

Identity Theft and Telemarketing Fraud

Your personal information is valuable. Protect it! Guard your:

Social Security number
Bank and credit card numbers
Driver's license number

Some criminals lie on the telephone to get your personal information. They may lie about who they are, claiming that they're from a legitimate company and that you have a problem with your account.

Or they may pose as representatives of a bank or government agency and ask you to confirm your billing information.

Once they have your personal information, they can use it to commit identity theft charging your existing credit cards, opening new credit card, checking, or savings accounts, writing fraudulent checks, or taking out loans in your name.

<http://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure>

What can I do to protect myself from phone fraud?

Register for the National DNC Program by calling toll free: 1-888-382-1222

You can limit the number of legitimate telemarketing calls you receive at your residence by registering your home phone number on the LPSC DNC Program and/or National DNC Program. Putting your number on these programs will stop most normal telemarketing calls - but not all. You still may get calls from businesses with which you normally do business, and a few other possible exemptions, but calls from sales people from unfamiliar businesses may be the sign of a scam. Because both of the DNC programs are working very well to keep legitimate telemarketers in compliance with their laws, registration does effectively reduce the total number of calls that you receive, making it easier for you to spot those that may be calling vishing, or for any other criminal purpose.

What is Vishing?

The Federal Bureau of Investigation describes Vishing as a new form of a phishing scam, or using technology to hijack identities and steal money. One of the latest breakthroughs in telecommunications-Voice Over Internet Protocol, or VoIP, enables telephone calls over the web, and unfortunately makes it that much easier for criminals to contact consumers. VoIP service is fairly inexpensive, especially for long distance, making it easy to make fake calls, and use technology to avoid costs and disguise identities. The intention is to provide the consumer with a false sense of security that will encourage the consumer to release personal information.

(http://www.fbi.gov/news/stories/2007/february/vishing_022307)

If I get the caller ID information it should be able to track them, right?

Wrong. Unfortunately, the technology is readily available for criminals to mask the numbers they are calling from, thwarting enforcement efforts to identify them. Remember, the good guys have to go through every LEGAL means to catch these criminals, the crooks go through every means available to evade detection. That's why it is important that you understand that educating yourself, and your friends and family, to the dangers of identify theft is your best protection against this type of crime. Do Not Call was never designed to stop fraud, but we can help you get your complaint to the appropriate authority.

What should I do if I suspect fraud?

First, if it is someone representing themselves as someone authorized by a company you do business with, and they want personal information, take their name and contact the company yourself before releasing any information. Do not accept a "call back" number from the representative, call the company yourself and ask to speak to the employee or someone in management. Don't ever be frightened into revealing personal information. Business are well aware of the problem of identity theft and will support your request if their activity is legitimate.

However, if you get a call and a recorded message offers you a product or service and asks you to "Press 1" if you are interested or another number to be placed on their Do Not Call rolls, we believe, at this time, that the bulk of these types of calls to be related to identity theft attempts or vishing scams. We recommend that you simply **hang up the phone without pressing either button**. You may report this call to the Federal Trade Commission by **visiting www.ftc.gov or calling toll-free, 1-877-FTC-HELP (1-877-382-4357)**.

Recognize Phone Fraud

File a Complaint Regarding Phone Fraud

The Federal Trade Commission (FTC) works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357).

The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad. Check out the FTC website for more information about your rights under the FTC's Telemarketing Sales Rule and ways to protect yourself from abusive and deceptive telephone sales practices.

<http://www.consumer.ftc.gov/articles/0341-file-complaint-ftc>

Anyone with a phone can be victimized by telemarketing scam artists. That's why every "sales" call you get by phone is an opportunity for a gut check: Ask yourself these questions - and if the answers give you some doubt about the caller's intentions or methods, end the call.

When you get what appears to be a telemarketing sales call, ask yourself some questions:

Who's calling - and why? Telemarketers must tell you it's a sales call, the name of the seller and what they're selling before they make their pitch. If they don't give you the required information, say "no thanks," and get off the phone.

What's their hurry? Fast talkers who use high pressure tactics could be hiding something. Take your time. Most legitimate businesses will give you time and written information about an offer before asking you to commit to a purchase.

If it's free, why are they asking me to pay? Question charges you need to pay to redeem a prize or gift. Free is free. If you have to pay, it's a purchase - not a prize or a gift.

Why am I "confirming" my account information - or giving it out at all? Some callers have your billing information before they call you. They're trying to get you to say "okay" so they can claim you approved the charge.

<http://www.ftc.gov/video-library/index.php/for-consumers/privacy-and-identity/hang-up-on-phone-fraud/1402334886001>

Could you be the Victim of Phone Fraud?

"Auto Warranty"
"prize winner"
"Online Pharmacy"
"Lower your interest rates"
"Free Cell phone"
"Health benefits"
"Burial insurance"
"Diabetic Supplies"



LPSC Do Not Call

Louisiana Public Service Commission
1-877-676-0773
www.lpsc.org