RINGING IN OUR FEARS

One year after new law, robocalls are down and phone company compliance is up, but skyrocketing robotexts are the latest problem

U.S. PIRG Education Fund

RINGING IN OUR FEARS

One year after new law, robocalls are down and compliance is up, but skyrocketing robotexts are the latest problem

WRITTEN BY:

TERESA MURRAY

U.S. PIRG EDUCATION FUND

JULY 2022

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:

- Alex Quilici, CEO of YouMail.
- Aaron Foss, founder of NomoRobo.
- Federal Communications Commission media relations office
- Margot Saunders, senior counsel, National Consumer Law Center

Thanks also to James Horrox of Frontier Group 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: U.S. PIRG Education Fund photo illustration, using photo by JESHOOTS-com via Pixabay

CONTENTS

EXECUTIVE SUMMARY

Riley Williams II thought the year-old federal law that was supposed to reduce scam robocalls was working alright. For the last year, the Oklahoma pharmacist had been getting only four or five calls a week on his cell phone marked as "scam likely." He never answered them. They often didn't leave messages.

But in the last month, the volume has doubled or tripled, to 10 to 15 robocalls per week. And they're leaving messages: It's someone asking whether he wants to sell his house (or more likely defraud him). His bank account needs attention. (Yeah, sure.) Some of the messages are in Chinese, which he doesn't speak.

Williams has also seen a similar increase in robotexts, which aren't directly covered by the federal law that took effect on June 30, 2021.

The calls and texts are annoying. They're time-suckers. He wants them to stop.

Don't we all.

Meanwhile, Bill Rucki of Ohio has enjoyed more consistent improvement. The retired electrical engineer used to get 10 to 20 spam robocalls a day on his cellphone last year and about the same volume on his home phone. Now he's down to one or two a day on his cell and a half-dozen on his landline. "It's been in the last six months that I really noticed it," he says happily.

While even one unwanted call is bad, there indeed is some good news in this years-long effort by regulators and lawmakers to fight one of American consumers' biggest problems:

- The number of voice providers that have installed the preferred robocall-blocking technology has nearly quadrupled since last year, according to U.S. PIRG Education Fund's new analysis of the Federal Communications Commission's robocall database.
- Scam robocalls nationwide have declined by about 47 percent since last June, according to YouMail, one of the largest robocall- and robotext-blocking companies in the United States.
- More cellphone and home phone companies are filtering calls and offering customers new services such as flagging suspicious calls to give the receiver the choice of answering, sending them to voicemail or blocking them.
- Regulators are requiring phone companies that serve as "gateway" providers – which often funnel scam calls from overseas – to do more to block them.
- Regulators are requiring smaller phone providers, which didn't have to follow the robocall technology rules last year, to now comply just like large companies. All 50 attorneys general last year pushed the FCC to crack down on small companies, which originally had exemptions until June 2023, because scam callers were leveraging the income-hungry small providers to bypass technology installed by large companies.
- The FCC has started partnering with state attorneys general on robocall investigations, sharing information and using the criminal enforcement

powers of states, which often can respond more nimbly. Just two weeks ago, the FCC and the Ohio attorney general worked together to go after one robocall operation that they allege is responsible for 8 billion illegal robocalls since 2018, most about auto warranties.
- The Federal Communications Commission (FCC) has taken enforcement action against two companies on grounds they didn't install the required Caller ID technology last year. It's only two out of hundreds who may not be complying, but it's a step.

Meanwhile, if you have either a cellphone or home phone, there's bad news too.

- Scam robocalls have declined by many measures, but they should have decreased more.
- Robotexts have increased twelvefold in the past year, from about 1 billion to 12 billion per month, according to RoboKiller. Con artists and identity thieves are taking advantage of loopholes in the law and the fact that consumers may have difficulty distinguishing a genuine text from a fake one, according to YouMail.
- The chair of the Federal Communications Commission (FCC) submitted a proposal in October 2021 to pass rules to attack robotexts. However, the full FCC hasn't yet acted on it.
- Nearly one-fourth of phone companies have older equipment on at least part of their systems that they tell the FCC keeps them from installing the industry-standard robocall-detecting technology.

Alex Quilici, CEO of YouMail, told PIRG the new law has been "a speed bump" for robocalls, especially scam calls. "But those are coming back," he said.

In the meantime, 80 percent of cellphone owners say they typically don't answer calls from an unrecognized phone number, according to Pew Research Center. While inconvenient and annoying, until the FCC cracks down on robocalls further, that may be the best way to avoid becoming one of the millions of people ripped off every year by a scam call.

WHAT IS A ROBOCALL?

Not all robocalls are illegal or even bad. Robocalls refer to phone calls that contain prerecorded or artificial voice or are made with help from software that does the dialing, using numbers from a database or by just dialing numbers at random.
There are four basic categories of robocalls:
Scams: *Any call that tries to deceive you about who is actually calling, or tries to trick you into providing personal information or buying something.*
Reminders/alerts: *Calls we ask for or at least consent to. We have a doctor's appointment this week. Our child's school is closed. A large purchase posted to our credit card account.*
Payment reminders/overdue bills: *Generally legal calls that we were notified about, whether we remember or not, generally involving overdue payments on loans or credit cards.*
Telemarketing: *Most of these are probably illegal, if the recipients didn't opt in to the calls or are on the Do Not Call Registry or both.*

A BRIEF HISTORY

Robocalls refer to phone calls that contain a prerecorded or artificial voice *or* are made with help from software that does the dialing, either using numbers from a database or by just dialing numbers at random. There are good robocalls (the ones we request and that help us), bad robocalls (the ones we don't want but aren't directly harmful besides wasting our time) and really dangerous robocalls (the ones trying to steal our money or our personal information).

