

How To Protect Your Identity from Being Stolen

Identity theft occurs when someone uses another person's identity. It can be an account takeover or posing as a financial institution member to obtain the members' personal financial information - pretexting.

ID thieves can do anything in your name – ID thieves can buy a house or a car, sell your house or car, use your current financial institution and credit card accounts, apply for new credit, and even be arrested and let out on bail in your name. Identity thieves also use false IDs to cash your checks, change your address, and board a plane all these things, in *your* name.

Although you only have to pay the first \$50 of fraudulent charges, the average identity theft victim spends an average of 175 hours and \$800 clearing their name.

Identity thieves obtain personal information by:

1. Stealing wallets and purses containing personal identification and credit cards.
2. Stealing mail to obtain credit card statements, monthly account statements, telephone bills, and tax information.
3. Filling out change-of-address forms to divert a person's mail to another location.
4. Going through a person's or company's trash – dumpster diving.
5. Fraudulently obtaining a person's credit report by posing as someone with a legitimate right to the information.
6. Purchasing copies of job or charge-card applications from store employees.
7. Computer hacking.
8. Shoulder surfing – looking over your shoulder when you are at an ATM.

Prevention Techniques

- Before allowing anyone access to personal information (e.g. Social Security Number (SSN), mother's maiden name, bank account numbers, etc.) ask how it will be used and if it can be kept confidential. Never give this information out over the telephone. Only give out your SSN when necessary, ask to use another form of identification, if possible. DO NOT carry your Social Security card in your purse or wallet.
- Place the contents of your wallet on a copy machine. Do both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call and cancel. Keep the copies in a safe place. Do not carry any more credit cards and identification than are absolutely necessary.
- Shred or destroy credit and debit card receipts, cancelled checks, expired credit cards, pre-approved credit card solicitations, convenience checks, insurance forms, financial statements, and any other documents you are disposing that contain personal information or account numbers. To stop receiving prescreened credit offers, you can call 888-5-optout. You can prohibit use of information in your credit bureau report from being used to determine if you qualify for offers not

initiated by you by calling toll-free 1-888-567-8688. You can reduce junk mail and telemarketing calls by going to the Direct Marketing Association website www.the-dma.org

- Mail all outgoing mail from post office collection boxes, from your work, or the local post office. Do not let your personal mail sit in the mailbox after it as been delivered.
- Keep a record of all the credit cards and accounts you have, including issuing company information, card or account numbers, expiration dates, and telephone numbers to call if the card or account is lost, stolen or fraudulently accessed. This record should be kept in a safe place. Be aware of when you receive credit card bills and immediately report bills not received. Review bills thoroughly for unauthorized charges. Your credit card has expired. Where is your new card? If you have moved but neglected to tell your credit card issuer, your new card could be sitting at your old address, and that could lead to trouble. If a stranger or even a family member receives your card by mistake, and gains access to personal information such as a Social Security number, date of birth, or mother's maiden name, they may be able to activate the card and go on a spending spree. The best way to protect yourself is to notify card companies each time you move and keep track of your plastic. If your new card is due, keep one eye on the mailbox and the other on the calendar.
- Notify your credit union if your checks are stolen and close that account. Stop payment on your checks. Ask your credit union to notify the check verification service with which it does business. Do not have your SSN or driver's license number preprinted on your checks.
- When assigning passwords to accounts, avoid using your mother's maiden name, your birth date, the last four digits of your SSN, your phone number, address, your driver's license number, or any series of consecutive numbers.
- Find out how your employer safeguards your personal information. Employers are obligated to store documents with personal information, such as SSN, in a secure format, whether the information is paper-based or electronic.
- Get a copy of your credit report annually from each of the three credit reporting agencies. Review the report to make sure it is accurate and includes only credit you have authorized. If you discover inaccurate information or a credit check conducted for an unfamiliar loan or lease, contact the credit bureau and report it immediately. Credit reports can cost up to \$8.50 per report. If you have been denied credit based on information from a credit report you are entitled to get a free copy of it.
- As of September 13, 1997, Florida residents can protect personal information in their driver's license and motor vehicle records from disclosure. There are exceptions as specified by law. You can view these exceptions and download a copy of the Request to Withhold Disclosure of Personal Information form at www.hsmv.state.fl.us/ddl/dppa.html
- Check your all financial statements for discrepancies or unauthorized transactions.
- Do not leave your wallet or credit cards in your car.

