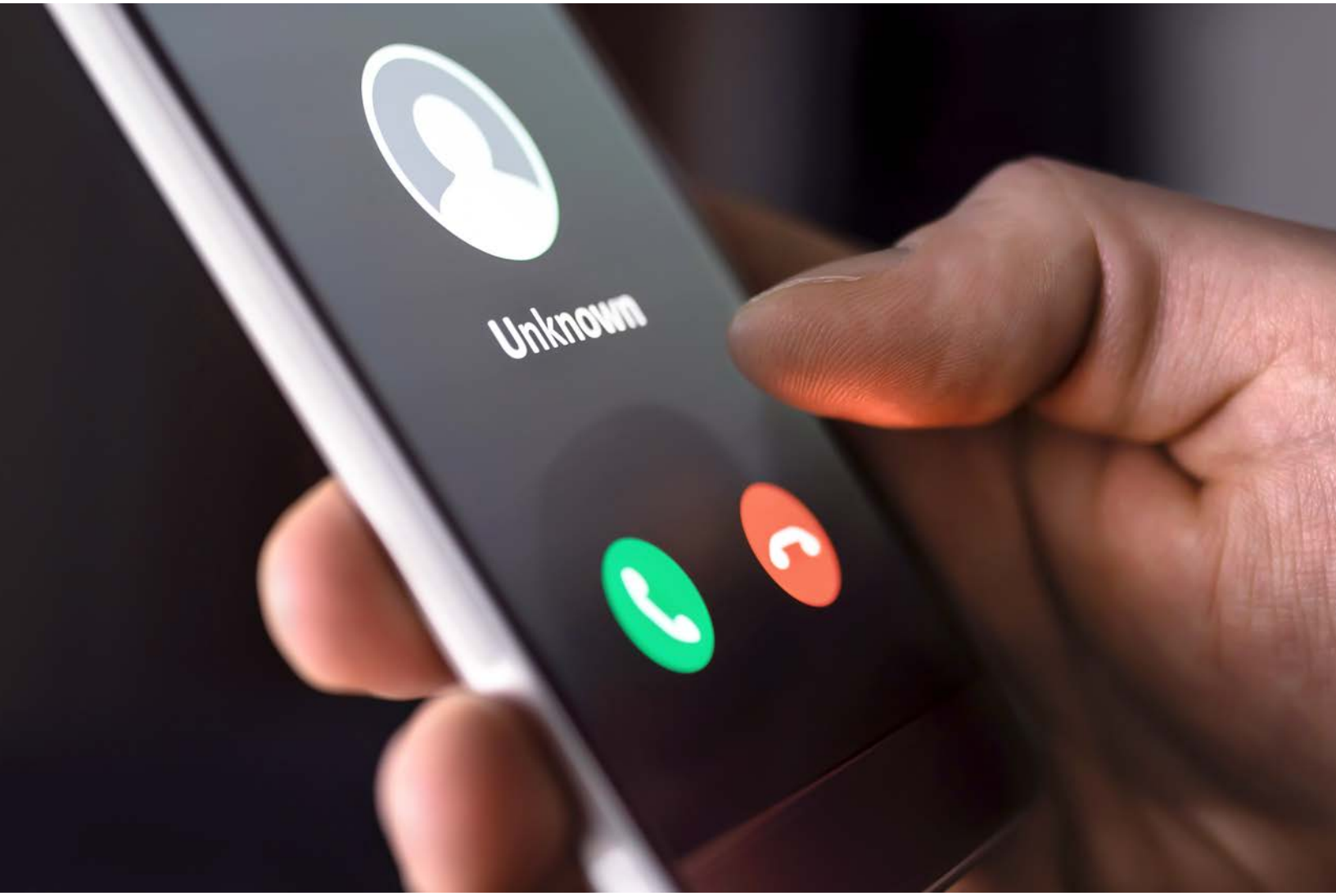


MAKE THE RINGING STOP: THE FCC IS FINALLY FIGHTING BACK AGAINST ROBOCALLS

But phone companies overall aren't doing enough to block spoofed calls and scam calls, despite the new law

SEPTEMBER 2021 // U.S. PIRG EDUCATION FUND

ConnPIRG Education Fund

Contents

WRITTEN BY:
TERESA MURRAY
U.S. PIRG EDUCATION FUND

ACKNOWLEDGMENTS

U.S. PIRG Education Fund thanks our donors for supporting our work on consumer protection and public health issues and for making this report possible.

The author wishes to thank the following for their insights and suggestions:

- Paloma Perez, press secretary for FCC Acting Chairwoman Jessica Rosenworcel
- Travis Litman, acting chief of staff to FCC Acting Chairwoman Jessica Rosenworcel
- Aaron Foss, founder of Nomorobo
- Alex Quilici, CEO of YouMail
- Chris Serico of Verizon
- Megan Ketterer of AT&T
- Katie Recken of T-Mobile
- Rich Ruggiero of Charter Communications
- Thomas Larsen of Mediacom
- Dave Miller of C Spire
- David McGuire of Comcast
- Matt Freeman of Cox Communications
- Zach Pickett for WOW
- Katie Frey of US Cellular
- Brigid Smith of Frontier Communications
- Diane Carragher of RCN
- Ann Nishida Fry of Hawaiian Telecom

Thanks also to James Horrox and Tony Dutzik of Frontier Group; Ed Mierzwinski, senior director of the PIRG Federal Consumer Program; and Consumer Watchdog Associates Jacob van Cleef, Hannah Rhodes and Isabel Brown, for editorial support.

The author bears responsibility for any factual errors. Policy recommendations are those of U.S. PIRG Education Fund. The views expressed in this report are those of the author and do not necessarily reflect the views of our funders or those who provided review.

With public debate around important issues often dominated by special interests pursuing their own narrow agendas, U.S. PIRG Education Fund offers an independent voice that works on behalf of the public interest. U.S. PIRG Education Fund, a 501(c)(3) organization, works to protect consumers and promote good government. We investigate problems, craft solutions, educate the public and offer meaningful opportunities for civic participation. For more information about U.S. PIRG Education Fund or for additional copies of this report, please visit www.uspirgedfund.org.

Design: Teresa Murray
Cover Image: Tero Vesalainen via Shutterstock.com

Executive summary

Bob Sopko used to get about 20 illegal robocalls a week. You're probably familiar with the ones that filled his voicemail box: Your car warranty is about to expire. You owe back taxes to the IRS. You can reduce your credit card interest rate. The types of scam calls go on and on.

A couple of months ago, Sopko's phone stopped ringing so much. He gets only about five calls a week now. "They have dropped significantly for us," said Sopko, a university entrepreneurship program director who lives near Cleveland.

Then there's Cheryl Carstens of Sioux Falls, S.D. She gets up to 25 illegal robocalls a day. Her callers also seem concerned about her expiring car warranty, for a Toyota she's never owned.

What's the difference between Sopko and Carstens? Sopko's phone company has completely adopted new caller ID technology that's aimed at reducing illegal robocalls. Carstens' phone company has not.

