

**Office of the
Attorney General**

Identity Theft



LAWRENCE WASDEN
Attorney General
700 West Jefferson Street
Boise, ID 83720-0010
www.ag.idaho.gov



State of Idaho Office of Attorney General Lawrence Wasden

Dear Fellow Idahoan:

Identity theft is a serious problem. It can be financially and emotionally devastating. Every year hundreds of Idaho victims file identity theft complaints with the Federal Trade Commission. Identity thefts involving government documents or benefits are the most commonly reported to the FTC.

Fortunately, there are steps you can take to reduce your risk of becoming a victim. You can avoid identity theft by understanding how it occurs and taking steps to protect your privacy. If your identity is stolen, it is imperative that you take steps to prevent further victimization.

As your Attorney General, I am committed to helping you prevent identity theft, stopping deceptive business practices and enforcing Idaho's consumer protection laws.

To assist you, my office publishes a variety of consumer manuals addressing specific topics. They are all free and available through the Consumer Protection Division and on my website at www.ag.idaho.gov.

If you have been a victim of identity theft, I encourage you to report the crime to your local police department or sheriff's office. I hope you find this publication helpful.

LAWRENCE G. WASDEN
Attorney General

Table of Contents

WHAT IS IDENTITY THEFT?	1
HOW DOES IDENTITY THEFT OCCUR?	1
HOW CAN I PROTECT MYSELF FROM IDENTITY THEFT?	2
DON'T ADVERTISE YOUR LIFE	2
PRE-APPROVED CREDIT OFFERS	3
PROTECT YOUR FINANCIAL RECORDS	3
HOW TO OBTAIN A FREE CREDIT REPORT	5
THE CREDIT REPORT PROTECTION ACT	6
PROTECT YOUR SOCIAL SECURITY NUMBER	7
PROTECT YOUR MAIL	8
PROTECT YOUR COMPUTER	9
OTHER TIPS TO PROTECT YOUR PRIVACY	10
IF MY IDENTITY IS STOLEN, HOW CAN I MINIMIZE THE DAMAGE?	11
HOW DO I REPAIR MY CREDIT?	14
HOW DO I STOP DEBT COLLECTORS FROM TRYING TO COLLECT ON A FRAUDULENT DEBT?	16
IDENTITY THEFT RESOURCES	18

WHAT IS IDENTITY THEFT?

Identity theft occurs when someone uses your personal information, such as your name, Social Security number, credit card number or other identifying information, without your permission, to obtain goods, services or money in your name.

Identity theft is a crime under Idaho Code § 18-3126. If the amount of money (or value of services) lost is more than \$300, the theft is a felony. The punishment for felony identity theft is five years in prison, up to a \$50,000 fine or both. If the amount lost is less than \$300, the theft is a misdemeanor, which is punishable by a fine and time in the county jail.

As a crime victim, you are entitled to a restitution order. You should work closely with the county prosecutor's victim assistance coordinator to ensure your rights are protected. To learn more about crime victims' rights, please read the *Idaho Manual on the Rights of Victims of Crime*, available on the Attorney General's website.

If you are a victim of identity theft, you may not know your identity was stolen until you are denied credit, turned down for a job or receive a bill for purchases you did not make. By that time, your good name and credit history may be damaged. Rebuilding good credit after identity theft can take months or even years.

HOW DOES IDENTITY THEFT OCCUR?

Identity theft sometimes begins with a lost or stolen wallet or purse. Identity thieves also steal bank and credit card statements from mailboxes or the trash, impersonate legitimate businesses to obtain credit card numbers or Social Security numbers, or hack into computer databases to steal

customers' financial data, birthdates and e-mails. They also steal confidential information from their employers, divert mail by completing a "change of address form" or pose as a landlord or employer to obtain access to credit reports.

In the past few years, computer data has become more vulnerable to hackers and many people have become careless about protecting their personal information. There have been frequent security breaches at banks, stores, government agencies, colleges and other organizations. Criminals sell and buy credit card and Social Security numbers on the Internet. Consumers who advertise their lives on the Internet are easy marks for identity thieves.