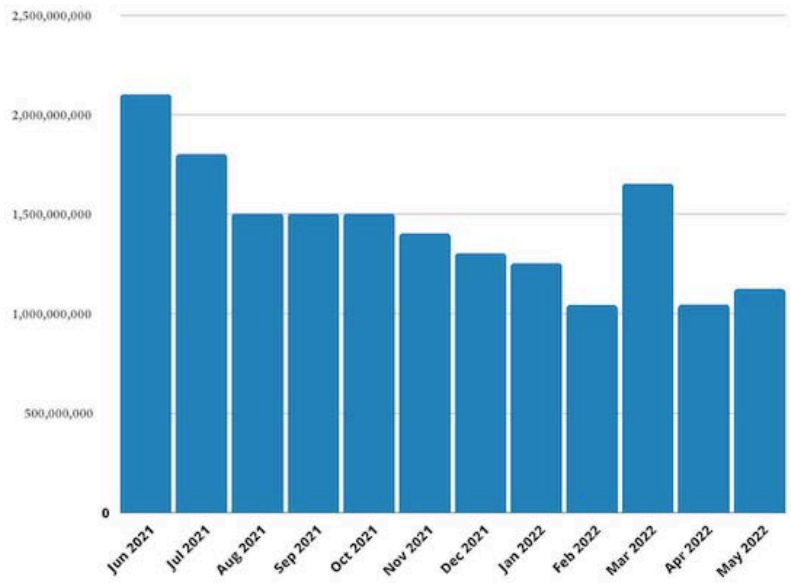
While most auto-dialed calls made without your permission with pre-recorded messages have been illegal for decades, the robocall as we know it became illegal on Sept. 1, 2009. That's when the FTC started prohibiting prerecorded telemarketing calls to any consumers who hadn't agreed to the calls in writing. (Consent can come from checking an authorization on an online form.)

Scam robocalls started becoming a monstrous problem in roughly 2006 – when cell phone ownership among adults hit 73 percent. Yet it took federal regulators, lawmakers and industry giants a decade to get serious about combating illegal robocalls by giving phone companies more leeway to block spoofed or suspected scam calls. But the voluntary measures did little if any good.

It wasn't until 2019, with Congress' passage of the bi-partisan TRACED Act, that we thought we were entering a new chapter. The TRACED Act led to the FCC requiring phone companies to install technology to identify whether calls are actually coming from the phone number on the Caller ID. (The industry standard technology is called STIR/SHAKEN; the standards provide "a common information-sharing language between networks to verify Caller ID information," the FCC says.) This helps phone companies determine whether the call should be blocked or flagged as a scam or spam call and helps consumers decide whether to answer the call.

But the technology only works if it's installed. And the entire system really only works well if every link in the phone chain is using the same technology.

Scam robocalls are down but not gone



Source: YouMail

PHONE COMPANY COMPLIANCE SOARS

That brings us the milestone we reached a year ago. June 30, 2021 was the deadline for most companies to install robocall-fighting technology and register on the FCC's public Robocall Mitigation Database and tell the FCC where they stand with Caller ID verification. Then there was a 90-day grace period until Sept. 28, 2021, or else their calls could be blocked.

Compliance as of September was unimpressive. Only 536 phone companies – 17 percent of those that didn't claim exemption – told the FCC they'd completely implemented the STIR/SHAKEN Caller ID technology.

Now, as of June 30, 2022, that number has nearly quadrupled, to 1,932 companies. That's nearly 2,000 phone companies nationwide that tell the FCC they've installed technology that verifies whether the calls are being spoofed.

Meanwhile, 817 companies said they'd partially implemented the technology last September. That has nearly doubled to 1,518 companies now.

Partial implementation generally means a company hasn't installed STIR/SHAKEN on the non-Internet-Protocol part of their networks. It's actually impossible for a company to have the STIR/SHAKEN technology on its non-IP lines, the FCC says. Instead, the companies are expected to figure out another way to squash illegal robocalls for now and tell the FCC what that plan is.

Here are the full results of our analysis of the FCC database this month:

- **7,514 phone providers registered.**
- **6,512 didn't claim exemption from anti-robocall technology.**

Of those not claiming exemption:

- **1,932 (29.7%) have completed the industry-standard STIR/SHAKEN technology, up from 536 companies last year.**
- **1,518 (23.3%) have partially completed the industry-standard STIR/SHAKEN technology, up from 817 companies last year.**
- **3,062 (47%) haven't implemented STIR/SHAKEN but are using their own robocall mitigation system. That compares with 1,710 companies last year. The increase reflects companies that didn't report their status last year.**

The FCC says it's pleased with what it categorizes as "widespread compliance" with both installation of Caller ID technology and registering with the database.

Also encouraging: The number of companies that have actually registered with the database has more than doubled, from 3,659 in September to 7,514 this month. Yes, they were supposed to do this last year. But they didn't before. Now, they have, likely for a variety of reasons.

It's curious, though, that the FCC had threatened last year to block phone calls from companies that hadn't at least registered on the database, regardless whether they'd installed robocall-fighting technology.
Yet not a single company has been prohibited from making phone calls for not registering with the database, according to an FCC spokesman. The FCC declined to comment on the reason no companies have been blocked from processing calls.

Quilici of YouMail, said in an interview that he's not surprised unwanted robocalls haven't decreased more. Yes, the vast majority of major cell phone and VoIP (voice over internet protocol) providers say they're using STIR/SHAKEN or some other new technology to fight illegal robocalls.