Across the country, 2021 is supposed to be the year when we can start answering our phones again without bristling over the likelihood that the call is an effort to rip us off, steal personal information or sell us something we'd never want. (Heck, you're not even supposed to be getting these calls anyway if you're on the Do Not Call Registry.)

Cellphone and landline companies were required under federal law to implement new robocall-fighting technology by June 30. That was nearly three months ago. Some smaller companies and providers whose lines don't run through internet/cable lines have extensions for now.

But research by PIRG Education Fund shows that among 49 of the largest phone companies nationwide (those that can serve 1 million or more), only 16 have reported to the Federal Communications Commission (FCC) that they have completely implemented anti-robocall technology. [1]

An additional 18 have partially implemented the technology, according to the FCC. The remaining 15 companies have told the FCC they haven't adopted the industry standard technology at all, but they're using their own methods to reduce robocalls, or they have not reported their status to the FCC's database, as required by law.

Partial implementation often means it hasn't been adopted on the non-digital/non-internet/non-cable parts of their network.

Overall, among 3,063 providers that reported their status to the FCC as of Sept. 3 and didn't claim an exemption from submitting information:

- Only 17 percent (536 companies) said they'd completely implemented anti-robocall technology.
- 27 percent (817 companies) had partially implemented the technology.
- And 56 percent (1,710 companies) said they were not using the industry standard technology but rather are using their own methods to manage robocalls. [2]

What does this mean? It means the industry isn't doing nearly as much as hoped to fight the crime that for years has caused so much heartache and aggravation among consumers nationwide.

Illegal robocalls lead to $10 billion a year in fraud, according to the Federal Trade Commission (FTC). [3] The calls cost consumers an additional $3 billion a year in wasted time, according to the FCC, [4] when you consider all of that time spent answering unwanted calls, blocking calls, reporting the calls to authorities and generally getting distracted.

Despite that, scam calls nationwide dropped by 29 percent from June to August, according to YouMail, a leading robocall filtering company. [5] This is encouraging news.

Among our other findings about 20 of the largest cell phone companies and Voice over Internet Protocol (VoIP) companies: [6]

- Only 13 of the 20 companies told PIRG Education Fund they block some known scam calls/spoof calls by default, which they've been permitted to do by the FCC since 2019.
- Only eight of the 20 say they provide on-screen warnings that a call may be a scam, as allowed by the FCC.
- Only eight of the 20 say they routinely allow customers to block calls with no caller ID, a service the FCC permits.
- Only four of the 20 say they routinely show on-screen check marks next to the caller's name or other verifications to customers that calls are coming from the number that's actually on the caller ID. They're allowed to do this as well. In fact, it's one of the keys of this whole effort to combat robocalls: to give consumers assurance that it's likely OK to answer these calls, even if we don't recognize the number.

"If the smaller providers weren't a big part of the problem, maybe a little more time would be warranted."

Ohio AG Dave Yost

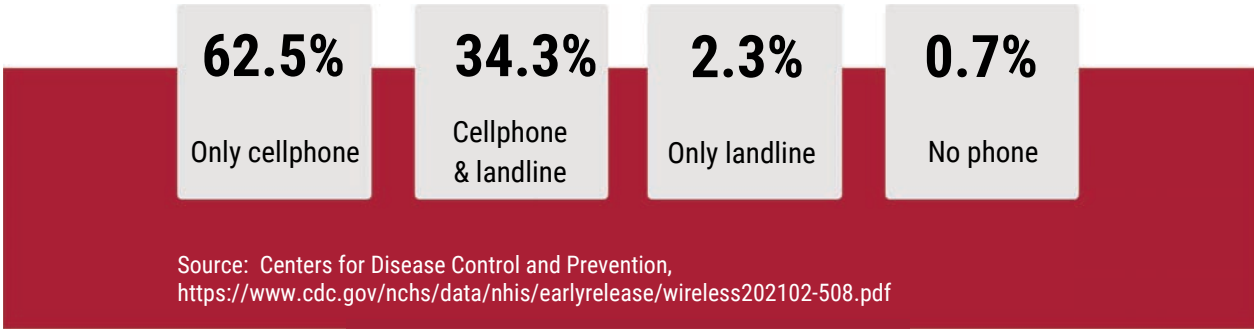
Robocall-filtering software companies say scam calls have dropped notably this summer but have by no means disappeared. However, consumers could start seeing greater compliance with the law starting Sept. 28, when providers nationwide will be required to block calls from companies that haven't at least reported to the FCC what they're doing to fight these nasty invasions in our lives.

At the same time, we're seeing new threats from robotexts not covered by the law and more targeted scam calls thanks to data breaches.

7.65 billion spam texts were made in August. That's 30 spam texts for every adult in the United States last month.

NEARLY ALL ADULTS HAVE A CELL PHONE; A THIRD HAVE A LANDLINE TOO

Nearly 97 percent of adults have a cellphone. Here's the percentage of adults in 2020 with:



Source: Centers for Disease Control and Prevention, https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless202102-508.pdf

Robocalls are actually declining

There is good news in this war on robocalls. Scam robocalls plunged by a whopping 29 percent from June to August, the first two months under the new law, according to one leading robocall-filtering software company, YouMail. [7] Meanwhile, the FCC says complaints about unwanted calls (which may not necessarily be scams or against the law) dropped by 10 percent from June to August. [8]

Not all robocalls are illegal or even bad. Robocalls generally refer to phone calls made with help from a computer that does the dialing, either using numbers in a database or just dialing numbers at random. We sign up for some helpful robocalls: Our prescription is in at the pharmacy. Our kid's school is closed. Our airline flight is delayed. Our cable repair technician will be there in 30 minutes. Also, auto-dialed calls from political organizations, non-profits, survey companies and debt collectors are generally exempt from robocall rules. [9]

But we colloquially use the term "robocalls" as a catch-all to describe the calls aimed at swindling us out of money, tricking us into providing personal information or selling us something we never wanted. Throughout this report, we'll use just "robocall" to refer to the illegal or unwanted calls.

Phone calls are generally illegal if:

- It's a telemarketing call with a recorded message, unless the caller has written permission from you allowing the company to call you.
- It's a call aimed at deceiving or defrauding you.
- It's a call from a legitimate company that you haven't done business with and it's calling you even if you've registered your number on the federal Do Not Call Registry.

It's the second group that have been the biggest problem for years as con-artists call and impersonate your bank, the IRS, the police, the Social Security Administration, Amazon or any other entity they think will get your attention and rattle you badly enough to cough up personal information or agree to wire money or run out to buy gift cards to pay some fabricated obligation.

These scammers rely on a practice called "spoofing." Using computers, they set up automated dialing software. Then they decide what to display on the caller ID.

Sometimes they may decide to call thousands of numbers with a specific area code and prefix and set the caller ID with the same area code and prefix to make the call appear local -- perhaps from a neighbor -- to increase the chance you'll answer.