Identity theft does not come with a warning message or bright, blinking lights. The theft happens quickly and quietly. Thieves are rarely identified and held accountable for the damage they cause. So, it is up to you to do what you can to protect your personal information.

HOW CAN I PROTECT MYSELF FROM IDENTITY THEFT?

Carefully guarding your privacy and personal information is your best protection against identity theft. This includes your financial records, Social Security number, Internet passwords and medical records.

Don't Advertise Your Life

The explosion of social networking, instant messaging, blogging, and tweeting has conditioned us to share our every thought, feeling, opinion, action, like, dislike and habit with the world. This is especially true among young adults. We publish photos of our families, our friends, our pets, our homes and our vacations on websites that will be viewable forever. Before you update your Facebook page, tweet your

location or shop online, remember the information you enter is one more byte of privacy that you can never get back.

Pre-Approved Credit Offers

Shred pre-approved credit offers. Do not just throw them in the trash.

Ask the consumer credit reporting agencies (credit agencies) to remove your name from lists for pre-approved, unsolicited credit and insurance offers: Call (888) 567-8688 or visit www.optoutprescreen.com to opt-out of pre-screened credit and insurance offers.

If you don't have access to the Internet, write each of the companies listed below. Tell them you want to permanently opt-out of pre-screened credit and insurance offers. Be sure to include your full name, home telephone number, Social Security number and date of birth in your letter.

A sample opt-out letter is available on the Attorney General's website and in Appendix A.

Experian Opt Out PO Box 919 Allen, TX 75013	TransUnion Name Removal Option PO Box 505 Woodlyn, PA 19094
Equifax, Inc. Options PO Box 740123 Atlanta, GA 30374-0123	Innovis Consumer Assistance PO Box 495 Pittsburgh, PA 15230-0495

Protect Your Financial Records

Shred old bank and credit card statements, cancelled checks, charge receipts, insurance forms and other financial

documents before disposal.

Review your monthly credit card and bank statements thoroughly. Question any item that looks wrong.

If your bank or credit card statements do not arrive on time, call the issuer to make sure the statements are being sent to the right address.

If you have several credit or debit cards, consider enrolling in a credit card registry service that will notify all of your creditors after one call from you. Research the service before you enroll to make sure it is reputable.

If you receive a credit card in the mail that you did not request, call the issuer to find out why it was sent to you. If someone else requested it in your name, cancel it immediately and follow the steps outlined in this brochure.

When you create passwords for ATM cards, long distance accounts or other forms of credit, do not use numbers others can associate with you such as your birth date or part of your Social Security number. Avoid using words, such as your mother's maiden name, which are likely to appear in public records accessible to thieves. The best passwords use a combination of letters and numbers.

Never provide your credit card or bank account numbers to anyone who initiates contact with you. Telemarketers who claim they can lower your credit card interest rate or qualify you for a new card are really identity thieves trying to get your account number. When shopping online, use only secure websites from established and reputable businesses. Never e-mail your credit card number to anyone.

Check your credit reports once a year. If you have children, review their credit reports, too. Identity thieves like to target

young people, even infants, because it is unlikely the theft will be discovered until the child grows up and applies for credit.

How to Obtain a Free Credit Report

You can receive free copies of your credit reports once a year from each of the three major national credit reporting agencies.

The federal Fair Credit Reporting Act (FCRA) requires Equifax, Experian and Trans Union to provide you with a free copy of your credit report every 12 months. However, you have to ask for your free credit reports.

The annual free reports are available only through the centralized source below. *If you contact the companies directly you will still be charged for your credit reports.*

To obtain your free reports:

- Call (877) 322-8228; or
- Order online at www.annualcreditreport.com; or
- Complete the Annual Credit Report Request Form, available at www.ftc.gov/credit, and mail it to:

Annual Credit Report Request Service
PO Box 105281
Atlanta, GA
30348-5281

In order to obtain the credit report, you will be asked for identifying information, including your Social Security number. Providing this information will ensure that credit reporting agencies send you your credit report.

