RINGING IN OUR FEARS 2023

Tens of millions of consumers lost money to scam calls last year, with a median loss of $1,400. We look at what's being done to fight robocalls and robotexts, and what's next.

U.S. PIRG Education Fund

Ringing in Our Fears 2023

Tens of millions of consumers lost money to scam calls last year, with a median loss of $1,400. We look at what's being done to fight robocalls and robotexts, and what's next.

WRITTEN BY:

TERESA MURRAY

CONSUMER WATCHDOG
U.S. PIRG EDUCATION FUND

JULY 2023

PIRG CONSUMER WATCHDOG

ACKNOWLEDGEMENTS

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 editorial support:
James Horrox, Policy Analyst, Frontier Group.

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 for 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

COVER IMAGE: Icons 8 team via unsplash.com

CONTENTS

EXECUTIVE SUMMARY

If you're still getting unwanted robocalls, you can blame some of the more than 5,000 phone providers that aren't protecting us from spoofed and scam robocalls. And most of them were supposed to as of two weeks ago.

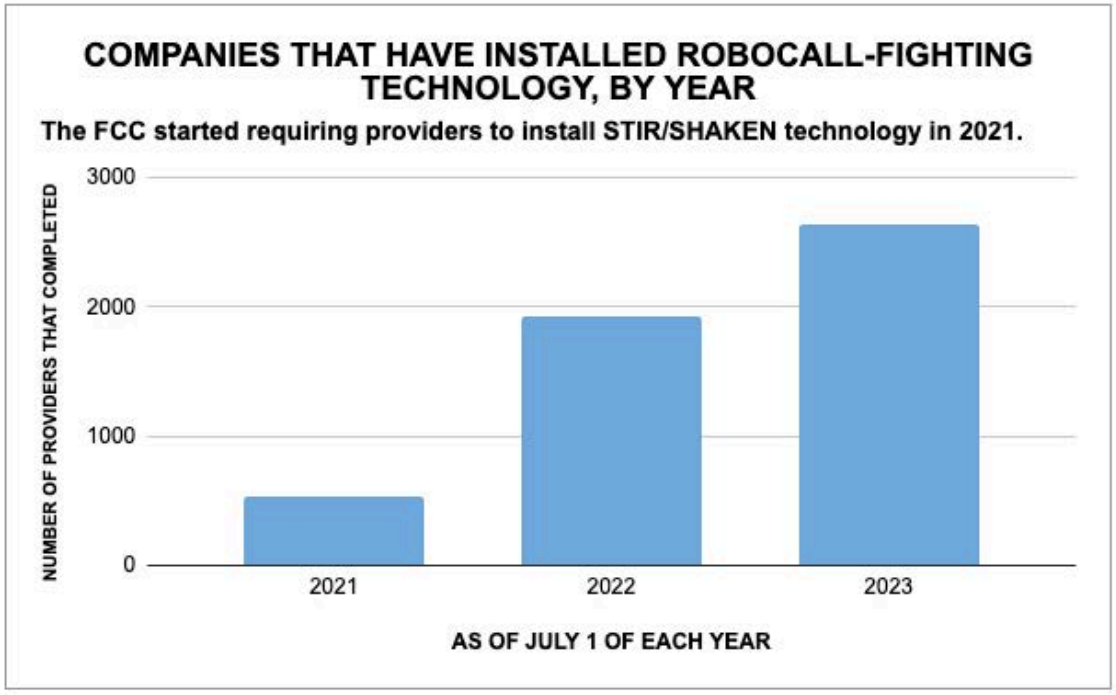
The robocall-fighting law took effect two years ago, on June 30, 2021, with deadlines for compliance staggered depending on the type and size of company. The last major deadline was last month – on June 30, 2023 – for cell and internet-based phone companies to install spoofed robocall defense standards.

For months, the Federal Communications Commission (FCC) has warned holdouts: Virtually all companies that didn't have an extension would be expected to comply by June 30.

Yet as of two weeks ago, an appallingly low percentage of companies tell the FCC their equipment is up to date. In fact, fewer than 40% of phone companies have completely installed the anti-robocall technology, a new analysis of FCC data by U.S. Public Interest Research Group Education Fund shows.

It breaks down this way:

- There were 8,336 total phone providers in the FCC robocall mitigate database as of July 1, 2023.
- 2,745 completed STIR/SHAKEN, the robocall-fighting technology mandated by the federal law.
- 5,591 have not completed STIR/SHAKEN.