Other times, they'll rig the caller ID to appear as if the call is coming from a specific company or government office. Then the computers start calling, with the ability to make millions of calls in just a few minutes, with each call costing just a few pennies. [10]

One victim can produce a payday of hundreds or thousands of dollars. Three recent examples:

- An elderly man in Rocky River, Ohio, outside of Cleveland, had his bank account drained of more than $124,000 in May after he was tricked into believing a call was from Amazon's security department. [11]
- Earlier this year, the FCC fined Texas-based telemarketers $225 million -- the largest fine in FCC history -- for making about 1 billion robocalls, many of them spoofed, to sell short-term health insurance plans that claimed to be through companies such as Blue Cross Blue Shield and Cigna, but they weren't. [12]
- In July, a New Jersey company, Environmental Safety International, Inc., agreed to pay $1.6 million to settle charges that it made 45 million illegal telemarketing calls to consumers nationwide during 2018 and 2019. [13]

The FTC said 31 million of those calls from ESI were made to numbers on the Do Not Call Registry. According to the U.S. Department of Justice complaint, the company told consumers who answered they were calling from an unnamed environmental company to provide free information about their septic tank. They instead were given a sales pitch on a product that cost money. The deception is what made all of the calls illegal even to those consumers not on the Do Not Call list.

So to those who ask why the con-artists continue making calls, when most of us don't answer or fall for the scams, it's simple: It takes only one a day, one a week or one a month to produce enough income to make it worth it.

"This is so lucrative for the people who are doing it," Aaron Foss, founder of Nomorobo, one of the nation's largest robocall-filtering software companies, said in an interview with PIRG. "If some of these calls didn't work, nobody's phone would be ringing."

About 34 percent of all robocalls (legal and illegal) were scam calls in August, according to YouMail. That's down from 42 percent of all robocalls in July. Scam calls have declined both in volume and as a percentage of all robocalls, according to YouMail. Scam calls totaled 2.1 billion in June, 1.8 billion in July and 1.5 billion in August.

Up until this year, scam calls represented the largest group of robocalls by a wide margin, according to YouMail. The breakdown from last year has been fairly consistent for years: [14]

- Scams: 46 percent
- Alerts and reminders: 26 percent
- Financial reminders/ late payments: 16 percent
- Telemarketing: 13 percent

How are these categories defined? Scams are scams. Alerts and reminders are the good calls we sign up for. Financial reminders may be unwanted, but we may have unknowingly agreed to an automated call if we're late on our mortgage or credit card payment.

Of the telemarketing calls, most are probably illegal, Alex Quilici, CEO of YouMail, said in an interview with PIRG, because the recipients didn't opt in to the calls or are on the Do Not Call Registry. [15]

Until the big decline in August, experts estimate we'd get roughly 2 billion illegal and unwanted phone calls every month in the United States; each consumer gets an average of a half-dozen scam calls per month. That's not counting telemarketing calls which may or may not be legal. [16]

Stephen Beard of Indianapolis used to get four or five scam robocalls a day on his cellphone. Everything from supposed fraud alerts from his bank, to prayer lines.
Then, sometime in July, they miraculously stopped. "In the past two months, I think I've had one robocall," he said. "It's been refreshing." For Beard, his phone company's anti-robocall software clearly is working.

How we got here

Robocalls date back to the 1980s when computer software made such calls possible on a wide scale for next to no cost. [17]

But they didn't really take off until about 2006, as cellphone ownership among U.S. adults hit 70 percent. [18] By 2007, regulators were chasing various accused robocallers. One of the first big cases led to two lawsuits in 2009 against companies from Florida and Illinois accused of making more than 1 billion unwanted calls from 2007 to 2009 about -- can you believe it -- bogus offers to extend a person's car warranty. [19] The companies sold worthless "warranties" for $2,000 to $3,000 each, generating more than $10 million in revenue.

The modern-day robocall became illegal on Sept. 1, 2009. That's when the FTC started prohibiting prerecorded telemarketing calls to any consumers who hadn't agreed to the calls in writing. [20] But you can only take action against those criminals that you can catch. As spoofed calls became more common, it became more difficult to track down those making calls, particularly considering many originate from overseas or a difficult-to-trace computer.

Over the years, regulators including the FCC and FTC started trying to crack down on robocalls not only by charging and shutting down the robocall operations, but also going after the phone companies that allowed the calls to occur. By 2016, more than 30 of the largest communications and technology companies, including AT&T, Apple, Comcast, Google and Verizon, agreed to work with the FCC to try to squash robocalls, particularly spoofed calls that tricked so many. [21] The idea of caller ID verification standards came out of this group. The ball was finally rolling.

"Starting Sept. 28, I think you'll start seeing more calls get blocked."
Alex Quilici,
CEO of YouMail

By November 2017, the FCC approved a radical change in policy: allow phone companies to block calls that claim to be from a number that couldn't possibly exist. It could be because no phone number is possible with that combination of area code and prefix, or because the number belongs to a company or government office that doesn't accept incoming calls to that number (called do-not-originate lines).

The rules allowed phone providers to block these calls without fear of liability. The new rules took effect in 2018, followed by others that gave companies the option of allowing customers themselves to block suspected robocalls and block calls with no caller ID.

In November 2018, the FCC asked phone companies to adopt caller ID verification by 2019. But it was a soft ask with no teeth. So it didn't happen.

In June 2019, the FCC voted unanimously to allow phone companies to block some calls they believe are scam or spoof calls by default, as long as they give consumers the chance to opt back in.

In August 2019, 12 of the largest phone companies reached agreements with the attorneys general in all 50 states to adopt anti-robocall practices and implement call-blocking and caller ID verification at no cost to their customers. [22]

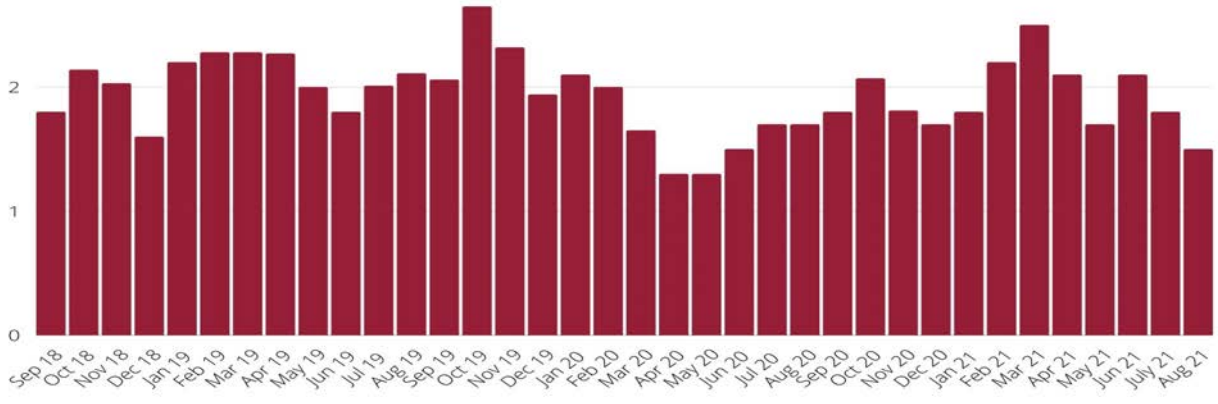
That brought us to the big development of 2019: The FCC proposed new requirements for all voice providers -- mobile, VoIP and old-fashioned landlines -- that would require them to install new technology to detect and block scam robocalls. The technology is called STIR/SHAKEN, which stands for Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted information using toKENs (SHAKEN).

