

CONSUMER ACTION NEWS

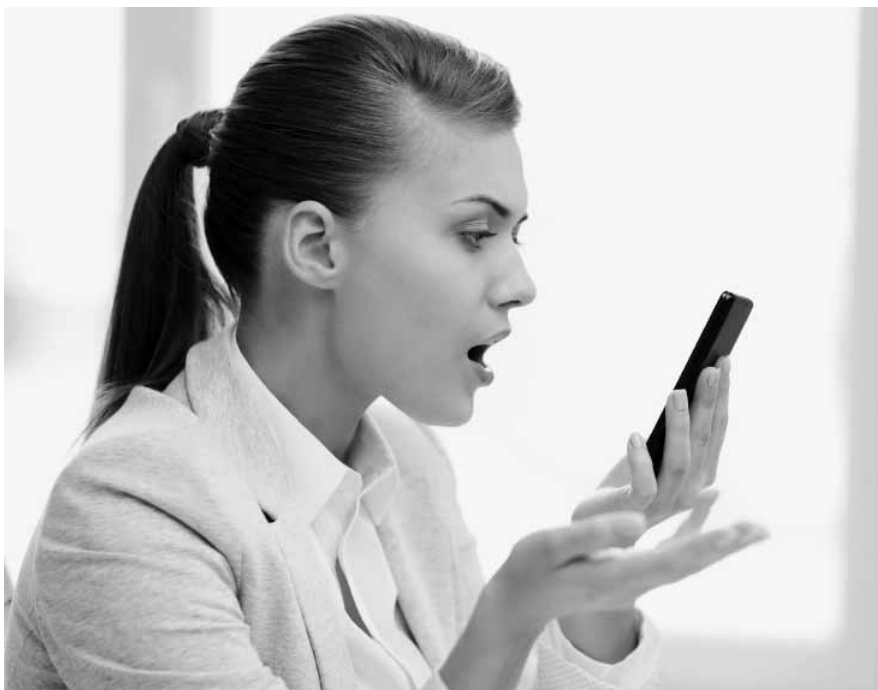
www.consumer-action.org • Spring 2019

Consumer Action
1170 Market Street, Suite 500
San Francisco, CA 94102

Non-Profit Org.
U.S. Postage
PAID
San Francisco, CA
Permit # 10402

Change Service Requested

The robocall scourge



Relentless robocalls anger consumers

By Lauren Hall

Those automated telephone calls that deliver pre-recorded messages to your landline or cell phone—aka “robocalls”—are bombarding consumers’ devices at alarming rates. Consumers received a whopping 47 billion robocalls last year alone. Estimates are that nearly half of them were from scammers.

Unless you have explicitly consented to the calls, robocalls are generally prohibited under the federal Telephone Consumer Protection Act (TCPA), especially on cell phones. (Certain types of robocalls, such as political or charitable pitches, may be legal.) But scammers and other disreputable callers don’t really care.

You might welcome robocalls that are automated calls from your child’s school about early school closings, or from your pharmacy about prescription refills or pickups. However, companies using “autodialers” to send out thousands of robocalls a minute to people who haven’t consented to receiving them are doing so illegally. Even prerecorded calls from legitimate companies offering you a hotel stay, a new credit card or a home security system are prohibited without consumer permission.

Spoofed robocalls are an increasing problem for phone owners. These calls use fraudulent caller identification (Caller ID) information to disguise the caller’s true identity. For instance, a con artist will “spoof” (fake) the name and/or number on a phone’s call display to make it seem like the call’s coming from a government office (e.g., the IRS or Social Security Administration), a neighbor or even your own phone number! Spoofing legitimate numbers makes it more likely you will answer the phone and fall for the con. Caller ID spoofing software is widely available and can send thousands of calls for very little money.

Robocalling is a huge and growing problem: In 2017, seven million consumers complained to the Federal Communications Commission (FCC) and Federal Trade Commission (FTC) about robocalls. According to the FCC, robocalls make up 60 percent of all the complaints it receives. The complaints have steadily increased despite the fact that consumers are taking what steps they can to protect themselves.

