ALLIANCE FOR CONSUMER PROTECTION NEWSLETTER

Robocalls are the bane of every phone owner's existence. Knowing this, and that the problem is getting worse, particularly as it relates to scam calls "spoofing" (faking) government numbers, our latest *Consumer Action News* is appropriately titled *The Robocall Scourge*! We cover what every consumer should know when dealing with robocalls. For example: Unless they are political or charitable in nature, the vast majority of robocalls are illegal. Perhaps most importantly, we tell you how to block obnoxious calls. Among your options? Join the DO NOT CALL REGISTRY, use a call blocker or a blocking app such Nomorobo, employ the built-in settings on your smartphone from certain numbers, and/or activate blockers via your wireless carrier. And, you can (and should) call on Congress to pass a bipartisan bill called the TRACED Act, which would force phone companies to adopt tech that alerts consumers/blocks the illegal calls. TRACED would require the Federal Communications Commission (FCC)—which has been slow to take action even though robocalls are *technically illegal*—to actually, you know, regulate. One plus (sorta): Earlier this month, the FCC passed a rule to "allow" (but not require) phone companies to block robocalls without requiring customer sign-off (a service for which the companies will, sadly, be permitted to charge extra). Under the new scenario, if your carrier blocks robocalls and you *want* to hear an artificial voice at the end of the line (who *are* you??), you can opt out. Free for landlines, Nomorobo screens your calls and matches the number with its massive database of over 1.2 million known, illegal spammers (and the list is updated all the time). If you receive a scam call, Nomorobo intercepts it after one ring and hangs up for you. If the call is legitimate, it will keep ringing and you can answer. One ring signals that a spam call was stopped by Nomorobo. Nomorobo also is available for mobile phones: After a free two-week trial, there is a $1.99 a month or $19.99 a year charge per device for iPhone and Android users.

"Robocalls are more than just annoying. Too often, scammers make the calls aiming, and succeeding, to steal money and sensitive personal data. This has cost consumers billions of dollars each year," .

Maintaining the anti-robocall momentum, the FCC on June 7 passed a rule that allows phone companies to block robocalls by default. While the FCC ruling does not require companies to offer this automatic call-blocking service, it assures carriers that they could do so legally, "as long as their customers are informed and have the opportunity to opt out of the blocking." (Questions remain about whether consumers will have to pay for such services, should carriers ultimately activate them.)

Anonymous call rejection for landlines

This landline calling feature blocks calls from those with anonymous, private or blocked Caller IDs. Enable the free service by picking up the phone and dialing *77—you'll hear three short beeps to know the service has been activated. To disable the service at any time, press *87. (Depending on carrier, this service may require a fee on business landlines.)

Despite these promising developments, there's much more work to be done before people can feel confident about answering their phones again. Consumers who want to urge their legislators to support the TRACED Act can do so through Consumer Action's online Take Action Center. Those who want to be proactive about thwarting robocalls to their cell and landlines should read Consumer Action's "Robocall combat tools" article for tips.

Detecting Fraud

If you suspect you are receiving calls from a scammer posing as a Charity or political campaign. hang up and immediately report the communication to the Federal Trade Commission.

If you suspect a scam, don't respond to any instructions such as "press X for" or "reply with

X," even if the message says it is to get more information. Pressing a number may be considered consent to use and sell your phone number to another company. It also lets scammers know they have a live line. Similarly, if you think you are dealing with a scammer, don't respond to the suspicious text with "STOP," as you might when unsubscribing from a legitimate company's marketing texts.

PHONE SCAMS

Lastly, be wary of any calls or texts that ask you for personal information, like your Social Security or driver's license number, birth date, address or account information. Also, be wary of any official-looking but unsolicited emails or texts that ask you to click on a link. Links inside scam texts and emails may install malware on your phone or computer. Mobile phone users with AT&T, T-Mobile, Verizon, Sprint and Bell service can copy the message and text it to 7726 to report a potential scam.

We may have entered the digital age, but the telephone remains scammers' weapon of choice. The Federal Trade Commission (FTC) received more than 940,000 fraud complaints in 2018 in which a contact method was identified, and 69 percent of the time a call was the swindler's way in. Once they get you on the line, phone scammers use false promises, aggressive sales pitches and phony threats to pry loose information they can use to steal your money or identity (or both).

It's easy to understand why crooks love to dial you up. The FTC reports that the median loss from a phone scam in 2018 was $840, more than double the median loss across all fraud types. And new technology is making this illicit work easier. With auto dialers, shady operators can blast out robocalls by the millions for just a few dollars a day. Readily available spoofing tools can trick your caller ID into displaying a genuine government or corporate number, or one that appears to be local, to increase the chances that you'll answer.

