

FarMar Law Group, PC

14900 Magnolia Blvd. #55997

Sherman Oaks, CA 91403

mail@farmarlaw.com

Excerpt from the Federal Trade Commission

<http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm> (visited July 2010)

IDENTITY THEFT VICTIMS: IMMEDIATE STEPS

If you are a victim of identity theft, take the following four steps as soon as possible, and keep a record with the details of your conversations and copies of all correspondence.

1. Place a fraud alert on your credit reports, and review your credit reports.

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374- 0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your SSN will appear on your credit reports. Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information, like your SSN, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. See [Correcting Credit Reports](#) to learn how. Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

Fraud Alerts

There are two types of fraud alerts: an initial alert, and an extended alert.

- An initial alert stays on your credit report for at least 90 days. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you've been taken in by a "phishing" scam. When you place an initial fraud alert on your credit report, you're entitled to one free credit report from each of the three nationwide consumer reporting companies.

- An extended alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an ["identity theft report."](#) When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years unless you ask them to put your name back on the list before then.

To place either of these alerts on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity: that may include your SSN, name, address and other personal information requested by the consumer reporting company.

When a business sees the alert on your credit report, they must verify your identity before issuing you credit. As part of this verification process, the business may try to contact you directly. This may cause some delays if you're trying to obtain credit. To compensate for possible delays, you may wish to include a cell phone number, where you can be reached easily, in your alert. Remember to keep all contact information in your alert current.

2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

If the identity thief has made charges or debits on your accounts, or on fraudulently opened accounts, ask the company for the forms to dispute those transactions:

- For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. If the company doesn't have special forms, use the [sample letter](#) to dispute the fraudulent charges or debits. In either case, write to the company at the address given for "billing inquiries," NOT the address for sending your payments.
- For new unauthorized accounts, ask if the company accepts the [ID Theft Affidavit](#). If not, ask the representative to send you the company's fraud dispute forms. If the company already has reported these accounts or debts on your credit report, dispute this fraudulent information. See [Correcting Credit Reports](#) to learn how.

Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

Proving You're a Victim

Applications or other transaction records related to the theft of your identity may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement. By law, companies must give you a copy of the application or other business transaction records relating to your identity theft if you submit your request in writing. Be sure to ask the company representative where you should mail your request. Companies must provide these records at no charge to you within 30 days of receipt of your request and your supporting documents. You also may give permission to any law enforcement agency to get these records, or ask in your written request that a copy of these records be sent to a particular law enforcement officer.

The company can ask you for:

- proof of your identity. This may be a photocopy of a government-issued ID card, the same type of information the identity thief used to open or access the account, or the type of information the company usually requests from applicants or customers, and
- a police report and a completed affidavit, which may be the [Identity Theft Affidavit](#) or the company's own affidavit.

3. File a report with your local police or the police in the community where the identity theft took place.

Then, get a copy of the police report or at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.

4. File a complaint with the Federal Trade Commission.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

You can file a complaint online at www.ftc.gov/idtheft. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653- 4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Be sure to call the Hotline to update your complaint if you have any additional information or problems.

The Identity Theft Report

An identity theft report may have two parts:

Part One is a copy of a report filed with a local, state, or federal law enforcement agency, like your local police department, your State Attorney General, the FBI, the U.S. Secret Service, the FTC, and the U.S. Postal Inspection

Service. There is no federal law requiring a federal agency to take a report about identity theft; however, some state laws require local police departments to take reports. When you file a report, provide as much information as you can about the crime, including anything you know about the dates of the identity theft, the fraudulent accounts opened and the alleged identity thief.

Note: Knowingly submitting false information could subject you to criminal prosecution for perjury.

Part Two of an identity theft report depends on the policies of the consumer reporting company and the information provider (the business that sent the information to the consumer reporting company). That is, they may ask you to provide information or documentation in addition to that included in the law enforcement report which is reasonably intended to verify your identity theft. They must make their request within 15 days of receiving your law enforcement report, or, if you already obtained an extended fraud alert on your credit report, the date you submit your request to the credit reporting company for information blocking. The consumer reporting company and information provider then have 15 more days to work with you to make sure your identity theft report contains everything they need. They are entitled to take five days to review any information you give them. For example, if you give them information 11 days after they request it, they do not have to make a final decision until 16 days after they asked you for that information. If you give them any information after the 15-day deadline, they can reject your identity theft report as incomplete; you will have to resubmit your identity theft report with the correct information.