Consumers have placed more than 230 million phone numbers on the FTC’s Do Not Call Registry (<https://www.donotcall.gov/>). Doing so prevents legiti-

See “Relentless” on page 2

Lawmakers throw down the gauntlet on robocalls

By Ruth Susswein

The Federal Communications Commission (FCC) estimates that nearly half (46%) of all robocalls are from scammers. All parties, including representatives from the telecom industry, are looking for lawmakers to get tough on illegal robocallers. New laws may be an easy lift, but whether or not they’ll be effective against out-and-out scammers remains to be seen.

Unlike with many other issues, the U.S. Congress has united around its desire to find useful ways to combat the unwanted automated calls popularly referred to as “robocalls.” In April, the Senate Commerce Committee unanimously approved legislation that would provide consumers with some relief from fraudulent, unwelcome robocalls.

While innovative approaches to stopping the scourge of illegal robocalls are more than welcome, it must be acknowledged that slightly more than half of robocalls are from legitimate businesses. The National Consumer Law Center’s Margot Saunders says that companies making legitimate robocalls would largely be spared in some of the legislation being considered by Congress, but points out that legitimate businesses making illegal calls to cell phones without consent is a major reason 2018 was the worst year on record for robocalls.

TRACED ACT (S.151): The Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act would require telephone companies to adopt technology to authenticate calls and alert consumers if an incoming call was from a “spoofed” (faked) number. (Depending on your carrier, it may say “Suspicious” or “Spam?” before the incoming number on Caller ID.) This technology is called STIR/SHAKEN (Secure Telephony Identity Revisited, or STIR, and Signature-based Handling of Asserted Information using

toKENs, or SHAKEN). In May, FCC chief Ajit Pai called on phone carriers to hurry up and voluntarily implement the call authentication system by the end of 2019, or be forced to do so by the commission.

The TRACED Act would give the FCC—the nation’s telecom regulator—more time and authority to take enforcement action against robocall violators. Currently, the FCC can only take action against robocallers for one year from when the call was placed. The TRACED Act would extend that time to three years, as well as require the FCC to craft rules to help prevent calls or texts with spoofed numbers from ever reaching consumers’ phones. It also would broaden the enforcement authority of the Federal Trade Commission (FTC).

The TRACED Act would allow for increased penalties for intentional violations of telemarketing regulations, up to \$10,000 per robocall. If the intentional violations continued, the fine could jump to \$30,000 per call. The bill calls for civil penalties for legitimate businesses that repeatedly call numbers that have been recycled (“reassigned”) to other customers or simply repeatedly flout the law. The bill would extend the window for the FCC to catch and take civil enforcement action against intentional violations from one to three years after a robocall is placed. The bill also eliminates a requirement that the FCC warn companies before bringing an enforcement action against them if they subsequently skirt the law. State attorneys general across the country support the TRACED Act.

Another bill, the **Robocall Enforcement Enhancement Act (S.2694)**, also would extend the time the FCC has to pursue robocall and Caller ID spoofing violations, and would authorize the agency to act without the currently required warning.

See “Lawmakers” on page 2

Consumer Action

www.consumer-action.org

Consumer Action has been a champion of underrepresented consumers nationwide since 1971. A non-profit 501(c)(3) organization, Consumer Action focuses on financial education that empowers low- and moderate-income and limited-English-speaking consumers to financially prosper.

By providing financial education materials in multiple languages, a free national hotline and ongoing financial services research, Consumer Action helps consumers assert their rights in the marketplace and make financially savvy choices.

Advice and referral hotline

Submit consumer complaints to our hotline:
https://bit.ly/CA_hotline_ENG
(415) 777-9635
Chinese, English and Spanish spoken

San Francisco

1170 Market Street, Suite 500
San Francisco, CA 94102
(415) 777-9648
Email: info@consumer-action.org

- Ken McEldowney**
Executive Director
- Michael Heffer**
Business Manager
- Kathy Li**
Director, San Francisco (SF) Office
- Nani Susanti Hansen**
Associate Director, SF Office
- Audrey Perrott**
Director, Strategic Partnerships
- Monica Steinisch**
Senior Associate, Editorial
- Jamie Woo**
Community Outreach Manager
- Joseph Ridout**
Consumer Services Manager
- Cui Yan Xie**
Project Associate
- Vickie Tse**
Development Coordinator
- Hazel Kong**
Administrative Associate/
Consumer Advice Counselor
- Angela Kwan**
Web Manager
- Ricardo Perez**
Mail Room Operations
- Rose Chan**
Consumer Advice Coordinator
- Schelly Gartner**
Consumer Advice Counselor
- Alden Chan, Robert La, Michelle Liu**
Support