Digging deeper, of the 8,336 phone providers:

- 1,195 are "intermediate" providers that carry or route calls but don't actually originate or deliver calls. They have an extension until Dec. 31, 2023, although some are already compliant.
- An additional 238 companies are U.S.-based "gateway" providers that receive calls directly from foreign providers. They were supposed to comply by June 30, 2023, but some may have an extension, the FCC said.

Among the remaining 6,903, all which originate or deliver calls, our analysis shows:

- 2,646, or 38%, have completed STIR/SHAKEN.
- 1,770, or 26%, have partially adopted STIR/SHAKEN.
- 2,480, or 36%, have not installed any STIR/SHAKEN systems.
- 7 responded N/A, indicating they hadn't adopted STIR/SHAKEN.

It's not like phone companies haven't known this was coming for a long time. The possibility of a nationwide mandate emerged in 2016, the FCC announced plans for rules in 2017 and the bipartisan law was passed in 2019 before taking effect in 2021.

There is good news: While our phones are still ringing with unwanted calls more often than we'd like, scam and telemarketing calls have declined significantly in the last two years. And the bad calls should continue to decline as more companies block illegal calls.

Of course we're all familiar with the consequence of fewer robocalls: a dramatic increase in scam robotexts, which can be more dangerous and weren't initially targeted by regulators.

Most concerning, though: The amount of money lost to scam calls has exploded, from $9 billion a year in 2018 to $40 billion a year in 2022, according to TrueCaller Insights, which compiles an annual spam and scam call report.

Put in terms that are more meaningful: Consumers who were defrauded through a phone call lost a median of $1,400 in 2022, according to the Federal Trade Commission.

EFFECT OF THE LAW AND WHAT IT MEANS

Few laws in recent years have passed with as much support as the anti-robocalls law – the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED) of 2019. The vote was 97-1 in the Senate and 417-3 in the House.

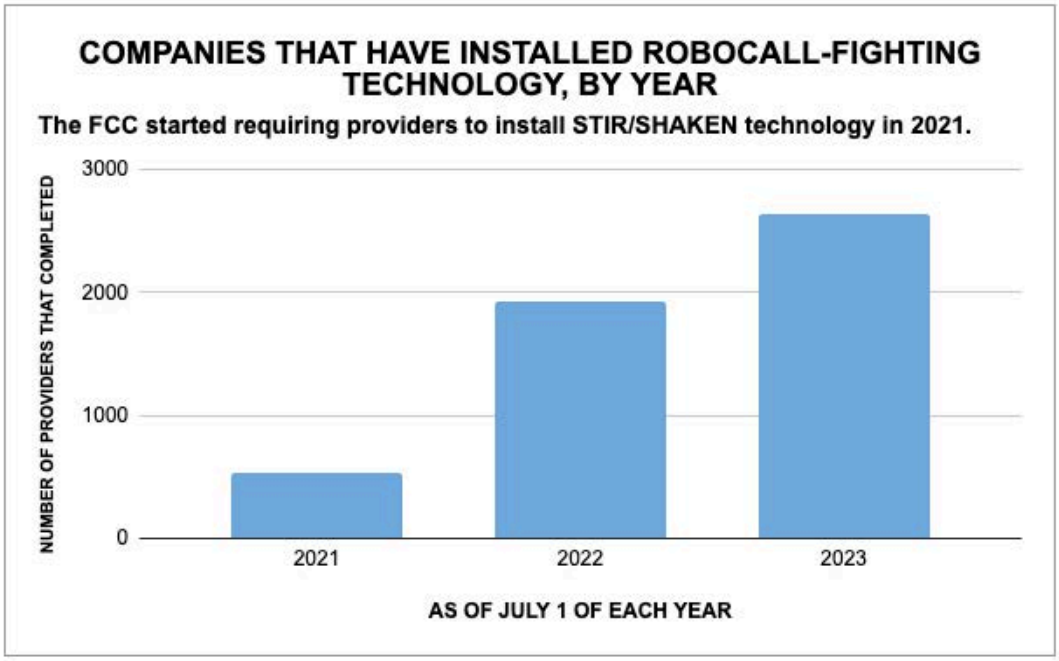
The crackdown that started in 2021 required "voice providers" to install technology that can verify whether a call is actually coming from the number on the Caller ID and detect other telltale signs of a spoofed or scam call. Most companies were expected to comply by June 30, 2021, but smaller companies and others that connect calls were given later deadlines.

The law requires companies to install the technology on all of their networks that route calls through the internet or cable, or tell the FCC what it's doing to reduce scam robocalls.

Small providers (with fewer than 100,000 subscriber lines) were supposed to comply by June 30, 2022 if their calls were transmitted through another provider.

