

Ten Timely Tips for Holiday Shopping *Courtesy of the Privacy Rights Clearinghouse*

Follow these tips to help avoid scams and rip-offs this holiday season. Be a privacy-smart consumer!

1. **Don't Debit.** Don't use a debit or check card to pay for your purchases. These cards typically put consumers at much greater risk than credit cards because they offer fewer consumer protections in the event of a loss. Because these cards access funds directly from your bank account, your money may remain missing while you and your bank sort out any theft, which could mean bounced checks, late fees, and numerous other problems. Your checking account (and related savings accounts) could be wiped out in minutes. Some crooks use "skimming" devices to steal your card information from merchant card-swipe machines. Debit or check cards pose a much greater risk to consumers in the event that a card is "skimmed."

2. **Many Unhappy Returns.** Be aware of a store's return policy. Some retailers require a state-issued ID or license when you return or exchange merchandise. Typically, stores swipe the shopper's driver's license when a return is being made and if the store's return limit is exceeded, the return is denied. Retailers do this to keep better track of possible return fraud. Some retailers maintain their own database while others use a third-party service. A number of national merchants outsource the collection of return and exchange data. If you make repeated returns or exchanges to a participating merchant, subsequent returns to that merchant's stores may be refused.

3. **No You Can't See It.** You are in a store paying for your purchase with your credit card. The cashier asks to see your driver's license. Do you have to show it? Probably not! Merchants may ask a customer for identification, but in most situations, a merchant may not condition acceptance of a Visa or MasterCard credit card upon the customer presenting identification. In other words, you can refuse to provide identification, and the merchant still must accept your credit card.

4. **The Gift that Keeps on Taking.** If you decide to purchase a gift card, be aware of expiration dates, fees, and what will happen if the card is lost.

5. **Truncation is Not a Dirty Word.** Make sure that the credit card receipts that you receive from merchants do not contain your full account number. Under federal law, all electronically printed credit and debit card receipts must shorten (truncate) the account information to no more than the last five digits of the card number. The receipt must also not include the card's expiration date.

6. **Check This Out.** Some states have laws that dictate what kind of information merchants cannot ask for or write down when a consumer pays with a check or credit card. For example, in California, when a consumer pays with a credit card, the merchant cannot record any personal information other than what is on the front of the credit card. When a consumer pays by check, the merchant cannot record the credit card number.

7. **Keep it Clean.** Clean out your wallet, purse, or pocketbook. Remove unnecessary credit cards, debit cards, your Social Security card, and other unneeded documents that could compromise your identity if lost or stolen while shopping. Keep them locked up in a safe place. Pickpockets will be out in force during the holiday season. The more you carry with you, the more difficult and time-consuming it will be to report and recover from your loss.

8. **Be Alert, Be Aware.** Don't forget to take simple precautions to protect your personal safety. Men can carry their wallets in a front pocket, which is less susceptible to pickpocketing. Women can place their purse strap over their head and across their chest. When shopping at night, park in a well-lit area. Be careful getting into and out of your car at the shopping mall -- people are sometimes targeted by muggers when doing so.

9. **Be Safe Online.** When shopping online, make sure that the Web site uses encryption technology before you provide your personal information. Encryption scrambles the information you send, such as your credit card number, in order to prevent computer hackers from obtaining it en route. You can tell when you are on a secure web page several ways. If you look at the top of your screen in the address bar where the Web site address is displayed, you should see <https://>. The "s" that is displayed after "http" indicates that web site is secure. You may not see the "s" until you are actually on the order page on the Web site. Another way to determine if a Web page is secure is to look for a closed padlock displayed at the bottom of your screen. If that lock is open, you should assume it is not a secure site.

10. **Seals of Approval.** Be sure to check out a Web site's privacy policy before providing any personal information online. You can also learn what type of information is gathered by the Web site, and how it is -- or is not -- shared with others by reading its privacy policy. A link to the privacy policy is often found at the bottom of the site's home page.