Please note that when you apply for your free credit reports,

the credit reporting agencies will likely try to sell you upgraded services for a fee. **You are under no obligation to purchase any upgraded services.** You may simply say no to these options and receive only your free report.

The Credit Report Protection Act

The Credit Report Protection Act allows you to place a “security freeze” on your credit report. It also prohibits a person from intentionally releasing your Social Security number to the general public. A security freeze, often called a “credit freeze,” generally prohibits a credit agency from giving your credit information to a third-party creditor. However, some types of business are allowed to access your credit report while a security freeze is in effect. These include your existing creditors, insurance companies and those screening potential tenants or employees. A freeze helps prevent identity thieves from obtaining credit in your name because most creditors won’t extend credit without first reviewing your credit report.

You may request that a credit agency place a security freeze on your credit report at any time and for any reason. If you believe that your personal or financial information has been disclosed without your permission, you should consider requesting a security freeze.

To obtain a security freeze, you must mail a written request to each of the credit reporting agencies (Equifax, Experian, Trans Union and Innovis) asking them to place a freeze on your credit report. You must pay a fee of up to \$6.00 to each credit reporting agency from which you request a freeze. However, if you are a victim of identity theft, you can obtain a security freeze for free. To obtain a free security freeze as a victim of identity theft, you must file a police report and provide a copy to the credit reporting agencies.

If you want to lift the security freeze only temporarily to allow a specific creditor to access your credit report, you must contact the credit agency that the creditor uses and request that your credit report be unfrozen temporarily. Each credit reporting agency determines its own fee to lift the freeze, but it cannot be more than \$6.00.

To permanently lift a security freeze, follow the same steps as requesting a temporary lift, but specify a permanent lift instead. Agencies cannot charge a fee to permanently lift a security freeze.

Credit agencies are responsible for providing an address, telephone number, fax number, or e-mail address that consumers can use to request a temporary lift of a security freeze. All agencies must provide a secure electronic method for consumers to use.

You may sue a credit reporting agency if it harms you by violating the Credit Report Protection Act. You may sue for damages and for the cost of your reasonable attorney fees. In some cases, a court may award you punitive damages.

If you believe that a person has violated the Credit Report Protection Act, you should consult with a private attorney about your legal rights and options. You also can file a consumer complaint with the Attorney General's Office.

Protect Your Social Security Number

Do not carry your Social Security card with you unless you need it for a job application.

Financial institutions or employers may request your Social Security number for legitimate wage and tax reporting purposes. When you apply for credit, private businesses may ask for your number to run a credit check. Although these

are appropriate requests, you should ask the following questions before giving out your Social Security number:

1. Why do you need it?
2. How will you use it?
3. How will you protect it from being stolen?
4. What will happen if I don't give it to you?

Never provide your Social Security number to anyone who initiates contact with you. Such contacts, which include e-mails, are probably fraudulent attempts to get your personal information. Do not respond to these e-mails. No legitimate company in the United States will contact you by e-mail for personal account information.

The Social Security Administration will send you a copy of your Earnings and Benefits Summary once a year. Review it carefully for accuracy. If you think you may be a victim of identity theft, order a copy of your Benefits Summary by contacting the Social Security Administration directly at (800) 772-1213 or visit www.ssa.gov.

Protect Your Mail

Take your outgoing mail to a post office or U.S. Postal Service collection box instead of leaving it in an unsecured mailbox.

Remove your mail promptly from your mailbox.

If you are going on vacation, ask the U.S. Postal Service for a vacation hold. The Postal Service will deliver your mail when you get home or hold it at your local post office until you pick it up. To request a vacation hold, call (800) 275-8777 or visit www.usps.gov.

Protect Your Computer

Install virus, malware and spyware protection software and keep it up-to-date.