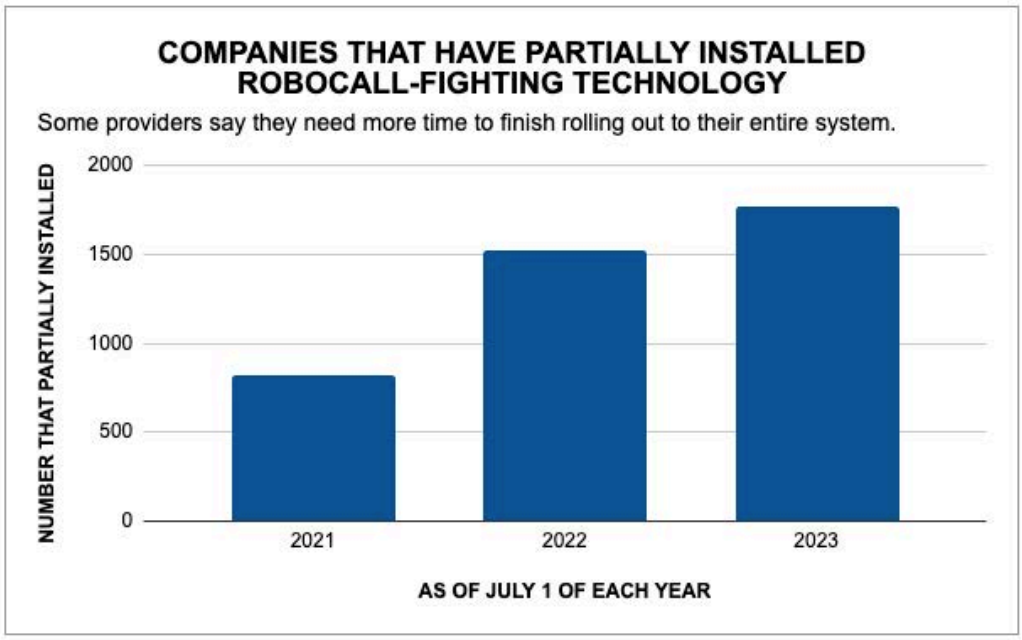
Small providers with their own equipment to originate calls were required to comply by June 30, 2023, along with gateway providers, which handle calls from overseas. Intermediate providers that transmit calls but don't originate or deliver them have until December 31, 2023.

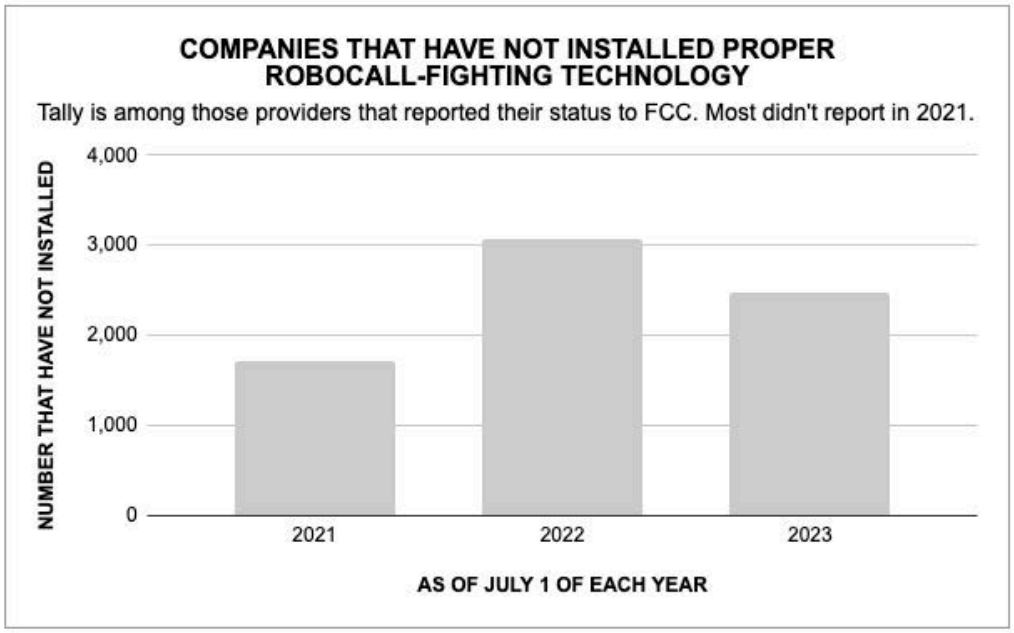
In 2021, only 536 companies were fully compliant; now that number is up to 2,646 companies. In 2021, 817 had installed the technology on *part* of their networks; now that's up to 1,770.



