

SOMEONE IS USING YOUR PERSONAL IDENTIFYING INFORMATION TO OBTAIN GOODS, SERVICES, MEDICAL INFORMATION, CREDIT OR TO OPEN FRAUDULENT CREDIT ACCOUNTS. YOU ARE A VICTIM OF...

# IDENTITY THEFT

HOW TO PREVENT BECOMING A VICTIM

WHAT TO DO IF IT HAPPENS TO YOU



## UCLA POLICE DEPARTMENT

601 WESTWOOD PLAZA  
LOS ANGELES, CA 90095-1364  
(310) 825-1491

[www.ucpd.ucla.edu/](http://www.ucpd.ucla.edu/)

THIS GUIDE PROVIDES INFORMATION ON THE CRIME OF IDENTITY THEFT AS WELL AS RESOURCES ON HOW TO PREVENT BECOMING A VICTIM OF IDENTITY THEFT AND WHAT TO DO IF YOU BECOME A VICTIM OF IDENTITY THEFT. VICTIMS MUST ACT QUICKLY TO MINIMIZE THE DAMAGE.

IN DEALING WITH THE CONTACTS, KEEP A LOG OF ALL CONVERSATIONS, INCLUDING DATES/TIMES, NAMES AND PHONE NUMBERS. CONFIRM CONVERSATIONS IN WRITING. SEND CORRESPONDENCE BY CERTIFIED MAIL, RETURN RECEIPT REQUESTED. KEEP COPIES OF ALL LETTERS AND DOCUMENTS.

IDENTITY THEFT DEFINED .....	4
FEDERAL TRADE COMMISSION STATISTICS ON IDENTITY THEFT .....	6
INTERNET CRIME COMPLAINT CENTER (IC3) STATISTICS ON INTERNET CRIME .....	6
PREVENTIVE ACTIONS .....	8
CREDIT MONITORING SERVICES .....	8
Equifax CreditWatch .....	8
Experian CreditExpert .....	8
TransUnion TrueCredit.....	8
PERSONAL FINANCIAL INFORMATION .....	10
Companies That May Send Privacy Notices .....	10
What You Can Stop — And What You Can't Stop.....	10
What Opting Out Means .....	11
Your Right To Opt Out.....	11
Privacy Notices You May Receive.....	12
What To Do When You Receive Your Notices .....	12
Additional Laws Affecting Your Personal Financial Information.....	12
FAIR AND ACCURATE CREDIT TRANSACTIONS ACT (FACTA) OF 2003.....	13
One-Call Fraud Alerts .....	13
Trade Line Blocking .....	13
Business Records Disclosure .....	13
Red Flag Guidelines for New Accounts and Change of Address Verification .	13
Credit Card Number Truncation on Consumer Reports .....	14
Social Security Number Truncation.....	14
Prohibits Sale or Collection of ID Theft Debts.....	14
Debt Collector Notice Requirements.....	14
Prevention of Repollution .....	14
Annual Free Credit Reports .....	14
Reinvestigations.....	14
FTC to Create Summary of Rights for Consumers .....	14
Credit Bureaus Must Provide Credit Scores.....	14
Mortgage Lenders Must Provide Credit Scores .....	15
One-Time Written Notification That Negative Information Will Be or Has Been Sent to Credit Bureaus.....	15
New Risk Based Pricing Notice.....	15
Higher Standard for Furnishers of Information to CRAs.....	15
Consumers Can Dispute Incorrect Information Directly With Furnisher .....	15
Improved Disclosure of Results of Reinvestigation .....	15
Requirement for Furnishers to Update Records.....	15
Notification of Address Discrepancy .....	15
Stronger Opt-Out for Prescreening Based on Credit Report Information .....	15
New Opt-Out for Marketing Solicitations That Are Based On Information Shared Among Affiliates .....	15
Medical Information Protections.....	16
Statute of Limitations .....	16
Workplace Investigations .....	16
State Preemptions .....	16
RECOMMENDATIONS.....	18
Direct Marketing Association .....	20

WHAT TO DO IF YOU ARE THE VICTIM OF IDENTITY THEFT.....	21
1. Law Enforcement.....	21
UCLA Police Department.....	21
2. Credit Bureaus.....	21
Equifax .....	22
Experian .....	22
Trans Union.....	22
3. Identity Theft One-Call Program .....	22
4. Freezing Credit Reports.....	23
How to Do It.....	23
4. Opt Out Of Pre-Approved Offers Of Credit .....	24
5. California's Identity Theft Database .....	24
California Attorney General's Office .....	25
6. Creditors .....	25
7. Stolen Checks .....	25
<b>BAD CHECK RESTITUTION PROGRAM</b> .....	26
8. ATM Cards .....	26
9. Fraudulent Change Of Address .....	26
10. Secret Service Jurisdiction .....	27
11. Social Security Number (SSN) Misuse .....	27
12. Passports.....	27
13. Phone Service .....	27
14. Driver's License Number Misuse .....	28
15. False Civil And Criminal Judgments .....	28
16. Legal Help .....	28
UCLA Student Legal Services.....	28
17. Dealing With Stress .....	29
UCLA Student Psychological Services .....	29
UCLA Center for Women and Men .....	29
18. Making Change .....	29
19. Don't Give In.....	29
RESOURCES.....	30
California Office of Privacy Protection.....	30
Federal Trade Commission.....	30
Federal Bureau of Investigation .....	30
California Department of Consumer Affairs.....	30
Los Angeles County Department of Consumer Affairs.....	30
United States Department of Justice.....	30
CALPIRG .....	30
Privacy Rights Clearinghouse .....	30
Identity Theft Resource Center .....	30
Identity Theft Survival Kit .....	30
National Fraud Information Center .....	30
Consumer Credit Counseling .....	31
Federal Citizen Information Center .....	31
Better Business Bureau of the Southland .....	31

# **IDENTITY THEFT DEFINED**

## **CALIFORNIA PENAL CODE SECTION 530.5 & 530.55**

### **UNAUTHORIZED USE OF PERSONAL IDENTIFYING INFORMATION TO OBTAIN, CREDIT, GOODS, SERVICES OR MEDICAL INFORMATION IN THE NAME OF ANOTHER PERSON.**

**530.5** (a) Every person who willfully obtains personal identifying information, as defined in subdivision (b) of Section 530.55, of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person, is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment in the state prison.

(b) In any case in which a person willfully obtains personal identifying information of another person, uses that information to commit a crime in addition to a violation of subdivision (a), and is convicted of that crime, the court records shall reflect that the person whose identity was falsely used to commit the crime did not commit the crime.

(c) (1) Every person who, with the intent to defraud, acquires, or retains possession of the personal identifying information, as defined in subdivision (b) of Section 530.55, of another person is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or both a fine and imprisonment.

(2) Every person who, with the intent to defraud, acquires or retains possession of the personal identifying information, as defined in subdivision (b) of Section 530.55, of another person, and who has previously been convicted of a violation of this section upon conviction therefor shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment in the state prison.

(3) Every person who, with the intent to defraud, acquires or retains possession of the personal identifying information, as defined in subdivision (b) of Section 530.55, of 10 or more other persons is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment in the state prison.

(d) (1) Every person who, with the intent to defraud, sells, transfers, or conveys the personal identifying information, as defined in subdivision (b) of Section 530.55, of another person is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment in the state prison.