The technology allows a company originating a call to verify the call is actually coming from the number on the caller ID and "sign off" on it before allowing it on its network.

Calls pass through different networks and different providers. Think of it like handing off a baton in a relay race. The calls travel through networks in seconds.

Robocalls have declined by 29 percent since June

There are four types of robocalls: scams; telemarketing; alerts; and payment reminders. All scam calls are illegal and many telemarketing ones are as well. There were 1.5 billion scam calls in August.
This chart shows scam calls have been dropping since June and are at their lowest level in three years, except for the first three months of the pandemic when call centers worldwide were mostly shut down.



Source: YouMail

Scam calls should get blocked along the route by any carrier whose caller ID technology flags the call. But call-blocking works best when the carrier originating the call doesn't allow it to begin with. [23]

The FCC gave phone carriers until June 30, 2021, to install the robocall-detecting technology.

With caller ID authentication, the hope is that the majority of scam calls will get blocked and the ones that get through will be labeled as possible scam so consumers either won't answer or will be suspicious. Over time, then, scam calls shouldn't be as effective and the con-artists will stop calling. That's the theory.

"Yes, we believe identifying that someone is truly calling from the number on the caller ID will help reduce the number of erroneous calls people receive," Chris Serico, spokesman for Verizon, which offers both mobile and landline service, told PIRG.

Because robocalls in general, and scam calls in particular, are such a huge problem, Congress on Dec. 30, 2019, passed the TRACED Act, giving the FCC the authority to enforce the caller ID verification rules. (TRACED stands for Telephone Robocall Abuse Criminal Enforcement and Deterrence Act.) [24]

June 30, 2021, was the deadline to implement the caller ID technology, although carriers with fewer than 100,000 customers or that have non-internet/cable phone lines have an extension. For now, that extension is until June 2023, but the FCC and the attorneys general in all 50 states want to move that up to June 2022 for many, if not all companies. "If the smaller providers weren't a big part of the problem, maybe a little more time would be warranted," Ohio Attorney General Dave Yost said in a statement. "But robust enforcement isn't going to happen until the same rules apply to all of them."

"If some of these calls didn't work, nobody's phone would be ringing."
Aaron Foss,
Founder of Nomorobo

The FCC originally approved the 2023 deadline but now says that for some smaller providers, there is "new evidence indicating that they are originating a high and increasing quantity of illegal robocalls." [25]

Foss of Nomorobo said robocalls will likely decline but will continue to be a significant problem until virtually all carriers have strong systems. Robocallers will pounce on "the weakest link in the chain," he said, meaning the smaller carriers that don't have strong caller ID detection. [26] While larger carriers with strong caller ID could block the calls, it's likely some will slip through, especially if the robocallers change numbers often enough to avoid suspicion.

Authorities hope robocallers will be deterred as more companies adopt caller ID verification systems, Paloma Perez, press secretary for FCC Acting Chairwoman Jessica Rosenworcel, told PIRG. [27]

"When small voice service providers and others with additional time for implementation must put STIR/SHAKEN in place, STIR/SHAKEN should become more effective," Perez told PIRG, adding: "To speed up this process, the FCC has proposed accelerating the implementation deadline for some small providers that are particularly likely to be the source of illegal robocalls."

The FCC has also stressed an important promise: For any carrier that hasn't converted to strong caller ID and is still allowing too many illegal robocalls, then the FCC may fine them or force them to convert, even if that means switching their old-fashioned lines to internet/ cable lines. On the fines, "I do think they're going to do that," said Quilici of YouMail. "It will shut down small guys who can't afford to pay the fine. Other guys will look at it as a cost of doing business. Even with a huge fine, they still make money."

The modern-day robocall became illegal on Sept. 1, 2009, when the FTC started prohibiting prerecorded telemarketing calls to anyone who hadn't agreed to the calls in writing.

Where we are

The FCC is done asking, prodding and urging. The telecommunications regulator has public sentiment on its side and, more importantly, the blessing of Congress to fight robocalls.

Here's the line in the sand: "Beginning September 28, 2021, providers can only accept calls directly from a voice service provider if that provider's filing appears in the Robocall Mitigation Database," Perez said.

This is big.

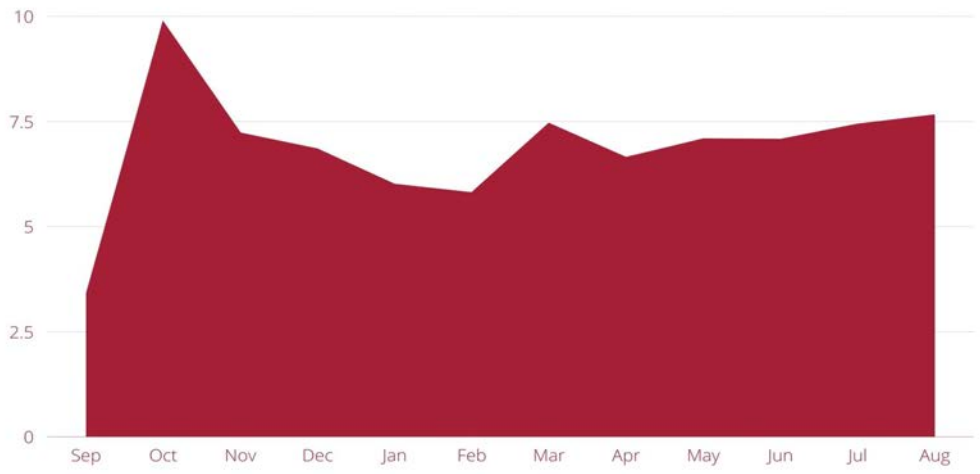
It doesn't mean companies must have adopted caller ID verification. But it must report its status to the FCC on the public database, or else other carriers must block calls from that company. While June 30 was the deadline, there's been an informal grace period of sorts for 90 days. That ends Sept. 28.

Quilici of YouMail said he believes the threat is real. "Starting Sept. 28, I think you'll start seeing more calls get blocked," he said.

For sure, the FCC database has been growing daily as companies flock to report their status as required. The list as of this month includes 3,659 phone company submissions, including, somewhat humorously, holding companies and divisions that don't necessarily need to

Robotexts are climbing

With the crackdown on robocalls, scammers are turning to robotexts. They've been rising for the last four months, to their highest level since the month before last year's election. In August, 7.65 billion robotexts were sent nationwide. Monthly numbers are are in billions.



Source: RoboKiller

report their robocall-fighting status. [28] They're being cautious. "Given the traffic blocking rule, we anticipate that many providers are very likely to file in the (Robocall Mitigation Database) against the threat of having their traffic blocked," Perez said.

