Identity Theft

PREVENTION & REPAIR KIT

The fastest growing white-collar crime in the US

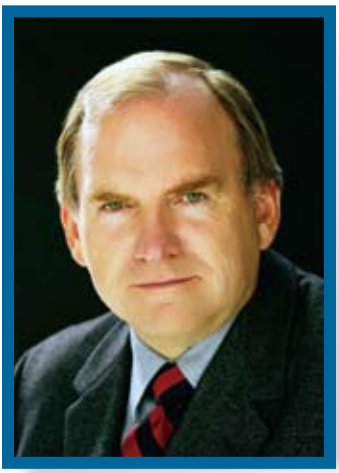
NM Attorney General
Gary K. King

NEW MEXICO ATTORNEY GENERAL
GARY K. KING


KNOW HOW TO
PROTECT YOURSELF

Message from Attorney General

Gary K. King



Precaution is better than cure. ~Edward Coke

Technology advances have been affecting our daily lives in so many ways that sometimes it's difficult to keep up. Arguably, these advances have made our lives easier by allowing us to do such things as banking and shopping online, or by telephone. Unfortunately, an unwanted side effect of this convenience is **Identity Theft**, one of the fastest growing crimes in the nation.

Even if you don't use a computer or telephone to conduct business, you can still be a victim of identity theft. This booklet shows you how to recognize ID theft, how to protect yourself from it and what to do to help repair the often devastating damage caused when someone illegally pretends to be you.

As your Attorney General, I urge you to study the information in this short publication and pass on what you learn to friends and family. There is no reason not to use and benefit from today's technology, but do so carefully. Combined with good old fashioned common sense and the advice in these pages, you can substantially reduce your risk of becoming a victim.

Table of Contents

3rd publication 2008

SIGNS OF IDENTITY THEFT

- You are denied credit;
- You find charges on your credit card that you don't remember making;
- Personal information, credit cards, ATM cards, checks or IDs have been stolen from you;
- You suspect someone has fraudulently changed your mailing address;
- Your credit card bills stop coming;
- You find something wrong with your credit report, such as loans you didn't take out or accounts you don't remember opening;
- A debt collector calls about a debt you don't owe and didn't know about;
- You are wrongly accused of a crime.

IF ANY of the above has happened to you, your identity may have been stolen. Turn to page 11 and find out how to get it back.

IF NONE of the above has happened to you, you may still be at risk for identity theft. Turn to page 3 to find out how to protect your identity.

credit denied

PREVENT IDENTITY THEFT

- Place a security freeze on your credit report;
- Review your credit report frequently;
- Put passwords on your accounts;
- Don’t carry your Social Security Card or number;
- Use a credit monitoring service;
- Pay attention to billing cycles and check about late bills;
- Review bills for any charges you didn’t make;
- Don’t give out personal information to anyone on the phone you didn’t contact first;
- Only give out personal information on the Internet over a secure connection.

Turn the page for more details ›››

PREVENTING ID THEFT

- **Place a security freeze on your credit report:** Control access to your credit report. See page 11 for details.

- **Place passwords on bank, credit card and phone accounts:** Don't use a password that could be easily guessed, such as your pet's name or your birth date. Choose a password that mixes random numbers with letters.

- **Don't carry your Social Security Number card:** Do not carry the number with you. Do not use it as your driver's license number either. Keep the card in a safe place and use the number only when necessary.

- **Order a copy of your credit report:** Order a copy from each of the three credit bureaus each year. A credit report contains information on where you live, where you work, how you pay your bills, whether you've ever been sued, arrested, or ever filed for bankruptcy, and what credit accounts have been opened in your name. Reviewing your credit report can alert you to any fraud or errors. This is very important and one of the best ways to catch identity theft. You are entitled to one free credit report annually from each of the three major credit reporting bureaus. Take advantage of it.

- **Pay close attention to billing cycles:** If a bill does not arrive on time, it is possible that an identity thief may have taken it. Remember to check with creditors about a late bill.

- **Guard your mail from theft:** Instead of leaving your mail to be picked up in an unlocked mailbox, take it to the post office or leave it in a post office collection box. Make sure you remove your incoming mail right away. Try not to leave mail in your mailbox overnight.