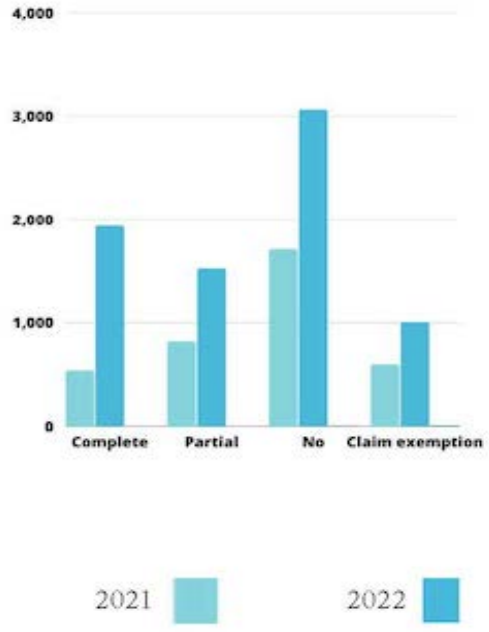
But the companies using their own system may be using inferior technology, Quilici said.

"An awful lot – 40 to 50 percent of all calls – still don't go through STIR/SHAKEN," he said. That likely will decrease as traffic gets blocked, either blocked because the company hasn't registered with the FCC or blocked because the company used to be exempt but now it's not, he said.

While the FCC hasn't outright blocked any companies yet, it has, however, sent quite a few cease and desist letters, 18 to be exact, as of March 2022, to companies the FCC believes are transmitting illegal robocalls. The letters demand that the companies stop allowing the robocalls immediately and tell the FCC what they're doing to make sure it doesn't happen again.

Companies install robocall-fighting technology

Phone providers are required to install new technology to verify whether calls are coming from the number displayed. Here are the numbers of companies nationwide that installed industry standard STIR/SHAKEN technology in all of their network, part of it, none of it or claim they don't have to.



Source: U.S. PIRG Education Fund analysis of FCC database

A typical letter says, in part:

We have determined that xxx is apparently transmitting illegal robocall traffic on behalf of one or more of its clients. You should investigate and, if necessary, cease transmitting such traffic immediately and take steps to prevent your network from continuing to be a source of apparently illegal robocalls. As noted below, downstream voice service providers will be authorized to ***block all*** *of xxx's traffic if you do not take steps to "effectively mitigate illegal traffic" within 48 hours, or if you fail to inform the Commission and the Traceback Consortium within fourteen (14) days of this letter of the steps you have taken to "implement effective measures" to prevent customers from using your network to make illegal calls.*

In addition, the FCC has taken action against two companies. In February, the FCC said Bandwidth Inc. of North Carolina and Vonage Holding Corp. of New Jersey lost their partial exemptions from STIR/SHAKEN because they didn't meet the "implementation commitments" of the June 30, 2021, deadline. They were also referred to the FCC's Enforcement Bureau for additional investigation.

"Those are big names," Aaron Foss, founder of Nomorobo, one of the nation's largest robocall-filtering software companies, told PIRG. "I think this will show that the FCC isn't just messing around. They mean business."

In a statement at the time, FCC Chairwoman Jessica Rosenworcel said, "We will not turn a blind eye to providers that have not done enough to protect consumers from spoofed robocalls."

To be sure, calls don't have to be spoofed to be illegal or potentially fraudulent. But spoofed calls are the worst problem. Consumers are more likely to pick up a call when it looks like it's local, for example, and more likely to fall for a scam when the call looks like it's coming from a major bank or a government office.

Frankly, if a call is spoofing another number, that alone is reason to be suspicious and strongly consider blocking the call. If the caller has good intentions, why would they want to make you think it's someone else calling?

Unwanted robocalls have been the No. 1 complaint to the FCC for years, and lead to $10 billion a year in fraud, according to the Federal Trade Commission (FTC). The calls cost consumers an additional $3 billion a year in wasted time, according to the FCC, when you consider all of that time spent answering unwanted calls, blocking calls, reporting the calls to authorities and generally getting distracted from whatever you were doing.

WHAT KIND OF PHONE LINE U.S. ADULTS HAVE

(July–December 2021)

68.7 percent – Only cell phone
28.9 percent – Cell and landline
1.7 percent – Landline only
0.6 percent – No phone

Source: https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless202205.pdf

MORE PHONE COMPANIES LABEL SPAM

Most major cell phone and home phone companies are doing a better job of flagging calls that appear suspicious by labeling them "potential spam," "likely scam" or something similar. That helps the person getting the call realize it could be trouble.

For example, at Verizon, all postpaid cell phone customers as of February can choose to send calls flagged as "potential spam" directly to voicemail or block the call completely. And home phone customers whose service goes through the internet will see a "V" on the screen for calls that are verified that they're actually coming from the number displayed.

At AT&T, the company says it's using artificial intelligence and machine learning to combat robocalls and detect fraudulent activity. And its Call Protect service offers spam and automatic fraudulent call blocking, warns customers about potentially unwanted calls and allows them to choose the level of robocall protection they want.

T-Mobile, meanwhile, said it added new features in 2021 to the Scam Shield service it launched at the end of 2020. Attempted scam calls reached new highs in 2021, the company said, but it's identifying or blocking an average 1.8 billion calls each month — or 700 calls per second.

Likewise, more and more large home phone companies like Xfinity, Spectrum and Frontier allow customers to block calls with no Caller ID, or that are labeled as spam, anonymous, private or unavailable, or to block or send other types of calls directly to voicemail.

Another large provider, CenturyLink, takes a different approach. It says customers "need assurance" they can make and receive legitimate calls without them being blocked. While CenturyLink offers tools to help them block or screen calls, it does not block or label calls as potential spam or anything else "based upon algorithm-based analytics or caller ID authentication information."

That's a shame. The FCC voted unanimously three years ago to allow phone companies to block some calls by default if they believe they're scam or spoof calls. They just have to give customers the choice of opting back in. That's reasonable.