Los Angeles

(213) 624-4631
Nelson Santiago
Community Outreach Manager
Linda Williams
Community Outreach & Training Manager

Washington, DC

(202) 544-3088
Linda Sherry
Director, National Priorities
Ruth Susswein
Deputy Director, National Priorities
(Editor, *Consumer Action News*)
Lauren Hall
Policy Advocate, National Priorities
Alegra Howard
Policy Advocate, National Priorities

Consumer Action News is printed by the Dakota Printing Company.
© Consumer Action 2019

Lawmakers

Continued from page 1

Stopping Bad Robocalls Act (H.R.946): This bill would require call authentication technology to end spoofing and make Caller ID reliable. It would help prevent robocallers from evading the law via a better definition of “autodialer,” clarify that the TCPA applies to text messages, and affirm that consumers may revoke any previously given permission to receive robocalls.

ROBOCOP (Repeated Objectionable Bothering of Consumers on Phones) Act (S.1212 and H.R.2298): This bill would require phone companies to supply customers with free call-blocking tools. The ROBOCOP Act also would require phone companies to verify that Caller ID is accurate (with exceptions for medical offices and domestic abuse shelters, among other select entities). It also would give consumers the right to sue a phone company that violates the law.

State legislation

While Congress and the FCC consider how to solve the relentless robocall problem, some states have stepped up to combat this growing harm.

Caller ID spoofing ban (SB 208): This bill before the California State Senate sets a deadline for telecoms to prevent “neighbor spoofing”—displaying Caller ID numbers that appear to be local calls, from the same area code and prefix. Sometimes scammers hijack the phone numbers of real government agencies and other legitimate sources to reach their targets. The imposters behind these misleading calls are blamed for identity theft scams, in-language claims from taxing authorities, and other frauds that cost Americans over \$900 million in 2017, according to the FTC.

SB 208 would require phone companies to implement the STIR/SHAKEN system to identify and reduce spoofed Caller ID numbers by July 1, 2020.

The New York State Senate has passed a bill that would ban telemarketers from contacting New Yorkers using an automated dialing system without consumers’ prior consent. This bill also mandates that phone companies provide free services to prescreen and block robocalls. Violators

could be hit with a \$2,000 penalty per call.

In 2018, Connecticut passed a law adding criminal fines to the state’s anti-robocall law. Massachusetts floated a bill that would ban robocalls to cell phones (under state law) and increase penalties to \$10,000 per violation, and New Jersey lawmakers launched a bill to press the FCC to require phone companies to provide free robocall blocking for cell phones and landlines.

In reality most of these measures would not block all robocalls. They will not stop fraudsters who don’t spoof phone numbers, nor will they stop legitimate companies (student loan lenders, credit card companies, debt collectors, etc.) from making legally allowed calls.

On June 6, the FCC voted to allow phone companies to automatically block robocalls to customers’ phones. While the FCC’s ruling does not require companies to offer this call-blocking service, carriers that do must inform consumers of the change to block robocalls by default and provide consumers with an option to opt out of having their calls blocked if they wish to continue to receive all calls.

TCPA

The Telephone Consumer Protection Act (TCPA) limits the use of automated dialing systems, prerecorded messages, texts, faxes and telemarketing sales calls. Outside of emergency warnings, recorded messages and automated calls and texts to your cell or residential phone are forbidden without your written consent. (However, for consumers who *have not* added their numbers to the Do Not Call Registry (<https://www.donotcall.gov>), prior consent is not required when sales calls are made *manually* and do not feature prerecorded messages.)

Under the TCPA, without your written consent, companies may not call before 8 a.m. or after 9 p.m. or fail to provide the name of the company from

which, or on whose behalf, they are calling. (Learn more: <https://tinyurl.com/y6d2h3ua>.)