- **Don't give out personal information** over the Internet, on the phone, or through the mail unless you have initiated contact with the receiving person or company or you are sure about the identity of the person or company. Be aware of schemes such as "phishing" in which the identity thief pretends to be from a legitimate organization or business in order to retrieve personal information from you. This might include calls or emails from someone claiming to be from your bank needing to confirm your Social Security Number or bank account number. Be aware of promotional scams that use phony offers as a way to obtain personal information.

- **Keep your information safe online:** Only send your personal information, such as your credit card number, over a secure connection (a secure connection has an address that begins with "https" and has a small padlock at the bottom of the page. A window should also pop up telling you that the website is secure). Make sure you have virus protection that you update regularly. Use a firewall program to protect your computer from being accessed by others, especially if you have high-speed Internet which keeps your computer connected 24 hours a day, and a secure browser. You may also want to unplug your Internet while you are not using it. Don't download any files or click on links sent to you by people you don't know.

- **Be wary of "pharming" scams:** Pharming happens when you type in the address for a legitimate bank or e-commerce Web site and get rerouted to a copycat Web site. Identity thieves use this scam to obtain your personal information when you log into the Web site. Here are some ways to spot pharming:

  - Login pages should be encrypted so you should see a padlock at the bottom of the browser and the address should begin with "https". You can click on the padlock as well to make sure the site's security is registered to the right company.

  - Other links on the page work.

  - Highlight text. The Web site is a copycat if the blocks of text are actually images.

  - Look for spelling or grammatical errors.

  - You should never be asked to verify information.

WHAT IS IDENTITY THEFT?

Identity theft is when someone fraudulently uses your personal identifying information to obtain credit, take out a loan, open accounts, get identification or numerous other things that involve pretending to be you.

It is a very serious crime that can cause severe damage to someone's financial well-being if not taken care of promptly. People can spend months as well as thousands of dollars repairing the damage done to their credit history and their name by an identity thief.

Some cases of identity theft are connected to other, more serious crimes which may lead law enforcement to you for a crime you did not commit.

Identifying Identity Theft

Here are some warning signs that you may be the victim of identity theft:

- You are denied credit;
- You find charges on your credit card that you don't remember making;
- Personal information, credit cards, ATM cards, checks or IDs have been stolen from you;
- You suspect someone has fraudulently changed your mailing address;
- Your credit card bills stop coming;
- You find something wrong with your credit report, such as loans you didn't take out or accounts you don't remember opening;
- A debt collector calls about a debt you don't owe and didn't know about;
- You are wrongly accused of a crime.

If any of these have happened to you, you may be the victim of identity theft.

You could be the victim of identity theft without noticing any of these things happening to you, but it is still good to keep a careful eye out for anything out of the ordinary by ordering your credit report at least once a year and being alert to these warning signs.

How Do They Get My Personal Information?

Identity thieves can obtain your personal information in a number of ways:

- **Finding personal information you share on the Internet;**
- **"Dumpster diving"** or going through your trash looking for personal information;
- **Stealing your mail;**
- **Stealing your wallet or purse;**
- **Stealing your debit or credit card numbers through "skimming"**, using a data storage device to capture the information through an ATM machine or during an actual purchase;
- **"Phishing":** a scam in which the user sends an email falsely claiming to be from a legitimate organization, government agency or bank in order to lure the victim into surrendering personal information such as a bank account number, credit card number or passwords. This same sort of scam can also be done over the phone by the scammer calling your home;
- **Obtaining your credit report** through posing as an employer or landlord;
- **"Business record theft"** involving the theft of files, hacking into electronic files, or bribing an employee for access to files at a business;
- **Diverting your mail to another location** by filling out a "change of address" form.

What Do They Do With It?

- **Drain your bank account with electronic transfers, counterfeit checks or your debit card;**
- **Open a bank account in your name and write bad checks with it;**
- **Open a credit card account that never gets paid off,** which gets reflected on your credit report;
- **Use your name if they get arrested** so it goes on your record;
- **Use your name for purchases involved in illegal activities,** such as products for methamphetamine production or an Internet domain for a child pornography site;
- **Use your name to file for bankruptcy or avoid debts;**
- **Obtain a driver's license with your personal information;**
- **Buy a car and use your information and credit history to get a loan for it;**
- **Obtain services in your name,** such as phone or Internet.

ORDER YOUR CREDIT REPORT
at least once a year

A free credit report is available at www.annualcreditreport.com.