The FCC has increasingly been giving phone companies leeway to protect their customers. In November 2017, the FCC approved what was a huge shift in policy at the time: allowing phone companies to block calls that pretend to be coming from a number that couldn't possibly exist. In some cases, no number exists with that combination of area code and prefix. In other cases, the phone number belongs to a company or government office that doesn't allow outgoing calls from that number. These are called do-not-originate lines. An example is the well-known Internal Revenue Service's 800-829-1040. You can call it, but no one can call you from that number. Yet con artists spoof that number all of the time.

The FCC's new rules, which took effect in 2018, allowed phone providers to block these calls without fear of liability. The FCC next told phone companies they could allow customers the choice of blocking suspected scam robocalls or calls with no caller ID.

FOUR REASONS TO BE ENCOURAGED

The hope has been that between the FCC's crackdown, phone companies' blocking and filtering and rising consumer awareness, con artists would find robocalls increasingly unproductive and stop making them.

That of course hasn't happened yet. But there are four big reasons to be encouraged.

First, scam robocalls did decline significantly after more phone companies started installing the robocall-fighting technology. In June 2021, before the law took effect, the nation saw 2.1 billion scam robocalls, according to YouMail. In May of this year, scam robocalls declined to 1.12 billion. That's a decrease of 47 percent.

Those figures don't include what are classified as telemarketing calls. These telemarketing calls could also be illegal if the callers don't have permission to call and some could be scams. Telemarketing calls jumped from 690 million in June 2021 to 830 million in May 2022, an increase of 20 percent, according to YouMail.

Second, the FCC has started partnering with state attorneys general to help both the FCC and the states to go after robocallers better. To date, the FCC has signed agreements with 36 states and the District of Columbia.

The FCC says it will be able to more easily pursue investigations like one last year that led to the largest fine in FCC history. That involved working with eight state attorneys general. The FCC fined health insurance telemarketers $225 million for making about 1 billion calls, many illegally spoofed, in violation of the Truth in Caller ID Act. The states are also filing suit seeking damages and a permanent injunction against the telemarketer, the FCC said. The calls aimed to sell short-term, limited-duration health insurance plans and falsely claimed to offer plans from companies like Cigna and Blue Cross Blue Shield.

The partnerships with the states are already helping, the FCC says. This big case was announced two weeks ago. Ohio Attorney General Dave Yost filed a lawsuit in U.S. District Court naming 22 defendants who are alleged to be part of an operation that made 8 billion illegal auto warranty robocalls since 2018. At the same time, the FCC issued cease and desist letters to eight phone companies and issued a notice to all U.S.-based voice providers to stop transmitting any calls from this operation. Violators could be put out of business by the FCC.

Many of us have likely received an auto warranty robocall similar to the ones targeted in this case:

Some of the robocalls, according to the FCC, contained this message: "We've been trying to reach you concerning your car's extended warranty. You should have received something in the mail about your car's extended warranty. Since we have not gotten a response, we are giving you a final courtesy call before we close out your file. Press 2 to be removed and put on our Do-Not-Call list. Press 1 to speak with someone about extending or reinstating your car's warranty. Again, press 1 to speak with a warranty specialist. (Pause) Or call our 800 number at 833-304-1447."

Rosenworcel of the FCC hopes for more joint investigations. "Protecting consumers from robocall and spoofing scams is an everyday challenge for local, state, and federal law enforcement. By sharing information and closely cooperating on investigations, we can better protect consumers everywhere," Rosenworcel said in a statement. "Our enforcement partnerships with state attorneys general have already paid dividends and I know these new agreements will only further that success."

In California, for example, Attorney General Rob Bonta said its agreement with the FCC will help with "critical information sharing" and allow both offices to get records, talk to witnesses, interview potential suspects, examine consumer complaints and generally help authorities build cases while preventing time-wasting, duplicative efforts. The agreements will also help the states work with other federal agencies and robocall-blocking companies.

They're already helping, said Quilici of YouMail. "The AG partnerships are keeping the problem from getting worse because they are shutting down generally high-volume scammers. Any time you can take 50 million or 100 million calls a month and stop them from happening, you're helping keep the volume down," he said.

"I think the challenge is that most AGs are doing one (robocaller) at a time, which means there are plenty of scammers that are untouched," Quilici said.

"These partnerships are great," agreed Foss of Nomorobo. "Giving more tools to law enforcement to go after more criminals is always a good idea. But it will not solve the problem completely.

"I also like the idea that these things will start to organically grow. AGs talk a lot amongst themselves. When they figure out what works, they'll share best practices and go get these guys," Foss said.

States with partnerships with FCC robocall investigators:

- Alaska
- Arizona
- Arkansas
- California
- Colorado
- Connecticut
- Florida
- Idaho
- Indiana
- Iowa
- Kansas
- Kentucky
- Louisiana
- Maine
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri
- Nevada
- New Hampshire
- New Jersey
- New York
- North Carolina
- North Dakota
- Ohio
- Oregon
- Pennsylvania
- South Carolina
- Tennessee
- Texas
- Vermont
- Virginia
- Washington
- West Virginia
- Wyoming
- District of Columbia

Third, the FCC in May approved new rules aimed at stopping illegal robocalls that originate overseas. U.S. lawmakers and regulators can't go after those robocallers but they can go after U.S. companies that allow the calls to use their lines. The FCC calls them "gateway providers," which serve as "on-ramps for international call traffic."

They're also on-ramps for some of the worst scam calls. The fraudulent calls we get that pose as the Social Security Administration (we're going to lose our benefits) or the Internal Revenue Service (we're behind on our taxes) or other government offices "almost always are coming from overseas," according to USTelecom, the industry trade association for cell phone, internet, cable and voice services.

The new rules demand that gateway providers comply with STIR/SHAKEN Caller ID requirements and take additional steps to verify the identities of providers originating the calls from overseas.

This is huge and long overdue, Foss of Nomorobo told PIRG. "This is the biggest win. Cutting off gateway carriers is one of the most important things that we can do. This is currently the weakest link in the telecom chain but needs to be the strongest."