For those that haven't adopted STIR/SHAKEN and are relying on their own robocall mitigation methods, the FCC isn't giving points for effort. The methods must work, Perez said. "If we find that a robocall mitigation program is ineffective or that a provider still originates illegal robocalls, we may take enforcement action.

"Enforcement actions may include removing an unsatisfactory provider from the Robocall Mitigation Database -- thereby requiring other providers to block their traffic," Perez said.

As mentioned, the FCC could also require a provider to adopt stronger robocall-blocking standards, or pay a penalty, or force the company to convert its network to internet/cable lines so it can install STIR/SHAKEN.

This could include companies that have adopted the caller ID verification on most of their network, but not the part that doesn't go through internet /cable lines. AT&T and Verizon are among those without STIR/SHAKEN on small parts of their networks.

Overall, the major mobile phone companies are doing the most to curtail robocalls and started years ago. AT&T, Verizon and T-Mobile combined have 99 percent of the cellphone market.

Verizon actually upgraded most of its network to STIR/SHAKEN caller ID verification in March 2019, more than two years before the deadline. As of the June 30 deadline, Verizon said it blocked more than 13 billion unwanted calls. It relies on analytics to identify sources of robocalls.

"We then take action, which could include stopping doing business with those network sources," Serico of Verizon told PIRG. "Those efforts have led to a reduction of 500 million calls per month on our network -- the vast majority of which are robocalls." Verizon also offers a free "call filter" that customers can use to set levels of spam detection to send suspicious calls directly to voicemail, or allow calls from certain numbers.

Interestingly, Verizon has also created "honey pots," or phone numbers in every state that are plants to receive the same illegal robocalls we all get. Verizon works with law enforcement to pursue charges against scam artists that are trying to profit from fraudulent or illegal robocalls.

T-Mobile, meanwhile, started warning customers back in 2017 about which calls may be scam robocalls, with an on-screen alert. T-Mobile started implementing call verification in 2019 and was among the first

to adopt the full STIR/SHAKEN caller ID technology in March. [29] T-Mobile and AT&T worked together early on to test the technology between networks.

In addition, T-Mobile blocks "known scam calls" by default, spokeswoman Katie Recken told PIRG. The company also displays the word "verified" or a checkmark on the phone screen when customers receive a call that's been verified as authentic and isn't spoofed, she said. T-Mobile gives customers the option of going a step further and filtering all suspected illegal robocalls and sending them straight to voicemail.

AT&T rolled out its "call protect" service for cellphone customers in 2019 to automatically block scam calls and offer on-screen spam alerts. [30] As of June, the company says it is blocking or labeling more than 1 billion calls a month. [31]

Many large companies that provide landlines, usually through internet or cable service, also offer extra services at no charge to customers. But much of the robocall-blocking is premised on detecting numbers that originate thousands or millions of calls in minutes, or that can't be verified as coming from the number on the caller ID, or that get reported as robocalls by consumers actually receiving the calls.

The latter point touches on one of the biggest challenges faced by any robocall-detection software: Robocallers latch on to a phone number, make millions of scam calls in a few minutes, then ditch the number. If the number started getting blocked, it doesn't matter because they're not using that number anymore.

It's the issue with verified phone numbers that could prove difficult in the short term. Robocallers can actually buy the use of verified phone numbers to increase the chances of their calls going through. "It's a real threat," said Quilici of YouMail. "It's clear that it's already starting."

"Beginning September 28, 2021, providers can only accept calls directly from a voice service provider if that provider's filing appears in the Robocall Mitigation Database."
Paloma Perez
FCC spokeswoman

What's next?

If all of us are cheering at the prospect of fewer robocalls, there's reason to temper our enthusiasm because there are two big threats on the horizon as robocallers pivot from their past strategies.

First, robotexts are on the rise. RoboKiller, another leading robocall filtering company, said we got 7.65 billion spam text messages in August. That's up 8 percent, from 7.07 billion in June. [32]

"We've seen a huge rise in text message scams," agreed Foss of Nomorobo, which also filters text messages for customers.

Some of the most common scam texts this year: An unemployment claim has been filed in your name, or your unemployment benefits are stopping. Whether you've been collecting unemployment or not, the message would likely startle you and maybe make you curious enough to click on the link in the message. That would take you to a website that would look just like your own state's unemployment office website, Foss said.

"How can you tell the difference? You really can't," he said. The server might be somewhere in Russia, or certainly controlled by someone focused on doing you harm, he said. Once you put in your Social Security number or other personal information, the thief is off to the races.

Another popular text scam right now: Anything involving Amazon, especially something supposedly involving delivery of your package. Anything to cause you to suspend your normal caution and click on a link in the text. These texts don't usually lead you to phishing sites, Foss said.

"They're usually trying to get you to buy something. They tell you, 'You've won!' Anything to get you to click through." If you do click through, it may be an effort to sell you some product or sign you up for a subscription.

"You kind of forgot about how you got there in the first place," Foss said. "This just has to work once or twice a day."

He noted that purchases like these can be more difficult to dispute with a credit card company if you actually ordered the product or subscription in a moment of weakness. It's not exactly fraud.

"If you want to buy something stupid, this is America. You can do it." Foss said.

Perez at the FCC said the current caller ID authentication doesn't include text messages.

"However, industry standards groups are in the early stages of working on authentication for text messages," she said.

Perez noted that complaints to the FCC about texts are up 35 percent from three years ago. That includes all unwanted texts, not just scams.

Foss said carriers don't necessarily have any incentive to control robotexts, particularly because they can make money from the senders. He noted that phone companies charge more for text messages with short codes than long codes.

Citing RoboKiller, Perez of the FCC added that spam text messages are expected to reach 86 billion for all of 2021, a 55 percent jump from last year. [33]

The second threat is more of what we've seen for a few years: Targeted scam calls, in which the caller knows your name, maybe your Social Security number and your date of birth, where you bank, who some of your relatives are and where they live. These are all the ammunition a con-artist needs to impersonate someone and convince you to provide more information such as bank account passwords or even to go buy untraceable gift cards to pay supposed tax bills or post bail for a grandson in trouble.

Much of this information has been compromised in data breaches over the last decade: A slew of retailers from Target to Home Depot, health insurance companies and even the Internal Revenue Service. Then there's the infamous Equifax data breach of 2017 that exposed detailed, personal information for half of the adults in the United States. [34] [35]

Identity thieves can fill in many of the gaps from information we provide willingly, often through social media: where we went to high school, what our hobbies are and all of the cities where we've lived before.

Quilici of YouMail predicts that robocalls may decrease over the next year, but the ones we get will be creepier, especially when it comes to health information.

There are already databases for sale on the dark web of people who likely have dementia or have had knee surgery, he said.

What happens when a scammer takes a list of Alzheimer's patients and crosses that with a database of Social Security numbers or other personal information?

That's when identity thieves specifically target people with cognitive issues and scare them into taking some action, he said. "They could call and pose as the Social Security Administration and say, 'Hey, you're going to lose your benefits ' . . . It's clearly doable." Then the recipient could be persuaded to disclose bank account information or any number of pieces of data that could hurt the consumer.