Do not open e-mail or click on links that you receive from strangers.

Install a firewall program, especially if your computer is connected to the Internet 24 hours a day.

Use the most current version of the browser of your choice. Select a secure browser, i.e. software that encrypts or scrambles information you send over the Internet, to protect the security of your online transactions. When you make a purchase online, make sure the URL address has an “https” and a padlock displaying a valid digital certificate.

Do not store financial information on your computer. If you do, use a complex password consisting of upper and lower case letters, numbers, and a special character such as # or &.

Before you dispose of your computer, use a “wipe” utility program to overwrite the entire hard drive. This makes the files unrecoverable. Even better, remove the hard drive from the computer and take it to a shredder. Many businesses that shred documents will also shred a hard drive for a small fee.

Review a website’s privacy policy before transacting any business through it. The website should contain a link to its privacy policy. Usually the link is located at the bottom of the page and is titled “Privacy Policy.” A reliable privacy policy should explain what information the website collects from you, how it protects that information, whether it uses “cookies” and whether it allows you to opt-in or opt-out of the website’s data collecting, sharing or retaining policies.

For more information about Internet privacy, please read the Attorney General's brochure entitled *Internet Safety*. For a free copy, visit www.ag.idaho.gov or call (208) 334-2424 or in state, toll-free (800) 432-3545.

Other Tips to Protect Your Privacy

Keep personal and financial information in a secure place, such as a locked safe, especially if you have roommates or workers in your home.

Ask your employer about the security of your personal information at work. Verify that access to your personal information is restricted to only those who need access and that the records are kept in a secure location.

Do not provide personal information over the phone, through the mail or over the Internet, unless you initiated the transaction and you know the person or institution receiving the information.

Do research to make sure an organization or business is legitimate. Contact your local Better Business Bureau (BBB) to check the reputation of a business or to obtain a reliability report. BBB reports for businesses are available at www.bbb.org. BBB reports for charities are available at www.give.org.

Limit the number of credit cards and other identification that you keep in your wallet or purse. Carry only what you need.

Watch out for promotional scams. Thieves may get personal information from you through fraudulent offers such as foreign lotteries, charitable donation requests, business opportunities and investment schemes.

To inquire about a business, call the Attorney General's Office at (208) 334-2424 or in-state, toll-free (800) 432-3545

or e-mail us at consumer_protection@ag.idaho.gov. Although our information is not related directly to identity theft, we can send you a report indicating whether the Attorney General's Office has received complaints about the business and whether the complaints have been resolved.

IF MY IDENTITY IS STOLEN, HOW CAN I MINIMIZE THE DAMAGE?

The steps differ depending on your circumstances. However, six basic actions are appropriate in almost every case.

Step 1: Call your financial institutions to report the identity theft and cancel stolen checks, credit cards and ATM cards.

If your checks were stolen, contact these major check verification companies and ask that retailers who use their databases not accept your checks:

Telecheck:	(800) 710-9898
Certegy, Inc.:	(800) 437-5120
International Check Services:	(800) 994-2949

To find out if the thief has passed bad checks in your name, call the Shared Check Authorization Network (SCAN) at (800) 262-7771. SCAN maintains a database of returned and fraudulent checks. If you determine checks were written in your name, contact your bank and stop payment on the checks. You also need to call the stores that accepted the stolen checks to tell them about the theft.

Step 2: File a report with your local police and the police in the community where the theft occurred.

Obtain certified copies of the report because you may need it

to validate your claims to creditors.

Step 3: Place a fraud alert on your credit reports and get copies of your credit reports.

A fraud alert makes it more difficult for a thief to get credit in your name. An initial fraud alert will remain in your credit file for at least 90 days. An extended alert, which requires you to provide specific information, stays in your file for seven years.

Call any **one** of the three major credit agencies to place a fraud alert in your credit file. Once the agency verifies the validity of the fraud, the other two will be notified automatically. You then will receive a free credit report from each of the major agencies.