"International robocall scams are widely understood to be a huge part of the robocall and spoofing problem facing American consumers and businesses," the FCC said in a news release. In fact, the Industry Traceback Group, the main industry group that traces robocalls to their origin found that 65 percent of operators that allowed illegal robocalls last year were either based in foreign countries or were gateway providers.

The new rules will require these gateway providers to block illegal calls, cooperate with regulators and own up to consequences of efforts that use their networks to send illegal robocalls. If a company doesn't do this, it could be blocked from transmitting any phone calls – "essentially ending its ability to operate," the FCC said.

Unfortunately, the gateway provider rules haven't taken effect yet. That will happen 60 days after they're published in the Federal Register. FCC officials said they don't yet know when that will be.

In addition, the FCC said it will explore cracking down on all intermediate providers in the United States, not just the gateway providers that transmit international calls. As of July 1, more than 13 percent of phone providers that registered with the FCC robocall mitigation database claimed they're exempt from the STIR/SHAKEN law. Of the 7,514 companies that had registered, 1,002 claimed compliance wasn't applicable. Of those, 994 said compliance wasn't applicable because they're intermediate providers

Fourth, the law that took effect on June 30, 2021, originally exempted smaller voice providers, defined as those with fewer than 100,000 customers. Their deadline to comply with robocall-prevention technology was supposed to be June 2023.

But after STIR/SHAKEN took effect last year, illegal robocall rings flocked to smaller providers, according to the FCC and a letter signed by all 50 attorneys general. "These small phone companies are suspected of facilitating large numbers of illegal robocalls," the FCC said in a release.

Now, most small providers must install Caller ID verification technology as of last month, June 30, 2022, on the internet-based parts of their networks. This doesn't yet apply to companies using, for example, old-fashioned copper-wire lines, which you often find in rural areas.

The FCC says it believes its efforts to date have helped curb unwanted robocalls but, of course, the work is ongoing. "We are well aware that robocalls are and will remain a problem," a spokesman said. "We will not let up in this fight."

And the fight keeps getting more difficult because of new ways to scam.

MOST COMMON ROBOCALL COMPLAINTS FILED WITH THE FCC IN 2021:

- ***Auto warranties***
- ***Credit/credit card***
- ***Insurance/healthcare***
- ***Lawsuit/criminal charges***
- ***Social Security number/phishing scams***

Source: https://www.fcc.gov/data-spotlight-top-robocall-complaints-2021

A FEW OF THE MOST COMMON ROBOCALLS REPORTED TO NOMOROBO RECENTLY

"This is My Business Verified calling about your Google My Business listing. Our records show your listing is either not verified or missing important information keeping your customers from finding you. Press one now so we can verify your Google My Business listing. If you are the business owner, press one now. If your account is not verified, customers searching for your services on Google will not find your listing. Press one now to verify your listing. Press two or call 634-0487 and My Business Verified will remove you from this list."

"Hi, my name is Cindy with Medicare Finder, and I am calling to inform you about medicare plans in your area, which may include extra benefits. So I understand that you have Medicare Part A and Part B. Is that correct?"

"This message is provided by the Administration of Energy Saving. The state has now set aside one $3 billion. Your home is eligible for up to ten. $0 to use for clean energy, upgrades, for exterior paint, new windows, HVAC, drought tolerant landscaping, cool roof and solar. To find out how much your home is qualified for, press one. If your home has already been qualified, press nine."

THE NEW NIGHTMARE – ROBOTEXTS

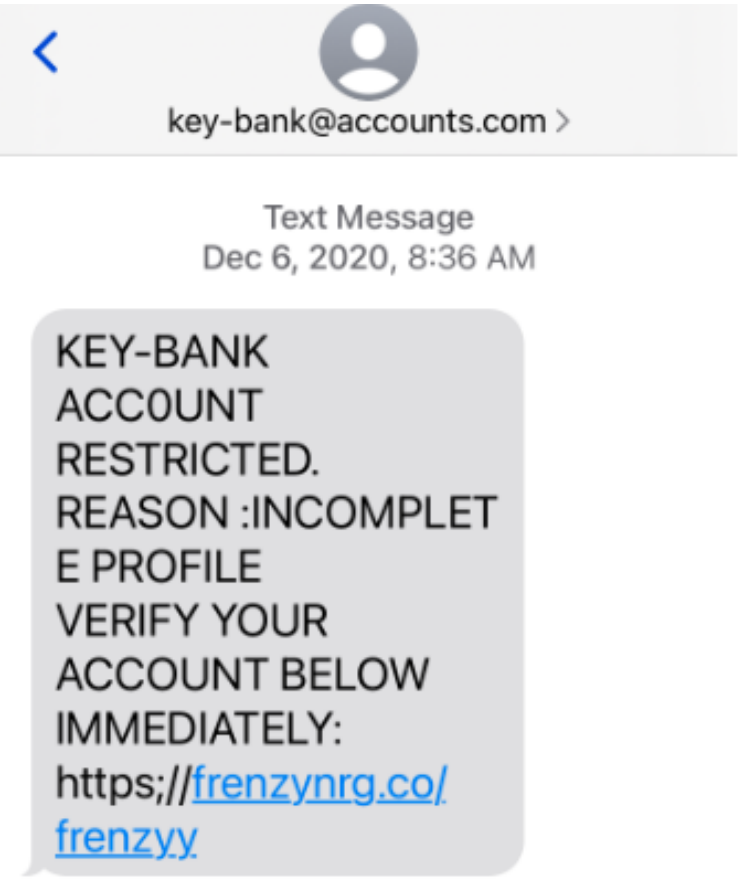
Robotexts are the next generation of scams. They've existed for several years but have been skyrocketing recently as regulators and phone companies fight back against the scam calls.