- Do not give out personal or financial information over the telephone or the Internet unless you know the caller or you initiated the call.
- Fraudsters are sending a fictitious IRS form and a fraudulent letter purporting to be from a bank by asking them to disclose personal and banking information. If a person returns the false IRS form to the fax number provided on the fake bank letter, the perpetrator of the fraud can contact the bank with enough information to appear credible, thereby gaining access to the victim's accounts, credit, and credit history. Contact the IRS to report the incident using the toll-free hotline number 800.829.0433.
- At an ATM, shield the screen and keyboard to prevent other people from seeing your PIN number. Put your cash in your wallet immediately and always take your receipt. According to law enforcement officials, thieves are putting thin plastic "sleeves" in ATM card slots so that when you insert your card, the machine cannot read the strip and keeps asking you to re-enter your PIN (personal identification number). Meanwhile, someone nearby is watching you enter your PIN, noting the numbers you hit. And when you walk away, assuming the machine ate your card, the thieves come up and remove the plastic sleeve and your card. Then they empty your account. To avoid falling prey to this scam, run your finger along the card slot before you put your card in. The sleeves have a couple of tiny prongs so the thieves can pull them out of the slot, and you will be able to feel these prongs.
- Identity thieves go digital – dumpster diving and pick pocketing aren't the only ways identity thieves can snatch your personal information these days. They now are hacking into computers and prowling the Internet in search of new victims.
- Online job search site Monster.com is warning users to beware of possible identity fraud when responding to job postings. Con artists reportedly posing as employers are looking for applicants' personal information. Meanwhile, the computer systems of a large university and a major credit card company were recently hacked. The mainframes held thousands of names, addresses, and Social Security numbers.
- Reduce the number of personal checks that you write.
- Do not join "savers clubs" or enter contest and sweepstakes.
- Keep personal and financial records under lock and key.

The agencies and numbers to call are:

Equifax – www.Equifax.com

To request a report – 800.685.1111 or write:
 PO Box 740241
 Atlanta, GA 30374-0241
 To report fraud – 800.525.6285

Experian (formerly TRW) – www.experian.com

To request a report – 888.397.3742 or write:
 PO Box 949
 Allen, TX 75013-0949

Trans Union – www.tuc.com

To request a report – 800.916.8800 or write:
 PO Box 1000
 Chester, PA 19022
 To report fraud – 800-680-7289 or write:
 Fraud Victim Assistance
 PO Box 6790, Fullerton, CA 92634

Should You Become A Victim

If you believe you have been the victim of ID theft, immediately take the following steps:

1. Call the Federal Trade Commission's Identity Theft Hotline at 877.438.4338 (877 ID THEFT). Other tips are given at the FTC's website at www.consumer.gov/idtheft. You can write them at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580
2. Report the fraud to the three major credit bureaus at the numbers given above and request a fraud alert placed on your name and SSN. In the past, if consumers suspected they were victims of identity theft, they had to call and report it to each of the three major credit bureaus (Experian, Equifax, and TransUnion). But now you can call just one of these three and they will contact the other two. The change in reporting procedure was enacted in an effort to make the process easier on victims of identity theft. The Federal Trade Commission reports that complaints of identity theft nearly doubled in 2002.
3. File a report with the police department in the locality where the fraud occurred.
4. Get new account numbers, ATM cards, and pin numbers.
5. It is a crime for someone to use your SSN to establish credit or open new accounts. Call the SSA Fraud Hotline at 1-800-269-0271.
6. Contact your creditors – credit card companies, phone companies, etc. for any accounts that have been tampered with or opened fraudulently. You should speak to someone in the fraud department. You must follow up with written correspondence.
7. If an identity thief stole your mail or falsified a change-of-address form, that is a crime. Report it to your local postal inspector.
8. Report all stolen cards to the issuers immediately and get replacement cards with new account numbers. Ask that the old accounts be processed as "account closed at consumer's request" so that a "lost or stolen" notation cannot be interpreted as blaming you. Follow up with written correspondence.
9. Check the section of the report that lists "inquiries" and request that "inquiries" from companies that opened the fraudulent accounts be removed. Follow up each conversation with a letter detailing the exact circumstances and action requested. Include copies (not originals) of documents that support your position. Send your letter by certified mail and request a return receipt. Keep copies of your dispute letter and any enclosures. Do not forget to follow up in a few months by requesting a new copy of your report so you can verify that the corrections were made.
10. If someone has filed for bankruptcy using your name, you will need to write to the U.S. Trustee in the region where the bankruptcy was filed. A list of regions can be found at www.usdoj.gov/ust
11. Request that creditors call you before opening any new accounts or changing existing ones. Add a victim's statement to your report and find out how long the fraud alert is posted on your account and extend it if possible.

Keep a log of all conversations, including dates and names. Send correspondence by certified mail. Keep copies of all letters and documents and be sure to have your police report case number with this documentation.