(2) Every person who, with actual knowledge that the personal identifying information, as defined in subdivision (b) of Section 530.55, of a specific person will be used to commit a violation of subdivision (a), sells, transfers, or conveys that same personal identifying information is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in the state prison, or by both fine and imprisonment.

(e) Every person who commits mail theft, as defined in Section 1705 of Title 18 of the United States Code, is guilty of a public offense, and upon conviction therefor shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment. Prosecution under this subdivision shall not limit or preclude prosecution under any other provision of law, including, but not limited to subdivisions (a) to (c), inclusive, of this section.

(f) An interactive computer service or access software provider, as defined in subsection (f) of Section 230 of Title 47 of the United States Code, shall not be liable under this section unless the service or provider acquires, transfers, sells, conveys, or retains possession of personal information with the intent to defraud.

**530.55** (a) for purposes of this chapter, "person" means a natural person, living or deceased, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity, or any other legal entity.

(b) for purposes of this chapter, "personal identifying information" means any name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license, or identification number, social security number, place of employment, employee identification number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, pin (personal identification number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the person, address or routing code, telecommunication identifying information or access device, information contained in a birth or death certificate, or credit card number of an individual person, or an equivalent form of identification.

## FEDERAL TRADE COMMISSION STATISTICS ON IDENTITY THEFT

The [Federal Trade Commission](#) (FTC) complaint figures are derived from self-reported and unverified consumer complaints contained in the FTC's database. Percentages are based on the total number of complaints in the Identity Theft Data Clearinghouse: 43,892 from California consumers and 258,427 from consumers in all locations. The FTC notes that 17% of identity theft complaints from California consumers and 16% of identity theft complaints from consumers in all locations include more than one type of identity theft. To read statistics for California go to [FTC California Identity Theft Statistics](#).

Consumer Sentinel, the complaint database developed and maintained by the FTC, receives consumer fraud and identity theft complaints. To read the statistics go to [FTC Consumer Sentinel](#).

- Credit card fraud (23%) was the most common form of reported identity theft followed by phone or utilities fraud (18%), employment fraud (14%) and bank fraud (13%). Other significant categories of identity theft reported by victims were government documents/benefits fraud (11%) and loan fraud (5%).
- Electronic fund transfer-related identity theft continues to be the most frequently reported type of identity theft bank fraud during calendar year 2007.
- The metropolitan areas with the highest per capita rates of reported identity theft are Napa, California; Madera, California; and Greeley, Colorado.

## INTERNET CRIME COMPLAINT CENTER (IC3) STATISTICS ON INTERNET CRIME

The 2008 Internet Crime Report at the [Internet Crime Complaint Center](#) is the annual compilation of information on complaints received and referred by the IC3. From January 1, 2008 to December 31, 2008, the IC3 website received 275,284 complaint submissions. This is a 33.1% increase when compared to 2007. These filings were composed of complaints primarily related to fraudulent and non-fraudulent issues on the Internet.

From the submissions, IC3 referred 72,940 complaints of crime to federal, state and local law enforcement agencies around the country for further consideration. The vast majority of cases were fraudulent in nature and involved a financial loss on the part of the complainant. The total dollar loss from all referred cases of fraud was \$264.6 million with a median dollar loss of \$931.00 per complaint. This is up from \$239.1 million in total reported losses in 2007. Other significant findings related to an analysis of referrals include:

- Non-delivered merchandise and/or payment was, by far, the most reported offense, comprising 32.9% of referred complaints. Internet auction fraud accounted for 25.5% of referred complaints. Credit/debit card fraud made up 9.0% of referred complaints. Confidence fraud, computer fraud, check fraud and Nigerian letter fraud round out the top seven categories of complaints referred to law enforcement during the year.
- Of those complaints reporting a dollar loss, the highest median losses were found among check fraud (\$3,000), confidence fraud (\$2,000), Nigerian (West African, 419, Advance Fee) letter fraud (\$1,650).
- Among perpetrators, 77.4% were male and half resided in one of the following

states: California, New York, Florida, Texas, District of Columbia and Washington. The majority of reported perpetrators (66.1%) were from the United States; however, a significant number of perpetrators were also located in the United Kingdom, Nigeria, Canada, China and South Africa.

- Among complainants, 55.4% were male, nearly half were between the ages of 30 and 50 and one-third resided in one of the four most populated states: California, Florida, Texas and New York. While most were from the United States (92.4%), IC3 received a number of complaints from Canada, United Kingdom, Australia, India and France.
- Males lost more money than females (ratio of \$1.69 dollars lost per male to every \$1.00 dollar lost per female). This may be a function of both online purchasing differences by gender and the type of fraudulent schemes by which the individuals were victimized.
- E-mail (74.0%) and web pages (28.9%) were the two primary mechanisms by which the fraudulent contact took place.

## PREVENTIVE ACTIONS

1. Subscribe to a credit monitoring service through one of the three credit bureaus. Typically, the service sends emails to alert the subscriber that an inquiry has been made to your credit file. The subscriber can go online to view the information on the inquiry. Some of the services also provide online access to copies of your credit report.

### CREDIT MONITORING SERVICES

#### Equifax CreditWatch

[www.equifax.com](http://www.equifax.com)

- E-mail alerts within 24 hours of possible identity theft activity
- \$20,000 identity theft insurance (no deductible; some limits apply) protects your finances
- Monthly "No Alerts" e-mail, delivers peace of mind
- Premium Customer Care 1-800 "hotline" available 24 hours a day, 7 days a week
- Victim assistance provided via personalized identity fraud specialist
- Online dispute saves you time and money
- Unlimited access to your Equifax Credit Report

#### Experian CreditExpert

[www.creditexpert.com](http://www.creditexpert.com)

- Unlimited access to your Experian credit report updated daily
- Unlimited access to your credit score updated daily
- Constant monitoring to alert you of potential fraudulent activity
- Your own personalized page to give you a snapshot of your credit and score trends
- Interactive score simulator to show you what factors most affect your credit score

#### TransUnion TrueCredit

[www.truecredit.com](http://www.truecredit.com)

- Receive weekly email alerts to changes in your report
- Immediately find out about credit report changes including fraudulent activity, new inquiries, new accounts, late payments, etc.
- Receive a brand new credit report four times per year  
Reports are easy-to-read with color graphics and free interactive guide
- Should you become a victim of identity theft, TrueCredit provides you with Fraud Resolution services to assist you in the recovery of financial and credit losses
- Graphical trending helps you manage your progress
- View colorful charts and graphs on changes to your debt, income, credit score and more.

2. Obtain a copy of your credit report each year from Equifax, Experian and/or TransUnion. Review the reports ensure no one is using your identity to open new accounts or to use your existing accounts. Check for fraudulent activity or other discrepancies.

A provision of the **Fair and Accurate Credit Transactions Act** requires the three national credit bureaus to operate a centralized resource from which consumers can obtain a free copy of each of their credit reports once every 12 months.

Equifax, Experian and TransUnion's electronic files frequently contain different data because some creditors report to one or two bureaus while some report to none.

Visit <http://www.annualcreditreport.com/> to identify the state where you live. You will be asked to enter key personal identifying information, which is all kept secure by a range of anti-hacker technology, including date of birth and Social Security number. Since some of the authentication questions will be highly specific, such as the name of your mortgage company or the amount of your monthly mortgage payment, it is strongly recommend that you have your personal financial documents handy when you visit the site. The authentication procedures will never require you to divulge credit card or bank account numbers.

