Congressional Research Service
Informing the legislative debate since 1914

Combating Robocalls and Robotexts: Background, Selected FCC Activity, and Legislative Activity in the 119th Congress

May 12, 2026

Congressional Research Service
https://crsreports.congress.gov
R48941

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R48941

May 12, 2026

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

Combating Robocalls and Robotexts: Background, Selected FCC Activity, and Legislative Activity in the 119th Congress

Curtailing robocalls and robotexts presents challenges for lawmakers, regulators, the telecommunications industry, and consumers. *Robocalls* are calls made with an automatic telephone dialing system—usually referred to as an "autodialer"—that transmits a message made with a prerecorded or artificial voice. *Robotexts* are text messages also made using autodialers. An *autodialer* is any equipment that can "store or produce telephone numbers ... using a random or sequential number generator" and dial those numbers. The term *robocall* generally encompasses both robocalls and robotexts.

The Federal Communications Commission (FCC) regulates robocalls and robotexts. Both are generally illegal if they are made to any mobile phone (and in the case of robocalls, to a nonbusiness landline) without the recipient's prior express written consent. Three laws are the primary basis for the FCC's authority to regulate robocalls:

- The Telephone Consumer Protection Act of 1991 (TCPA; P.L. 102-243) restricts the use of autodialers, the use of prerecorded/artificial voice messages, and unsolicited advertisements both by voice phone call and by fax. The TCPA and its implementing regulations generally prohibit prerecorded advertising calls to residential landline numbers unless the called party has given prior express written consent.
- The Truth in Caller ID Act of 2009 (P.L. 111-331) prohibits any person, in connection with any voice service or text messaging service, to "cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value."
- The Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act; P.L. 116-105) expanded the actions the FCC could take to fight illegal robocalls. The TRACED Act is the basis for many of the tools targeting illegal robocalls. For example, the TRACED Act led to implementing the protocol designed to limit the completion of illegal robocalls and prevent caller ID spoofing.

FCC regulations have provided the framework through which the telecommunications industry has developed network-based tools to stop robocalls from reaching customers. The telecommunications industry, both service providers and equipment manufacturers, and third-party application (app) developers have created end-user tools for consumers to block suspected robocalls and robotexts, including built-in phone features, carrier services, and apps. Combining one or more methods may provide a more effective defense for consumers than any single approach.

Through legislation and rulemaking, the FCC uses several methods to fight illegal robocalls, but scammers may adapt their methods over time, such as adopting internet-based calling systems and artificial intelligence (AI), making technical solutions partly effective. The FCC has taken a range of enforcement actions to stop illegal robocalls, including revoking certain certifications of service providers, disconnecting noncompliant voice service providers from the U.S. telephone network, issuing fines, and publicly classifying some entities as threats to communication services.

Four bills have been introduced in the 119th Congress that would affect robocall regulation: The Foreign Robocall Elimination Act (H.R. 6152/S. 2666) would direct the FCC to establish a task force on unlawful robocalls; the Quashing Unwanted and Interruptive Electronic Telecommunications Act (H.R. 1027) would establish a disclosure requirement for robocalls that use AI to emulate a human being and increase forfeiture and fine amounts for certain violations of the TCPA; and the Creating Legal and Ethical AI Recordings Act (H.R. 334) would provide statutory authority to apply standards to systems that transmit artificial or prerecorded telephone messages generated using AI. Further, H.R. 6152 would require voice providers to post a bond before being able to conduct business, potentially pushing them and their insurers to more rigorously prevent scam traffic. Congress may consider a range of options to target robocalls and texts, including passing one or more of the pending bills, expanding the FCC's authority to collect the civil penalties it issues for illegal robocalls, examining recent FCC actions for consistency with congressional intent, or deferring to the FCC to continue its efforts to stop robocalls.

Contents

Figures

Tables

Contacts

Introduction

Robocalls are prerecorded or artificial voice calls, and robotexts are automated text messages.[1] Both robocalls and robotexts are transmitted using an automatic telephone dialing system—usually referred to as an *autodialer*. An autodialer is equipment that can "store or produce telephone numbers ... using a random or sequential number generator" and dial or text those numbers.[2] The Federal Communications Commission (FCC) restricts the use of autodialers and prohibits *spoofing*—when a caller deliberately falsifies the data transmitted to a caller ID display to disguise that caller's identity—in making robocalls and robotexts.[3]

Because the FCC has classified robotexts as a type of call, they are generally treated the same as robocalls from a regulatory standpoint; however, some rules apply only to robotexts. In this report, the term *robocall* refers to both robocalls and robotexts, and the term *robotext* is used when referring only to texts.