IF YOU ARE A VICTIM OF IDENTITY THEFT

Follow these steps immediately:

1 File a police report.

2 Close any accounts that have been tampered with or opened without your knowledge.

3 Call the 3 credit reporting bureaus and place a fraud alert on your credit file or place a security freeze on your credit file.

4 Review your credit report for:
- Accounts you did not open;
- Debts on your account that you did not know about;
- Inquiries from companies you don't know;
- Inaccurate information.

5 File a complaint with the Federal Trade Commission.

Turn the page for more details ›››

File a police report.

WHEN YOUR IDENTITY IS STOLEN

There are steps you will need to take to protect yourself. You may have to spend some time and money dealing with having your identity stolen, but it can be done.

You must follow these steps without hesitation. Acting quickly is the best way to make sure that this crime does not get out of control. The longer you wait, the more money you lose and, potentially, the greater the damage to your credit.

Always remember to act quickly.

STEP 1: CONTACT THE POLICE

File a report with your local police department and, if the identity theft did not take place within your area, file a report with the police from the area where the theft took place. Make sure to get a copy of the police report. You may need that documentation to support your claims to credit bureaus, creditors, debt collectors or other companies. If you are unable to obtain a copy of the police report, be sure to get the report number.

STEP 2: CLOSING ACCOUNTS

If you notice any accounts under your name that have been tampered with or opened without your consent, close them immediately. The longer that an identity thief has access to these accounts, the more money you could lose. Call each bank or company and then follow up in writing. If there are fraudulent charges or debts on your account, or if a new account has been opened, you should immediately file a fraud report with your bank's fraud department. If a new account has been opened without your knowledge and consent, ask the company with which the account has been opened if they have a fraud department. If they do, file a fraud report with that department. If not, ask if they will accept the ID Theft Affidavit from the Federal Trade Commission (see Step 5 page 20). If you close an existing bank account and open a new one, be sure to create new PINs (Personal Identification Numbers) and passwords.

STEP 3: CREDIT REPORT FREEZE

You can now ask each credit reporting agency to freeze your credit report to prevent an identity thief from opening an account in your name. You must contact each of the three major credit bureaus (consumer reporting agency) listed on page 12 individually to have security freezes placed on each one. You must pay a fee of $10 to a credit bureau for a credit report freeze. You are exempt from this fee if you are 65 or older or if you are a victim of identity theft. Within 5 days of requesting the freeze, you will be sent a written confirmation of the freeze and a unique PIN or password to be used for authorizing a lifting of the freeze. The freeze will remain in place until you request its removal. Once the freeze is in place you will need to contact each agency to have the freeze lifted if you plan to apply

Cont. on next page

for a new account or loan. Before September 1, 2008, the credit reporting bureaus have 3 business days after your request to temporarily lift the freeze. After that date, the credit report freeze must be lifted within 15 minutes.

You can also request a fraud alert be put on your file. With a fraud alert on your account, credit lenders should try to contact you by phone before opening a new account. If they cannot reach you, the account should not be opened. Fraud alerts won't necessarily prevent unauthorized accounts from being opened in your name because lenders aren't legally obligated to contact you if there is a fraud alert in your file. If you place a fraud alert on your credit file, you are entitled to a free credit report from each credit reporting agency. If you place a fraud alert with one credit bureau, that credit bureau is required by law to contact the other two bureaus. The other bureaus will include the fraud alert in their reports.

If you lose your **Social Security card** or think an unauthorized person has it, contact a credit bureau and have an initial credit freeze placed on your credit reports.

Once you have placed a security freeze on your credit file, request a copy and review your report for these things:

- Accounts you did not open;
- Debts on your account that you did not know about;
- Inquiries from companies you don't know;
- Inaccurate information.