Equifax Fraud Report: (888) 766-0008

Experian Fraud Report: (888) 397-3742

TransUnion Fraud Report: (800) 680-7289

Step 4: Carefully review your credit reports.

Close any accounts that show fraudulent activity. If you open new accounts, use new passwords.

If your credit report contains fraudulent information, ask the information provider to send you its fraud dispute form.

The provider also may accept what is called an Identity Theft Affidavit. The following link provides information on how to prepare an ID Theft Affidavit: www.consumer.ftc.gov.

The affidavit can help you close unauthorized accounts and eliminate debts wrongfully attributed to your name.

If you don't have a police report or any paperwork from creditors, send the completed affidavit to the three major credit agencies. They will use it to start the dispute investigation process.

Not all companies accept the affidavit. Some may require you to use their forms instead. So, check with the company before sending the affidavit.

Step 5: Notify the U.S. Postal Service if someone filed a change of address form in your name.

You also should contact the U.S. Postal Inspectors if the thief used the mail to commit credit or bank fraud in your name.

File a mail fraud complaint at:

Criminal Investigations Service Center
Attn: Mail Fraud
222 S. Riverside Plaza, Ste. 1250
Chicago, IL 60606-6100
postalinspectors.uspis.gov

Step 6: File a complaint with the Federal Trade Commission (FTC).

Reporting your identity theft to the FTC provides information to help law enforcement officials find and stop identity thieves.

You can file a complaint online at www.ftc.gov, by telephone at (877) 438-4338 or TDD (202) 326-2502 or by mail:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Ave. N.W.
Washington, D.C. 20580

HOW DO I REPAIR MY CREDIT?

Idaho law provides a way for identity theft victims to clear negative credit records if the identity theft results in negative information on your credit report(s).

1. File a police report.

Explain the facts of the identity theft and obtain certified copies of the report.

2. Contact the credit agencies.

Call the agencies and follow up in writing. Identify all inaccurate information and include copies of documents, such as a certified copy of the police report and an Identity Theft Affidavit, to support your position.

Your letter to the credit agencies should contain your name, address, telephone number and an explanation of why you dispute the incorrect information. Include a copy of your credit report with a circle around the disputed items.

Send your letter by certified mail, return receipt requested, so you can document when the agencies received it. Keep a copy of your letter and all attachments.

Sample dispute letters to the credit agencies and creditors are available on the Attorney General's website at www.ag.idaho.gov.

The federal Fair Credit Reporting Act (FCRA) explains how to dispute mistakes on your credit report. Both the credit agency and the information provider, like a bank or credit card company, must correct inaccurate information in your report.

3. The credit agency will investigate your claim.

The credit agency must complete its investigation within 30 days unless you submit additional documents. If your claim is frivolous, the agency must tell you so within five business days. Otherwise, the agency must send the information provider all relevant documents you provide about the dispute.

4. The information provider will investigate your claim.

The information provider reviews the findings of the credit agency's investigation and reports back to the credit agency. The provider must report the inaccuracy to any nationwide credit agency to which it reports. The agency then can correct your file.

5. The credit agency will provide you with a written report.

Following its investigation, the agency will provide you a report and a copy of your credit report if any information is changed. The agency may not put the disputed information back in your file unless the information provider verifies that the information is accurate. The agency also must send you a written notice that includes the name, address and phone number of the information provider.

6. Request notices of corrections.

Ask the credit agency to send notices of corrections to anyone who received your report in the past six months.

If the investigation doesn't resolve your dispute, write a 100 word statement explaining your dispute, send it to the agency and ask that it be included in your file.

7. Contact your creditors.

Write to the information provider, informing it that you dispute what it reported. Send copies (not originals) of documents that support your position.

Most creditors provide specific addresses for sending dispute letters. If the address is not specified in your credit agreement, call the creditor to verify the address.

If the creditor requires a special form, complete and return it. If the creditor then reports the disputed item(s) to a credit agency, it must include a notice of dispute.

