Calls from Your Own Phone Number- How is it Possible?

From the Office of Minnesota Attorney General Lori Swanson

"Shelly" and her family sat down to dinner when the phone rang. Before she answered the call, Shelly looked at the caller ID and saw her own name and phone number! She answered the call and heard a recording that offered to lower her credit card interest rate. Shelly hung up and reported the call to her phone company.

Scam artists now use technology to make a person's caller ID show their own name and phone number—making it appear as though a person is calling him or herself. These scam artists are falsifying—or "spoofing"—caller ID information. Spoofing scams are often perpetrated by criminal gangs located outside the state or country attempting to mask their identity and evade law enforcement.

Under the Federal Truth in Caller ID Act of 2009, using caller ID spoofing to defraud someone is a crime. Scam artists who use spoofing technology perpetrate so-called card services scams, medical alert device scams, and a number of other scams. These scams are usually designed to steal money or personal information, so it is very important to be wary of calls that appear to come from your own name and phone number. You should never provide your personal or financial information to unknown callers. Theft of personal and financial information is a crime and should be reported to local authorities.

It is generally a good idea *not* to answer a phone call that appears to be from your own phone number. There is typically no legitimate reason for a person to receive such a call, and by answering, the scam artist is notified that your number is active, often leading to more scam calls. Unfortunately, scammers who use caller ID spoofing to steal money or personal information ignore established means of stopping unwanted calls, such as the National Do Not Call Registry, and are not dissuaded from calling by the fact that a person's number is on the no-call list.

If you receive a call that appears to come from your own name and telephone number, you should take the following steps:

1. Report the call to your **phone company**, which may be able to offer calling features that block unwanted calls.

2. Report the call to the **Federal Trade Commission** ("FTC") and the **Federal Communications Commission** ("FCC"). These agencies have the authority to enforce federal laws that regulate caller ID spoofing, as well as autodialed and prerecorded message calls. The FCC can also impose fines on individuals and entities that violate those laws. You may contact these agencies as follows:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue Northwest
Washington, DC 20580|
Toll-free: 1-877-382-4357
www.ftccomplaintassistant.gov

Federal Communications Commission
Consumer & Governmental Affairs Bureau
Consumer Inquiries and Complaints Division
445 12th Street Southwest
Washington, DC 20554
Toll-free: 1-888-225-5322
www.fcc.gov/complaints

3. Report the call to the Minnesota Public Utilities Commission ("MPUC"), which has authority over local telephone services like caller ID. The Minnesota Attorney General's Office previously asked the MPUC to require phone companies that sell caller ID technology to the public to take action to stop spoofed calls, but the MPUC declined to do so. It is very important that the MPUC hear from citizens affected by caller ID spoofing. You may contact the MPUC as follows:

   Minnesota Public Utilities Commission
   121 7th Place East, Suite 350
   St. Paul, MN 55101
   (651) 296-0406
   Toll-free: 1-800-657-3782
   www.mn.gov/puc

4. If you lost money to a criminal scam, report the matter to your **local police or county sheriff or the FBI.** These agencies have the authority to investigate and prosecute criminal matters.