Companies that don't comply are supposed to get hit with significant consequences, including fines and possibly being blocked from offering phone service. That hasn't happened much yet, however.

In November, the FCC for the first time essentially shut down a company, Global UC, for non-compliance. The move prohibits other phone companies from routing any of Global UC's phone traffic. The FCC has warned other phone companies and has sanctioned several large operations accused of being responsible for billions of scam calls.





ROBOCALLS HAVE DECLINED BUT NOT ENOUGH

The volume of robocalls that are clearly scams dropped nearly in half in the first year after the law took effect, from 2.1 billion a month in 2021 to 1.1 billion in 2022, according to YouMail, one of the largest robocall-blocking companies in the United States that the FCC itself cites.

And as of last month, scam calls dropped to 800 million per month, YouMail said.

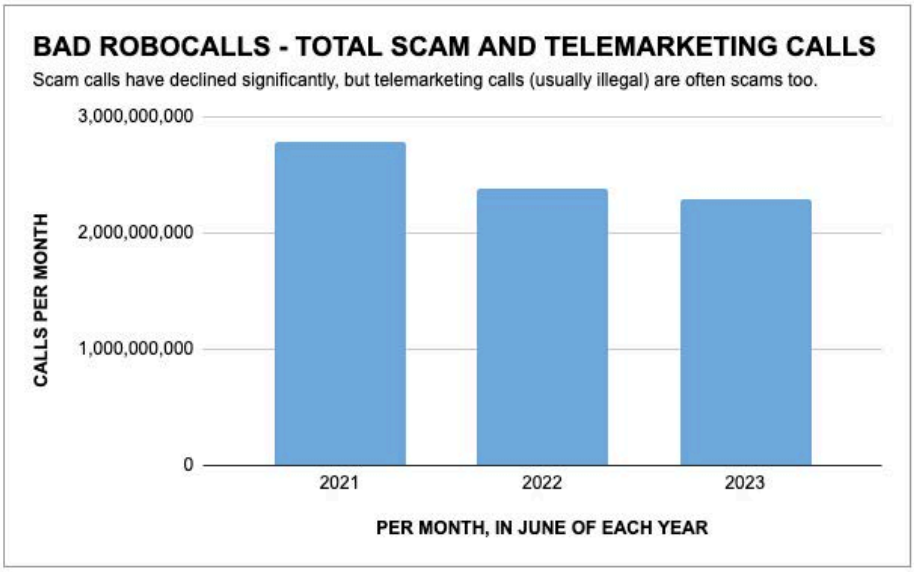
But many calls that are categorized as telemarketing calls are actually scam calls, YouMail says, and the number of telemarketing calls has nearly doubled in the last two years, from 700 million a month or 1.33 billion a month.

Now, YouMail combines scam calls and telemarketing calls as ones we don't want and are usually illegal, either for being deceptive or violating consumer consent laws.

Adding the two categories together, unwanted calls have dropped from 2.8 billion a month in June 2021 to 2 billion last month. That's a significant decline but is still way too many.

The FCC-required technology helps phone companies determine whether the call should be blocked or flagged as a spoofed, scam or spam call, and for calls that go through, helps consumers decide whether to answer them. 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.

Remember that more than 60% of companies aren't using the technology across all of their system. One would expect that unwanted calls will continue to decline as more providers start using the technology.



The flip side is that some companies may not want to comply. Companies make money from routing phone calls, even if they're a middleman with no actual individual or business customers. They might get a penny or two per call that uses their equipment. Upgrading that equipment would cost money.

Comments submitted last year to the FCC by the non-profit National Consumer Law Center (NCLC) and the Electronic Privacy Information Center (EPIC) made an important point:

"While the Commission has undertaken several efforts to mitigate scam robocalls over the last 20 years, none address the root problem: it is more profitable to transmit illegal robocalls than to mitigate them effectively."

The consequences to us: Irritation. A waste of time. A distraction when we're in the middle of something. And in way too many cases, fraud or money lost. The FCC has estimated that lost productivity alone totals some $3 billion a year. The actual monetary losses have skyrocketed the last few years to nearly $40 billion a year.

Phone calls and texts are generally illegal if they're:

- *Prerecorded telemarketing calls to a cell or home phone without **written** permission.*
- *Autodialed calls or texts to your cell phone without your verbal or written permission.*
- *Prerecorded calls to your cell phone without your verbal or written permission.*
- *Calls aimed at deceiving or defrauding you.*
- *A telemarketing call, even from a live person, if you're on the Do Not Call list.*

Note: You always retain the right to revoke permission you give to a company at any time.