CREDIT BUREAUS

EQUIFAX
www.equifax.com

P.O. Box 740241
Atlanta, GA 30374-0241
1-888-766-0008

EXPERIAN
www.experian.com

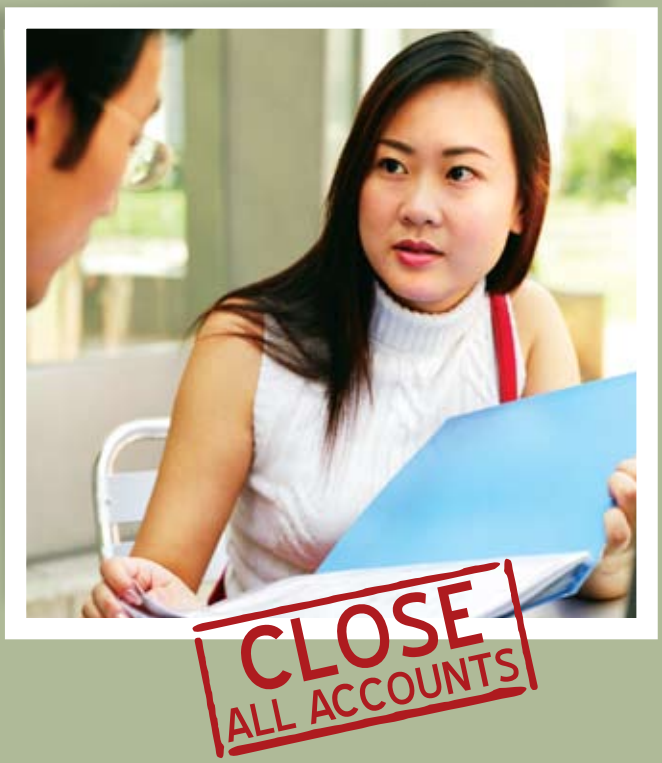
P.O. Box 9532
Allen, TX 75013
1-888-EXPERIAN (397-3742)

TRANSUNION
www.transunion.com

Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
1-800-680-7289

Contact all three credit bureaus immediately.

Act quickly!



STEP 4:
FIXING SPECIFIC PROBLEMS

You've identified the problems in your credit report as well as identity theft problems elsewhere. Now it is time to fix them. Here's how:

See CONTACTS on page 26 for contact information on these organizations.

EVENT	ACTION REQUIRED	CONTACT
You find any accounts tampered with or opened without your knowledge	Close the accounts immediately. Get new passwords and PINs for new accounts.	Credit Bureaus and creditors (banks, credit card issuers), merchants, utility and cell phone companies
Your ATM card, credit cards or checks were stolen	Close the accounts immediately. Get new PINs and passwords for new accounts. Notify each bank and major check verification companies. If your checks are stolen, put "stop-payments" on all checks remaining in the stolen checkbook. Ask any check verification company to put a fraud alert on your account.	Bank, credit card issuer, creditors, major check verification companies and the police
You find inquiries on your credit report that you did not know about	By phone and then in writing, notify the three major credit bureaus that unauthorized credit inquiries on your credit history were made and request that those inquiries be removed.	Credit Bureaus
You find inaccurate information on your credit report	By phone and then in writing, notify the three major credit bureaus and request the information be corrected.	Credit Bureaus

Cont. on next page

EVENT	ACTION REQUIRED	CONTACT
You have reason to believe your Social Security Number (SSN) has been stolen or misused	Report your allegations to the Social Security Administration (SSA), request a copy of your Social Security Statement and/or call SSA to verify the accuracy of the earnings reported on your SSN.	Social Security Administration
An identity thief has falsified change-of-address forms, stolen your mail or committed any other kind of mail fraud in order to get your personal information	Report it to your local post office. Contact your credit card companies, banks, etc. to notify them that your address was fraudulently changed. Have any changes of address done only in writing.	U.S. Postal Inspection Service (USPIS)
You've lost your passport, it was stolen or you believe it is being misused	Contact the United States Department of State through a field office or on their website.	United States Department of State (USDS).
You think your name or SSN is being used to obtain a fake driver's license	Contact the Motor Vehicle Division (MVD). Make sure you don't use your SSN as your driver's license number.	Motor Vehicle Division (MVD)
You think an identity thief has interfered with your security investments or a brokerage account	Report it to your broker or account manager as soon as possible. File a complaint with the U.S. Securities and Exchange Commission.	Your broker/account manager, U.S. Securities and Exchange Commission

