

PROTECT  
YOURSELF

FROM

IDENTITY  
*theft*

PRESENTED BY  
ELLIOTT WILCOX

1. **Order your credit reports.** Order your credit report this week and make sure that the information is correct. Here are the numbers for the major credit reporting services.

	<b>Equifax</b>	<b>Experian (TRW)</b>	<b>Trans Union</b>
<b>To report fraud</b>	(800) 525-6285 or PO Box 740250, Atlanta, GA 30374-0250	(888) EXPERIAN, fax to 888-397-3742, or PO Box 1017, Allen, TX 75013	(800) 680-7289 or PO Box 6790, Fullerton, CA 92634
<b>To order a copy of your credit report</b>	(800) 685-1111 or PO Box 740241, Atlanta, GA 30374-0241	(888) EXPERIAN, or PO Box 2104, Allen, TX 75013	(800) 888-4213 or PO Box 390, Springfield, PA 19064
<b>To opt out of pre-approved offers of credit</b>	(800) 567-8688 or Equifax Options, PO Box 740123, Atlanta, GA 30374-0123	(800) 353-0809, or (888) 5OPTOUT or PO Box 919, Allen, TX, 75013	(800) 680-7293 or (888) 5OPTOUT or PO Box 97328, Jackson, MS 39238

2. **Buy a shredder.** You probably receive lots of invitations to obtain pre-approved credit cards or home equity loans. Don't just throw the information away – identity thieves can use it. Instead, shred all of that paperwork before discarding. Shred credit card receipts, credit card bills, pre-approved credit offers, and anything that has your account number on it. Get a shredder for home and one for the office. (Cross-cut shredders are more effective than strip shredders.)
3. **Be careful of who you give the information to.** Don't give out your information over the phone or email unless you initiated the conversation or are positive about who you're dealing with. (How do you know that the person you're talking with is a bank executive? Because of the baritone voice? Con men can be very convincing. If he works for the bank, why would he need your account number anyway?)
4. **Secure your home.** Secure your personal information (social security numbers, driver licenses, credit card account numbers or bills) inside your home, especially if you have roommates, employ outside help, or are having service work done.
5. **Account passwords.** Use passwords on your accounts – not your mom's maiden name. When CitiBank asks for your mother's maiden name so they can open an account, tell them her name was, "X45JH76T." No thief will ever guess that. You can also rotate them on a regular basis, too.
6. **Mail.** Guard your mail and trash from theft. Consider getting a locked mailbox if you don't pick up your mail until very late in the day. Drop your outgoing mail in a secure drop box. Ask a friend to pick up your mail or ask the postal service to stop delivery. Call 1-800-275-8777 to request a vacation mail hold, or visit [www.USPS.com](http://www.USPS.com)
7. **Know who to call.** Write down the phone numbers for all of your accounts – if your wallet is stolen, you want to be able to call the companies and freeze the accounts.
8. **Secure your social security card.** Keep your social security card in a secure place. Keep it separate from your driver's license. Also, be careful of keeping anything that has your social security number on it separate from your driver's license information. Insurance cards, Medicare cards, and military ID's typically have your social security number emblazoned on them.
9. **Be vigilant at work.** Keep your wallet or purse in a safe place at work.

