

Guarding Against Identity Theft

Identity theft is the fastest-growing white collar crime in the United States. A survey by the Federal Trade Commission (FTC) found that an estimated 27 million Americans have become victims of identity theft in the past five years. A staggering 10 million thefts occurred in the past year. In the United States an identity is stolen every 22 seconds. The top 10 locations in terms of numbers of victims are Washington D.C., California, Arizona, Nevada, Texas, Florida, New York, Washington, Maryland, and Oregon.

Identity theft occurs when someone uses your personal information, such as your name, social security number (SSN), credit card number, or other identifying information, without your permission, to commit fraud or other crimes.

How identities are stolen

According to the Privacy Rights Clearinghouse, thieves obtain your SSN, driver's license, credit card numbers, and other pieces of identification in a variety of ways, including these:

- "Dumpster diving" in trash bins for unshredded credit card and loan applications and documents containing SSNs and account numbers.
- Stealing mail from unlocked mailboxes to obtain newly issued credit cards, bank and credit card statements, pre-approved credit offers, investment reports, insurance statements, benefits documents, or tax information.
- Accessing your credit report fraudulently, by posing as an employer, loan officer, or landlord, for example.
- Obtaining names and SSNs from personnel or customer files in the workplace.
- "Shoulder surfing" at ATM machines and phone booths in order to capture PIN numbers.
- Finding identifying information on Internet sources, via public records sites, and through fee-based information broker sites.

While there is no way to ensure that you will never become a victim of identity theft, you can take steps to lower your risk. Exercise caution and guard your personal information by following these guidelines:

Protect your information

- Minimize the amount of information that a thief can steal. Don't carry more credit cards than you need. Don't carry social security cards, birth certificates, or passports.
- Don't carry items with your SSN on them, such as insurance and Medicare cards, unless you need them that day.
- Never give out your SSN, credit card number, or other personal information over the phone, mail, or Internet unless you initiated the contact and you have a trusted business relationship.
- Place passwords (PINS) on your bank, credit card, and phone accounts. Do not use passwords that are easily identified such as birth date, phone number, maiden name, or the last four digits of your social security number.
- Make a list of the contents of your wallet. Also make photocopies of the fronts and backs of all your credit and debit cards. This will give you the account numbers and phone numbers to call if it becomes necessary to cancel your cards. Keep the copies and list in a safe place.

Protect your mail

- Pay attention to your mail, especially billing cycles. Contact creditors immediately if your bills arrive late. A missing bill could mean an identity thief has taken over your credit accounts and changed the billing address.
- Deposit outgoing mail in post office collections boxes or at your local post office. Use a locking mailbox for your home delivery and do not allow mail to pile up.
- To prevent thieves from retrieving personal information from your trash, shred or burn all correspondence that contains personal information about you and your family. Shred information you plan to discard such as your charge receipts, credit applications, insurance forms, bank statements, expired credit cards, and preapproved credit offers.

Practice computer safety

- On the Internet, look for Internet addresses that begin https rather than http. The “s” indicates a secure connection. A small padlock symbol should appear in the bottom right corner of your screen, indicating it is safe to transmit your credit card number or other personal data.
- Regularly update your virus protection software and use a firewall. Avoid opening files sent to you by strangers, clicking on hyperlinks, or downloading programs from people or companies you do not currently do business with or recognize.

Guard your accounts

- Never fax your credit card numbers. You do not know who has access to that information and it is probably not secure.
- When having new checks printed, use your initials for your first name. With your initials on your check instead of your first name, a thief will not know how to sign your checks. A check arriving at your bank improperly signed should raise “red flags.”
- If you have a post office box use that address on your checks rather than your physical address. If you need a phone number on your checks, use your office number. When paying bills with a personal check never put your full account number in the memo line. Use only the last four digits of your account number.
- Inquire about security measures at your workplace, doctor’s office, or any place that gathers your personal information. When asked to give personal information find out why it is needed, how it will be used, and how it will be protected.
- If you are in the military and deployed, place an “active duty alert” in your credit file. The alert requires creditors to verify your identity before granting credit in your name.
- Reduce the amount of personal information about you that is “out there.” Remove your name from the marketing lists of major credit bureaus, opt out of the sale or sharing of your information when you are offered the chance, and sign up for the Federal Trade Commission’s National Do Not Call Registry. To opt out of receiving pre-approved credit offers, contact 1-888-567-8688.
- Order a copy of your credit report from each of the three major credit reporting agencies and check for errors. To obtain a free copy of your credit report log on to www.annualcreditreport.com or call toll free to 1-877-322-8228.

- If you find errors on your credit report or suspect identity theft, contact each of the credit reporting agencies, immediately.

Equifax—1-800-525-6285

Experian—1-888-397-3742

TransUnion—1-800-680-7289

There is no guarantee that you will avoid identity theft, but by taking these steps you can help to minimize your risk. Think about taking care of your identity on a regular basis just as you take care of your health; an ounce of prevention can be worth a hundred pounds of cure!

To learn what to do if your identity is stolen read “When Identity Thieves Strike” in Bulletin 841, *Credit Cents*, from University of Idaho Extension.

Author: Marsha Lockard, University of Idaho Extension Educator, Owyhee County