Scam robotexts are pretty much the same as scam robocalls: They're sent by the thousands or millions at a time. They try to hide their identity in order to convince you to click on a link or call a phone number. Such a misstep could lead to you getting defrauded, compromising personal information, buying something you didn't want or getting some kind of virus on your device.

Robotexts are different from robocalls in a few ways – first that they're not specifically covered by the law aimed at spoofed robocalls. That's what led Rosenworcel last October to propose new rules prohibiting robotexts.

"We've seen a rise in scammers trying to take advantage of our trust of text messages by sending bogus robotexts that try to trick consumers to share sensitive information or click on malicious links," she said in a statement.

And have we ever seen a surge. Scam robotexts have increased twelvefold in the past year, from about 1 billion to 12 billion per month, according to RoboKiller, as con artists and identity thieves take advantage of loopholes in the law and the difficulty consumers may have distinguishing a genuine text from a fake one. Con artists also gravitate to scam texts in part because consumers increasingly communicate via text, according to YouMail.



"It's not shocking that robotexts are increasing," said Quilici of YouMail. He said there are a range of efforts aimed at squashing them. Some carriers, for example, require marketing campaigns to be registered.

"But by and large, the same ease with which you can get a telephone number and make calls, means you can get a telephone number and send texts," he said. "The scammers are multi-channel marketers and will simply optimize traffic through the various channels so the most gets through with the biggest impact. The hard part is always deciding and detecting illegal traffic."

Foss said robotext scams not only are increasing, but they're becoming "sophisticated phishing scams." They're no longer just simple "You've won a prize" tricks, he said. They make the landing pages look like pages for actual companies or government offices. And they look so real, they're difficult to spot as fakes, he said.

Foss provided a spree of recent messages imitating Citibank, for example, includes alerts that said:

- "Your Citi-debit card is under review, please verify your contact info. CitiSecured05.com"
- "CITI® Your account has been disabled due to possible suspicious activity, Your online banking and ATM debit card have been blocked until we can verify your identity. Follow the one time link here and verify your identity [URL] failure to verify identity may lead to permanent hold on your account."
- "Citi #7361:Your online access has been locked. Please verify your info here [URL] to regain access."
- "Citi Card: We face a problem in the ratification of the real owner of the account, We need to confirm some of your account information : http:// [URL]
- "Citi Alerts #5145: Your account is temporarily locked due to usual activities ,to resolve visit [URL]"

"They jump from SMS provider to SMS provider and one domain to another and send out messages until they get shut down," Foss said. "They only need to get a few victims to make it worth it." SMS stands for Short Message Service, which involves routine texts sent with a cellular signal.

Quilici noted that scammers have shifted from using "funky URLs" that are long and obnoxious, to more normal-looking five-digit SMS numbers or regular 10-digit phone numbers. In some cases, the text may be from some unrecognizable number but the con artist will drop in a local or more normal-looking phone number to call.

The FCC already bans text messages sent by an autodialer without the recipient's expressed permission. (An exception is texts sent for emergency purposes.) You don't have to be on the Do-Not-Call list for it to be illegal. Here's the newsflash: People who like to defraud people often don't care about breaking other laws.

In October, Rosenworcel proposed new rules that would require cell phone providers to block illegal text messages.
Nine months later, the proposed robotext rule remains open for a vote before the full FCC. It's unclear why it hasn't been voted on yet. "The chairwoman strongly supports it and hopes her colleagues will join her in supporting it," an FCC spokesman said.

The proposal calls for applying Caller ID authentication standards – as exist for phone calls with STIR/SHAKEN – to text messages. The rules could also protect consumers from illegal robotexts through blocking them at the network level.

Scam texts are more problematic than phone calls in some ways. Consumers may be able to detect fraud attempts in a phone call either from an awkward recorded voice (even if it calls you by name,) or a live caller who sounds inauthentic or who uses a tone or language that sounds suspicious.

But with texts, fraudulent ones may not look much different from genuine texts. Texts are usually short. It's easier to mimic and spell words correctly than pronounce them correctly. And it's easier to sound authoritative and impersonate a large bank or a delivery service or a government office in a text and then include an information-stealing link.

TOP SCAM TEXTS OF 2021

26% - DELIVERIES (23.1 billion)
(impersonating Amazon, the Postal Service, FedEx or UPS) that can't be made, are expected tomorrow, etc.

6.5% - COVID-19 (5.7 billion)

3.5% - BANK (3.1 billion)
(impersonating a bank and claiming there's a problem with the account)

3% - APPLE SWEEPSTAKES (2.6 billion)

1.2% - HEALTHCARE (1.1 billion)