"I'm really worried about imposter calls," Quilici added.

Conclusion

Dishonest people have been around since the beginning of time. Cons in various forms have existed for all of our lives and will continue. We still get phishing emails and postcards about free dinners or prizes we've "won." The cons just take different forms over time. Everyone needs to do more to protect themselves and others.

Recommendations:

1. The FCC must follow through with its promise to monitor how effectively all providers are reducing/ blocking robocalls. If a given phone company's system isn't working, they'll need to try something else or be forced to upgrade to internet/cable lines so they can implement the industry standard caller ID.

2. The FCC should move up the deadline for smaller providers and those with non-internet/ cable lines to comply with STIR/SHAKEN. It's currently June 2023. It should move up to June 2022 at the latest, as all 50 attorneys general have recommended.

3. In addition to implementing STIR/ SHAKEN, phone companies should offer customers an array of free services to provide more protection, such as:
* Extra filters that send suspected scam calls to voicemail.
* On-screen warnings for suspicious calls or unverified numbers.
* Filters that block calls with no caller ID and white lists of numbers that can call through. This can be immensely helpful for children, the elderly and anyone with cognitive issues.

4. Consumers who want to reduce the number of illegal robocalls should ask their phone company whether there are additional services, as mentioned in the previous paragraph, that are available to protect them.

5. Consumers whose phone companies don't provide the protections they want should shop around for a one that better meets their needs.

6. Phone providers and the FCC need to address the growing problem of robotexts.

7. We must all do more to protect our friends and relatives, especially the most vulnerable. We should occasionally strike up conversations with loved ones about scams that are out there and make sure they know they can talk to us if there's ever a question about a call or text message they received.

8. We should never belittle people who fall for scams. We need to eliminate the stigma so people feel free to reach out for help.

9. Consumers should report violations:

* Report robocalls to the FCC.

* Report unwanted calls to your state attorney general. Here's a list of the attorney general's contact information in every state.

Methodology

The U.S. PIRG Education had a goal of discovering how many voice providers nationwide are complying with the Federal Communications Commission's (FCC) requirements regarding STIR/SHAKEN, the industry's name for sophisticated caller ID verification, which is aimed at reducing robocalls.

STIR/SHAKEN compliance

Voice providers are required by the FCC to report their status as it relates to implementation of STIR/SHAKEN technology. The deadline to report was June 30, 2021. As of Sept. 28, 2021, companies will be prohibited from completing calls from other companies that aren't in the database.

The FCC's Robocall Mitigation Database was downloaded by PIRG Education Fund on Sept. 3, 2021. It contained 3,659 listings. Of those:

- 536 said they'd completed STIR/SHAKEN implementation.
- 817 said they'd partially implemented STIR/SHAKEN and were performing robocall mitigation.
- 1,710 said they had not implemented STIR/SHAKEN but were performing robocall mitigation.
- 596 said the question about implementation was not applicable because they're intermediate providers that don't originate calls.

When you subtract the 596, that leaves 3,063 companies that reported their status to the FCC as of Sept. 3 and didn't claim an exemption from submitting information.

Surveying the major phone companies nationwide

PIRG Education Fund set out to discover the compliance levels among the major phone companies nationwide, both mobile carriers and landlines, most of which rely on internet/cable service. However, companies don't have to report information about their numbers of customers, the FCC says.

To build a list of major companies nationwide, we relied on the population covered by each company, whether in one state or multiple states added together. We included all voice providers with a population reach of at least 1 million, which of course doesn't mean the company has 1 million customers.

We used the website broadbandnow.com to compile the population reach and the states where each company is able to operate.

49 companies have a population reach of at least 1 million.

Survey of additional services

In June, we started contacting each of the 49 companies by email or phone or both to learn whether they offer additional services that customers can use to better protect themselves from unwanted calls. Most of these services were permitted by the FCC only in the last three years. For those companies that didn't respond in a timely manner, we contacted them again in July and/or August.

Most of the 20 companies with the largest population reach responded with the information we requested. Few of the remaining 29 responded.

APPENDIX 1 - 20 OF THE LARGEST PROVIDERS NATIONWIDE STIR-SHAKEN COMPLIANCE AND EXTRA SERVICES OFFERED

Company	Status of strong Caller ID implementation as required by law	Block some known scam calls/spoofed numbers by default as allowed by FCC (since 2019)	Warn on screen that call may be spam or scam, as allowed by FCC	Offer "verified number" or check mark display on screen	Allow customers to opt in and block illegal robocalls through single source	Allow customers to blocks all calls with no Caller ID	Offer white list, as allowed by FCC since 2019	Inform customers of services available to reduce unwanted calls?
AT&T Mobile and VoIP (1)	**Partial - Performing robocall mitigation to supplement**	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Verizon Mobile and VoIP	**Partial - Performing robocall mitigation to supplement**	Yes	Yes	Sometimes	Yes	No (2)	Yes	Yes
T-Mobile	**Complete STIR/SHAKEN Implementation**	Yes	Yes	Yes	Yes	No	No	Yes
US Cellular	**Partial - Performing robocall mitigation to supplement**	Yes	Yes	No	No (3)	In some cases.	No	Yes
Metro by T-Mobile (formerly Metro PCS)	**Complete STIR/SHAKEN Implementation**	Yes	Yes	Yes	Yes	No	No	Yes
XFINITY from Comcast	**Complete STIR/SHAKEN Implementation**	Yes	No (planned before year-end)	Yes	No (planned before year-end)	Yes	No	Yes
Spectrum Voice (Charter Communications)	**Complete STIR/SHAKEN Implementation**	Yes	Yes	No	Yes	Yes	Yes	Yes
Century Link	**Partial - Performing robocall mitigation to supplement**	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond
Frontier Communications	**Partial - Performing robocall mitigation to supplement**	Yes, blocks do-not-originate numbers.	Yes	No. In process	Yes, through Nomorobo	Yes	Yes	Yes
Rise Broadband	**Partial - Performing robocall mitigation to supplement**	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond
Cox Communications	**Partial - Performing robocall mitigation to supplement**	Yes, blocks do-not-originate numbers.	No	In process; expected by Oct.	No (planned before year-end)	Yes	No	Yes
Windstream	**Complete STIR/SHAKEN Implementation**	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond
Optimum by Altice	**Complete STIR/SHAKEN Implementation**	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond
Wide Open West (WOW)	**Complete STIR/SHAKEN Implementation**	Yes	Yes	No	Yes	Yes	Yes	Yes
Mediacom Cable	**Partial - Performing robocall mitigation to supplement**	Yes	No	No	Yes	Yes	No	No
Suddenlink Communications	**Complete STIR/SHAKEN Implementation**	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond
Nextlink	Did not respond; not in FCC database	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond
Consolidated Communications	**Partial - Performing robocall mitigation to supplement**	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond	Did not respond
RCN	**Partial - Performing robocall mitigation to supplement**	Yes	No, but expect to by end of 2022.	No, but will begin in mid-2022.	No, but planned before year-end.	Yes	Yes	Yes
C Spire Wireless (Parent is Telapex Inc.)	**Partial - Performing robocall mitigation to supplement**	Yes	No, but in process	No	No	No	No, but in process	Did not respond
(1) With AT&T VoIP, some services require opt-in to Call Protect.	(2) Available to mobile customers through Smart Family service for $4.99 a month; available to some VoIP customers	(3) Highest risk calls blocked automatically. For $3.99/month, customers can set up additional blocks based on risk level.						

