Leave Me Alone!

This chart tells who to contact if you want to stop direct mail and other offers.

Who	What	Where to call
EQUIFAX experian 	Pre-screened credit card offers (TransUnion, Experian, Equifax)	1-888-5-OPTOUT
experian Marketing Lists	Targeted marketing lists	1-800-407-1088
Direct Mailers	To remove your name from many national direct mail lists	DMA Mail Preference Service P.O. Box 9008 Farmingdale, NY 11735-9008 Click here to get a form to mail them.
Direct E-Mail	To remove your e-mail address from many national direct e-mail lists	DMA E-mail Preference Service
Telemarketing	Avoid unwanted phone calls from many national marketersd	FTC National Do Not Call Registry. (New rights and new rules about telemarketing calls to your home.)
		DMA Telephone Preference Service P.O. Box 9014 Farmingdale, NY 11735-9014 Click here to get a form to mail them.
Canadian Marketing Association	Marketing list name removal. .	CMA "Do not contact service" registration web page.
Canada	Information about getting your Canadian Credit Report.	
Junk Fax Advertising	To report unsolicited junk fax ads sent to you or your business	The FCC

Other Crime Prevention Resources On The Web

Identity Theft
Identity Theft Resource Center www.idtheftcenter.org
Federal Trade Commission www.consumer.gov/idtheft
Annual Credit Report www.annualcreditreport.com

Fraud
www.Mesaaz.gov/police/fraud/default.aspx
National Consumers League www.natlconsumersleague.org
Consumer Fraud www.consumer.gov

Charity Fraud
Better Business Bureau www.give.org
Information on Charities www.charitynavigator.com

Internet Fraud
Federal Trade Commission www.consumer.gov/idtheft
U.S. Department of Justice www.cybercrime.gov

Mail Fraud
United States Postal Service www.usps.com/postalinspectors/fraud

To Remove Your Name From Mailing Lists
Direct Marketing Association www.dmaconsumers.org
National Do Not Call Registry www.donotcall.gov

Illegal Online Pharmacies
National Drug Intelligence Center www.usdoj.gov/ndic
U.S. Drug Enforcement Center www.dea.gov
U.S. Food and Drug Administration www.fda.gov

Securing Your Computer
National Cyber Security Alliance www.staysafeonline.org
Federal Government www.onguardonline.gov

Crime Prevention (general)
Arizona Crime Prevention Association* www.acpa.net
Crime Prevention Coalition of America www.ncpc.org
Bureau of Justice Statistics www.ojp.usdoj.gov/bjs

U.S. Department of Justice www.usdoj.gov
U.S. Department of Homeland Security www.ready.gov
National Center for Victims of Crime www.ncvc.org
Office for Victims of Crime www.ojp.usdoj.gov/ovc

COMMON QUESTIONS ABOUT IDENTITY THEFT

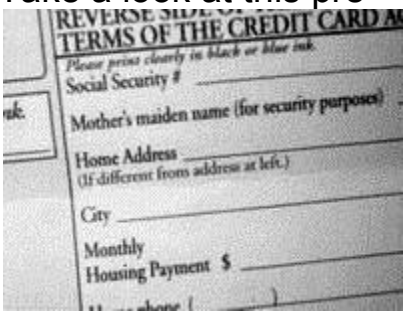
How Did They Get My Name?

The credit card company that sent you the pre approved offer, in most cases, doesn't even know who you are. They've contracted with one of the big credit repositories (or a company working with the repositories) for a bulk *prescreen* - a certain number of mailings to be made to people with credit scores falling in a certain range.

Only when *you* respond do they find out who *you* are.

What if an Identity Thief Responds?

As it turns out, an identity thief digging through your trash has nearly everything needed to get a credit card, *in your name*, mailed to a different address. Take a look at this pre-approved offer application form.



“Home Address (If different from address at left)”

The thief simply writes **a different** address and phone, making it look like you've moved. Since the "former" address is correct (it's the address to which the pre approved offer was sent) there will still be enough address information for the credit check to go through.

“Mother's Maiden Name (for security purposes.)”

The identity thief can enter *any* name in this space without a problem. The credit card company is not asking this to verify identity *now*. They want the mother's maiden name *for future use,* to verify identity of the cardholder on future customer service calls. Unfortunately, the future cardholder will be the identity thief, not you.

“Social Security #”

The Social security number is probably the only thing that would give an ID thief a real problem, if it were not known. A correct social security number (with name and former address) are probably going to be enough for the credit card issuer to verify credit, and open an account.

Let's hope you didn't discard your paycheck stub in the same dumpster!

A security alert on your credit report is the most important measure to take if you are an identity theft victim or have reason to believe you are at high risk of becoming one.

A security alert is a warning that can be placed on your credit report if you are a likely identity theft victim. It warns the following:

- Fraudulent credit applications might be submitted in your name
- An impostor might have used your identity to obtain goods or services.
- Before extending credit, verify all information and contact you personally.
-

Equifax, Experian, and Trans Union have been providing alerts for affected consumers who request them at their fraud alert phone numbers but laws have improved consumer rights for security alerts with, the **security freeze.**

California Senate Bill 168 (CA SB 168)

You may request that a security alert be placed on your credit report. The credit reporting agency must comply within 5 business days, and must show it to those who request your credit report for 90 days.

