

## Preventing Scams

- **Resist sympathy lines** (a stranger saying her purse was stolen & could you give her a ride to your bank or some money.) If someone's purse is stolen, contact the police department.
- **Anyone having a driver's license, social security or credit card stolen should make a police report immediately.**
- **Never be pressured into withdrawing large amounts of money.**
- **Always read a document before you sign it.** If you don't understand it, get it into the hands of a trusted person who can help you. Don't be pressured into signing anything.
- **Never lend your identification, credit cards or ATM card to anyone.**
- **Do research before you invest your money.** Make certain you are dealing with an established, reliable investment firm.
- **Check the reliability of people you are dealing with;** ask for references and contact them.
- **Keep blank checks in a safe place and don't sign until you are ready to use.**
- **Don't leave money or valuables in plain view.**
- **Know your rights with door-to-door sales.** Under the law, you may cancel a door-to-door sale within three business days of the sale by notifying the seller in writing.
- **Beware of verbal promises.** Remember that oral promises are not usually binding if a written signed contract does not agree.



## You've been scammed! Now what?

If you think your identity has been stolen, take these steps:

1. **Contact the fraud department** of any one of the three major credit bureaus to place a fraud alert on your credit file. Their contact info is:
  - **Equifax** 1-800-525-6285  
website: [equifax.com](http://equifax.com)
  - **Experian** 1-888-397-3742  
website: [experian.com](http://experian.com)
  - **TransUnion** 1-800-680-7289  
website: [tuc.com](http://tuc.com)
2. **Close the accounts** that you know or believe have been tampered with or opened fraudulently.
3. **File a police report** and get a copy of the report to submit to your creditors and others that may require proof of the crime.



## Protecting Your Money & Identity: Tips for Seniors

Developed by  
Council on Aging of  
Greater Nashville

*with funding from*  
The Exchange Club Charities



95 White Bridge Road  
Suite 114  
Nashville, TN 37205

Phone: 615-353-4235  
Fax: 615-353-4235  
E-mail: [info@coamidtn.org](mailto:info@coamidtn.org)  
Web: [www.coamidtn.org](http://www.coamidtn.org)

## Telephone Sales Pitches: Legitimate or Fraud?

It's sometimes hard to tell if a sales pitch is real or not. You can't judge by the tone of someone's voice or how friendly or sincere the person *seems*. It's probably a scam if:

- **The caller informs you that you've won a prize, but you must pay for processing or administrative fees, customs or taxes.**

*Legitimate sweepstakes or prize offers don't ask for payment because it's illegal to do so.*

- **The caller says you have to take the offer immediately or you'll miss the opportunity.**

*Legitimate companies don't pressure people to act without time to look into the deal.*

- **The caller refuses to send you written information before you commit to anything.** *Legitimate companies are always glad to send information about what they are offering.*
- **The caller claims that you can make huge profits in an investment with no risk.** *All investments are risky; legitimate companies must relay possible risks involved.*
- **The caller asks for a donation but won't say how the money will be used and/or what the charity does.** *Legitimate charities are willing to say what percentage of contributions is used for services and how much goes to overhead and fundraising.*
- **The caller asks for cash.** *Legitimate companies don't demand cash, but con artists do since they want to be hard to trace.*
- **The caller asks for your social security number.** *Unless you contacted them, legitimate companies NEVER ask for this.*



- **The caller asks for your credit card or bank account number when you aren't buying anything or paying with those accounts.** *Legitimate companies only ask for the information to bill you or debit your account for purchases you've agreed to make.*
- **The company offers to get you a loan or credit card or to "repair" your bad credit if you pay an up-front fee.** *Legitimate companies do not demand payment in advance; no one can get bad information removed from a credit file if it is accurate.*

## Helpful Numbers

TN Dept. of Commerce & Insurance  
1-800-342-8385

For complaints about unfair trade practices, deception, fraud, or illegal practices.

Legal Aid Society  
1-800-238-1443

Free legal assistance by lawyers and paralegals.

Middle TN Better Business Bureau  
1-800-989-4222

Information on companies to determine reliability of business, complaint assistance, fraud seminars, and charity evaluations.

### Monthly Scam Alerts

Be in the know about current scams. Sign up for the Council on Aging's monthly email Scam Alert. To begin receiving this information, simply send an email to: [scams@coamidtn.org](mailto:scams@coamidtn.org).

National "Do Not Call" Registry  
1-888-382-1222

Dial from the number you want to register on the Do Not Call registry, or visit the website at [www.donotcall.gov](http://www.donotcall.gov).



## Protecting Your Identity

Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information without your permission.

To prevent identity theft:

- **Destroy receipts** that contain your credit card or bank account numbers.
- **Destroy credit card offers** with your bank account or Social Security number.
- **Don't carry your Social Security card** with you.
- **Never give anyone your Social Security number or credit card number over the phone—** unless you initiated the call.
- **Trust your instincts—**If you receive a piece of mail with an offer that sounds too good to be true, it probably is a scam designed to take money or personal information from you. Ignore it.
- **Do not give out any financial or personal information through email.** If you get an email message asking for this information, do not reply or click on the link in the message. This is called "phishing" and is an attempt to scam you.
- **Order a copy of your credit report to insure no accounts have been opened that you did not authorize.** Everyone is entitled by law to a FREE copy of their report once each year.
- **Check your bank statements carefully** for unauthorized transactions.
- **Cancel your ATM card if you don't use it.**
- **Don't endorse a check until you are in the bank.**
- **Use direct deposit,** especially for your social security check.