SOURCES: FCC AND COMPANY RESPONSES TO PIRG SURVEY

APPENDIX 2
49 OF LARGEST PROVIDERS NATIONWIDE STIR-SHAKEN COMPLIANCE

Company	Status of strong caller ID verification as of Sept. 3
AT&T Mobile	**Partial - Performing robocall mitigation to supplement**
Verizon	**Partial - Performing robocall mitigation to supplement**
T-Mobile	**Complete STIR/SHAKEN Implementation**
US Cellular	**Partial - Performing robocall mitigation to supplement**
Metro by T-Mobile (formerly Metro PCS)	**Complete STIR/SHAKEN Implementation**
XFINITY from Comcast	**Complete STIR/SHAKEN Implementation**
Spectrum Voice (Charter Communications)	**Complete STIR/SHAKEN Implementation**
Century Link	**Partial - Performing robocall mitigation to supplement**
Frontier Communications	**Partial - Performing robocall mitigation to supplement**
Rise Broadband	**Partial - Performing robocall mitigation to supplement**
Cox Communications	**Partial - Performing robocall mitigation to supplement**
Windstream	**Complete STIR/SHAKEN Implementation**
Optimum by Altice	**Complete STIR/SHAKEN Implementation**
Wide Open West (WOW)	**Complete STIR/SHAKEN Implementation**
Mediacom Cable	**Partial - Performing robocall mitigation to supplement**
Suddenlink Communications	**Complete STIR/SHAKEN Implementation**
Nextlink	Not in FCC Robocall Mitigation Database
Consolidated Communications	**Partial - Performing robocall mitigation to supplement**
RCN	**Partial - Performing robocall mitigation to supplement**
C Spire Wireless (Parent is Telapex Inc.)	**Partial - Performing robocall mitigation to supplement**
TWN Communications	Not in FCC Robocall Mitigation Database
Sparklight	**Complete STIR/SHAKEN Implementation**
Ranch Wireless	Not in FCC Robocall Mitigation Database
WATCH Communications	**Partial - Performing robocall mitigation to supplement**
BarrierFree	Not in FCC Robocall Mitigation Database
Nextera Communications	**No STIR/SHAKEN Implementation - Performing robocall mitigation**

APPENDIX 2 CONTINUED
49 OF LARGEST PROVIDERS NATIONWIDE STIR-SHAKEN COMPLIANCE

Company	Status of strong caller ID verification as of Sept. 3
Google Fiber	**Complete STIR/SHAKEN Implementation**
Sonic	**Complete STIR/SHAKEN Implementation**
Stimulus Technologies	**Partial - Performing robocall mitigation to supplement**
TDS Telecom	**Partial - Performing robocall mitigation to supplement**
Wave Broadband (part of RCN)	**Partial - Performing robocall mitigation to supplement**
Metronet	**Complete STIR/SHAKEN Implementation**
lv.net	Not in FCC Robocall Mitigation Database
cal.net	Not in FCC Robocall Mitigation Database
ERF Wireless	Not in FCC Robocall Mitigation Database
Atlantic Broadband	**Complete STIR/SHAKEN Implementation**
Mercury Wireless	**Complete STIR/SHAKEN Implementation**
Cincinnati Bell	**Partial - Performing robocall mitigation to supplement**
KwiKom Communications	**Complete STIR/SHAKEN Implementation**
Aerux Broadband	Not in FCC Robocall Mitigation Database
Grande Communications	**Partial - Performing robocall mitigation to supplement**
Ziply Fiber	**Complete STIR/SHAKEN Implementation**
Surf Broadband Solutions	**No STIR/SHAKEN Implementation - Performing robocall mitigation**
Hawaiian Telcom	**Partial - Performing robocall mitigation to supplement**
Rock Solid Internet and Telephone	Not in FCC Robocall Mitigation Database
Blast Communications	**No STIR/SHAKEN Implementation - Performing Robocall Mitigation**
North Coast Wireless Communications	Not in FCC Robocall Mitigation Database
E-Vergent Wireless	**No STIR/SHAKEN Implementation - Performing Robocall Mitigation**
Argon Technologies	Not in FCC Robocall Mitigation Database

SOURCE: FCC

APPENDIX 3
49 of the largest voice providers nationwide

Largest mobile providers nationwide (these make up 99% of mobile market share)
AT&T
Verizon
T-Mobile
US Cellular
Metro PCS

Landline providers (Voice over Internet Protocol, meaning phone lines that run through internet or cable lines, or traditional landlines) Ranked by population reach.

XFINITY from Comcast

State(s): Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Idaho, Illinois, Indiana, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin

Spectrum

State(s): Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming

BarrierFree

State(s): Connecticut, District of Columbia, Maryland, New Jersey, New York, Pennsylvania, Rhode Island, Virginia

Century Link

State(s): Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming

Frontier Communications

State(s): Alabama, Arizona, California, Connecticut, Florida, Georgia, Illinois, Indiana, Io Michigan, Minnesota, Mississippi, Nebraska, Nevada, New Mexico, New York, North Carolina, Ohio, Pennsylvania, South Carolina, Tennessee, Texas, Utah, Washington, West Virginia, Wisconsin

Rise Broadband

State(s): Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, Wyoming

Cox Communications

State(s): Arizona, Arkansas, California, Connecticut, District of Columbia, Florida, Georgia, Idaho, Iowa, Kansas, Louisiana, Massachusetts, Nebraska, Nevada, North Carolina, Ohio, Oklahoma, Rhode Island, Virginia

Windstream

State(s): Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming

Optimum by Altice

State(s): Connecticut, New Jersey, New York, Pennsylvania

Wide Open West (WOW)

State(s): Alabama, Florida, Georgia, Illinois, Indiana, Kansas, Michigan, Ohio, South Carolina, Tennessee

Mediacom Cable

State(s): Alabama, Arizona, California, Delaware, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Maryland, Michigan, Minnesota, Mississippi, Missouri, North Carolina, Ohio, South Dakota, Tennessee, Virginia, Wisconsin

Suddenlink Communications

State(s): Arizona, Arkansas, California, Idaho, Kansas, Kentucky, Louisiana, Mississippi, Missouri, Nevada, New Mexico, North Carolina, Ohio, Oklahoma, Texas, Virginia, West Virginia

C Spire Fiber

State(s): Alabama, Arkansas, California, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Ohio, South Carolina, Tennessee, Texas, West Virginia

