

Consumer Complaints:

Online: https://consumercomplaints.fcc.gov

Phone: (888) 225-5322 TTY: (888) 835-5322

Videophone: 1-844-432-2275

Media Contact:

Will Wiquist, (202) 418-0509 will.wiquist@fcc.gov

For Immediate Release

CONSUMER ALERT: PROTECT YOURSELF AGAINST 'NEIGHBOR SPOOFING', SCAM CALLERS PLACING PHONE CALLS THAT APPEAR TO BE LOCAL

Caller ID Information Can Be Manipulated to Fool and Defraud Consumers

WASHINGTON, March 8, 2018—The Federal Communications Commission is warning consumers about "neighbor spoofing" scams where thieves manipulate caller ID information in ways that make calls appear to have been placed locally. While a call might originate overseas, the caller ID information on the recipient's phone would appear as though the call is coming from the consumer's own area code and local exchange. In general, scammers use such spoofing to increase the likelihood that consumers pick up the phone and to increase the consumer's trust in the call.

Consumer Tips

- Be Aware: Caller ID showing a "local" number no longer means it is necessarily a local caller.
- Don't answer calls from unknown numbers.
- Don't provide any personal information to callers.
- Review call blocking <u>tools</u> provided by your phone company or 3rd party app developers.
- File a complaint with the FCC.

FCC Chairman Ajit Pai also outlines tips for consumers in this recent video: https://www.youtube.com/embed/j8m-NDEWiBQ?rel=0

The FCC is confronting the problem of illegal robocalls and malicious spoofing through strong enforcement and policy changes. In 2017 alone, the Commission proposed over \$200 million in fines against telemarketers who apparently used malicious spoofing to try and sell time-shares and insurance. These enforcement actions were the first of their kind and were built in large part as a result of complaints from the public filed at https://consumercomplaints.fcc.gov

The FCC is also working on various policy changes to help unmask and to block scam callers. The agency recently adopted <u>new rules</u> allowing phone companies to proactively block calls that are likely to be fraudulent, like purporting to be from area codes that do not exist. The FCC also <u>began</u> exploring ways to set up a reliable system to verify that a phone call is really coming from the phone number that it claims to be. The agency began seeking public comment on standards to help differentiate legitimate phone calls from those that attempt to trick consumers through caller ID spoofing. A reliable

authentication system would help confront this behavior and strengthen call-blocking and enforcement actions.

Today's technology also allows scammers to more easily and cheaply spoof telephone numbers, manipulating the caller ID information so that they appear to be calling from your local area. Although spoofing technology has legitimate uses, it is often abused by scammers. The Truth in Caller ID Act prohibits spoofing with the intent to cause harm, defraud, or wrongfully obtain anything of value. Consumers rely on caller ID information to make decisions about what calls to accept, ignore, or block. Accurate caller ID information is a vital tool that consumers use to protect their privacy, avoid fraud, and ensure peace of mind.

To help consumers confront such scams, the FCC will be partnering with the Federal Trade Commission in two upcoming events aimed at furthering the fight against illegal robocalls and caller ID spoofing. The agencies will co-host a <u>policy forum</u> later this month and a <u>technology expo</u> in April. The Commission also provides helpful consumer protection tips on social media via #FCCtips.

More Consumer Tips

- If the caller claims to be from a legitimate company or organization, hang up and call them back using a valid number found on their website or on your latest bill if you do business with them.
- If you answer and the caller (often a recording) asks you to press a button to stop receiving calls, or asks you to say "yes" in response to a question, just hang up. Scammers often use these tricks to identify, and then target, live respondents, or to use your "yes" to apply unauthorized charges to your bill.
- If you answer and the caller asks for payment using a gift card, it's likely a scam. Legitimate organizations like law enforcement will not ask for payment with a gift card.
- If you have lost money as a result of a scam call, contact your local law enforcement agency for assistance.
- Consider registering all of your telephone numbers in the <u>National Do Not Call Registry</u>. Lawful telemarketers use this list to avoid calling consumers on the list.

Everyone who believes they have been targeted by a robocall scam may file a complaint with the FCC Consumer Complaint Center, the FTC Complaint Assistant or the Better Business Bureau's Scam Tracker. The FCC reviews consumer complaints and may utilize them in enforcement actions and to inform its policy-making work.

###

Office of Media Relations: (202) 418-0500 ASL Videophone: (844) 432-2275 TTY: (888) 835-5322 Twitter: @FCC www.fcc.goy/office-media-relations

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action. See MCI v. FCC, 515 F.2d 385 (D.C. Cir. 1974).