The site will not require ordering all three credit reports simultaneously. Stretching out your right to a free annual credit report over a period of months might be useful for anyone who anticipates significant financial events during the year ahead.

For example, you plan to buy a house early in 2010 and you are eligible for a free report December 1. You could order your Experian free credit report now and check for any errors or omissions, well in advance of applying for a mortgage. And you also expect to purchase a new vehicle next year. You could order your free TransUnion report in advance of your loan application, again checking for errors or omissions that could affect your borrowing costs. Finally, you could order your free Equifax report next fall and start the whole process over again next December.

Once you've selected a bureau report, AnnualCreditReport.com will transfer you to that bureau's site, where you should get your file within a short time. The credit bureau also will let you order your credit score, plus an array of other proprietary credit tools and services. For example, only Equifax sells FICO scores, which are used by most credit lenders to evaluate your application for a loan. The cost will be \$6.95 per FICO score. TransUnion and Experian will sell their own non-FICO scores for approximately \$4 each.

Experian will offer a new "Triple Alert" credit-monitoring system for \$4.95 a month, which will notify consumers of every inquiry or credit file change in each of their three online bureau credit files. The alerts will come in the form of cell phone text messages and emails and will direct consumers to check their customized credit pages at the Experian site to see what changes occurred.

## **PERSONAL FINANCIAL INFORMATION**

You've probably been receiving privacy notices from banks and other financial companies. These notices explain:

- What personal financial information the company collects
- Whether the company intends to share your personal financial information with other companies
- What you can do, if the company intends to share your personal financial information, to limit some of that sharing
- How the company protects your personal financial information.

Financial companies share information for many reasons: to offer you more services, to introduce new products, and to profit from the information they have about you. If you like to know about other products and services, you may want your financial company to share your personal financial information; in this case, you don't need to respond to the privacy notice. If you prefer to limit the promotions you receive or do not want marketers and others to have your personal financial information, you must take some important steps.

First, it is important to read these privacy notices. They explain how the company handles and shares your personal financial information. Keep in mind that not all privacy notices are the same. This guide tells you about the other steps you can take to help protect the privacy of your personal financial information.

### **COMPANIES THAT MAY SEND PRIVACY NOTICES**

Companies involved in financial activities must send their customers privacy notices, including:

- Banks, savings and loans, and credit unions
- Insurance companies
- Securities and commodities brokerage firms
- Retailers that directly issue their own credit cards (such as department stores or gas stations)
- Mortgage brokers
- Automobile dealerships that extend or arrange financing or leasing
- Check cashers and payday lenders
- Financial advisors and credit counseling services
- Sellers of money orders or traveler's checks.

### **WHAT YOU CAN STOP — AND WHAT YOU CAN'T STOP**

Federal privacy laws give you the right to opt out of some sharing of your personal financial information. These laws balance your right to privacy with financial companies' need to provide information for normal business purposes. You have the right to opt out of some information sharing with companies that are:

- Part of the same corporate group as your financial company (or affiliates)
- Not part of the same corporate group as your financial company (or non-affiliates).

- But, you cannot opt out and completely stop the flow of all your personal financial information. The law permits your financial companies to share certain information about you without giving you the right to opt out. Among other things, your financial company can provide to non-affiliates:
  - Information about you to firms that help promote and market the company's own products or products offered under a joint agreement between two financial companies
  - Records of your transactions —such as your loan payments, credit card or debit card purchases, and checking and savings account statements—to firms that provide data processing and mailing services for your company
  - Information about you in response to a court order
  - Your payment history on loans and credit cards to credit bureaus.

#### WHAT OPTING OUT MEANS

- If you opt out, you limit the extent to which the company can provide your personal financial information to non-affiliates.
- If you do not opt out within a “reasonable period of time”, generally about 30 days after the company mails the notice, then the company is free to share certain personal financial information.
- If you didn't opt out the first time you received a privacy notice from a financial company, it's not too late. You can always change your mind and opt out of certain information sharing. Contact your financial company and ask for instructions on how to opt out.
- Remember, however, that any personal financial information that was shared before you opted out cannot be retrieved.

#### YOUR RIGHT TO OPT OUT

A privacy notice contains information about the company's data collection and information sharing policies. If a financial company does not plan to share your information except as permitted by law, the notice will tell you this. In this case, you don't have a right to opt out.

**Non-affiliates.** If you have the right to opt out (that is, if the company plans to share your information), the privacy notice will include instructions on how to opt out of sharing some information. Unless you opt out, your financial company can provide your personal financial information (for example, information on the kinds of stores you shop at, how much you borrow, your account balances or the dollar value of your assets) to non-affiliates for marketing and other purposes.

**Affiliates.** The privacy notice may also give you the right to opt out of certain information sharing with affiliates. For example, if a company intends to provide an affiliate with personal information from your credit report or loan application, you will usually first be given a chance to opt out. Companies, however, can share information about you with affiliates when the information is based solely on your transactions with that company (transaction information includes whether you pay your bills on time, the type of accounts you have with the company, etc.). Read your notices carefully to see if this type of opt out applies.

If you want to opt out of information sharing, you must follow the directions provided by

your financial company. For example, you may have to call a toll-free number or fill out a form and return the form to the company. In some cases, your financial company may give you the choice to opt out of different types of sharing. For example, you could opt out of certain categories of information the company provides to other companies but allow the company to share other kinds of information.

Credit bureaus may also sell information about you to lenders and insurers who use the information to decide whether to send you unsolicited offers of credit or insurance. This is known as prescreening. You can opt out of receiving these prescreened offers by calling **(888) 567-8688**.

#### **PRIVACY NOTICES YOU MAY RECEIVE**

**Initial Privacy Notice.** You will usually receive a privacy notice when you open an account or become a customer of a financial company. If you open an account over the phone, however, and you agree, the company may send you a notice at a later time.

**Annual Privacy Notices.** Each financial company you have an ongoing relationship with. For example, the bank where you have a checking account, your credit card company or a company that services your loan must give you a notice of its privacy policy annually.

**Notice of Changes in Privacy Policies.** If a company changes its privacy policy, it will either send you a revised privacy notice or tell you about the changes in the company's next annual notice.

A privacy notice may be included as an insert with your monthly statement or bill or it may be sent to you in a separate mailing. If you agree to electronic delivery from an on-line financial company, the notice may be sent to you by e-mail or it may be made available to you on the company's web site.

If you have more than one account with the same company, the company may send you only one privacy notice for all of your accounts or it may send you separate notices for each of your accounts.

If you have a joint account with another person (for example, a joint checking account or a mortgage loan), the financial company may send a notice to one of you or to each person listed on the account. If the company provides an opportunity to opt out, it must let one of the account holders opt out for all joint account holders.

#### **WHAT TO DO WHEN YOU RECEIVE YOUR NOTICES**

- Read all privacy notices.
- Get answers to your questions from your financial company.
- If applicable, decide whether you want to opt out.
- If you want to opt out, follow the instructions in the notice—and, if necessary, shop around for a financial institution with the privacy policy you want.

#### **ADDITIONAL LAWS AFFECTING YOUR PERSONAL FINANCIAL INFORMATION**

Two federal laws cover different aspects of how companies can share your financial

information, as described in this guide: The **Fair Credit Reporting Act** and the **Gramm-Leach-Bliley Act**.