The FCC created rules to implement the TCPA and established the Do Not Call Registry, which allows consumers to register their landline and cell phone numbers at <https://www.donotcall.gov/> or 888-382-1222, at no charge. Marketers are prohibited from calling numbers on the Do Not Call list. You also can verify

Robocall loopholes

Without your permission, robocalls to your cell phone are illegal, but “non-commercial” robocalls may be placed to your landline without your permission. Non-profit groups, political organizations and pollsters are allowed to robocall your *landline* even if your phone number’s on the Do Not Call list.

Debt collectors often place robocalls to cell and landlines if you gave consent when you took out the loan, even inadvertently.

If you are on the Do Not Call list, all *telemarketing* calls (robo- and otherwise) are prohibited unless you have given the caller permission. For more about this, see “When telemarketing protections don’t apply” on page 4.

if your phone number is on the list or report unwanted calls to the FTC at the site.

If companies violate the TCPA, consumers should document the illegal calls, including date, time, caller’s identity and a summary of the call. (Voicemails left on answering machines by telemarketers and scammers are valuable documentation—use your mobile phone to re-record them and turn them into digital files.) Submit the information to the FCC and the FTC. This information is useful as proof in lawsuits against telemarketers or debt collectors. Consumers can recover up to \$500 for each violation, and up to \$1,500 if they can prove the TCPA was knowingly violated.

Debt collection rules

In May, the Consumer Financial Protection Bureau (CFPB) proposed to allow debt collectors to call borrowers seven times a week, and have one conversation per week—per debt—plus send unlimited text and email messages. There currently is no set limit on the number of debt collection calls allowed per day if they are not automated robocalls. The proposed changes would modify the 42-year-old Fair Debt Collection Practices Act. ■

Relentless

Continued from page 1

mate telemarketers from calling numbers on the list, but really does nothing to stop fraudsters from repeatedly robocalling.

There are a variety of tools consumers can use to curb the onslaught of unwanted robocalls—from call-blocking apps to alerts (through your phone company) that let you decide which calls to block. For details on these options, see page 3. The FTC also offers a guide (<https://tinyurl.com/y5lwr5lq>) to apps that block calls (both on cell and landline phones).

Finally, cell phone owners can set their phones to block calls from certain numbers or enable “Do Not Disturb” mode to keep the phone from ringing.

These tools are helpful but insufficient to combat these relentless calls, particularly from scammers. The FCC is working with telephone providers to determine ways for them to identify and block spam robocalls before they reach your phone. According to the FCC, “many voice provid-

ers have held off developing and deploying call-blocking tools by default because of uncertainty about whether these tools are legal under the FCC’s rules.” The FCC erased that uncertainty by voting, on June 6, to allow (but not require) phone companies to automatically block robocalls to customers’ phones.

Robocalls are regulated by the FCC and, to a lesser extent, the FTC. The FCC’s telemarketing rules apply to robocalls, which are limited and/or prohibited under the TCPA (<https://tinyurl.com/>

See “Relentless” on page 3

Robocall combat tools

By Monica Steinisch

There has been enough of an outcry against robo-calls and spam texts that service providers, app developers and inventors are finally providing some legitimate, effective options against the intrusions. Not all options work for all phones—some are carrier or device specific—but there’s sure to be some tool available that will give you some relief from the onslaught.

Do Not Call Registry

The Federal Trade Commission’s National Do Not Call Registry (<https://www.donotcall.gov/>) is designed to reduce the number of unwanted telemarketing calls made to consumers’ home or mobile phones. There’s no cost to register your landline and mobile phone numbers.

Adding your number(s) to the list won’t stop calls from charities, political groups, debt collectors, survey-takers or entities you already do business with, which you may find equally unwelcome, but it will put a dent in the total volume of unwanted calls.

The main shortcoming of the Do Not Call Registry is that the people who inundate consumers with unwanted robocalls generally are not particularly concerned with obeying the law.

Call-blocking tools

Anonymous-call rejection is free and available regardless of which carrier provides your residential landline service. It’s easy to activate: Just listen for the dial tone and press *77 (touch-tone phones) or dial 1177 (rotary phones); hang up after you hear the confirmation tone or announcement. If you have any problems activating the feature, call your carrier for assistance. (There may be a fee for this service on business landlines.) While this feature will block calls from hidden phone numbers, it won’t stop unwanted calls from sources that spoof (fake) their numbers on Caller ID.

