

# PROTECT YOUR IDENTITY

## IDENTITY THEFT NEWSLETTER

Don't become a victim.

JANUARY 2008 / VOL. 2

# TAKE CHARGE

## AVOID IMPERSONATION/ IDENTITY FRAUD

Impersonation fraud occurs when someone assumes your identity to perform a fraud or other criminal act. Criminals can get the information they need to assume your identity from a variety of sources, such as the theft of your wallet, sifting through your trash, or from credit or bank information. They may approach you in person, by telephone or on the internet and ask you for the information.

### ***Some Tips to Avoid Impersonation/Identity Fraud:***

- Never throw away ATM receipts, credit statements, credit cards, or bank statements in a usable form.
- Never give your credit card number over the telephone unless you make the call.
- Reconcile your bank account monthly and notify your bank of discrepancies immediately.
- Keep a list of telephone numbers to call to report the loss or theft of your wallet, credit cards, etc.
- Report unauthorized financial transactions to your bank, credit card company, and the police as soon as you detect them.
- Review a copy of your credit report at least once each year. Notify the credit bureau in writing of any questionable entries and follow through until they are explained or removed.
- If your identity has been assumed, ask the credit bureau to print a statement to that effect in your credit report.
- If you know of anyone who received mail from credit card companies or banks in the names of others, report it to local or federal law enforcement authorities.

## WHERE'S MY REFUND?



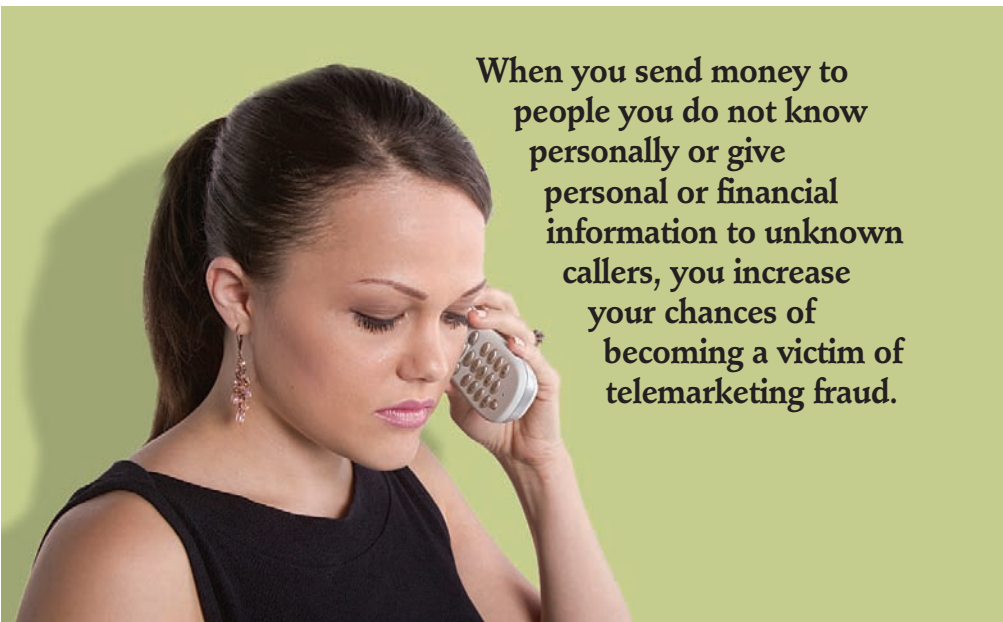
Another recent e-mail scam tells taxpayers that the IRS has calculated their "fiscal activity" and that they are eligible to receive a tax refund of a certain amount. Taxpayers receive a page of, or are sent to, a Web site (titled "Get Your Tax Refund!") that copies the appearance of the genuine "Where's My Refund?" interactive page on the genuine IRS Web site. Like the real "Where's My Refund?" page, taxpayers are asked to enter their SSNs and filing status. However, the phony Web page asks taxpayers to enter their credit card account numbers instead of the exact amount of refund as shown on their tax return, as the real "Where's My Refund?" page does. Moreover, the IRS does not send e-mails to taxpayers to advise them of refunds or to request financial information.

Recipients of questionable e-mails claiming to come from the IRS should not open any attachments or click on any links contained in the e-mails. Instead they should forward the e-mails to [phishing@irs.gov](mailto:phishing@irs.gov).

If you want to see some of the other scams involving the IRS you can go to <http://www.irs.gov>. In the center of the home page is a link to the current scams.

**HOW TO OBTAIN A FREE CREDIT REPORT:**  
[www.annualcreditreport.com](http://www.annualcreditreport.com) (877) 322-8228

# TELEMARKETING FRAUD



**When you send money to people you do not know personally or give personal or financial information to unknown callers, you increase your chances of becoming a victim of telemarketing fraud.**

## **SOME TIPS to Avoid Telemarketing Fraud:**

- Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.
- Always ask for and wait until you receive written material about any offer or charity. If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But, unfortunately, beware -- not everything written down is true.
- Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state Attorney General, the National Fraud Information Center, or other watchdog groups. Unfortunately, not all bad businesses can be identified through these organizations.
- Obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out



false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.

- You must not be asked to pay in advance for services. Pay services only after they are delivered.
  - Some con artists will send a messenger to your home to pick up money, claiming it is part of their service to you. In reality, they are taking your money without leaving any trace of who they are or where they can be reached.
    - Always take your time making a decision. Legitimate companies won't pressure you to make a snap decision.
    - Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
- Never respond to an offer you don't understand thoroughly.
- Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.
- If you have information about a fraud report it to state, local, or federal law enforcement agencies.

## **WARNING SIGNS - What a caller may tell you:**

- "You must act 'now' or the offer won't be good."
- "You've won a 'free' gift, vacation, or prize." But you have to pay for "postage and handling" or other charges.
- "You must send money, give a credit card or bank account number, or have a check picked up by courier." You may hear this before you have had a chance to consider the offer carefully.
- "You don't need to check out the company with anyone." The callers say you do not need to speak to anyone..
- "You don't need any written information about their company or their references."
- "You can't afford to miss this 'high-profit, no-risk' offer."

## **JURY DUTY SCAM**

**ALERT!**

Most of us take summons for jury duty seriously, but enough people skip out on their civic duty, that a new and ominous kind of scam has surfaced. The caller claims to be a jury coordinator. If you protest that you never received a summons for jury duty, the scammer asks you for your Social Security number and date of birth so he or she can verify the information and cancel the arrest warrant.

Give out any of this information and bingo - your identity just got stolen.

The FBI and the federal court system have issued nationwide alerts on their web sites, warning consumers about the fraud.

*brought to you by*



**ChelseaGroton**  
Feel good about your bank.™

448-4100 • 823-4800 • 599-2406

Member  
FDIC

[chelseagroton.com](http://chelseagroton.com)