**The Fair Credit Reporting Act** protects the privacy of certain information distributed by consumer reporting agencies (CRA's). Most CRA's are credit bureaus that gather and provide information about you, such as if you pay your bills on time or have filed for bankruptcy, to creditors and other businesses. Under the law, credit bureaus and other CRA's can release your information only to those third parties that have certified that they have a purpose permitted by the law to obtain your consumer report, such as to evaluate your application for credit, Insurance, or employment, or to rent you an apartment.

When a financial company obtains your credit report from a credit bureau, it may want to share that information with an affiliate, meaning a company that owns your financial company that your financial company owns, or that is part of the same parent organization or corporate family. Under the Fair Credit Reporting Act, however, if the financial company plans to share certain information, for example, from your credit report or your credit application, with its affiliates, it will usually first notify you and give you an opportunity to opt out. This notice is likely to be included in the privacy notice you receive from the financial company under the Gramm-Leach-Bliley Act.

### **FAIR AND ACCURATE CREDIT TRANSACTIONS ACT (FACTA) OF 2003**

**One-Call Fraud Alerts:** Establishes the right of any consumer to request a fraud alert for 90 days or if a consumer provides an identity theft report, the consumer could place an extended fraud alert of seven years in his or her credit file. The alert must be included with a credit report and with the delivery of a credit score. Users of reports and scores have a new duty to honor fraud alerts. They cannot issue a new credit line, extension of credit, new cards or a requested higher credit limit on existing accounts unless the consumer is called or other reasonable verification steps are taken. Any credit bureau contacted by a consumer must inform other bureaus that a fraud alert has been placed (one-call fraud alert). Persons who file an extended fraud alert are automatically opted out of pre-screening for five years. Active duty military personnel gain the right to request one-year "active-duty" alerts. All consumers who place an alert may receive a free credit report. Persons who place an extended fraud alert may also get two free reports in the first year.

**Trade Line Blocking:** Requires Consumer Reporting Agencies (CRA's or credit bureaus) to block fraudulent trade lines when a consumer provides an identity theft report, provided that it has been filed with a law enforcement agency.

**Business Records Disclosure:** Allows ID theft victims with a police report (a higher standard than "identity theft report") to request and get copies of records from businesses where an identity thief opened accounts or obtained goods or services, to help clear their names. The business may insist on a police report and may take 30 days to provide the information.

**Red Flag Guidelines for New Accounts and Change of Address Verification:** Regulators are required to establish guidelines for issuers to follow to identify patterns and practices leading to identity theft. The regulations will require reasonable procedures to comply with the guidelines. The regulations will also require card issuers

to verify changes of address in certain circumstances (e.g. when a request for a new card comes within 30 days following a change of address).

**Credit Card Number Truncation on Consumer Reports:** Requires credit card machines to truncate all credit and debit card numbers on non-manual receipts by 2007.

**Social Security Number Truncation:** Allows a consumer to request that the credit report disclosed to the consumer truncate any included Social Security Numbers.

**Prohibits Sale or Collection of ID Theft Debts:** Prohibits any person or business from selling, transferring or placing for collection any item subject to an identity theft trade line block or debt which resulted from identity theft once the block has been placed and the creditor has notice of the block. However, there is an exemption for information provided in the securitization of debts.

**Debt Collector Notice Requirements:** Any third-party debt collector that is notified that the debt they are trying to collect may be fraudulent must notify the third-party and also must provide the consumer upon request with notice of his/her rights in debt collection.

**Prevention of Repollution:** Creditors and others who furnish information to a CRA and who are notified by a CRA of the existence of an identity theft trade line block must maintain reasonable procedures to prevent refurnishing (repollution) of the information arising from the ID theft. A furnisher receiving an identity theft report at a proper address may not refurnish such information unless it subsequently verifies that information.

**Annual Free Credit Reports:** Each national credit bureau must provide a free report upon request within 15 days of a request by phone, Internet or mail through a one-call centralized source to be established by the FTC within a year. Reports will also be available from specialty bureaus, such as landlord-tenant or insurance reporting services, with the method of distribution to be established in regulations to be issued within six months, effective six to nine months thereafter. States are preempted from increasing the frequency of the provision of free reports.

**Reinvestigations:** CRA's have 45 days to conduct reinvestigations of disputed items resulting from free report requests (compared to 30-45 days for all other reinvestigations). This does not apply if the CRA has not been continuously providing consumer reports for 12 months preceding request.

**FTC to Create Summary of Rights for Consumers:** These rights include the availability of free credit reports, the right to dispute information in a credit report and how to request and obtain credit score. The summary of rights will be distributed with adverse action notices (if a consumer is denied or offered credit at less than favorable terms) and actively promoted by FTC and posted on its website. This summary must also tell consumers that they may have additional rights under state law.

**Credit Bureaus Must Provide Credit Scores** and information on up to four key factors (or five factors if the number of inquiries was a factor and not among the four key factors) adversely affecting a consumer's score. Bureaus can charge a "fair and reasonable fee" for score, as determined by the FTC. This does not apply to mortgage scores, such as those created by automated underwriting programs.

**Mortgage Lenders Must Provide Credit Scores** and information on key factors lowering a consumer's score to those who apply for mortgages. No fee is authorized for this disclosure. States are preempted from acting further regarding the disclosures of credit scores for credit granting purposes (California statutes grandfathered). States are allowed to continue to act in the area of insurance scores, credit based scores used in connection with insurance, and credit score issues other than disclosure issues.

**One-Time Written Notification That Negative Information Will Be or Has Been Sent to Credit Bureaus:** Any financial institution that submits negative information to national CRA must give consumers one-time written notice that they have done so or will do so. This notice may be included in a notice of default or a billing statement, but not with Truth in Lending disclosures.

**New Risk Based Pricing Notice:** The Act establishes a new notice for certain additional circumstances. Whenever credit is extended on terms "materially less favorable than the most favorable terms available to a substantial proportion of consumers" from that creditor, creditors must provide notice that the terms offered are based on information in a consumer's credit report and that the consumer can request a free copy of the report. (No civil enforcement is allowed – federal enforcement only.)

**Higher Standard for Furnishers of Information to CRAs:** The new standard prohibits reporting of inaccurate information if the furnisher "knows or has reasonable cause to believe that the information is inaccurate."

**Consumers Can Dispute Incorrect Information Directly With Furnisher:** The new law requires financial regulators and the FTC to prescribe regulations outlining circumstances when creditors and other furnishers of information to CRAs should reinvestigate complaints that come directly from a consumer. (Exempts disputes filed by credit repair organizations. This new right does not provide a private right of action.)

**Improved Disclosure of Results of Reinvestigation:** CRAs must notify furnishers when changes are made because of a reinvestigation based on a consumer complaint about a credit reporting error.

**Requirement for Furnishers to Update Records:** Furnishers must change records, delete records, or permanently block reporting to CRAs of information found to be inaccurate or incomplete.

**Notification of Address Discrepancy:** CRAs must notify anyone requesting a consumer's report if the address on the request substantially differs from the address in the consumer's file.