THE THREAT FROM ROBOTEXTS GROWS

While unwanted robocalls have declined, scam and spam texts have exploded, from 1 billion a month in 2021, to 12 billion a month in 2022, to 14 billion a month last month, according to Robokiller, which offers robocall- and robotext-blocking technology. This humongous increase was not unexpected because robotexts – for reasons that escape understanding – were not included in the robocalls law passed more than three years ago, or anything soon after.

Just this spring, the FCC approved new rules requiring mobile wireless carriers to block texts originating from invalid, unallocated, or unused numbers. Texts from these numbers are most likely to be illegal, the FCC says.

"These robotexts are making a mess of our phones. They are reducing trust in a powerful way to communicate," FCC Chairwoman Jessica Rosenworcel said in a statement after the new rule was approved.

"Scam artists have found that sending us messages about a package you never ordered or a payment that never went through along with a link to a shady website is a quick and easy way to get us to engage on our devices and fall prey to fraud," she said.

For now, the robotext rules affect only 10-digit numbers and toll-free numbers, not short code messages.

More rules could be coming that would affect::

- Short code numbers.
- Texts to numbers on the Do Not Call Registry and
- Texts from marketers who didn't get permission directly, but tried to piggyback on consent given to a partner. Our phone numbers could actually be getting provided by lead generators and data brokers, the FCC says.

Many experts believe scam texts are even more dangerous than scam calls for two key reasons:

First, while you can avoid answering a suspected scam call (and they usually don't leave a message,) you cannot avoid seeing at least a preview of a text, even if you don't open it (and you shouldn't open suspicious texts.)

Second, it's easier for a thief to trick you in a text, which is short, may offer fewer clues about whether it's legit and may include a link to a website that can contain logos and language stolen from an organization's real website.

No wonder, perhaps, that among all fraud reports filed with the FTC last year, more people lost money through scam texts than any other source. In 22% of all fraud reports, consumers said they were contacted by text.

Meanwhile 20% of fraud victims were contacted through scam calls, while 19% were contacted by email.

The median loss involving scam text messages was $1,000 in 2022, less than the $1,400 stemming from scam calls, the FTC said.

Overall, Americans lost $330 million to text message scams in 2022. That's double from 2021.

The top five scam texts comprised more than 40% of randomly sampled texts last year, the FTC said. The top five:

- Security alerts from thieves impersonating large banks.
- Claims about free gifts or prizes, supposedly from a retailer or cell phone company.
- Claims about package delivery problems from USPS, UPS or FedEx.
- Bogus job offers for tasks such as mystery shopping and car wrapping.
- Security alerts pretending to be from Amazon.

The fake bank security messages often impersonate Chase, Bank of America, Citi and Wells Fargo, which are the four largest banks and have tens of millions of customers. Text messages claiming to be from any one of those are almost surely going to reach some people who actually *are* customers of those banks. That increases the odds of someone falling for the scam.

The sender's text usually says that a large payment has been made from the account, and the person needs to call this number to stop it.

Of course, no payment has been made, but some people might understandably be alarmed and make a bad decision to call the number, rather than look up the true number for their bank. Those who believe the text and respond or call the number are then connected to a fake bank representative. Next steps could involve the consumer sharing login information or two-factor authentication codes meant to be an extra security measure.

Scam texts such as these have increased 20-fold since 2019. Clearly, they work often enough to make them worthwhile for thieves. Even one or two victims a day could yield thousands of dollars, perhaps tens of thousands of dollars.

The FTC says texts such as these are designed to create "a sense of urgency" that something really bad will happen if they don't respond, or something really good will happen if they do.

BLUER SKIES AHEAD?

While scam robocalls haven't declined nearly as much as we'd like, it's rational to think it could continue to get better. Here are three key reasons why:

1. Two big holes in the system were gateway providers and small phone companies. As of two weeks ago, all of those are expected to comply with robocall-reducing technology. Gateway providers are "on-ramps for international call traffic," according to the FCC. And they're on-ramps for thieves. Experts say a significant number of scam calls originate from overseas. There are more than 200 gateway providers in the FCC's database.

In 2021, 65 percent of operators that allowed illegal robocalls were either based in foreign countries or were gateway providers, according to the Industry Traceback Group, the main industry group that traces robocalls to their origin.

Some of the most egregious scam calls, such as those posing as the Internal Revenue Service or Social Security Administration, "almost always are coming from overseas," according to USTelecom, the industry trade association for cell phone, internet, cable and voice services.

Robocall-filtering software companies say gateway providers have been the weakest link in the chain.

Another weak link has been small providers, which were originally exempted. Small providers have fewer than 100,000 customers. After the law took effect in 2021, 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. Compliance by small providers was moved up, with most being required to install Caller ID verification technology on the internet-based parts of their networks in 2022. The rest of the small companies were required to comply as of two weeks ago.