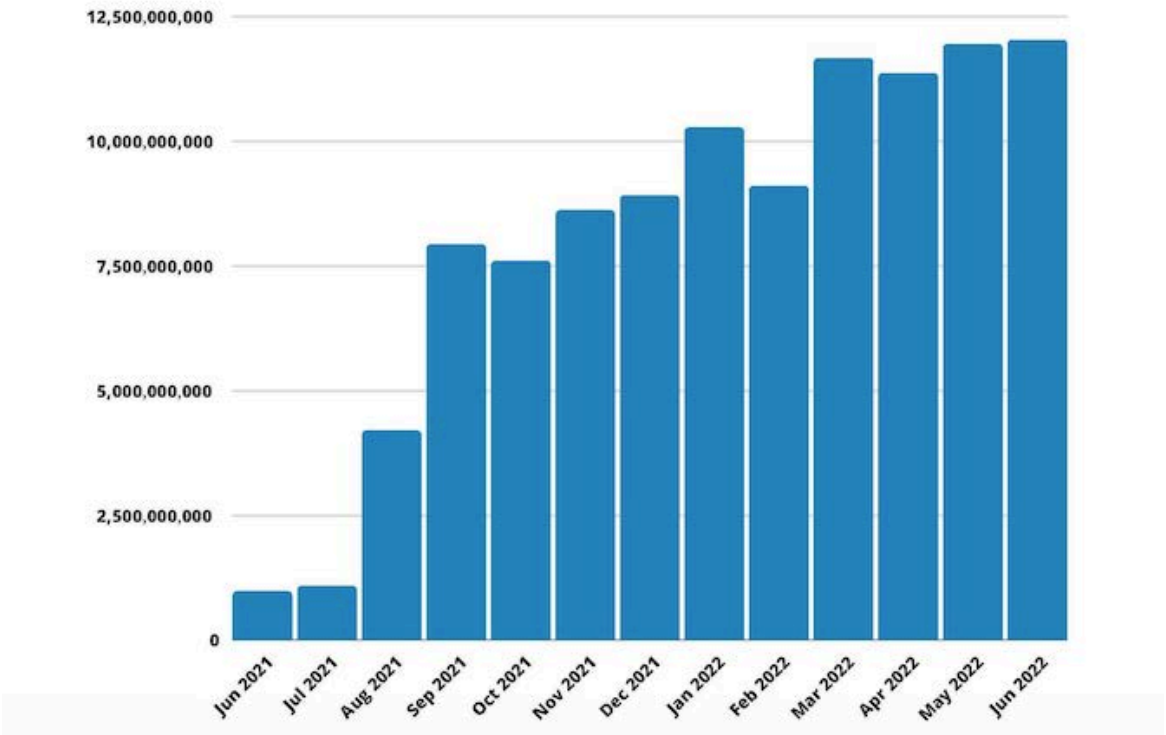
Source: RoboKiller 2021 PHONE SCAM INSIGHTS

Just like car warranty robocalls inundated us the last couple of years (regardless whether we own a car,) delivery notification texts have popped up on phones nationwide. Con artists have capitalized on the increase in online shopping and deliveries during the pandemic. The texts try to cause us to be concerned, or at least curious. Our package from the Postal Service or FedEx or Amazon couldn't be delivered. Or it's coming tomorrow. Or we need to update our delivery preferences. It doesn't matter whether we ordered anything being delivered by anyone or even have an Amazon account. The scammer just needs to get you to click or call.

Other popular scam texts dangle that your bank account has been frozen or hacked, or you owe back taxes, or your health insurance claim has been denied, or someone has run a background check on you. The scammers will write whatever they think could cause you to become rattled enough for a few seconds so that you click or call.

Spam robotexts skyrocket

Spam robotexts have been around for years but increased dramatically last year after regulators cracked down on robocalls.



Source: RoboKiller

RECOMMENDATIONS

We continue to be threatened and attacked by our own belongings – our phones. Thieves take advantage of technology and the vulnerability we all have at times to steal our information, our money or, at the very least, our time that we'll never get back. We'd like to not be stressed when our phone rings or when we miss an important call we were afraid to answer.

Illegal robocalls and robotexts likely will never go away. But they'll continue to bombard us as long as enforcement is lax, phone companies don't try harder and enough consumers fall for scams to make it worthwhile for thieves. According to one study, roughly one in four adults was the victim of a phone scam in some way last year. Even if that's high, just consider that a con artist needs only one or two victims a day to make it worth it.

Here are some of the strategies that could help reduce robocalls and robotexts:

- The FCC needs to crack down more on phone providers that flout the law. Congress passed a law that said companies must install robocall-fighting technology on the digital and internet parts of their networks by June 30, 2021. And all voice providers were expected to register their robocall technology status with the FCC as of Sept. 28, 2021. There's a ton of non-compliance. The FCC could block offenders from being allowed to transmit calls, basically putting them out of business. It hasn't yet blocked a single company from transmitting calls. That needs to change.

- The FCC in 2020 figured out a little late that companies that transmit calls from international robocall rings are a problem. But it's passed new rules to address "gateway" providers that should take effect soon. It needs to enforce those rules.

- Likewise, the FCC in 2020 underestimated how much robocall rings would gravitate to small phone companies, which were supposed to be exempt from robocall technology rules until June 2023. It's great the FCC moved the compliance deadline up to June 2022; now it needs to enforce it.

- The public and government officials need more information about the entities that are making and allowing illegal robocalls. There's an Industry Traceback Group (ITG) that tracks thousands of "tracebacks" each year to discover where illegal calls originate and who along the way allowed the calls on their lines. The information is kept mostly private and released on a limited basis to regulators.

  As recommended in June by U.S. Sen. Ben Ray Luján and 11 other senators, this information about who is allowing illegal robocalls should be released publicly to help consumers, victims and law enforcement hold offenders accountable. The FCC needs to make this happen. Bi-partisan legislation introduced in December by Sens. John Thune and Edward Markey – authors of the TRACED Act – would

protect the ITG and phone companies from liability if they share information about illegal calls. The bill is in committee.

- Most phone companies need to do more to protect their customers. Companies are allowed to block suspected scam or spoof calls from ever reaching consumers, as long as they give their customers a chance to opt back in. Companies are also allowed to label calls as possible scams or spam. And they're allowed to display a checkmark or V next to a phone number, indicating the call is coming from the number displayed. Too few companies do these things for their customers.
- Companies also should give customers the power to block suspicious calls or calls with no Caller ID if they want. Many companies don't offer this or, if they do, they don't make their customers aware of the service.
- The FCC needs to pass proposed rules to combat robotexts, requiring phone companies to block obviously illegal text messages.
- We all need to remain vigilant and do whatever we can to help educate our friends and loved ones about the dangers of illegal robocalls and robotexts.