Nextlink Internet

State(s): Illinois, Iowa, Kansas, Nebraska, Oklahoma, South Dakota, Texas

Consolidated Communications

State(s): Alabama, California, Colorado, Florida, Georgia, Illinois, Iowa, Kansas, Maine, Massachusetts, Minnesota, Missouri, New Hampshire, New York, North Dakota, Ohio, Oklahoma, Pennsylvania, South Dakota, Texas, Vermont, Virginia, Washington, Wisconsin

Sparklight

State(s): Alabama, Arizona, Arkansas, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Minnesota, Mississippi, Missouri, Nebraska, New Mexico, North Dakota, Oklahoma, Oregon, South Dakota, Tennessee, Texas, Washington

WATCH Communications

State(s): Illinois, Indiana, Kentucky, Ohio

RCN

State(s): District of Columbia, Illinois, Maryland, Massachusetts, New Jersey, New York, Pennsylvania, Virginia

TWN Communications

State(s): Arizona, Indiana, New Mexico, Oklahoma, Texas

Ranch Wireless

State(s): Texas

Ziply Fiber

State(s): Idaho, Montana, Oregon, Washington

TDS Telecom

State(s): Alabama, Arizona, California, Colorado, Florida, Georgia, Idaho, Illinois, Indiana, Kentucky, Maine, Michigan, Minnesota, Mississippi, Nevada, New Hampshire, New Mexico, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington, Wisconsin

Google Fiber

State(s): Alabama, California, Georgia, Kansas, Missouri, North Carolina, Tennessee, Texas, Utah

Nextera Communications

State(s): Minnesota, Wisconsin

Wave Broadband

State(s): California, Oregon, Washington

Stimulus Technologies

State(s): Arizona, California, Missouri, Nevada

Metronet

State(s): Illinois, Indiana, Iowa, Kentucky, Michigan, Minnesota, Ohio

Sonic (Sonicnet)

State(s): California

Atlantic Broadband

State(s): Alabama, Connecticut, Delaware, Florida, Maine, Maryland, Mississippi, New Hampshire, New York, Pennsylvania, South Carolina, Virginia, West Virginia

lv.net

State(s): Nevada

ERF Wireless

State(s): Texas

Cincinnati Bell

State(s): Arizona, Arkansas, California, Florida, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Massachusetts, Michigan, Minnesota, New Jersey, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Tennessee, Texas, Utah, Virginia

Mercury Wireless

State(s): Indiana, Kansas, Michigan, Missouri, Ohio, Texas

cal.net

State(s): California

KwiKom Communications

State(s): Kansas, Missouri

Aerux Broadband

State(s): Colorado

Grande Communications

State(s): Texas

Surf Broadband Solutions

State(s): Illinois, Indiana, Michigan

Hawaiian Telcom

State(s): Hawaii

Rock Solid Internet and Telephone

State(s): Texas

Blast Communications

State(s): Illinois

North Coast Wireless Communications

State(s): Ohio

E-Vergent Wireless

State(s): Illinois, Wisconsin

Argon Technologies

State(s): Texas

Notes

1. Largest providers defined as cellular and VoIP providers that have a population reach of 1 million or more total in the states where they operate.

2. PIRG analysis of FCC Robocall Mitigation Database.

3. https://webcache.googleusercontent.com/search?q=cache:XxCQXkOPy6oJ:https://docs.fcc.gov/public/attachments/DOC-362883A1.pdf+&cd=2&hl=en&ct=clnk&gl=us

https://www.fcc.gov/document/chairman-pai-proposes-mandating-stirshaken-combat-robocalls

4. https://docs.fcc.gov/public/attachments/DOC-362883A1.pdf

5. https://www.prnewswire.com/news-releases/just-under-4-1-billion-robocalls-in-august-mark-4-monthly-drop-says-youmail-robocall-index-301368134.html?tc=eml_cleartime ;
https://www.prnewswire.com/news-releases/just-over-4-4-billion-robocalls-in-june-mark-11-monthly-increase-says-youmail-robocall-index-301327740.html?tc=eml_cleartime ;
2.1 billion scam calls in June; 1.5 billion in August.

6. PIRG research

7. https://www.prnewswire.com/news-releases/just-under-4-1-billion-robocalls-in-august-mark-4-monthly-drop-says-youmail-robocall-index-301368134.html?tc=eml_cleartime ;
https://www.prnewswire.com/news-releases/just-over-4-4-billion-robocalls-in-june-mark-11-monthly-increase-says-youmail-robocall-index-301327740.html?tc=eml_cleartime ;
2.1 billion scam calls in June; 1.5 billion in August. Difference is 28.57 percent.

8. PIRG interview with FCC, which said consumer complaints from January through June 2021 averaged about 15,500 unwanted call complaints per month. In August, the number of complaints was 14,000.

9. https://www.fcc.gov/rules-political-campaign-calls-and-texts

10. https://www.consumer.ftc.gov/articles/robocalls;
https://www.consumer.ftc.gov/blog/2019/03/robocallers-youre-out

11. https://www.news5cleveland.com/news/local-news/oh-cuyahoga/rocky- river-man-loses-over-124-000-after-2-men-pose-as-amazon-security

12. https://docs.fcc.gov/public/attachments/DOC-370869A1.pdf

13. https://www.ftc.gov/news-events/press-releases/2021/07/ftc-takes-action-against-septic-tank-cleaning-company-made

14. https://www.prnewswire.com/news-releases/americans-hit-by-just-under-46-billion-robocalls-in-2020-says-youmail-robocall-index-301215139.html

15. Interview with PIRG, August 2021.

16. YouMail

17. https://www.keoghlaw.com/the-history-of-robocalls/

18. https://www.pewresearch.org/internet/fact-sheet/mobile/

19. https://money.cnn.com/2009/05/15/news/companies/ftcsuit_robocalls/index.htm

20. https://www.ftc.gov/news-events/press-releases/2009/08/new-rule-prohibiting-unwanted-robocalls-take-effect-september-1

21. https://www.reuters.com/article/us-usa-robocalls/att-apple-google-to-work-on-robocall-crackdown-idUSKCN10U18L

22. https://www.washingtonpost.com/technology/2019/08/22/phone-companies-state-attorneys-general-announce-broad-campaign-fight-robocalls/

23. https://www.fcc.gov/call-authentication

24. https://www.congress.gov/bill/116th-congress/senate-bill/151

25. https://docs.fcc.gov/public/attachments/DOC-373714A1.pdf

26. Interview with PIRG, August 2021

27. Interview with PIRG, September 2021

28. FCC Robocall Mitigation Database

29. https://www.t-mobile.com/news/network/stir-shaken-all-networks

30. https://www.theverge.com/2019/7/9/20687720/at-t-robocalls-block-automatically-call-protect

31. https://about.att.com/story/2021/robocalls.html

32. https://www.robokiller.com/spam-text-insights/

33. https://www.prnewswire.com/news-releases/total-robocalls-decrease-by-3-in-the-first-month-of-stirshaken-release-301350380.html

34. https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car;
https://ir.homedepot.com/news-releases/2014/09-08-2014-014517970;
https://www.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/

35. https://uspirg.org/reports/usp/equifax-breach-one-year-later