You may find that most federal and state agencies, and some local police departments, offer only "automated" reports a report that does not require a face-to-face meeting with a law enforcement officer. Automated reports may be submitted online, or by telephone or mail. If you have a choice, do not use an automated report. The reason? It's more difficult for the consumer reporting company or information provider to verify the information. Unless you are asking a consumer reporting company to place an extended fraud alert on your credit report, you probably will have to provide additional information or documentation when you use an automated report.

Cal Civ Code § 1788.18 (2011)

Accessed via Lexis Nexis October 2011

§ 1788.18. Identity theft; Debt collector to stop collection activities when certain information provided; Written statement; Penalty for false information; Recommencement of collection upon good faith determination; Notification to credit reporting agencies and creditors of specified information; Definition

(a) Upon receipt from a debtor of all of the following, a debt collector shall cease collection activities until completion of the review provided in subdivision (d):

(1) A copy of a police report filed by the debtor alleging that the debtor is the victim of an identity theft crime, including, but not limited to, a violation of *Section 530.5 of the Penal Code*, for the specific debt being collected by the debt collector.

(2) The debtor's written statement that the debtor claims to be the victim of identity theft with respect to the specific debt being collected by the debt collector.

(b) The written statement described in paragraph (2) of subdivision (a) shall consist of any of the following:

(1) A Federal Trade Commission's Affidavit of Identity Theft.

(2) A written statement that contains the content of the Identity Theft Victim's Fraudulent Account Information Request offered to the public by the California Office of Privacy Protection.

(3) A written statement that certifies that the representations are true, correct, and contain no material omissions of fact to the best knowledge and belief of the person submitting the certification. A person submitting the certification who declares as true any material matter pursuant to this subdivision that he or she knows to be false is guilty of a misdemeanor. The statement shall contain or be accompanied by the following, to the extent that an item listed below is relevant to the debtor's allegation of identity theft with respect to the debt in question:

(A) A statement that the debtor is a victim of identity theft.

(B) A copy of the debtor's driver's license or identification card, as issued by the state.

(C) Any other identification document that supports the statement of identity theft.

(D) Specific facts supporting the claim of identity theft, if available.

(E) Any explanation showing that the debtor did not incur the debt.

(F) Any available correspondence disputing the debt after transaction information has been provided to the debtor.

(G) Documentation of the residence of the debtor at the time of the alleged debt. This may include copies of bills and statements, such as utility bills, tax statements, or other statements from businesses sent to the debtor, showing that the debtor lived at another residence at the time the debt was incurred.

(H) A telephone number for contacting the debtor concerning any additional information or questions, or direction that further communications to the debtor be in writing only, with the mailing address specified in the statement.

(I) To the extent the debtor has information concerning who may have incurred the debt, the identification of any person whom the debtor believes is responsible.

(J) An express statement that the debtor did not authorize the use of the debtor's name or personal information for incurring the debt.

(K) The certification required pursuant to this paragraph shall be sufficient if it is in substantially the following form:

Click here to view form

(c) If a debtor notifies a debt collector orally that he or she is a victim of identity theft, the debt collector shall notify the debtor, orally or in writing, that the debtor's claim must be in writing. If a debtor notifies a debt collector in writing that he or she is a victim of identity theft, but omits information required pursuant to subdivision (a) or, if applicable, the certification required pursuant to paragraph (3) of subdivision (b), if the debt collector does not cease collection

activities, the debt collector shall provide written notice to the debtor of the additional information that is required, or the certification required pursuant to paragraph (3) of subdivision (b), as applicable, or send the debtor a copy of the Federal Trade Commission's Affidavit of Identity Theft form.

(d) Upon receipt of the complete statement and information described in subdivision (a), the debt collector shall review and consider all of the information provided by the debtor and other information available to the debt collector in its file or from the creditor. The debt collector may recommence debt collection activities only upon making a good faith determination that the information does not establish that the debtor is not responsible for the specific debt in question. The debt collector's determination shall be made in a manner consistent with the provisions of subsection (1) of Section 1692 of Title 15 of the United States Code, as incorporated by Section 1788.17 of this code. The debt collector shall notify the debtor in writing of that determination and the basis for that determination before proceeding with any further collection activities. The debt collector's determination shall be based on all of the information provided by the debtor and other information available to the debt collector in its file or from the creditor.

(e) No inference or presumption that the debt is valid or invalid, or that the debtor is liable or not liable for the debt, shall arise if the debt collector decides after the review described in subdivision (d) to cease or recommence the debt collection activities. The exercise or nonexercise of rights under this section is not a waiver of any other right or defense of the debtor or debt collector.