A smaller piece is intermediate providers, which don't originate or deliver calls, but route them along the way. They'll be required to comply by Dec. 31, 2023. There are nearly 1,200 intermediate providers on file with the FCC, about 14% of all phone companies.

It will be interesting to see what effect these new mandates have on scam calls.

2. The attorneys general in 44 states plus Washington DC and Guam have partnered with the FCC to help the regulator and the states go after robocallers with more resources.

We can expect to see more cases like one in 2021 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.

In 2022, 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.

Last month, the FCC notified Avid Telecom LLC, also known as Michael D. Lansky, LLC d/b/a Avid Telecom, that it's accused of originating apparently illegal robocall traffic and must take steps to stop these calls or else be blocked from other providers blocking all of Avid's traffic.

The move followed a lawsuit filed in May by the attorneys general in 48 states and Washington DC and against Avid, accusing it of making more than 7.5 billion robocalls to people on the National Do Not Call Registry. In Arizona, where Avid is based, Arizona Attorney General Kris Mayes said about 197 million robocalls were made from December 2018 to January 2023. The attorneys general want a jury trial to force Avid to end the practice. In Ohio, one of the four lead states in the suit, Avid is accused of sending or trying to transmit about 24.5 million illegal calls, according to Ohio Attorney General Dave Yost. More than 90% of the calls lasted less than 15 seconds, which strongly suggests they were robocalls, Yost said. This was the first legal action by the Anti-Robocall Multistate Litigation Task Force, which formed last year.

3. The FCC continues to refine its rules to try to squash even more unwanted robocalls. For example, the FCC in March announced new rules to require all providers, regardless whether they've installed STIR/SHAKEN, to take "reasonable steps to mitigate illegal robocall traffic" and detail what they're doing in the FCC's Robocall Mitigation Database.

The FCC is also weighing new rules to stop so called "lead generators" from calling people on the Do Not Call Registry just because the individual gave consent to one of the company's marketing partners. Bottom line: Consent shouldn't be able to be shared. The plan to stop lead generators and data brokers from abusing people's phone numbers is supported by 28 attorneys general and of course a number of consumer advocates.

In some cases, telemarketers rely on consent submitted through a single webform.

Here's the discouraging issue to realize: New laws don't guarantee illegal practices will stop. People who like to defraud people, which is obviously illegal, often don't care about breaking other laws.

TIPS FOR CONSUMERS

We frequently get asked: How can you identify a scam text, call or email? You really can't, with certainty. The bad guys are better at this than we are. You should assume that ***any*** request is a scam if it's unexpected, and if you're asked to provide or confirm any information, or to pay money or buy gift cards.

Here are some robocall and robotext tips to live by and share with vulnerable friends or relatives:

On robocalls:

1. If someone calls and claims to be with a company you do business with and you think the call may be legitimate, hang up and call them back at a phone number you look up independently. And never confirm or provide personal information to any caller you weren't expecting, no matter who they say they are. Not your name, your ZIP code, your shoe size … Nothing.

2. Don't ever pay bills or debts with gift cards. Period. Full stop. Gift cards are for gifts or to make a purchase for yourself. No legitimate operation accepts gift cards to pay for an obligation — not the Internal Revenue Service or a jail or a bank.

3. If you get some kind of call that you're supposedly a victim of fraud or you're behind on taxes or your grandchild is in jail, call someone you trust before you do anything — maybe a friend, a trusted relative or a neighbor. Just saying what's going on out loud can help you realize it's a scam.

4. If any caller wants you to take action immediately or pressures you not to tell anyone about the call, hang up and contact a trusted relative or friend.

5. On your outbound voicemail message, don't provide your full name. There's no sense giving potential scammers information they may not already have.

6. Don't trust your caller ID. A call appearing to be from a neighbor or a government agency could be coming from a con-artist halfway around the world. A scammer could even potentially spoof a number in your contacts list. In the past, you presumably would recognize if the voice was unfamiliar. That's not even a sure thing these days given the rise of Artificial Intelligence technology that can spoof our voices.

7. Don't be fooled if a caller knows your name, address, family members' names or even your Social Security number. All of this and more was exposed for half of the adult population in the Equifax data breach of 2017 and numerous other breaches in recent years.

8. If you have a voicemail box with your phone line, set up a password. Some voicemail services give access to messages if you call from your own phone number. But if an identity thief spoofs your number

and there's no password, they potentially could access your messages and personal information.

