as witnesses and suspect information, an investigator may be assigned to the case. Unfortunately, all cases will not be assigned to an investigator.
- Victims can now get information on fraudulent credit accounts opened or applied for using their identity. Use the identity Theft Victim's Fraudulent Account Information Request form and the Letter to Credit Grantors or Utilities to request the information. Download the forms at:
  www. privacyprotection.ca.gov

important resources

Web resources

Anti-Phishing Website:
www.antiphishing.org

Federal Trade Commission:
www.ftc.gov/privacy/protect.htm

ID Theft Center:
858-693-7935 or www.idtheftcenter.org

The Internet Fraud Complaint Center:
www.ifccfbi.gov

Privacy Rights Clearinghouse:
619-298-3396 or www.privacyrights.org

Social Security Administration:
www.ssa.gov

U.S. Postal Service:
www.usps.gov

Direct Marketing Assc. (Mail Fraud):
www.e-mps.org

Direct Marketing Assc. (Phone Fraud):
www.the-dma.org

Calif Department of Consumer Affairs:
www.dca.ca.gov

CardCops:
www.cardcops.com

Sacramento Hi-Tech Task Force:
www.sachitechcops.org
www.stanislaussheriff.com
www.modestopolice.com

Credit Bureaus Main Opt-Out Line
888-567-8688 or www.optoutprescreen.com

test your "Identity Quotient"

Are you at risk for identity theft? Test your "identity quotient" by taking the test below.

1) I receive several pre-approved credit offers every month. (add 1 point) Add 2 more points if you do not shred them before putting them in the trash.
2) I receive several convenience checks in the mail (from credit card companies) every month. (1 pt) Add 2 more points if you do not shred them before putting them in the trash.
3) I carry my Social Security card in my wallet. (3 pts)
4) I do not have a locked, secured mailbox or PO Box in which to receive mail. (1 pt)
5) I leave mail for pickup in an open box at work, clipped to a mailbox or in an unlocked box at my home. (2 pts.)
6) I carry my military ID or Medicare card in my wallet at all times. (1 pt)
7) I do not crosscut shred banking and credit information before I throw it in the trash. (2 pts)
8) I provide my social security number (SSN) whenever asked, without asking how that information will be safeguarded, or why it is necessary for them to have it in the first place. (2 pts)
9) I don't check for people who might be listening before giving out information. (2 pts)
10) My SSN is publicly displayed, or used at work or school. (timecards, receipts, badges) (1 pt for each violation)
11) I have my SSN or driver's license number printed on my personal checks. (2 pts)
12) My SSN is also my driver's license number, and I have made no effort to change that. (2 pts)
13) I carry my insurance card in my wallet and either my SSN, or that of my spouse, is the ID number. (1 pt)

14) I have not ordered copies of my credit reports for at least 1 year. (2 pts) Add 1 more point if it has been more than 2 years.

15) I do not believe people would root around in my trash looking for credit or financial information. (1 pt)

16) I am connected to the Internet, but do not have (or know if I have) firewall software. (2 pts)

Subtract 1 point from your score for each of the following positive steps:

17) I have opted-out of marketing lists through my bank by calling 888-5OPT-OUT.

18) I keep an eye on my credit cards whenever they leave my hands to avoid skimming.

19) I do not respond to Internet scams and hang up on telephone solicitors.

20) I keep personal identifying information in a locked or protected area of my home, one that visitors can't access.

Each one of these questions represents a possible risk factor or protection against ID theft.

More than 20 points —You are at high risk. We recommend you purchase a paper shredder, become more security aware in document handling and start to question why people need your personal data.

10-20 points —You understand identity theft crime trends but still have a ways to go.

0-9 points —Congratulations. Keep up the good work and don't let your guard down now.

Note: Original ID Theft test provided by Utility Consumers' Action Network (UCAN) and Privacy Rights Clearinghouse.

can you tell the difference?

Take an interactive test to see if you can tell the difference between a legitimate website and a phishing website.

Access the test online at Assemblyman Dave Cogdill's website at www.assembly.ca.gov or at www.stanislaussheriff.com.

(Special thanks to Kiplinger's Personal Finance magazine for the use of the interactive phishing test.)

other important numbers

(examples: police fraud hotline, utilities, phone, calling cards, wireless, cable)

fill out & keep in a safe place

credit card name | account number | exp. date

phone numbers | customer service | fraud department

credit card name | account number | exp. date

phone numbers | customer service | fraud department

credit card name | account number | exp. date

phone numbers | customer service | fraud department

credit card name | account number | exp. date

phone numbers | customer service | fraud department

credit card name | account number | exp. date

phone numbers | customer service | fraud department

credit card name | account number | exp. date

phone numbers | customer service | fraud department

credit card name | account number | exp. date

phone numbers | customer service | fraud department

credit card name | account number | exp. date

phone numbers | customer service | fraud department

bank name | account number

phone numbers

bank name | account number

phone numbers

bank name | account number

phone numbers

OTHER ACCOUNTS

Assemblyman Dave Cogdill

District Office
1912 Standiford Ave., #4
Modesto, CA 95350
Phone: (209) 576-6425
Fax: (209) 576-6426

Capitol Office
State Capitol
P.O. Box 942849
Sacramento, CA 94249-0025
Phone: (916) 319-2025
Fax: (916) 319-2125

Web
www.assembly.ca.gov/Cogdill

Email
Assemblymember.Cogdill
@assembly.ca.gov