You may request a **security freeze**. A security freeze has the following provisions:

- Your credit report must not be displayed without your permission. (If *you* need to apply for credit, you can have the freeze temporarily lifted by contacting the credit bureau.)
- You are to be notified if anyone makes changes to your credit file identity information, such as name, address, date of birth or social security number.
- You must be notified, in writing, of any name, address, Social Security number, or date of birth change to your file.

Other States

It is expected that many of these rules will be adopted in other states, or that the credit bureaus will start applying them voluntarily.

Security Freeze Exceptions

The new security freeze laws will not apply to:

- Companies with whom you already have accounts.
- Court orders

- Child support and tax investigations
- Pre-approved credit offers

In other words, you won't be able to use a security freeze as a way to hide from those having a legal permissible purpose to see your credit report.

Pitfalls of security alerts

Security alerts are not always heeded, and currently, it is completely up to whoever reads a credit report whether or not to pay attention to them. That's why the security freeze will be a much better option. You'll be able to ensure, for a period of time, that nobody will be able to see your credit report in order to grant credit to someone attempting identity theft.

There are other pitfalls of security alerts:

- You must contact each credit reporting agency
- They make it less convenient for you to obtain credit for yourself
- Companies who saw the credit report before the alert (and who, perhaps, already granted credit to the identity thief) are not automatically notified.

What to Look for On Your Credit Report

Your credit report is the most effective tool available for detecting identity theft. If you are fortunate enough not to have been victimized, it also provides great peace of mind to have verified that everything on your credit report is the result of **legitimate activity**, based on **your** finances, *and* ***only your finances.***

Inquiries
Inquiries should correspond to applications **you** submitted, or requests **you** made for credit. (In addition, your creditors, employers, or collection agencies might recheck your credit periodically.) Inquiries that seem clearly out of place, based on the date or company, should be investigated carefully as evidence of **possible identity theft.**

Incorrect Address, Employment
It is not uncommon to find a small "typo" here or there, but a bogus recent address or employment change calls for careful investigation.

Inactive Accounts with Activity
Thieves have been known to change the billing address on on old accounts you've forgotten about, a use them as if it were their own. A credit report shows whether each account is open or closed, and the activity.

Accounts You Are Unaware You Have
It may be wise to close accounts you no longer use. A credit report can remind you of them.

Unexpected Public Records
Credit reports show court judgments, liens, foreclosures, evictions, and other public records. Look for anything that is incorrect, and clearly not yours.

Unexpected Derogatory Information
The typical pattern of an identity thief is to run up lots of bills, then not pay them. Look for unexpected past-due items.

Who To Notify of ID Theft
In the event of identity theft, each affected company should be notified. Your credit report provides a convenient listing for you of who to notify. Your Identity Theft Kit (**Form A**) should be sent to each one. The KCSO Form A should ONLY BE USED **AFTER** you have received a complete ID Theft Kit with a KCSO case number on it.

The crime of identity theft occurs when someone, without your knowledge, acquires a piece of your personal information and uses it to commit fraud.

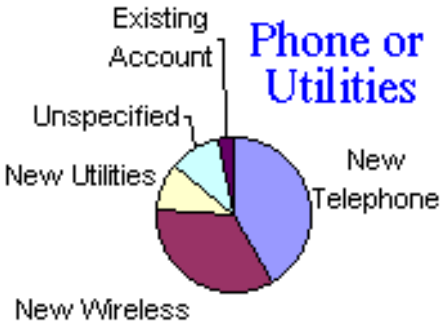
Look what identity thieves have been known to do...

In some cases, with as little as a stolen name, date of birth, and social security number, the identity thief is able to cause major damage.

Credit card fraud is the most common type of identity theft.

- The thief pretends to be the victim, calls the credit card company and changes the mailing address on an existing account.
- Or, more commonly, the thief opens a new credit card account in the victim's name.

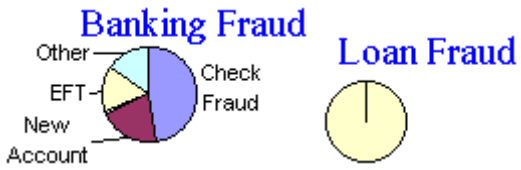
Because the bills are being sent to a new address, the victim doesn't realize there's a problem. The thief then uses the credit card without paying the bills, ruining your credit.



The second category, (about half the number of victims as credit card fraud) is where an identity thief signs up for cell phone, long distance service, or utilities in the victim's name.

The third category, (about one third the size of credit card fraud) involves depository accounts. The thief opens a bank account in the victim's name, makes electronic funds transfers, and/or writes bad checks on the account.

Loan fraud involves using a victim's name to take out a loan.



Other categories include,

- Employment - getting a job using the victims name and identity
- Social Security
- Tax Returns
- Medical
- Residential Leases
- Securities and Investments
- Bankruptcy Fraud
- Illegal Immigration and Miscellaneous government documents

If it happens to you, the damage to your credit and daily life can be devastating. ID theft victims often are unable to get new credit cards or loans because their credit ratings are harmed so badly.