There are a slew of call blocker devices available for purchase that you attach to the phone line. These mainly are intended for copper-based landlines. Typically, the devices come pre-programmed with thousands of

known spam numbers to block, and they allow you to add new numbers as they come in. You can find retailers and product reviews (such as this from Mashable: <https://tinyurl.com/y5mblmms>) by doing an online search for “landline call blockers.” Or, your carrier might offer devices on their website (like Verizon: <https://tinyurl.com/y469h6q5>).

Free for landlines, Nomorobo screens your calls and checks each incoming phone number against its constantly updated list of over 1.2 million known, illegal spammers. If you receive a spam call, Nomorobo intercepts it after one ring and disconnects it. If the call is legitimate, it will keep ringing.

Nomorobo is only available for VoIP (Voice over Internet Protocol) landline phones, not those connected to traditional copper lines. However, this covers the majority of landline customers. Visit the Nomorobo website (<https://www.nomorobo.com/>), or check directly with your carrier. Some carriers, including Spectrum Communications (<https://tinyurl.com/y6247e53>) and Comcast (Xfinity) (<https://tinyurl.com/y9x5rbym>), offer it through their website.

While Nomorobo is an option for most landline customers regardless of phone service provider, many carriers offer additional tools for combatting spam calls. Some tools alert you, others block suspicious calls, and still others do both. For example, Verizon customers who subscribe to Caller ID get a landline feature that blocks some calls automatically if the system detects a spoofed number or one associated with illegal spam calls. For other suspect calls, the word “SPAM?” appears in front of the caller’s name and number and you choose whether or not to answer.

Likewise, AT&T’s Digital Phone Call Protect automatically blocks calls from known scammers and alerts you on Caller ID if a call is suspected spam and what category it falls into (for example, Debt Collector, Political, Nonprofit, Telemarketer, Survey or Robocaller). An app version of this tool—AT&T Call Protect—is available for cell phones.

Because anti-spam features vary

across carriers and are constantly in development, the best way to know what’s available to you is to call your carrier or visit the company’s website. You also can do an online search for your carrier’s name plus keywords “residential anti-spam call tools” (or something similar).

Smartphone settings

All smartphones have built-in features that allow you to block certain calls. Blocking calls on an iPhone is pretty straightforward and entails the same (or very similar) steps for all Apple operating systems 7 or later. Since the Android operating system (OS) runs on phones from different manufacturers, the steps for blocking calls can vary. Digital Trends offers step-by-step instructions for a variety of phones (<https://tinyurl.com/y8cbeyf4>).

Depending on which Android device you’re using, you might have built-in tools. For example, Samsung devices offer “Smart Call” (<https://tinyurl.com/y89p7pp8>), and Google Pixel phones can provide a real-time transcript of the call and allow you to block it (<https://tinyurl.com/ya8qu8bu>). For the latest information about your spam-fighting options on your particular device, do an online search for your phone model and OS along with keywords “how to block spam.”

A more extreme option for smartphone users is to turn on the “Do Not Disturb” function (available on all iPhones but only some Android phones) and choose to allow only calls from people in your contacts list. While this might prevent you from receiving desired calls from people not in your contacts list, you will see which calls you’ve missed and can choose whether to return them.

Blocking apps

There are dozens of independently developed apps that make it possible to block unwanted calls and/or text messages on cell phones. They vary in:

- Purpose: Block just calls, just texts or both.
- Method: For example, blocking calls from numbers phone owners have “blacklisted” (denied access), allowing only calls from allowed “whitelisted” numbers, or providing a warning of some type versus blocking the call outright.
- Cost: Free and paid versions

are available. CTIA, a trade association representing the U.S. wireless communications industry, offers lists of apps, with step-by-step instructions, to help consumers block nuisance communications on these devices:

- iPhone (<https://tinyurl.com/yypynh5y>);
- Android phone (<https://tinyurl.com/y2rlqa9a>);
- Blackberry (<https://tinyurl.com/y2dkfvae>); and
- Windows (<https://tinyurl.com/y58khudc>).