**Stronger Opt-Out for Prescreening Based on Credit Report Information:** Prescreened offers of credit must contain a phone number to opt out of such offers in a simple and easy to understand format, as outlined by regulation within one year of enactment. Extends the duration of the telephone-initiated opt out from two years to five years. (Under current law, a mailed "notice of election" results in a permanent opt out.)

**New Opt-Out for Marketing Solicitations That Are Based On Information Shared Among Affiliates:** Consumers must be provided the opportunity to opt out of receiving solicitations for marketing purposes based on information shared among corporate

affiliates, effective for at least five years, after which the consumer must be given notice and the opportunity to opt out again. Exempts marketing when a preexisting relationship has existed with customers within 18 months, for employee benefit plans, and to perform services on behalf of an affiliate (but one affiliate cannot solicit on behalf of an affiliate that is prohibited from soliciting), and in response to communications initiated by the consumer or in response to solicitations initiated by or requested by consumer. Does not apply to information received prior to the effective date of regulations. This notice can be combined with other notices.

**Medical Information Protections:** Any medical information in a consumer report must be coded to obscure the specific healthcare provider and the nature of medical services provided. Creditors are prohibited from obtaining or using medical information in credit decisions. Prohibits the sharing among affiliates of medical information, including individual or aggregate lists based on payments for products or services. Medical providers must identify themselves as such within 15 months.

**Statute of Limitations:** Provides for opportunity to sue two years following discovery or five years following date of violation, whichever is earlier.

**Workplace Investigations:** The act weakens certain protections provided to employees when investigations are conducted in the workplace of alleged sexual harassment, embezzlement, drug use, etc.

### **State Preemptions**

The Act makes permanent the seven preemptions enacted in 1996 and otherwise set to expire:

- Prescreening of consumer reports;
- Time frames for handling accuracy disputes;
- Duties of persons who take adverse actions (notices and disclosures);
- Duties of persons who use consumer reports in connection with credit or insurance transactions not initiated by a consumer;
- Information contained in consumer reports;
- Duties of furnishers of information to consumer reporting agencies, and
- Sharing information among affiliates.

The Act enacts the following new preemptions:

- Obligation on businesses who grant credit or provide goods or services to ID thieves to provide information to victims;
- Consumers' rights to opt out of solicitations based on affiliate shared information;
- Risk based pricing notices;
- Annual free credit reports (with grandfathering of existing laws), and
- Credit score disclosure by CRA's and by mortgage lenders when the score is for credit granting purposes;

The Act enacts narrower ID theft preemptions, whereby state laws are restricted only with respect to the "conduct required by the specific provisions of" these identified sections of the FCRA:

- Truncation of credit/debit card numbers on receipts;

- Placement of fraud alerts and active duty military alerts;
- Blocking of information resulting from ID theft;
- Allowing consumer to request truncation of Social Security Numbers on communications sent to them;
- Red flag guidelines regarding ID theft;
- Prohibiting the sale or collection of debts resulting from ID theft and requiring third party debt collectors to notify creditors if they learn that a debt has resulted from ID theft;
- Referral process between CRA's regarding ID theft complaints, fraud alerts, and blocking of information;
- Various disclosures, including the summary of rights to obtain credit report and score and to dispute information, the summary of ID theft victim rights, and the right of ID theft victim to get information from businesses;
- Procedures to prevent refurnishing of information resulting from ID theft;
- Annual free credit reports for ID theft victims (this is listed in two parts of the bill), and
- Disposal of records containing information from credit reports.

**The Gramm-Leach-Bliley Act** requires financial companies to tell you about their policies regarding the privacy of your personal financial information. With some exceptions, the law limits the ability of financial companies to share your personal financial information with certain non-affiliates. A non-affiliate is a company that is unrelated to your financial company and may include:

- **Service providers** – companies hired by your financial company to perform a specific service, such as printing your checks
- **Joint marketers** – companies that have an agreement with your financial company to offer you other financial products or services
- **Other third-party non-affiliates** – which could include companies that may want access to your financial company's mailing list to tell you about other products and services.

Under the Gramm-Leach-Bliley Act, your financial company can provide your personal financial information to non-affiliated service providers including joint marketers.

But before it shares your information with other third party non-affiliates (outside of these exceptions), your financial company must tell you about its information sharing practices and give you the opportunity to opt out.

## RECOMMENDATIONS

- ❖ **Remove your listing from the UCLA electronic directory** through URSA. Students may change address information, telephone numbers, e-mail address and privacy options through URSA Online. If you need an email address for classes or online shopping, use a free browser based service. <http://www.ursa.ucla.edu/>
- ❖ **Remove your personal information** from personal profile websites such as MySpace and Facebook.
- ❖ **Review privacy choices for your personal financial information.** Consider opting out of allowing your financial institution or other specified company from sharing your personal information.
- ❖ **Never give personal information over the telephone**, such as your social security number, date of birth, mother's maiden name, credit card number or bank PIN code, unless you initiated the phone call. Protect this information and release it only when absolutely necessary. Similarly, avoid confirming such information to a stranger on the telephone.
- ❖ Before disclosing any personal information, make sure you **know why it is required** and how it will be used.
- ❖ **Do not give out your Social Security number (SSN)** to people or companies that you do not know.
- ❖ **Do not write your SSN or credit card numbers on checks.** The SSN is a prime target of criminals and provides them with the key to unlock a variety of personal information.
- ❖ **Do not leave your backpack, laptop computer, briefcase, purse or wallet unattended** when away from home.
- ❖ **Keep the personal information you have at home and at work in a safe place.**
- ❖ At work, **lock up your property** in a locked desk drawer or filing cabinet.
- ❖ On campus, **do not leave your property unattended** in a library or classroom.
- ❖ Use a **locking mailbox** for incoming mail or consider using a commercial mailbox service.
- ❖ **Promptly remove mail** from your mailbox after delivery.
- ❖ Deposit **outgoing mail in post office collection mailboxes or at your local post office.** Do not leave mail in unsecured mailboxes.
- ❖ **Shred pre-approved credit applications, credit card receipts, bills** and other financial information you don't want before discarding them in the trash or recycling bin.
- ❖ The credit issuer must verify address if both of the following occur: an application of credit shows a different address than the one on the pre-approved offer and a request for an additional credit card comes within 10 days of a request for a change of address per California Civil Code § 1747.06.
- ❖ **Shred information you no longer need** that contains personally identifiable information and account numbers. For example, credit card receipts, billing statements and pre-approved credit offers should be shredded before you discard them.
- ❖ **Do not carry extra credit cards**, your birth certificate or passport, or other cards that display your Social Security number in your wallet or purse, except when necessary.
- ❖ **Empty your wallet of extra credit cards and ID's**, or better yet, cancel the ones you do not use and maintain a list of the ones you do.
- ❖ **Create unique passwords and personal identification numbers (PINS)** and

avoid using easily available information such as mother's maiden name, date of birth or the last four digits of your Social Security number. Use passwords on your banking and brokerage accounts.