10. **Do they need your social security number?** You can tell them “no” when they ask for your social security number. Your employer and financial institution may need it, but the grocery store doesn’t. Don’t be afraid to ask:
- Why do you need it?
  - How will it be used?
  - How do you protect it from being stolen?
  - What will happen if I don’t give it to you?
11. **Protect your card numbers.** When entering your PIN at the ATM, cover the keypad so that no one else can see it. Watch the person behind you in line at the ATM or at the checkout line – some identity thieves use camera phones to photograph your credit card numbers. Cover your card number with your thumb to secure it.
12. **Don’t write the numbers on your card.** Never write the PIN on the card. Don’t pre-print your driver’s license number or social security number on your checks. I also write, “Check my identification” on the back of my credit cards. When I feel particularly whimsical, I write, “This card may be stolen – double check my ID” on the back.
13. **Know about spoof emails.** What is a spoof email? It appears to come from a trusted source (eBay, Citibank, PayPal, your bank, etc.) and tells you that there’s a problem with your account. They then direct you to a website that also trustworthy. The site will ask you to enter your account numbers, last transaction, or other personal information. Trusted institutions won’t do that – they already have your account information. If you think there may be an actual problem with your account, contact the institution directly by typing their web address in manually (rather than clicking on a link) or calling their primary number. If you receive a suspected spoof email, you can usually forward it to [spoof@\[YOURBANK.COM\]](mailto:spoof@[YOURBANK.COM]) so your bank can take appropriate action. Remember, email is not secure unless you encrypt it, so never send your account numbers or private information over email.
14. **Don’t enter unfamiliar contests.** They often ask for your social security number or other personal information. If they say you’ve won, check the group with your Better Business Bureau before sending them any personal information.
15. **Ask your bank about ID theft tools.** Citibank offers credit protector account – many other financial institutions offer similar protections. Some banks offer single use VISA numbers for transactions on the internet. Contact your bank and see what they offer.
16. **Check your account balances regularly.** You can check balances on the internet or over the phone. This way you can know very quickly whether unauthorized purchases were made on your account. And how many credit cards do you need to keep in your wallet? Keep a minimal number of cards and you’ll be able to check the balances more easily.
17. **If your bills don’t show up – call!** If your Visa bill didn’t arrive this month, call them to confirm where it was sent. Some identity thieves change their victim’s billing address to a post office box and then ask for a duplicate card to be sent there.

# WHAT TO DO IF YOU BECOME A VICTIM OF IDENTITY THEFT

**Report lost or stolen credit and ATM cards immediately.**

**File a police report.** The police may be reluctant to take a report. They may tell you that you're not even a victim, since it is usually the credit card company that suffers the loss. Be persistent and file a report anyway. Typing up an affidavit for the officer makes it easier for them to quickly file their reports. Chances of catching the thief are low, but you should still file a report. It's better to have a paper trail to show credit bureaus and financial institutions.

**Notify creditors of the dispute.** Call the credit reporting agencies to report and disputed items. Follow up in writing with a list of disputed accounts.

**Don't pay the disputed amount.** You will lose your rights to contest the disputed amounts if you pay them.

**Close the tampered accounts.** After your credit card company removes the disputed charges, you should request a new account number. Ask them to tell the credit bureaus that the account was closed due to fraud.

**Fill out an identity theft affidavit.** For a copy, visit <http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>

**Tell the FTC.** File a complaint with the Federal Trade Commission. [www.FTC.gov](http://www.FTC.gov)

**File a fraud alert with the consumer reporting companies and your credit card company.**

**Stolen checks.** If checks were stolen, issue a stop payment order on them. Renew the stop payment order every six months. (Some identity thieves wait for the stop payment order to expire, the cash the checks.)

**Social Security Fraud.** Call the Social Security Administration's Fraud Hotline: 800-269-0271

**Driver's license fraud.** Contact your state department of motor vehicles. Request a fraud alert be placed on your license. If stopped, you'll have to prove you are who you say you are. This may involve fingerprints and other aggravations, perhaps even a trip to the jail to sort out your identity.

**Hire an attorney.** If the thief committed a crime using your name, you should hire an attorney. This is the most difficult situation of all to deal with, and you'll want experienced help. Sometimes, that may mean hiring an attorney in another city or state, if the crime was committed outside of your home region. There may be an arrest warrant with your name on it for that crime – you want an expert to deal with the situation.

**Final note.** It's not my intention to scare you with this information, but to inform you so that you can protect yourself from theft. Once you are a victim of identity theft, it is very difficult to undo the damage. You know the old adage, "An ounce of prevention..." Stay safe, and call me if you have any concerns.

- Elliott →

CONTACT ELLIOTT WILCOX TO SPEAK TO YOUR BUSINESS OR ASSOCIATION  
[Elliott@ElliottWilcox.com](mailto:Elliott@ElliottWilcox.com) (407) 375-3833 [www.ElliottWilcox.com](http://www.ElliottWilcox.com)