

## Silence the Sales Pitches

## Protect Yourself Offline

The majority of credit-related crimes occur offline via purse snatchings, mailbox and trash digging, and phone calls from strangers requesting information that'll give them access to your dough.

As you make your way through this "to do" list, you'll become less vulnerable to offline credit crimes.

- Register your home and cell phone with the FTC's "Do Not Call" list:** Go online to [www.donotcall.gov/](http://www.donotcall.gov/) or call (888) 382-1222 (TTY (866) 290-4236). You must call from the number you wish to register. Registration is free.
- Stop the flow of pre-approved credit card offers** by calling (888) 5OPTOUT ((888) 567-8688). Or you can write to one of the credit reporting agencies (such as TransUnion Name Removal Option, P.O. Box 505, Woodlyn, PA 19094) and provide your first, middle, and last names (including Jr., Sr., III), current address, previous address (if you've moved in the last six months), Social Security number, date of birth, and signature. Your request will be shared with Experian, Equifax, and Innovis (the other major credit reporting agencies) and you will be removed from their mailing lists, too.
- Tell the Direct Marketing Association membership to stop calling and mailing you.** The catch is that only DMA members are required to check the association's database. To opt out of mailings, go to:  
[www.dmaconsumers.org/cgi/offmailinglist](http://www.dmaconsumers.org/cgi/offmailinglist)  
For phone calls, go to:  
[www.dmaconsumers.org/cgi/offtelephone](http://www.dmaconsumers.org/cgi/offtelephone)
- Offline Safety Tips** Here are other things you can do to thwart real-world thieves (as opposed to the virtual ones we'll show you how to avoid in the next section).
- Make your credit off-limits to intruders.** If you've been a victim of identity theft or credit fraud, you can place a fraud alert on your credit by contacting any one of the credit reporting agencies. (Contact information is contained on the *Credit Report Patrol Worksheet*.) If you are active duty military personnel serving away from your regular duty station, you can place "active duty" alerts to help prevent identity theft.
- Tell everyone else to buzz off, too.** To remove yourself from other mailing/calling list not covered by the above, you'll have to contact the offending companies directly and ask to be put on their internal cease-fire list (or "in-house suppress file"). Junkbusters.com offers sample opt-out letters on its website at [www.junkbusters.com/optout.html](http://www.junkbusters.com/optout.html).
- Xerox your wallet's contents.** Take a break at work and photocopy the contents of your wallet — front and back — and then keep a copy in a safe place at work and one at home. That way you have the vital information (customer service phone numbers, card numbers) if your wallet is stolen.
- Buy a shredder.** Tear or shred any documents that contain personal information. These include credit card receipts, insurance forms, physician and bank statements, credit card offers, and especially those blank "convenience checks" your lender sends.

**Silence the Sales Pitches**

- Don't answer financial information questions** unless you initiate contact. Don't give out personal information on the phone, through the mail, or online unless you initiate the contact or know the caller. Thieves will pose as bank representatives, Internet service providers, government agents, and ex-boyfriends to get you to reveal personal information.
- Note billing cycle dates** (e.g. second week of the month) for major bills like your mortgage, credit cards, and car loans. Notify the billing institution if an account statement is late. A missing bill may mean that some meanie called the company using your name and changed the billing address to prevent you from noticing their shopping spree.
- Consider having your address removed from the phone book.** In some instances a thief needs only your name, address, and phone number to commit fraud.
- Don't include too much information on your checks.** Next time you order checks, have only your name pre-printed on the check if possible. At the very least, leave off your Social Security and driver's license number as well as your phone number.

In general, practice vigilance with your own data. For example:

- Actually look at your credit card and bank account statements instead of just glancing over them quickly or passing them along to your spouse to pay. This is usually the first place unauthorized activity will show up.
- Deposit outgoing mail directly into post office boxes, not in your own mailbox. A shocking number of thieves troll mailboxes for your personal information. If you're

going on vacation, place a hold on your mail at the post office.

- If you're one of the few people who actually knows where your Social Security card is located, don't carry it with you! Stash it away in a safe place, and only carry a minimum number of ID and credit cards with you.
- Give out your Social Security number only when absolutely necessary. Ask to use other identifiers when possible.

Sadly, this is only a partial list of protective measures. If you're really paranoid, make the FTC's ID theft website's your home page: [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/) It's regularly updated with the latest scams.