



purchased, the company only needs the purchase date, model and serial numbers, and how you can be contacted if there is a product recall. Ignore unrelated questions, like those about income or hobbies.

**11. LOCK IT UP.** Protect your information by keeping it in a secure place at home and at work. Don't carry your Social Security card in your wallet or write the number on checks. Similarly protect your PIN and other personal numbers. For example, don't write your PIN on a slip of paper that can be lost or stolen. Shield the keypad from view by others when using ATMs and phones.

**12. TELL YOUR BANK NOT TO SHARE YOUR INFORMATION.** Assert your rights by opting out of information sharing under the *Financial Services Modernization Act* and the *Fair Credit Reporting Act* by calling or writing your financial institution (e.g., bank, insurance company, brokerage firm) and instructing it that: • **It does not have your permission to sell or share** your *personally identifiable information* with non-affiliated third parties (Financial Services Modernization Act) *or* to share information about your *creditworthiness* with any affiliate of the company (Fair Credit Reporting Act). • **Tell the bank you do not want to receive marketing offers** from the company or its affiliates. Although a financial institution is not required by law to do so, you can request that it not disclose *any information about you*, including transaction and experience information, to its affiliates or in connection with direct marketing agreements between it and another company.

**13. SIMPLIFY YOUR BANK CHECKS.** Remove any "extra" information from your checks, such as your Social Security number, drivers license number, middle name and telephone number. Pick up your checks at the bank instead of having them sent to your home address.

**14. SECURE YOUR MAIL DELIVERIES.** To reduce mail theft install a locked mailbox at your residence or use a post office box. Remember to collect mail promptly. Ask your

post office to put your mail on hold when you are away from home for more than a couple of days. Pay attention to your billing cycles; if bills or financial statements are late, contact the business.

**15. SCREEN YOUR PHONE CALLS BEFORE ANSWERING.** Most modern phones can automatically identify callers or incoming phone numbers before you answer a call. For a fee, you can also subscribe to a "call intercept" service. Calls that appear on your caller ID screen as "anonymous" or "private" are intercepted and diverted to a message that tells the caller you don't accept unidentified calls. Once the caller identifies himself, the phone rings and you have the option to answer or reject the call.

**16. DISCONNECT FROM THE TELEPHONE BOOK.** "Unlist" your name, address and number by removing your information from public information databases such as telephone books, reverse directories, and city directories. Doing so can reduce access to your personal information on the Internet and by telemarketers and identity thieves that mine data from public databases. Fees may apply.

- *To block your address or to remove your information from the phone book and directory assistance call your service provider:* Frontier Communications at 1-800-921-8101 or Verizon at 304-954-6200
- *To remove your information from a city directory contact:* R.L. Polk Company, 37001 Industrial Rd., Livonia, MI 48150; 1-800-275-7655

**17. DON'T RESPOND TO UNSOLICITED REQUESTS** for personal information in the mail, over the phone, or online. Know the tricks that ID thieves use, such as pretending you've won a contest.

**18. TALK ABOUT PRIVACY IN YOUR HOME.** Everyone, *especially children*, should understand what information is and is not appropriate to share on the phone, using a computer, and in other situations where your privacy could be compromised. ♦

*This information presented by*  
**Darrell V. McGraw, Jr.**  
**West Virginia Attorney General**

**CONSUMER PROTECTION HOTLINE**

1-800-368-8808

[WWW.WVAGO.GOV](http://WWW.WVAGO.GOV)

*Follow us on* **FACEBOOK** *and* **TWITTER**



FROM THE OFFICE OF  
**DARRELL McGRAW**  
WEST VIRGINIA ATTORNEY GENERAL



# 18 THINGS YOU CAN DO TO PROTECT YOUR PRIVACY

**The convenient ways** that modern technology manages the data of our everyday lives can have dangerous side effects, including loss of privacy and the potential for identity theft.

**Every time you** fill out an application, get a credit card or loan approved, renew a driver's license, get your prescriptions filled at the local pharmacy, or transfer funds between accounts – you are giving out personal information that can be changed, reported inaccurately, or stolen.

**Some companies and industry groups** have adopted voluntary policies that address privacy and confidentiality concerns. **But staying vigilant is the best way to keep your information safe.**

# 18 THINGS YOU CAN DO TO PROTECT YOUR PRIVACY

**1. CHECK YOUR CREDIT REPORT.** Obtain a copy of your credit report each year to ensure it is accurate and to see what companies have requested information about you. Check your report more frequently if you suspect someone has gained access to your accounts. The *Fact ACT of 2003* allows everyone to receive a *free* credit report from each of the three credit reporting agencies once every year.

**BY PHONE:** 1-877-322-8228

**ONLINE:** [www.annualcreditreport.com](http://www.annualcreditreport.com)

**BY MAIL:** Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30374-5281

If you find inaccurate information in your credit report, dispute it in writing to the credit reporting bureaus.

**2. OPT OUT OF CREDIT CARD OFFERS.** Stop prescreened credit card offers by calling **1-888-5OPTOUT** (1-888-567-8688) or writing to Equifax, Experian, and TransUnion.

