ALERT: Ensure you know who is calling!

"Spoofing" occurs when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Spoofing is often used as part of an attempt to trick someone into giving away valuable personal information so it can be used in fraudulent activity or sold illegally. U.S. law and FCC rules prohibit most types of spoofing.

How does spoofing work?

Caller ID lets consumers avoid unwanted phone calls by displaying caller names and phone numbers, but the caller ID feature is sometimes manipulated by spoofers who masquerade as representatives of banks, creditors, insurance companies, or even the government.

What you can do if you think you're being spoofed

You may not be able to tell right away if an incoming call is spoofed. Be careful about responding to any request for personal identifying information.

- Never give out personal information such as account numbers, Social Security numbers, mother's maiden names, passwords or other identifying information in response to unexpected calls or if you are at all suspicious.
- If you get an inquiry from someone who says they represent a company or a government agency seeking personal information, hang up and call the phone number on your account statement, in the phone book or on the company's or government agency's website to verify the authenticity of the request.
- Use caution if you are being pressured for information immediately.