- ❖ **Order a copy of your credit report** from each of the three credit-reporting agencies at least once a year. Review the reports to be sure no one else is using your identity to open new accounts or to use your existing accounts. Check for fraudulent activity or other discrepancies.
- ❖ **Never leave receipts** at bank machines, bank counters, trash receptacles or unattended gasoline pumps. Keep track of all your paperwork. When you no longer need it, destroy it.
- ❖ **Memorize your social security number and all of your passwords.** Do NOT record them on any cards or on anything in your wallet or purse.
- ❖ **Sign all new credit cards upon receipt.**
- ❖ **Save all credit card receipts and match them against your monthly bills.**
- ❖ **Be conscious of normal receipt of financial statements.** Contact the sender if they are not received in the mail.
- ❖ **Notify your credit card companies and financial institutions in advance of any change of address or phone number.**
- ❖ **Never loan your credit cards** to anyone else.
- ❖ **Never put your credit card or any other financial account number on a postcard or on the outside of an envelope.**
- ❖ **If you applied for a new credit card and it hasn't arrived in a timely manner, call the bank or credit card company involved.**
- ❖ **Report all lost or stolen credit cards immediately.**
- ❖ **Closely monitor expiration dates of your credit cards.** Contact the credit card issuer if replacement cards are not received prior to the expiration dates.
- ❖ **Beware of mail or telephone solicitations disguised as promotions** offering instant prizes or awards designed solely to obtain your personal information or credit card numbers.
- ❖ **Use a secure browser** software that encrypts the information you send over the Internet to protect the security of your information as it is transmitted. Be sure your browser has up-to-date encryption capabilities by using the latest version available. When submitting your information, look for the "lock" icon on the browser's status bar and "https" in the URL address for a site, to be sure your information is secure during transmission.
- ❖ **Check the privacy policy** before you provide any personal information to a site. Specifically, determine how the information will be used or shared with others. Check the site's statements about the security provided for your information. Some website disclosures are easier to find than others. Look at the bottom of the home page, on order forms or in the FAQs section of a site. If you're not comfortable with the policy, consider doing business elsewhere.
- ❖ **Use caution when disclosing** checking account numbers, credit card numbers or other personal financial data at any web site or online service location unless you are using a secured protocol.
- ❖ **When you subscribe to an online 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. Reputable Internet service providers (ISP) will not request this information.
- ❖ **Business and government agencies are required to notify individuals when**

**unencrypted personal information in the categories of Social Security Number, driver's license number, account number or credit/debit card number has been accessed in a computer security breach per California Civil Code § 1798.29 and 1798.82.**

- ❖ **Remove your name from mailing lists and phone lists.**

**DIRECT MARKETING ASSOCIATION**

To remove your name from mail and phone lists.

Mail Preference Service, P.O. Box 9008, Farmingdale, NY 11735

Telephone Preference Service, P.O. Box 9014, Farmingdale, NY 11735

<http://www.the-dma.org/>

## WHAT TO DO IF YOU ARE THE VICTIM OF IDENTITY THEFT

**1. LAW ENFORCEMENT.** Report the crime to the police or sheriff's department where you live. Give them as much documented evidence as possible. Make sure the police report lists the fraud accounts. Get a copy of the report and make photocopies. Keep the report number of your police report handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report in order to verify the crime. It is a violation of federal law (18 USC § 1028) and the laws of the State of California (Penal Code 530.5) to assume someone's identity for fraudulent purposes.

Per California Penal Code § 530.6 you are entitled to a copy of your identity theft report.

### **UCLA Police Department**

**(310) 825-1491      24-HOUR NUMBER**

**(310) 206-8126      RECORDS – COPIES OF REPORTS**

**[Identify Theft Encyclopedia](#)**

**[www.ucpd.ucla.edu/](http://www.ucpd.ucla.edu/)**

**2. CREDIT BUREAUS.** Immediately call the fraud units of the credit reporting companies Experian, Equifax and Trans Union. Report the theft of your credit cards/numbers and request a credit report. Ask that your file be flagged with a fraud alert. Add a victim's statement to your report. ("My ID has been used to apply for credit fraudulently. Contact me at [your phone number] to verify all applications.") Ask how long the fraud alert is posted on your file and how you can extend it if necessary. ***Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the impostor. Request a copy of your credit report every few months so you can monitor any new fraudulent activity.***

The credit bureau must place fraud alert within five business days of receipt of the alert from the consumer per California Civil Code § 1785.11.1

If you submit police report to a credit bureau listing the fraudulent accounts, the credit bureau must promptly block the information about those accounts. Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit bureaus to remove inquiries that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months in order to alert them to the disputed and erroneous information (two years for employers). When you provide your police report to the credit bureaus, they must **block** the fraudulent accounts from your credit report and inform the credit grantors that the information has been removed per California Civil Code § 1785.16(k).

An identity theft victim who provides the credit bureau with a copy of a police report is entitled to 12 free credit reports, one per month, in the 12 months from the date of the police report per California Civil Code § 1785.15.3 You are entitled to a **free credit report** if you are a victim of identity theft, if you have been denied credit, if you receive welfare benefits or if you are unemployed.

#### Equifax

P.O. Box 105069, Atlanta, GA 30348.

Report fraud: Call (800) 525-6285 or (888) 766-0008 and write to address.

Order credit report: (800) 685-1111.

<http://www.equifax.com/>

#### Experian

P.O. Box 9532, Allen, TX 75013.

Report fraud: Call (888) EXPERIAN (397-3742) and write to address.

Fax: (800) 301-7196.

Order credit report: (888) EXPERIAN.

<http://www.experian.com/>

#### Trans Union

P.O. Box 6790, Fullerton, CA 92834

Report fraud: (800) 680-7289 and write to address.

Order credit report: (800) 888-4213.

<http://www.transunion.com/>

**3. IDENTITY THEFT ONE-CALL PROGRAM.** When a victim calls any one of the three national credit reporting companies, the company contacted will share that information with the other two. Each company will follow a standardized three-step process to post a security alert on the credit file, opt the victim out of pre-approved offers of credit or insurance and mail the victim a copy of his or her credit file.

Here is what the process will look like in more detail once the victim makes a call:

- The company receiving the initial call will notify the victim of the ID fraud initiative and will electronically notify the other two credit reporting companies of the crime;
- A fraud alert will be put on the victim's credit report at all three nationwide credit reporting companies within 24 hours;
- The victim will be opted out of all pre-approved offers of credit and insurance for two years;
- The victim's request for a copy of his or her credit report will be handled in no more than three business days. Each of the three national credit-reporting companies will work with the victim to verify the information in their respective reports and to delete any fraudulent data. If the victim files a police report, the process is even quicker. Credit reporting companies will voluntarily expedite services for the victim by immediately deleting fraudulent data without the usual reinvestigation procedure; and,
- The fraud alert will be displayed by each national credit-reporting agency to all lenders or other users that access the reports in the future. Once notified that the consumer has been a victim of ID fraud, the lender can then avoid opening a fraudulent account.

**4. FREEZING CREDIT REPORTS.** California residents have the right to freeze their credit reports, prohibiting credit from being issued in their names. Credit bureau must enable consumer to establish a "freeze," prohibiting the credit bureau from giving report to anyone without the consumer's consent per California Civil Code § 1785.11.2

Fraud alerts are supposed to alert you when someone applies for credit in your name and signals creditors to contact you for permission to issue credit in your name. Creditors, however, aren't required to abide by or even check the fraud alert.

A credit freeze goes a step further. With a credit freeze, no one can open any form of credit in your name. Your credit file is off limits to potential lenders and even potential employers.

When you apply for credit the company issuing credit contacts one of the three credit reporting agencies and requests to see your credit file. If you have a freeze on your account, the company will be told that it cannot see your credit file because your account is frozen. At this point, most companies would not grant the credit.