8. Take legal action if the credit agency doesn't comply.

You have the right to sue a credit agency for failing to block incorrect information resulting from identity theft. You may sue the agency, the information provider or both for damages and injunctive relief. A judgment in your favor must include an award of attorney fees and other relief as granted by the court. Consult with a private lawyer to advise you of your specific options.

9. Be skeptical of businesses that offer “credit repair” services.

They often require high up-front fees and do nothing to fix your credit. Some just disappear with your money.

HOW DO I STOP DEBT COLLECTORS FROM TRYING TO COLLECT ON A FRAUDULENT DEBT?

To stop a debt collector from contacting you, you must write a letter to the collection agency telling them to stop. Include

copies of documents that support your position. After the debt collector receives your letter, it may not contact you again except to:

- (1) Tell you that it will stop contacting you; and
- (2) Tell you that it or the creditor will take some specific action.

The debt collector must provide proof of the debt's validity. If you receive documents from the collector, review them carefully. The thief may have completed a credit application in your name. You then can dispute the collector's evidence.

Under the federal Fair Debt Collection Practices Act (FDCPA), a debt collector is prohibited from using unfair or unconscionable practices to collect any debt. Failure to comply with the FDCPA subjects a collector to civil liability.

IDENTITY THEFT RESOURCES

Better Business Bureau (S.W. Idaho)
(208) 342-4649

Better Business Bureau (S.E. Idaho)
(208) 523-9754

Better Business Bureau (N. Idaho)
(509) 455-4200

Direct Marketing Association
(202) 955-5030

Federal Bureau of Investigation
(202) 324-3000

Federal Communications Commission
(888) 225-5322

Federal Trade Commission
(877) 382-4357

Idaho Attorney General's Office
(800) 432-3545

Idaho Department of Finance - Toll-free (only within Idaho)
(888) 346-3378

Idaho Department of Insurance
(800) 721-3272

Idaho Public Utilities Commission
(800) 432-0369

Idaho State Bar Lawyer Referral Service
(208) 334-4500

United States Postal Service
(877) 876-2455

**APPENDIX A
SAMPLE OPT-OUT LETTER**

<<Enter Today's Date>>

<<Enter Address Provided on Page 3>>

Re: Opt-Out Request

To whom it may concern:

I request to opt-out from pre-screened credit and insurance offers and have my name removed from your company's marketing lists. The following information is provided exclusively to facilitate my request.

FIRST NAME	MIDDLE NAME	LAST NAME	SUFFIX
CURRENT MAILING STREET ADDRESS			
CURRENT MAILING CITY, STATE, ZIP			
PRIOR MAILING STREET ADDRESS (IF MOVED IN LAST 6 MONTHS)			
PRIOR MAILING CITY STATE ZIP			
SOCIAL SECURITY NUMBER		BIRTH DATE	

Thank you for your prompt attention to my request.

SIGNATURE

Consumer Protection Manuals

Buying a Home	Pyramids, Gift Schemes & Network Marketing
Charitable Giving	
Credit and Debt	Residential Construction
Foreclosure Prevention: A Workbook	Rules of Consumer Protection
Guidelines for Motor Vehicle Advertising in Idaho	Rules of Telephone Solicitations
Idaho Consumer Protection Manual	Senior Citizens Manual
Idaho Lemon Law	Service on an Idaho Nonprofit Board of Directors
Identity Theft	Telephone Solicitation
Internet Safety	
Landlord and Tenant Guidelines	Young Adult Handbook

Funds collected by the Attorney General's Consumer Protection Division as the result of enforcement actions paid for these pamphlets. No tax monies were used to pay for these publications.

The Consumer Protection Division enforces Idaho's consumer protection laws, provides information to the public on consumer issues, and offers an informal mediation process for individual consumer complaints.

If you have a consumer problem or question, please call (208) 334-2424 or in-state toll-free (800) 432-3545. TDD access and Language Line translation services are available. The Attorney General's website is available at www.ag.idaho.gov.