EVENT	ACTION REQUIRED	CONTACT
A phone service account has been opened in your name, someone is using your calling card or unauthorized calls are being billed to your cellular phone	Cancel your account and/or calling card. Use new PINs if you open new accounts.	Your service provider
A debt collector contacts you trying to collect on a loan that you did not take out	Write a letter to the debt collector. State your reasons why you dispute the debt and include supporting documentation, such as a copy of the police report, or the FTC Identity Theft Affidavit.	Debt collector
You have been wrongfully accused of having committed a crime perpetrated by someone pretending to be you	File an impersonation report, have your identity confirmed and prove your innocence by comparing your information to that of the identity thief.	You will possibly need the assistance of a lawyer, i.e., a criminal defense attorney (public or private) in order to clear your name. Contact the Public Defenders' Office or the State Bar Association in order to find an attorney.
You believe someone has filed for bankruptcy in your name	Write to the U.S. Trustee and include supporting documentation. File a complaint with the U.S. Attorney and/or the FBI.	U.S trustee in the region where the bankruptcy, U.S. Attorney, FBI in the city the bankruptcy was filed, and you may want to contact the Public Defenders' Office or the State Bar Association in order to find an attorney to help you.

You can check your credit report online immediately at www.annualcreditreport.com.

Getting Your Credit Report Fixed

If you find inquiries on your credit report that you did not know about, contact the credit bureau and request that those inquiries be removed. If you find inaccurate information, again, contact the credit bureau as well to have it fixed. First call them and then follow up in writing. Provide copies of documents for support. If you cannot get any documentation from the creditor, send the credit bureau copies of your police report. Clearly identify what information you are disputing. Once your credit report is corrected you can ask for the credit bureau to send notices of the corrections to anyone your credit report was sent to in the last six months.

Creditors

If your credit card was stolen or you find fraudulent charges on your credit card bill, close the account immediately. Then contact the credit card company about the fraudulent charges. Make sure your letter includes your account number and a description of the unauthorized charges as well as your name and address. Send the creditor a copy of your police report and a copy of your ID Theft Affidavit (see page 20). If they do not accept the ID Theft Affidavit, fill out the creditor's fraud dispute forms. Request a return receipt so that you have proof of when the letter was received and show that the letter arrived within the required 60 days after you received the bill with fraudulent charges. Even if the address on your account was changed, you must still notify the creditor in writing within 60 days after the bill would have reached you. Keep track of your billing statements. If you do not notify the creditor within 60 days, you may be liable for the fraudulent charges.

See Liability on page 23 for more information.

Criminal Violations

If an identity thief has impersonated you when they were arrested or cited for a crime, there are things you can do to correct your record. First, to help prevent being mistakenly arrested, carry copies of documents showing that you are a victim of identity theft even if you do not know that criminal violations have been attributed to your name. You may also want to get a lawyer to help you.

STEP 5:
FILING COMPLAINTS

The Federal Trade Commission is the federal consumer protection agency. The FTC, in conjunction with the FBI, maintains an Identity Theft Data Clearinghouse. The FTC aids identity theft investigations by collecting complaints from identity theft victims and sharing the information with law enforcement agencies, credit bureaus, companies where the fraud took place, and other government agencies. File a complaint with the FTC by going to www.consumer.gov/idtheft or by calling their toll-free number: 1-877-ID-THEFT (1-877-438-4338).

Identity Theft Affidavit

A piece of documentation you need to fill out is the Identity Theft Affidavit offered by the Federal Trade Commission. This form will help you report information about your identity theft with just one form. Many companies accept this form, though others will require you to use their own form or submit more forms. If a new account has been opened in your name, you can use this form to provide the information that will help companies investigate the fraud. Once you have filled out the ID Theft Affidavit as completely and accurately as possible, mail a copy to any of the companies concerned with the fraud you describe in the form, such as banks or creditors. The ID Theft Affidavit as well as more detailed information about filling it out can be found at *www.consumer.gov/idtheft.*

Make sure that you keep copies of all of your paperwork including records of everyone you have corresponded with, fraudulent bills, police reports and complaint forms.

Go to the link below to view information on how to fill out an ID Theft Affidavit and Fraudulent Account Statement in order to help you dispute accounts fraudulently opened in your name by an identity thief.

http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf

FILE A COMPLAINT WITH THE FTC

the FASTER you act

THE LESS LIABLE YOU ARE

LIABILITY

To ensure that you don't end up paying hundreds or even thousands of dollars in fraudulent charges made by an identity thief, the best course of action is to act quickly. The faster you act, the less liable you are for unauthorized charges.

Credit Cards

According to the Truth in Lending Act, your liability is limited to $50 in unauthorized credit card charges per card in most cases. In order for this to come into effect, however, you must write to the creditor within 60 days of receiving the first bill that contained the fraudulent charge. If an identity thief changed your mailing address, you must still send your letter within 60 days of when you were supposed to have received it (keep track of your bills!).