This does not mean that you won't be able to get credit for yourself or allow potential employers to run a background check. The credit bureaus assign a PIN for you when you freeze your report. Using this PIN, you can lift the freeze when necessary. No credit will be issued in California. Once the credit bureaus receive your request, they must freeze your report within five business days.

**How to Do It**

To freeze a credit report, California residents must contact each of the three credit reporting agencies. There is no cost if you are a victim of identity theft, as long as you have a report from the police. Residents who are not identity theft victims must pay to freeze their credit reports. None of three bureaus charge to permanently lift the freeze, but there are fees for a temporary lift even for identity theft victims.

Each agency has a different procedure and fee for locking down your credit. Here's what you need to do to freeze your credit report with each agency.

<b>Equifax CASD P.O. Box 105788 Atlanta, GA 30348</b>	
<b>Phone</b>	(800) 685-1111
<b>What to do</b>	Mail a certified letter and check with your name, address, date of birth, Social Security number and a written request to freeze your file.
<b>Cost and length of freeze</b>	A \$12 fee will freeze the report indefinitely. It is free for victims with proof of identity theft from the police or DMV.
<b>Cost to temporarily unfreeze</b>	\$8 for a date range; \$25 for a specific granter.

<b>Experian Security Freeze P.O. Box 9554 Allen, TX 75013</b>	
<b>Phone</b>	(888) 397-3742
<b>What to do</b>	Mail a certified letter and check with your full name (including middle initial); your current address; Social Security number; date of birth; your addresses for the previous five years; and two proofs of address (utility bill, bank statement, driver's license).
<b>Cost and length of freeze</b>	\$59.95 per year. It is free for identity theft victims with proof from the police or DMV
<b>Cost to temporarily unfreeze</b>	Free. Call (888) 397-3742, or visit Experian's consumer center.

<b>TransUnion Fraud Center Attn: File Freeze P.O. Box 6790 Fullerton, CA 92834</b>	
<b>Phone</b>	(888) 909-8872
<b>What to do</b>	Call the toll-free number, request a security-freeze form and mail it to the address above.
<b>Cost and length of freeze</b>	\$29.95 to indefinitely freeze your account. It is free for identity theft victims with proof from the police or DMV.
<b>Cost to temporarily unfreeze</b>	\$14.95 for a specific date range. All will be charged, even ID theft victims.

**4. OPT OUT OF PRE-APPROVED OFFERS OF CREDIT.** For all three bureaus, call **(888) 5OPTOUT**. This establishes a two-year opt-out. For permanent opt-out status, put your request in writing.

**5. CALIFORNIA'S IDENTITY THEFT DATABASE.** The California Identity Theft Database was established to help victims of identity theft who have been wrongfully accused or associated with crimes. 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 the Identity Theft Database.

Once confirmed, your information will be entered into the statewide database and used to show others that you were actually not responsible for the crime. This information will be available via a toll-free number to the identity theft victim, criminal justice agencies and other individuals and agencies authorized by the victim to see the information.

To register as a victim of identity theft, you must obtain a registration application packet from the DOJ. You can call (888) 880-0240 or visit [caag.state.ca.us/idtheft/general.htm](http://caag.state.ca.us/idtheft/general.htm). The packet will contain all the necessary forms and/or instructions that you must complete and submit to DOJ.

### **California Attorney General's Office**

[caag.state.ca.us](http://caag.state.ca.us)

**6. CREDITORS.** Contact all creditors immediately with whom your name has been used fraudulently, by phone and in writing. You may be asked to fill out fraud affidavits. (No law requires these to be notarized at your own expense.) Get replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processed as "account closed at consumer's request." (This is better than "card lost or stolen," because when this statement is reported to credit bureaus, it can be interpreted as blaming you for the loss.) Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report it immediately to credit grantors.

To make certain that you do not become responsible for the debts incurred by the identity thief, you must provide proof that you didn't create the debt to each of the companies where accounts were opened or used in your name.

A group composed of credit grantors, consumer advocates and the FTC developed an ID Theft Affidavit to help you report information to many companies using just one standard form. Use of this affidavit is optional for companies. While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it.

You can use this affidavit where a new account was opened in your name. The information will enable the companies to investigate the fraud and decide the outcome of your claim. (If someone made unauthorized charges to an existing account, call the company to find out what to do.)

### **Federal Trade Commission (FTC)**

ID Theft Affidavit

<http://www.ftc.gov/opa/2002/02/idtheft.shtml>

Banks, public utilities and certain other companies must provide both the victim and law enforcement (on request) with copies of applications, checks, account statements and records of transactions initiated by an imposter per California Penal Code § 530.8.

**7. STOLEN CHECKS.** If you have had checks stolen or bank accounts set up fraudulently, report it to the appropriate check verification companies (see next page). Put stop payments on any outstanding checks that you are unsure of. Close your checking/savings accounts and obtain new accounts. Give the bank a password for your account (not mother's maiden name). If your own checks are rejected at stores where you shop, contact the check verification company that the merchant uses.

**To report fraudulent use of your checks:**

CheckRite	(800) 766-2748
Chexsystems	(800) 428-9623
CrossCheck	(800) 843-0760
Equifax	(800) 437-5120
International Check Services	(800) 631-9656
SCAN	(800) 262-7771
TeleCheck	(800) 710-9898

Any person who receives a bad check is eligible to participate in the program if the following conditions are met:

- It was received in Los Angeles County, deposited in a bank in exchange for goods or services and presumed good at the time of acceptance. There are no minimum restrictions based on dollar amount.
- A courtesy notice was sent to the check writer allowing 10 days to cover the check.
- It was submitted to the program within 120 days from the date on the check.
- Photo identification such as drivers license, military ID or state identification card was recorded at the time of the transaction.

**Los Angeles County District Attorney's Office**

[da.co.la.ca.us/cpd/idtheft.htm](http://da.co.la.ca.us/cpd/idtheft.htm)

**BAD CHECK RESTITUTION PROGRAM**

PMB 880  
7095 Hollywood Blvd., Suite 104  
Hollywood, CA  
90028-8903  
Victim Hotline (800) 842-0733  
Check Writers (800) 269-0206  
<http://da.co.la.ca.us/badcheck.htm>

**8. ATM CARDS.** If your ATM or debit card has been stolen or compromised, report it immediately. Get a new card, account number and password. Do not use your old password. When creating a password, don't use common numbers like the last four digits of your SSN or your birth date. Monitor your account statements. You may be liable if fraud is not reported quickly.

**9. FRAUDULENT CHANGE OF ADDRESS.** Notify the Postal Inspector if you suspect an identity thief has filed a change of address with the post office or has used the mail to commit fraud. (Call the U.S. Postal Service to obtain the phone number, (800) 275-8777). Find out where fraudulent credit cards were sent. Notify the local Postmaster for that address to forward all mail in your name to your own address. You may also need to talk with the mail carrier.

**United States Postal Service**

**(800) 275-8777**

<http://www.usps.gov/websites/depart/inspect>

**10. SECRET SERVICE JURISDICTION.** The Secret Service has jurisdiction over financial fraud, but it usually does not investigate individual cases unless the dollar amount is high or you are one of many victims of a fraud ring. To interest the Secret Service in your case, you may want to ask the fraud department of the credit card companies and/or banks, to notify the particular Secret Service agent they work with.