**3. STOP JUNK MAIL.** Instruct major mailing list companies to remove your name from their databases. Write each one and include your complete name, name variations (*e.g.*, Jane Doe, J.C. Doe, Mrs. John Doe) and mailing address at:

**DMA Choice**, Mail Preference Service, PO Box 643, Carmel, NY 10512

**R.L. Polk & Co.**, List Compilation, 26955 Northwestern Hwy., South Field, MI 48034

**First Data Info-Source Donnelley Marketing, Inc.**, Data Base Operations, 1235 N Ave., Nevada, IA 50201

**Metromail Corp.**, List Maintenance, 901 West Bond, Lincoln, NE 68521

**4. STOP TELEMARKETING CALLS.** Sign up for the federal government's **National Do Not Call Registry** by calling **1-888-382-1222** from the phone you want to register or register online at [www.donotcall.gov](http://www.donotcall.gov). Telephone numbers remain on the registry until they are disconnected or reassigned. Placing your number on this list will stop most telemarketing calls but will not prevent calls from political organizations or charities.

Also instruct the **Telephone Preference Service** to remove you from its lists. Write to them, providing your complete name, address, and telephone number with area code at:

**Telephone Preference Service**, Direct Marketing Association, PO Box 1559, Carmel, NY 10512

**5. TELL BUSINESSES NOT TO SHARE YOUR INFORMATION.** Look for a company's privacy statements on its websites, sales materials, and application forms. Don't assume companies will automatically keep your personal information confidential. Ask what information they collect, how it will be used, and whether they will sell or share it.

**6. SECURITY FREEZE.** Consider placing a security freeze on your credit report. For details, go to [www.wvago.gov](http://www.wvago.gov) or call the WV Attorney General's Office at 1-800-368-8808.

**7. BE SMART WHEN YOU USE COMPUTERS.** Do not send sensitive information over the Internet unless it is absolutely necessary to do so and then only through a familiar, *secure* connection with "https" in its web address, a notice that you are on a secure site, or a closed lock or unbroken key at the bottom of your screen. A secure website encrypts personal information so that it cannot be easily intercepted. • **Beware: Scammers set up fake sites that look authentic.** • **Think twice before posting information on social media networks** like Facebook or Twitter. For example, your year of birth can help identity thieves figure out your Social Security number. • **Avoid unsecure and public wi-fi connections** and beware of identity spies trying to catch a glimpse of your screen.

• **Don't provide your credit card number** or other personal information (*ex.*: proof of age) to access or subscribe to a website run by a company with which you are not acquainted. • **Be suspicious of email offers, contests, awards, requests, and other unsolicited messages, even when they appear to be from a familiar source.** They could be "phishing" emails designed to bait you into disclosing personal information • **Protect your passwords.** Memorize the codes and don't share with others. • **Instruct your children to never give out their real name and address on the Internet or agree to meet anyone they communicate with over the Internet without your knowledge and**

## CREDIT REPORTING AGENCIES

**Equifax Credit Information Services**  
P.O. Box 740241, Atlanta, GA 30374  
1-800-685-1111 [www.equifax.com](http://www.equifax.com)

**Experian National Consumer Assistance Center**  
P.O. Box 949, Allen, TX 75013  
1-888-397-3742 [www.experian.com](http://www.experian.com)

**TransUnion Consumer Relations**  
P.O. Box 1000, Chester, PA 19022  
1-800-916-8800 [www.tuc.com](http://www.tuc.com)



permission. • **Use virus-detection and anti-spyware software and install firewalls** on your computer to help deter dangerous malware programs and sketchy websites that can record your keystrokes, phish for personal data, or collect information about your activity on the Internet.

• **Stop spam.** Remove your email address from mailing lists by clicking on the eMPS link at [www.dmachoice.org](http://www.dmachoice.org).

• **Disable pop-ups in your web browser.** Many browsers, including Internet Explorer and Firefox, allow you to block pop-up advertisements in their options settings. • **Backup important files.** Make a secure copy of important private information on another computer or removable storage drive. • **Wipe or destroy old hard drives.** Remove all of your information from hard drives by demagnetizing, using special software, or otherwise wiping the hard drive clean before donating, selling or dumping a used computer – even if the computer or hard drive "doesn't work."

**8. SHRED IT.** Tear up or shred receipts, credit card offers, account statements, expired credit cards, and other documents with personal data before disposing of them.

**9. PAY WITH CASH.** Every purchase with a credit card creates information in business databases. Remember, however, that paying with a credit card gives you some rights to dispute charges that aren't available if you pay cash. Ask for any carbons and incorrect or extra charge slips created in your transaction.

**10. BE SELECTIVE ABOUT WHAT INFORMATION YOU PROVIDE WHEN YOU BUY.** Unless merchandise is being shipped to you, sellers generally don't need information such as your address or telephone number. If they ask for it, find out why. Know your seller. • **You can cut down on the information supermarkets and other stores have about you** by not using "frequent shopper" or "savings club" cards. • **When registering for a warranty on an item you have** →