9. Don't give your phone number to anyone who doesn't really need to reach you immediately, especially if they're going to put your number in a database. Instead, opt for email notifications from retailers, pharmacies, etc., particularly if you get your email on your cell phone.

10. For those times when you need to give a business a phone number, consider getting a free phone number to link to your phone, such as a Google Voice number. You can set it up to require callers to state their name before you decide whether to answer or let the call go to voicemail. Using this number to make phone calls also prevents businesses from automatically capturing your real cellphone number when you call a toll-free number.

11. Use multiple robocall filters. Each one offers an opportunity to catch something that slips through the previous filter. You can route calls that are flagged straight to your voicemail. Start by asking your phone company what robocall filters it offers at no charge. For more information on call blockers, the FTC recommends consulting with the CTIA, the wireless industry's trade association.

Here are lists of reputable robocall filtering software for cell phones. Some are free; some cost money.
For Apple (iOS):
https://www.ctia.org/consumer-resources/how-to-stop-robocalls/ios-robocall-blocking/
For Androids:
https://www.ctia.org/consumer-resources/how-to-stop-robocalls/android-robocalls-blocking

12. Never respond in the affirmative to unknown callers who ask something like, "Can you hear me?"

13. If you answer an unwanted call, never press a button to be removed from the call list or call a number back to get off their list. It doesn't work; it just lets the caller know there's a live person at this phone number. Just hang up. Never call back.

14. If you don't want to receive sales calls, register your phone number with the federal Do Not Call Registry. Legitimate businesses will honor your request because it's the law. Registering with the Do Not Call Registry also gives you more legal rights to file complaints.

15. Report illegal/unwanted robocalls and texts:
** Call the FTC at 1-877-382-4357 or file a complaint online at ftc.gov/complaint
** Report scam robocalls or texts to the Federal Communications Commission.
** Report Do Not Call List violations to the Federal Trade Commission. (Or sign up if you haven't.)

You should note the number on your Caller ID and any number left on the message that you're supposed to call back. You should also report illegal or unwanted calls to your state attorney general. See the contact information for the attorneys general in every state here.

16. If you continue to get more than a few illegal robocalls a week, complain to your phone company and ask what more it can do to help protect your privacy. Companies are allowed to block spoofed and known scam calls, provide on-screen warnings of suspicious calls, offer to let customers divert calls with the caller ID blocked to voicemail, etc.

17. Consumers whose landline providers don't do a good enough job of filtering robocalls may consider buying a phone that requires the caller to announce their name or else the call won't ring. They're available for $50 or less. This is a particularly good idea for older folks who like to answer all calls and may be more trusting.

18. Vow to do more to protect your 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 those we care about know they can talk to us if there's ever a question about a call or text message they received. And we should never belittle people who fall for scams. We need to eliminate the stigma so people feel free to reach out for help.

On robotexts, there are some additional warning signs and advice:

1. If you get a text message from an entity that you never agreed to get texts from, the message is almost surely an attempt to defraud you. Entities that send robotexts are required to get upfront consent before sending any messages.

2. If you get a text you weren't expecting or from a company you've never exchanged texts with before, watch out.

3. If a text is urging you to act immediately, don't do it. Scammers trick us by causing us to think we have to do something right now — pay a debt, buy gift cards, stop fraud —or else bad things will happen. Scammers hope people won't take a moment to think through the request.

4. If a text contains awkward language or spelling or grammatical errors, it's likely not coming from the entity it claims to be from: a bank, a government office, FedEx, Amazon, etc.

5. If the text appears to be from an email address instead of a phone number or five-or six-digit sender, it's more likely to be a scam.

6. If you get a suspicious text and you've already opened it, send it to your carrier by forwarding it to 7726 (SPAM). And report it to the Federal Communications Commission.

RECOMMENDATIONS

Wouldn't it be nice if we could go back to the good ol' days, when we could tell who was calling based on the Caller ID, we didn't have to worry about missing an important call if we didn't answer and we weren't getting bombarded with disruptive and potentially costly calls and texts?

Progress is being made but the severe threats of scam robocalls and robotexts will continue until more is done. According to one study, one in four adults is the victim of a phone scam per year. 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. There's a ton of non-compliance – more than 60% of companies have not implemented the robocall defense standards. The FCC could block offenders from being allowed to transmit calls, basically putting them out of business. Only in recent months has it actually done that. This needs to change.

- The public and government officials need more information about the entities that are making and allowing illegal robocalls. The industry's Traceback Group (ITG) 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 2021 by Sens. John Thune and Edward Markey and in the House in 2022 would protect the ITG and phone companies from liability if they share information about illegal calls. This bill or something like it needs to be adopted soon.