IN RECENT YEARS, THE FCC STARTED ALLOWING PHONE COMPANIES TO:

- *Block suspected scam or spoof calls from ever reaching consumers, as long as they give their customers a chance to opt back in.*
- *Provide on-screen warning that a call may be spam or scam so customers can decide whether to answer.*
- *Display a check mark or V or "verified number" next to a phone number, indicating the call is coming from the number displayed.*
- *Give customers the option of blocking suspicious calls or calls with no Caller ID.*
- *Offer customers the option of creating a "white list" and allowing only those calls to come through.*

APPENDIX

TYPICAL FCC CEASE AND DESIST LETTER

Re: Official Correspondence from the Federal Communications Commission

Dear xxx:

We have determined that xxx is apparently transmitting illegal robocall traffic on behalf of one or more of its clients. You should investigate and, if necessary, cease transmitting such traffic immediately and take steps to prevent your network from continuing to be a source of apparently illegal robocalls. As noted below, downstream voice service providers will be authorized to **block *all*** of xxx's traffic if you do not take steps to "effectively mitigate illegal traffic" within 48 hours, or if you fail to inform the Commission and the Traceback Consortium within fourteen (14) days of this letter of the steps you have taken to "implement effective measures" to prevent customers from using your network to make illegal calls.[1]

Why You Are Receiving This Notification. You are receiving this letter because one or more investigations conducted by the Commission, in conjunction with the Traceback Consortium, revealed that xxx apparently transmitted multiple illegal robocall campaigns from the sources listed in Attachment A.

Actions You Should Take Now. xxx should take the following steps to resolve this matter:

1. Promptly investigate the transmissions identified in Attachment A.
2. If necessary, "effectively mitigate" the identified unlawful traffic by determining the source of the traffic and preventing that source from continuing to originate such traffic.
3. Implement effective safeguards to prevent customers from using your network as a platform to originate illegal calls.
4. Within 48 hours, inform the Commission and the Traceback Consortium of steps taken to mitigate the identified apparent illegal traffic.

WHICH ROBOCALLS/SALES CALLS AREN'T ALLOWED

- Telemarketing calls to a cell phone or home phone that use a prerecorded or artificial voice, without your upfront, written permission. (If a residential line is listed on the Do Not Call Registry, then all telemarketing calls or texts, whether prerecorded, live, autodialed or manually dialed, are prohibited, without upfront, written permission.)

- Any autodialed call or text message to your cell phone without your permission, either in writing or verbally. (However, the caller has the burden of proving consent, which verbal permission won't do.)

- Autodialed or prerecorded voice calls to a cell phone that concern a political campaign, unless there is upfront consent. (Political campaign-related autodialed or prerecorded voice calls are permitted to a home phone, even without consent.)

- Phone solicitation calls to your home after 9 p.m. or before 8 a.m. (Remember that cellphones may qualify as a home phone in certain situations.)

- Telemarketing calls to numbers you have registered on the Do Not Call registry, unless you've given that company upfront, written permission to call. The Do Not Call registry applies only to telemarketing calls, not calls from political organizations; tax-exempt, non-profit organizations; religious organizations; or pollsters and those conducting surveys.

Note: Telemarketers are no longer able to place prerecorded robocalls to your home phone based on an "established business relationship" that you may have had if you bought something from the company, got an estimate from the company or had some contact with them once upon a time. A call from a live telemarketer is legal if there's an established business relationship.

Source: FCC, FTC

HISTORY OF ROBOCALLS

1980s: Robocalls were born when computer software made such calls possible on a wide scale for virtually no cost.

1991: Telephone Consumer Protection Act passed, prohibiting telemarketers and other companies from calling consumers on their cell phones or home phones using a prerecorded or artificial voice without their consent. Callers are also prohibited from using an auto-dialer to call cell phones.

2006: Robocalls started taking off as cell phone ownership among U.S. adults hit 73 percent.

2007: Regulators started trying to crack down on robocallers, especially ones committing fraud.

2009: One of the first big robocall cases led to two lawsuits against companies from Florida and Illinois accused of making more than 1 billion unwanted calls from 2007 to 2009 about bogus car warranties.

Sept. 1, 2009: The robocall as we know it became illegal as the Federal Trade Commission started prohibiting prerecorded telemarketing calls to consumers who hadn't agreed to the calls in writing.

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 unwanted robocalls, particularly spoofed calls.

2017: The FCC approved allowing phone companies to block calls that claim to be from a number that couldn't possibly exist, such as an impossible area code-prefix combination or from a do-not-originate phone number that can't make calls.

2018: The blocking rules took effect, allowing phone providers to stop calls from numbers that couldn't exist without fear of liability.

(continued)

2018: Additional rules took effect to give phone companies the option of allowing customers to block suspicious calls or calls with no Caller ID.

2018: The FCC asked phone companies to adopt caller ID verification by 2019. But it wasn't required, so it didn't happen.

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.

June 2019: The FCC proposed new requirements for all voice providers -- mobile, VoIP and old-fashioned landlines -- to require them to install new technology to detect and block scam robocalls. 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. It became part of the TRACED Act passed by Congress in December 2019.

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 callblocking and caller ID verification at no cost to their customers.

June 30, 2021: Caller ID verification technology for phone companies became law. after it was passed by Congress in December 2019.

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 install Caller ID verification systems and report their status as it relates to implementation of the industry-standard technology, referred to as STIR/SHAKEN. The deadline to report was June 30, 2021. As of Sept. 28, 2021, companies were to 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 at 5 a.m. on July 1, 2022. It contained 7,514 listings. Of those:

- 1,932 said they'd completed STIR/SHAKEN implementation.
- 1,518 said they'd partially implemented STIR/SHAKEN and were performing robocall mitigation.
- 3,062 said they had not implemented STIR/SHAKEN but were performing robocall mitigation.
- 1,002 said the question about implementation was not applicable; for all except eight of them, they said it's because they're intermediate providers that don't originate calls.