(f) The statement and supporting documents that comply with subdivision (a) may also satisfy, to the extent those documents meet the requirements of, the notice requirement of paragraph (5) of subdivision (c) of Section 1798.93.

(g) A debt collector who ceases collection activities under this section and does not recommence those collection activities shall do all of the following:

(1) If the debt collector has furnished adverse information to a consumer credit reporting agency, notify the agency to delete that information.

(2) Notify the creditor that debt collection activities have been terminated based upon the debtor's claim of identity theft.

(h) A debt collector who has possession of documents that the debtor is entitled to request from a creditor pursuant to *Section 530.8 of the Penal Code* is authorized to provide those documents to the debtor.

(i) Notwithstanding subdivision (h) of Section 1788.2, for the purposes of this section, "debtor" means a natural person, firm, association, organization, partnership, business trust, company, corporation, or limited liability company from which a debt collector seeks to collect a debt that is due and owing or alleged to be due and owing from the person or entity. The remedies provided by this title shall apply equally to violations of this section.



Identity Theft Victim's Complaint and Affidavit

A voluntary form for filing a report with law enforcement, and disputes with credit reporting agencies and creditors about identity theft-related problems. Visit ftc.gov/idtheft to use a secure online version that you can print for your records.

Before completing this form:

1. Place a fraud alert on your credit reports, and review the reports for signs of fraud.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

About You (the victim)

Now

- (1) My full legal name: _____
First Middle Last Suffix
- (2) My date of birth: _____
mm/dd/yyyy
- (3) My Social Security number: _____ - _____ - _____
- (4) My driver's license: _____
State Number
- (5) My current street address:

Number & Street Name Apartment, Suite, etc.

City State Zip Code Country
- (6) I have lived at this address since _____
mm/yyyy
- (7) My daytime phone: (____) _____
 My evening phone: (____) _____
 My email: _____

Leave (3) blank until you provide this form to someone with a legitimate business need, like when you are filing your report at the police station or sending the form to a credit reporting agency to correct your credit report.

At the Time of the Fraud

- (8) My full legal name was: _____
First Middle Last Suffix
- (9) My address was: _____
Number & Street Name Apartment, Suite, etc.

City State Zip Code Country
- (10) My daytime phone: (____) _____ My evening phone: (____) _____
 My email: _____

Skip (8) - (10) if your information has not changed since the fraud.

About You (the victim) (Continued)

Declarations

- (11) I did OR did not authorize anyone to use my name or personal information to obtain money, credit, loans, goods, or services — or for any other purpose — as described in this report.
- (12) I did OR did not receive any money, goods, services, or other benefit as a result of the events described in this report.
- (13) I am OR am not willing to work with law enforcement if charges are brought against the person(s) who committed the fraud.

About the Fraud

(14) I believe the following person used my information or identification documents to open new accounts, use my existing accounts, or commit other fraud.

Name: _____
 First Middle Last Suffix

Address: _____
 Number & Street Name Apartment, Suite, etc.

_____ City State Zip Code Country

Phone Numbers: (____) _____ (____) _____

Additional information about this person: _____

(14):
Enter what you know about anyone you believe was involved (even if you don't have complete information).

(15) Additional information about the crime (for example, how the identity thief gained access to your information or which documents or information were used):

(14) and (15):
Attach additional sheets as needed.

Documentation

(16) I can verify my identity with these documents:

- A valid government-issued photo identification card (for example, my driver's license, state-issued ID card, or my passport).
If you are under 16 and don't have a photo-ID, a copy of your birth certificate or a copy of your official school record showing your enrollment and legal address is acceptable.
- Proof of residency during the time the disputed charges occurred, the loan was made, or the other event took place (for example, a copy of a rental/lease agreement in my name, a utility bill, or an insurance bill).

(16): Reminder:
Attach copies of your identity documents when sending this form to creditors and credit reporting agencies.

About the Information or Accounts

(17) The following personal information (like my name, address, Social Security number, or date of birth) in my credit report is inaccurate as a result of this identity theft:

(A) _____

(B) _____

(C) _____

(18) Credit inquiries from these companies appear on my credit report as a result of this identity theft:

Company Name: _____

Company Name: _____

Company Name: _____

(19) Below are details about the different frauds committed using my personal information.