Whether live or automated, scam callers often pose as representatives of government agencies or familiar tech, travel, retail or financial companies, supposedly calling with important information. It might be good news. (You're eligible for a big cash prize! You've been preselected for this great vacation

deal!) It might be bad. (You owe back taxes. There's a problem with your credit card account. Your computer is infected with that virus you've been hearing about.) Whatever the issue, it can be resolved.

Phone fraudsters might also impersonate charity fundraisers or even your grandchildren, playing on your generosity or family bonds to get you to fork over money. And, like the rest of us, they are rapidly going mobile. According to a data analysis by telecommunications security firm First Orion, more than 44 percent of mobile calls will be fraudulent in 2019, compared with just 3.7 percent in 2017. First Orion calls it a brewing "epidemic" of scam calls, but you can take steps to inoculate yourself.

Warning Signs

- Unsolicited calls from people claiming to work for a government agency, public utility or major tech firm, like Microsoft or Apple. These companies and institutions will rarely call you unless they have first communicated by other means or you have contacted them.
- Unsolicited calls from charity fundraisers, especially after disasters.
- Calls pitching products or services with terms that sound too good to be true. Common scam offers include free product trials, cash prizes, cheap travel packages, medical devices, preapproved loans, debt reduction, and low-risk, high-return investments.
- An automated sales call from a company you have not authorized to contact you. That's an illegal robocall and almost certainly a scam. (Automated calls are permitted for some informational or non-commercial purposes — for example, from political campaigns or nonprofit groups like AARP.)

Do's

- Do put your phone number on the FTC's National Do Not Call Registry. It won't stop all fraudulent calls but will make them easier to spot because most legitimate telemarketers won't call you if you're on the registry.
- Do consider using free low-cost call-blocking apps and services that screen your calls and weed out spam and scams. You can also ask your phone-service provider if it offers any blocking tools.
- Do verify the caller. If the robocall claims to be from Social Security or your bank, hang up and
- Lookup the real number for that entity. Call and ask if they contacted you.
- Do report scam calls to the proper authorities. Every report helps authorities piece together a fuller picture of what scammers are doing.
- Do slow down and ask questions of telemarketers. Legitimate businesses and charities will answer questions and give you time to consider a purchase or donation. Scam callers will pressure you to commit right away.
- Do review a company's privacy policies before you give it permission to call you. You might be authorizing them to share your contact information with others.

Don’ts

- Don’t answer calls from unknown numbers. The FCC recommends letting them go to voice mail.
- Don’t return one-ring calls from unknown numbers. These may be scams to get you to call hotlines in African and Caribbean countries that have U.S.-style three-digit area codes, and you could incur hefty connection and per-minute fees.
- Don’t follow instructions on a prerecorded message, such as “Press 1” to speak to a live operator (it will probably lead to a phishing expedition) or press any key to get taken off a call list (it will probably lead to more robocalls).
- Don’t give personal or financial data, such as your Social Security number or credit card account number, to callers you don’t know. If they say they have the information and just need you to confirm it, that’s a trick.
- Don’t pay registration or shipping charges to get a supposed free product or prize. Such fees are ploys to get your payment information.
- Don’t make payments by gift card, prepaid debit card or wire transfer. Fraudsters favor these methods because they are hard to trace.
- Don’t judge a call by caller ID alone. Scammers mask their location by tricking your phone into displaying a legitimate government or corporate number, or one similar to your own (a practice called “neighbor spoofing”).

How and Where to Report A Scam

Annuities: Is control between you and your insurance company for payment while you are living.

Www.insurance.pa.govscams@attorney-general.gov

Officer of Consumer Advocate: is problems with electric, natural gas, telecommunications, wastewater.

Www.oca.state.pa.us

Pa senior law helpline: Is legal advice for themselves and property. This is a free service.

www.seniorlaw center.org or 1-877-727-7529

Veterans Affairs-----www.dmva.pa.gov

Government Advisory council in Veteran Services - 800-547-2838

RA-VA-info@pa.gov Local Veterans office- 724-770-4452

We would like to welcome our newest business sponsor. The Greater Allegheny Financial Group, LLC. 131 Pleasant Drive Suite 2U, Aliquippa, PA 15001 Phone 724-512-5095.

Abbey Carpet and Flooring AEI INTERIORS, LLC. have also sent their renewal for sponsor.