Nomorobo is one of these many anti-spam apps. While free for landlines, there’s a \$1.99 a month or \$19.99 a year charge per mobile device after a no-cost 14-day trial. When used on a smartphone, Nomorobo also protects against spam text messages.

Note: Many call-blocking apps request access to your contacts list and other data. If that raises your privacy warning flag, be sure to choose a service that is less intrusive. You’ll most likely have to pay a small purchase or subscription fee for the privilege of maintaining your privacy.

For instructions on integrating third-party apps into your iPhone’s OS, see <https://support.apple.com/en-us/HT207099>.

Carrier apps and tools

Many wireless service providers offer their own anti-spam apps. For example, Verizon’s free Call Filter app (<https://tinyurl.com/yymr-8bx4>), available for both iPhone (<https://tinyurl.com/yy965dx7>) and Android (<https://tinyurl.com/ybg-2d7yh>), alerts you to unwanted calls and texts, and allows you to report and block calls. Those who pay \$2.99 per month, per line, get some enhanced capabilities, such as the ability to create a personal robocall block list.

Other service providers offer protection as an account feature, without the need to install a separate app. For example, once you activate T-Mobile’s free Scam Block (<https://www.t-mobile.com/resources/call-protection>) on your account, the system will notify you of likely scam calls and allow you to block the calls before they reach you.

Check with your carrier or service provider to learn about its latest tools for preventing unwanted calls. ■

Relentless

Continued from page 2

[yyuwm4c4](https://www.ftccomplaintassistant.gov/)). That’s the law that requires marketers to get consumers’ specific, written (“express”) consent before calling or texting, with a small set of exceptions. Calls that involve an attempt to collect a debt also are subject to the Fair Debt Collection Practices Act (FDCPA), enforced by the FTC.

So what recourse do consumers have when bombarded with

robocalls? First, hang up immediately and report the call to the FCC (<https://tinyurl.com/newygtj>), and to the FTC if you believe it is a scam or if you received the call despite having placed your number on the Do Not Call registry (<https://www.ftccomplaintassistant.gov/>).

Next, know that under the TCPA, consumers can take a robocaller to state court. (This would be most easily done if the call were from a recognized company that did not have the consumer’s permission to ro-

bocall, or was calling a number on the Do Not Call list without permission.) If the court finds that the caller “willfully or knowingly” violated the TCPA, it can award victims up to \$1,500 per call. In addition, consumers can take certain callers to court under the FDCPA, which protects them from unfair, deceptive and abusive debt collectors (including those making robocalls). Consumers also can join with others in class action lawsuits against robocallers.

Robocallers who violate the Do

Not Call Registry or any of the other relevant laws also could face fines by the FCC and/or FTC.

Congress is considering legislation (like the TRACED Act) to levy even bigger fines against lawbreaking robocallers and require telephone companies to improve their technology to help consumers avoid the unwanted calls. ■



When telemarketing protections don't apply

Some robocalls, texts and prerecorded calls are allowed

By Alegria Howard

If the volume of unwanted robocalls and scam texts reaching your phone lines has mushroomed, you're not alone. Many are from illegal scammers, but the calls and texts can come from companies and organizations that are exempt from the Telephone Consumer Protection Act (TCPA), a federal law that limits telemarketing calls and autodialed, prerecorded calls.

Legal exemptions

Placing your number on the Federal Trade Commission's Do Not Call list (<https://www.donot-call.gov/>) is intended to prohibit sales calls, but businesses can still legally contact you with prerecorded messages as long as they don't try to sell you something. Messages from an airline about a flight cancellation, appointment reminders from your doctor, and pharmacies reminding you to refill your prescription all are allowed. Prerecorded calls from debt collectors are more complicated, but are allowed to landlines, not cell phones, unless you gave the caller or the firm they're working for prior permission. Non-profit organizations and political campaigns also are exempt from many, but not all, TCPA robocall restrictions.

You may have unintentionally made yourself a target of legal robocalls from businesses by checking a box when signing up for a service or visiting a website, when asked if the business can market to you directly. Perhaps

that box was checked by default when you were making an online purchase or inquiry. If you're tired of hearing from a business, you can unsubscribe from future sales calls and texts. You can usually end legitimate marketing text messages by texting "STOP." But don't respond to a text if you think it's a scam, because doing so just lets the scammer know your number works.

