



## Guarding Your Privacy in a Digital World

---

### **Social Security Number (SSN):**

Guard your Social Security number to the fullest extent possible! Your employer, bank, brokerage and anyone else who is required to report your income to the IRS has a legitimate need for your SSN. Beyond that, don't give it out; don't write the number on checks, credit cards or envelopes and resist disclosing it to merchants. In general, insist on knowing if your SSN's disclosure is "required" or merely "requested." Avoid using your SSN as a student ID and medical record number. Try not to carry your social security card in your wallet, because that is where many identity-theft cases begin.

### **Questionnaires, Polls and Consumer Surveys:**

Resist the temptation to complete shoppers' cards, consumer questionnaires and health surveys unless you can be assured that your information will not be shared or sold to third parties such as marketers or list brokers. When returning warranty cards, provide only information essential to the warranty service; ignore personal inquiries

used only for marketing purposes. When participating in marketing or public opinion polls, verify how your responses will be used and insist on assurances that no personal information can be traced back to you.

### **Credit Reports:**

Review your credit statements monthly to ensure that are accurate and are not being used fraudulently. In addition, obtain a copy of your credit report annually; fees charged by local credit bureaus and the big-three credit bureaus (Equifax of Atlanta, Trans Union of Chicago and Experian of Allen, Texas) should not exceed eight dollars. If you are rejected for credit, ask why. Then request a copy of your credit report; in this case the report should be provided free. Moreover, the federal Fair Credit Reporting Act requires credit bureaus to reinvestigate the facts if they are disputed.

### **Financial Information:**

Bank accounts, especially those with touch-tone or automated access, are vulnerable to snooping. Check your bank statements carefully each month. Choose a unique password or "PIN" number that is *not* your SSN or your mother's maiden name. Ask your bank to agree in writing to disclose personal financial records only to legally authorized requesters and to notify you when such requests are granted. Be cautious when banking and shopping with credit on interlinked networks in cyberspace.

### **Caller ID:**

Caller ID is a way to view a caller's telephone number and name before answering the phone. But if you, as a caller, want to skirt caller ID, dial \*67 (star-six-seven) before the seven-digit number; this will block the transmission of your name and phone number.

### **Unsolicited Advertising and Telemarketing:**

The Federal Communication Commission (FCC) regulates telemarketing and has a "Do Not Call Rule" which requires telemarketers to keep records of customers who demand to be added to the Do-Not-Call list and not be called again for ten years. (Unfortunately, FCC Do-Not-Call regulations do not apply to telephone survey companies!). If you receive unwanted telemarketing calls, announce firmly that you want your name added to the Do-Not-Call list.

Whenever possible, check "opt out" boxes provided for solicitation, warranty and subscription cards.

If you want to reduce the number of telephone solicitations you receive, send your name, address and phone number to the:

Direct Marketing Association Telephone  
Preference Service  
P.O. Box 9014  
Farmingdale, NY 11735-9014

The Association publishes a list of consumers who don't want to get solicitation calls.

If you wish to reduce unwanted *mail* solicitations, write the:

Direct Marketing Association Mail Preference  
Service  
P.O. Box 9008  
Farmingdale, NY 11735-9014

### **Electronic Mail:**

Be discrete when sending e-mail. Consider e-mail to be a post-card rather than a sealed letter, as electronic messages can be read at any stop along the way, from your Internet service provider to the addressee. That is why it is important to avoid sending account numbers, Social Security Numbers, passwords or other sensitive data via e-

mail. Don't forget that in most cases employers reserve the right to review employee's e-mail messages.

**Internet Privacy:**

Engage in commercial or credit transactions on the Internet with care. Be aware that there are authorized and unauthorized means of capturing personal information on the 'net. If you make purchases or engage in financial transactions on the Internet, make certain that they are encrypted. Check out your Internet service provider to ensure that the provider protects customer data, especially credit card numbers and personal information of interest to marketers.

**Medical Reports:**

In Wisconsin, patients are permitted to review their medical records; it is your right to review your medical records for accuracy. Whenever possible, insist on a unique number for your medical record or clinic number; resist having that number be your Social Security Number. When rejected for insurance, ask why. Then verify the accuracy of the data used in making the underwriting decision.

If you wish to receive a copy of a centralized medical file that may exist at the Medical Information Bureau, write the:

Medical Information Bureau  
160 University Avenue  
Westwood, MA 02090  
Or call 617-426-3660

The MIB is an agency used by more than 750 insurance companies to calculate financial risks for insurance underwriting. MIB databases contain summaries of health conditions for more than 12 million Americans. If (in consultation with your doctor) you detect errors in your

medical records, contact MIB and demand that the record be corrected.

**Social Security:**

Obtain a statement of your earnings from the Social Security Administration every two years. This will tell you if someone else is earning wages under your social security number, which can lead to many difficulties at retirement. To obtain your statement, complete a Request for Earnings and Benefit Estimate Statement Card (Form 7004) that may be ordered by telephone using the Social Security Administration's toll-free number: 800-772-1213.

**Identity Theft:**

Theft of identity is among the fastest-growing crimes in this country. With a few key pieces of information -- name, address, date of birth, mother's maiden name and Social Security Number -- criminals can unlock the door to various financial, credit and medical records. They can use this information to impersonate you, run up debts in your name, destroy your good credit and even stalk you. Guard these identifiers with great care.

**Passwords:**

Choose neutral and unique passwords for your account access. Don't use your Social Security Number, mother's maiden name or numerical date of birth, because these identifiers are widely used.

**Opt Out:**

Whenever given the chance, opt out of having your personal information disclosed or used for secondary purposes. Whether subscribing to a magazine, making a catalog purchase, seeking pre-approval for credit card offerings or joining an altruistic organization, take the time to ensure that your name and address will not be shared,

reused or sold to third parties without your permission.

**To opt out of phone solicitations from four major credit agencies**, call 1-888-5OPTOUT (1-888-567-8688), prompt #3. This routes you to the operator to remove you permanently from the agencies Experience, Equifax, Enovis, and Trans Union.

**(Note:** By opting out of credit bureau releases, your credit application may be affected in ways that you did not intend.)

*For More Information visit [www.aclu-wi.org](http://www.aclu-wi.org)*

*ACLU of Wisconsin  
207 E. Buffalo Street, Suite 325  
Milwaukee, WI 53202  
Phone: 414.272.4032*