ATM/Debit Cards

If your ATM or debit card is lost or stolen, report it as quickly as possible. If you report it within two business days, you are only responsible for $50 in unauthorized withdrawals or transfers. If you report it between three and 60 days after, you may be responsible for up to $500 in unauthorized withdrawals or transfers. If you do not report it within 60 days, you can lose any money the thief withdraws or transfers from your account after the 60 day period.

CHECKLISTS

Plan of Action List

We have provided you with a checklist to go through to make sure you have taken all the necessary steps after becoming an identity theft victim. Remember, you must complete all of these steps in a timely manner to avoid further problems.

- [ ] 1. Filed a police report.
- [ ] 2. Obtained a copy of your credit report.
- [ ] 3. Identified errors, inquiries you did not know about, accounts you did not open, debts you did not know about or anything else that seems wrong or out of place on your credit report.
- [ ] 4. Placed a security freeze on your credit report.
- [ ] 5. Closed any accounts that might have been tampered with or opened without your knowledge or consent.
- [ ] 6. Contacted a major credit bureau by phone and by writing to correct inaccurate information.
- [ ] 7. Filled out the Identity Theft Affidavit.
- [ ] 8. Contacted the correct agencies to fix inaccurate information, close accounts or report identity theft.
- [ ] 9. Filed a complaint with the Federal Trade Commission.

Document List

Here is a list of documents you should have. You won't be able to keep the originals of some of the documents so it is very important that you make a copy for yourself.

It is also a good idea to keep copies of the documents with you that prove you are an identity theft victim, such as a copy of your police report.

- [ ] 1. Police report
- [ ] 2. Identity Theft Affidavit
- [ ] 3. Bills with fraudulent charges
- [ ] 4. Documentation of accounts opened in your name without your consent
- [ ] 5. Copies of letters sent to credit bureaus and creditors


experian
Investigation results
About our dispute verification process
credit
CLEARED

CONTACTS

New Mexico Attorney General's Office

www.nmag.gov

111 Lomas NW, Ste 300
Albuquerque, NM 87102

P.O. Drawer 1508
Santa Fe, NM 87501

For complaints call:
(505) 222-9100 (Albuquerque)
(800) 678-1508 (In-State Toll Free)
(505) 827-6060 (Santa Fe)
(575) 526-2280 (Las Cruces)
Fax: (505) 827-6685

For general info. call:
(505) 222-9100 (Albuquerque)
(505) 827-6000 (Santa Fe)

Federal Trade Commission (FTC)

www.ftc.gov/idtheft

FTC
Consumer Response Center
Room 130-B
600 Pennsylvania Avenue
N.W. Washington, D.C., 20580
1-877-ID-THEFT (1-877-438-4338)

Major Credit Bureaus

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

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

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

A free copy of your credit report is available from the website *www.annualcreditreport.com*

Or write to:
Annual Credit Report Request Service
P.O. Box 105283
Atlanta, Georgia 30348-5283
Or call: 1-877-322-8228
TDD: 1-877-730-4104

Major Check Verification Companies

To find out if an identity thief has been passing bad checks in your name: SCAN 1-800-262-7771

To request a copy of your consumer report specifically about your checking account: Chex Systems, Inc. at 1-800-428-9623 or *www.chexhelp.com*

To request that your checks not be accepted by retailers:

TeleCheck at 1-800-710-9898

Social Security Administration

www.ssa.gov

SSA Fraud Hotline
P.O. Box 17768
Baltimore, MD 21235
SSA Fraud Hotline: 1-800-269-0271

U.S. Postal Inspection Service

http://postalinspectors.uspis.gov/

Call your local post office to find the nearest USPIS district office

OptOutPrescreen.com

Opt out of receiving preapproved and prescreen credit and insurance offers by going to:
www.optoutprescreen.com
or call toll free 1-888-567-8688


KNOW HOW TO
PROTECT YOUR

NEW MEXICO ATTORNEY GENERAL'S OFFICE | **www.nmag.gov**

Toll-Free 1.800.678.1508
Albuquerque 505.222.9000
Santa Fe 505.867.6000
Las Cruces 505.526.2280

NM Attorney General's Office
111 Lomas NW, Ste 300
Albuquerque, NM 87102

WE ARE HERE TO HELP YOU!