**United States Secret Service**

**(213) 894-4830**

<http://www.treas.gov/usss>

**11. SOCIAL SECURITY NUMBER (SSN) MISUSE.** Call the Social Security Administration to report fraudulent use of your SSN. As a last resort, you might want to change your SSN. The SSA will only change it if you fit their fraud victim criteria. Also order a copy of your Personal Earnings and Benefits Statement and check it for accuracy. The thief might be using your SSN for employment purposes.

**Social Security Administration**

**(800) 269-0271**

Order Personal Earnings and Benefits Statement: (800) 772-1213

<http://www.ssa.gov/>

**12. PASSPORTS.** Whether you have a passport or not, write the passport office to alert them to anyone ordering a passport fraudulently.

**United States Department of State**

Passport Services

Consular Lost/Stolen Passport Section

1111 19th Street, NW, Suite 500

Washington, DC 20036

Call 24 hours/day at **(202) 955-0430**

<http://travel.state.gov/passport/>

**13. PHONE SERVICE.** If your long distance calling card has been stolen or you discover fraudulent charges on your bill, cancel the account and open a new one. Provide a password, which must be used any time the account is changed. Eliminate or block third party billing and international dialing features if you do not need these services.

**14. DRIVER'S LICENSE NUMBER MISUSE.** You may need to change your driver's license number if someone is using yours as identification on bad checks. Call the Department of Motor Vehicles (DMV) to see if another license was issued in your name. Put a fraud alert on your license. Go to your local DMV to request a new number. Also, fill out the DMV's complaint form to begin the fraud investigation process. Send supporting documents with the completed form to the nearest DMV investigation office.

If you discover that you have become a victim of fraud as a result of DL or ID card identity theft, immediately contact your local DMV for an appointment. At the time of your appointment be prepared to:

- Complete a statement describing the facts of the fraud.
- Submit a copy of the police report, or a written explanation why a report was not filed with the police.
- Submit copies of canceled checks, bills, or letters from companies or banks proving the fraud.
- In addition, you will need to prove your identity. With the exception of an expired California DL or ID card, only current documents are accepted.

**Department of Motor Vehicles (DMV)**

**(866) 658-5758**

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

[DLFraud@DMV.CA.gov](mailto:DLFraud@DMV.CA.gov)

**15. FALSE CIVIL AND CRIMINAL JUDGMENTS.** Sometimes victims of identity theft are wrongfully accused of crimes committed by the impostor. If a civil judgment has been entered in your name for actions taken or debts incurred by your impostor, contact the court where the judgment was entered and report that you are a victim of identity theft. If you are wrongfully prosecuted for criminal charges, contact the California Department of Justice. CA Penal Code 530.6 provides a procedure for an identity theft victim to obtain a court's determination of factual innocence upon presentation of a valid police report and other information, even before the victim has been wrongfully arrested or charged with a crime.

**16. LEGAL HELP.** You may want to consult an attorney to determine legal action to take against creditors and/or credit bureaus if they are not cooperative in removing fraudulent entries from your credit report or if negligence is a factor. Call the local Bar Association or Legal Aid office to find an attorney who specializes in consumer law, the Fair Credit Reporting Act and the Fair Credit Billing Act.

**UCLA Student Legal Services**

70 Dodd Hall

**(310) 825-9894**

<http://www.studentlegal.ucla.edu/>

**17. DEALING WITH STRESS.** Psychological counseling may help you deal with the stress and anxiety commonly experienced by victims. Know that you are not alone. Contact CALPIRG or the Privacy Rights Clearinghouse for information on how to network with other victims.

**UCLA Student Psychological Services**

4223 Math Sciences

**(310) 825-0768**

<http://www.saonet.ucla.edu/sps.htm>

**UCLA Center for Women and Men**

2 Dodd Hall

**(310) 825-3945**

<http://www.thecenter.ucla.edu/>

**18. MAKING CHANGE.** Write to your state and federal legislators. Demand stronger privacy protection and fraud assistance by creditors and credit bureaus. Contact CALPIRG for information on any pending state or federal legislation.

**19. DON'T GIVE IN.** Do not pay any bill or portion of a bill, which is a result of identity theft. Do not cover any checks, which were written and/or cashed fraudulently. Do not file for bankruptcy. Your credit rating should not be permanently affected, and no legal action should be taken against you. If any merchant, financial institution or collection agency suggests otherwise, simply restate your willingness to cooperate, but don't allow yourself to be coerced into paying fraudulent bills. Report such attempts to government regulators immediately.

## RESOURCES

### **California Office of Privacy Protection**

**(866) 785-9663**

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

### **Federal Trade Commission**

You may obtain assistance from and file your complaint with the FTC Consumer Response Center.

**(877) ID-THEFT**

<http://www.consumer.gov/idtheft>

### **Federal Bureau of Investigation**

Internet Fraud Complaint Center – FBI and NW3C

<http://www.ic3.gov/>

### **California Department of Consumer Affairs**

**(800) 952-5210**

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

### **Los Angeles County Department of Consumer Affairs**

[consumer-affairs.co.la.ca.us](http://consumer-affairs.co.la.ca.us)

### **United States Department of Justice**

**(202) 514-7023**

<http://www.usdoj.gov/criminal/fraud/websites/idtheft.html>

### **CALPIRG**

11965 Venice Blvd., Suite 408, Los Angeles, CA 90066

**(310) 397-3404** or **(916) 448-4516**

[calpirg@pirg.org](mailto:calpirg@pirg.org) or <http://www.calpirg.org/>

### **Privacy Rights Clearinghouse**

1717 Kettner Ave., Suite 105, San Diego, CA 92101

**(619) 298-3396.**

[prc@privacyrights.org](mailto:prc@privacyrights.org) or <http://www.privacyrights.org/>

### **Identity Theft Resource Center**

<http://www.idtheftcenter.org/>

### **Identity Theft Survival Kit**

<http://www.identitytheft.org/>

### **National Fraud Information Center**

**(800) 876-7060**

<http://www.fraud.org/>

**Consumer Credit Counseling**

Consumer Credit Counseling Service might be able to help remove fraudulent claims from credit report.

**(800) 388-2227**

<http://www.nfcc.org/>

**Federal Citizen Information Center**

<http://www.consumeraction.gov/>

**Better Business Bureau of the Southland**

<http://www.bbbsouthland.org/>

FOR ADDITIONAL INFORMATION OR QUESTIONS CONTACT

Sergeant Tony Dueñas  
UCLA Police Department  
601 Westwood Plaza  
Los Angeles, CA 90095-1364  
(310) 825-1491

[duenas@ucpd.ucla.edu](mailto:duenas@ucpd.ucla.edu)  
[www.ucpd.ucla.edu](http://www.ucpd.ucla.edu)

THIS GUIDE IS A COMPILATION OF INFORMATION FROM NUMEROUS SOURCES INCLUDING POLICE DEPARTMENTS, GOVERNMENT AGENCIES, PRIVATE ORGANIZATIONS AND OTHER GROUPS THAT PROVIDE RESOURCES ON PREVENTING AND REPORTING IDENTITY THEFT.

IT IS INTENDED TO INCORPORATE AS MUCH INFORMATION AS POSSIBLE ABOUT IDENTITY THEFT INTO ONE REFERENCE GUIDE FOR EDUCATIONAL PURPOSES ONLY.

4-24-09