Name of Institution	Contact Person	Phone	Extension
Account Number	Routing Number	Affected Check Number(s)	
Account Type: <input type="checkbox"/> Credit <input type="checkbox"/> Bank <input type="checkbox"/> Phone/Utilities <input type="checkbox"/> Loan <input type="checkbox"/> Government Benefits <input type="checkbox"/> Internet or Email <input type="checkbox"/> Other			
Select ONE: <input type="checkbox"/> This account was opened fraudulently. <input type="checkbox"/> This was an existing account that someone tampered with.			
Date Opened or Misused (mm/yyyy)	Date Discovered (mm/yyyy)	Total Amount Obtained (\$)	

Name of Institution	Contact Person	Phone	Extension
Account Number	Routing Number	Affected Check Number(s)	
Account Type: <input type="checkbox"/> Credit <input type="checkbox"/> Bank <input type="checkbox"/> Phone/Utilities <input type="checkbox"/> Loan <input type="checkbox"/> Government Benefits <input type="checkbox"/> Internet or Email <input type="checkbox"/> Other			
Select ONE: <input type="checkbox"/> This account was opened fraudulently. <input type="checkbox"/> This was an existing account that someone tampered with.			
Date Opened or Misused (mm/yyyy)	Date Discovered (mm/yyyy)	Total Amount Obtained (\$)	

Name of Institution	Contact Person	Phone	Extension
Account Number	Routing Number	Affected Check Number(s)	
Account Type: <input type="checkbox"/> Credit <input type="checkbox"/> Bank <input type="checkbox"/> Phone/Utilities <input type="checkbox"/> Loan <input type="checkbox"/> Government Benefits <input type="checkbox"/> Internet or Email <input type="checkbox"/> Other			
Select ONE: <input type="checkbox"/> This account was opened fraudulently. <input type="checkbox"/> This was an existing account that someone tampered with.			
Date Opened or Misused (mm/yyyy)	Date Discovered (mm/yyyy)	Total Amount Obtained (\$)	

(19):
 If there were more than three frauds, copy this page blank, and attach as many additional copies as necessary.

Enter any applicable information that you have, even if it is incomplete or an estimate.

If the thief committed two types of fraud at one company, list the company twice, giving the information about the two frauds separately.

Contact Person:
 Someone you dealt with, whom an investigator can call about this fraud.

Account Number:
 The number of the credit or debit card, bank account, loan, or other account that was misused.

Dates: Indicate when the thief began to misuse your information and when you discovered the problem.

Amount Obtained:
 For instance, the total amount purchased with the card or withdrawn from the account.

Your Law Enforcement Report

(20) One way to get a credit reporting agency to quickly block identity theft-related information from appearing on your credit report is to submit a detailed law enforcement report ("Identity Theft Report"). You can obtain an Identity Theft Report by taking this form to your local law enforcement office, along with your supporting documentation. Ask an officer to witness your signature and complete the rest of the information in this section. It's important to get your report number, whether or not you are able to file in person or get a copy of the official law enforcement report. Attach a copy of any confirmation letter or official law enforcement report you receive when sending this form to credit reporting agencies.

Select ONE:

- I have not filed a law enforcement report.
- I was unable to file any law enforcement report.
- I filed an automated report with the law enforcement agency listed below.
- I filed my report in person with the law enforcement officer and agency listed below.

(20):
Check "I have not..." if you have not yet filed a report with law enforcement or you have chosen not to. Check "I was unable..." if you tried to file a report but law enforcement refused to take it.

Automated report:
A law enforcement report filed through an automated system, for example, by telephone, mail, or the Internet, instead of a face-to-face interview with a law enforcement officer.

Law Enforcement Department State

Report Number Filing Date (mm/dd/yyyy)

Officer's Name (please print) Officer's Signature

Badge Number (____) Phone Number

Did the victim receive a copy of the report from the law enforcement officer? Yes OR No

Victim's FTC complaint number (if available): _____

Signature

As applicable, sign and date *IN THE PRESENCE OF* a law enforcement officer, a notary, or a witness.

(21) I certify that, to the best of my knowledge and belief, all of the information on and attached to this complaint is true, correct, and complete and made in good faith. I understand that this complaint or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may violate federal, state, or local criminal statutes, and may result in a fine, imprisonment, or both.

Signature

Date Signed (mm/dd/yyyy)

Your Affidavit

(22) If you do not choose to file a report with law enforcement, you may use this form as an Identity Theft Affidavit to prove to each of the companies where the thief misused your information that you are not responsible for the fraud. While many companies accept this affidavit, others require that you submit different forms. Check with each company to see if it accepts this form. You should also check to see if it requires notarization. If so, sign in the presence of a notary. If it does not, please have one witness (non-relative) sign that you completed and signed this Affidavit.

Notary

Witness:

Signature

Printed Name

Date

Telephone Number