Charities and non-profits

Prerecorded calls made by (or on behalf of) a non-profit organization to landlines for fundraising or informational purposes are allowed—even if your name is on the Do Not Call list. However, the name of the organization and a return telephone number must be provided at the start of the message. Non-profits and politicians may not robocall or text your cell phone unless you have given prior consent (written or oral). You could be giving consent when you sign up to volunteer, receive a newsletter or make a donation, so double-check which "I agree" boxes have been checked before submitting your contact information. Be aware that individual, manually dialed calls from non-profit staffers are still allowed to your cell phone.

To stop non-profits and campaigns from calling you, ask to be placed on the organization's own do-not-call list. This also applies to third-party telemarketers calling on behalf of a charity. If any company or charity fails to

stop calling, you can complain to the Federal Trade Commission (<https://www.ftccomplaintassistant.gov/>).

Before you donate to a charity, make sure to check its donor privacy policy to see if your contact information might be sold to other organizations. Sites like the Better Business Bureau's Give.org (<http://www.give.org/>) and Charity Navigator (<https://www.charitynavigator.org/>) provide an overview of an organization's donor privacy standards (when available) if you're unable to find it on the charity's website.

Political campaigns

Phone calls and texts from campaigns are legal, but there are a few restrictions. The last few years have seen an uptick in campaigns using texting as a way to rally support for candidates. From donation requests to election day reminders, political texts are the biggest trend on the campaign trail. With the 2020 campaign season right around the corner, consumers may wonder what rights they have to stop the barrage of communications from candidates.

Campaigns usually obtain registered voters' phone numbers from voter registration files, which are public. While political campaigns legally can autodial or send prerecorded calls to your landline without your consent, it is illegal for campaigns to use an automated dialing system to mass call or text your cell phone without your consent.

You might be wondering, then, why you are receiving so many campaign text messages that you've never consented to. There's a loophole in the TCPA's protection against unsolicited text messages: peer-to-peer texting (<https://tinyurl.com/y6dsvyu>). This technology allows a campaign staffer or volunteer to send a large number of unsolicited text messages without recipient consent. As long as staffers have to press a send button each time they send a text, the system technically isn't automated, even if a staffer contacts 1,000 voters per day.

You have the right, at any time, to opt out of receiving automated or prerecorded calls and texts to your cell phone. Once you ask, the campaign must place your number on its own do-not-call list. If they fail to do so, report it to the FTC (<https://www.ftccomplaintassistant.gov/>).

Another annoying but legal practice is campaigns that sell supporters' contact information to other campaigns and political organizations. During the 2016 GOP presidential primary campaign, nearly every presidential candidate sold supporter data for big money.

A CNN Money analysis of 2016 Federal Election Commission records found that by selling supporter lists, Marco Rubio made \$504,651, Rand Paul pulled in \$212,495 and former Wisconsin Governor Scott Walker made \$142,757. Democratic campaigns run by Barack Obama and Hillary Clinton made millions from sharing their supporter lists after past elections.

So, what can you do to stop your data from being sold? When you donate or register with a campaign, the fine print may state that the campaign is able to sell your information. Opt out by asking each campaign to place you on its own do-not-call list.

Detecting fraud

If you suspect you're receiving calls or texts from a scammer posing as a charity or political campaign, hang up and immediately report the communication to the Federal Trade Commission (<https://www.ftccomplaintassistant.gov/>).

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.

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. ■

Join Consumer Action

Consumer Action depends on the financial support of individuals. Consumer Action members receive a subscription to *Consumer Action News*. New members also receive *How to Complain*.

☐ \$25, Regular Membership

☐ \$15, Senior or Student Membership

☐ \$_____ Donation to our Publications Fund, supporting the free distribution of Consumer Action materials to consumers

Name _____ Address _____

City _____ State _____ ZIP _____

Email address _____

Mail to: Consumer Action, 1170 Market St., Suite 500, San Francisco, CA 94102. Donations are tax-deductible. 5/19



You can join or donate online with a credit, debit or prepaid card using our secure server: www.consumer-action.org/join.



Stand up for your rights!

Hit the red button on our homepage to use Consumer Action's free Take Action! Center (bit.ly/email-Congress) to email your elected officials.