- 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. This is happening more now than a year ago, but still, too few companies do these things for their customers.

- More 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 it.

- The FCC is weighing new rules to stop so called "lead generators" from calling people on the Do Not Call Registry just because the individual gave consent to one of the company's marketing partners.

  Bottom line: Consent shouldn't be able to be shared. The plan to stop lead generators and data brokers from abusing people's phone numbers is supported by 28 attorneys general in a letter sent just last month, and of course a number of consumer advocates. In some cases, telemarketers rely on consent submitted through a single webform.

- The FCC continues to refine its rules to try to squash unwanted robocalls. For example, the FCC in March announced new rules to require all providers, regardless whether they've installed STIR/SHAKEN, to take "reasonable steps to mitigate illegal robocall traffic" and detail what they're doing in the FCC's Robocall Mitigation Database. The FCC must follow through with its promises to protect us.

- The FCC needs to pass more rules to combat robotexts, requiring phone companies to block obviously illegal text messages. The FCC took baby steps this spring and has more proposed rules on the table. The rules passed require mobile wireless carriers to block texts originating from invalid, unallocated, or unused numbers. Texts from these numbers are most likely to be illegal, the FCC says. The rules affect only 10-digit numbers and toll-free numbers, not "short code" messages.

  Other rules proposed would affect short code numbers, texts to numbers on the Do Not Call Registry and texts from marketers who didn't get permission directly but tried to piggyback on consent given to a partner. Our phone numbers could be getting provided by lead generators and data brokers, the FCC says.

- But all of the laws in the world don't guarantee illegal practices will stop. People who like to defraud people, which is obviously illegal, often don't care about breaking other laws. So 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.

APPENDIX

KEY DATES IN THE HISTORY OF ROBOCALLS

Robocalls refer to phone calls that either contain a prerecorded or artificial voice *or* are made with help from software that does the dialing. The numbers may come from a database or could just be dialed at random. There are good robocalls (the ones we request or agree to and that help us with reminders or alerts), 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.)

All calls to your cell phone that are either prerecorded or autodialed without your permission are illegal. So are prerecorded telemarketing calls to your home phone.

Here's how we got to this point:

2006 – Scam robocalls started becoming a monstrous problem around this time, when cell phone ownership among adults hit 73 percent.

2009 – 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 bogus offers to extend a person's car warranty. The companies were accused of selling worthless "warranties" for $2,000 to $3,000 each, generating more than $10 million in revenue.

2009 – The robocall as we know it became illegal. 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.) We all know there were plenty of bad actors who violated the law.

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 fool so many. The idea of caller ID verification standards came out of this group.

2017 – Federal regulators, lawmakers and industry giants got serious about combating illegal robocalls by giving phone companies more leeway to block spoofed or suspected scam calls. The voluntary measures did little if any good.

2018 – Other new rules took effect that gave companies the option of allowing customers themselves to block suspected robocalls and block calls with no caller ID.

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.

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.

2019 – Congress passed the bi-partisan TRACED Act (Telephone Robocall Abuse Criminal Enforcement and Deterrence Act). 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, which stands for Secure Telephone Identity Revisited [STIR] and Signature-based Handling of Asserted information using toKENs [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.

2021 – The compliance deadline for companies to begin to use robocall defense standards on phone lines. Various groups of providers have faced implementation deadlines over recent years:

- June 30, 2021 – Largest voice service providers.
- June 30, 2022 – Non-facilities-based small providers.
- June 30, 2023 – Facilities-based small providers and gateway providers.
- December 31, 2023 – Intermediate providers that receive unauthenticated IP calls directly from domestic originating providers.
- TBD – Non-IP networks. The FCC has launched an effort to figure out ways to for non-IP networks – old-fashioned hard-wired phone lines – to implement caller ID authentication. They cannot implement STIR/SHAKEN.

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

METHODOLOGY

We downloaded the FCC's Robocall Mitigation Database at 7:26 a.m. ET on July 1, 2023. This database contains information about phone companies (voice service companies,) including their level of compliance with the anti-robocall law, what type of provider the company is and the date of the last update.

The database contained 8,336 listings. The Federal Communications Commission (FCC) said that June 30, 2023, was the last major deadline.

We then filtered out the 1,195 intermediate providers, which don't have to comply until Dec. 31, 2023, but some already have. We then filtered out the 238 gateway providers, some of which may have filed for and received an extension, even though their deadline was June 30, 2023.

We then sorted the remaining 6,903 companies according to their declared implementation of robocall defense standards (STIR/SHAKEN) – complete, partial, no or N/A.

The 2022 and 2021 numbers were taken from U.S.PIRG Education Fund's report from 2022.