Robocalls have a derogatory connotation, as many people consider them a nuisance or an attempt to defraud. However, many robocalls are legal and not intended to defraud. Robocalls are often used by legitimate call originators, for example, to announce school closures or to remind patients of medical appointments. Political, public service, and emergency messages are also examples of legal uses.

The Telephone Consumer Protection Act of 1991 (TCPA; P.L. 102-243) is one of three existing federal laws that address robocalls. Per the TCPA, both robocalls and robotexts are generally illegal if they are made to any mobile phone (and in the case of robocalls, to a nonbusiness landline) without the recipient's prior express written consent. The TCPA treats calls to mobile phones differently from calls to landlines and treats calls to consumers differently from calls to businesses. The TCPA generally requires prior express consent for all automated calls to mobile phones, whereas residential landlines allow for more noncommercial flexibility. While consumers receive broad protection under the National Do Not Call Registry (Registry), businesses are primarily protected only against automated calls made to their mobile devices.

In the words of one lawmaker, advances in call routing technology[4] have made it

> easier and cheaper for bad actors to make illegal robocalls from anywhere in the world. These new technologies have also made it easier for scammers to hide from law enforcement and seek to gain their victims' trust by displaying fake caller ID information.[5]

Robocalls often follow a script that attempts to mislead the recipient into providing money or personal information that may be used in further fraudulent activity. Scammers sometimes use "neighborhood spoofing" so it will appear that an incoming call is coming from a local number. Scammers may also spoof a number from a legitimate company or a government agency that

[1] *Text message* is the colloquial term that encompasses both short message service (SMS) and multimedia messaging service (MMS) messages.

[2] 47 U.S.C. §227(a).

[3] Federal Communications Commission (FCC), "Unwanted Communications: Robocalls, Caller ID Spoofing, Do-Not-Call Registry, and Junk Faxes," December 20, 2022, https://www.fcc.gov/enforcement/areas/unwanted-communications.

[4] *Call routing technology*, as it relates to robocalls, refers to automated, internet-based systems that transmit, distribute, and manage telephone calls at scale without human intervention.

[5] Sen. John Thune, "Thune Leads Commerce Committee Hearing Examining the Problem of Abusive Robocalls," press release, April 18, 2018, https://www.thune.senate.gov/public/index.cfm/2018/4/thune-leads-commerce-committee-hearing-examining-the-problem-of-abusive-robocalls.

consumers recognize.[6] As with robocalls more generally, spoofing can also be used for legitimate purposes, such as hiding the number of a domestic violence shelter.

This report

- briefly summarizes the extent of the problem with unwanted and illegal robocalls;
- identifies existing FCC enforcement authority regarding illegal robocalls under the TCPA, the Truth in Caller ID Act of 2009 (P.L. 111-331), and the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act; P.L. 116-105);
- discusses the regulatory classification of robocalls;
- describes the technological and procedural tools approved by the FCC to combat robocalls and robotexts;
- presents selected recent FCC actions intended to combat robocalls and robotexts;
- describes the potential impact that the use of artificial intelligence (AI) may have on robocalls and other calls intended to defraud consumers; and
- provides an overview of legislation introduced in the 119th Congress intended to stop illegal robocalls.

Unwanted Robocalls

As illustrated in **Figure 1**, robocall activity in the United States ebbs and flows. In April 2026, individuals in the United States collectively received 4.2 billion robocalls or an average of about 13 calls per person. Put another way, that is nearly 140 million calls each day or 1,600 calls per second.[7]

The FCC reports that unwanted calls, including robocalls, are the "top consumer complaint" that it receives annually (approximately 135,000 in 2023)[8] and its "top consumer protection priority."[9] Some robocalls also pose a financial threat to consumers; for example, in 2025, there was over $3.5 billion in reported losses to imposter scams in the United States, and robotexts were the most common contact method for these scams.[10]

[6] FCC, "Caller ID Spoofing," March 7, 2022, https://www.fcc.gov/consumers/guides/spoofing-and-caller-id.

[7] YouMail, "Robocall Index," March 2026, https://www.robocallindex.com.

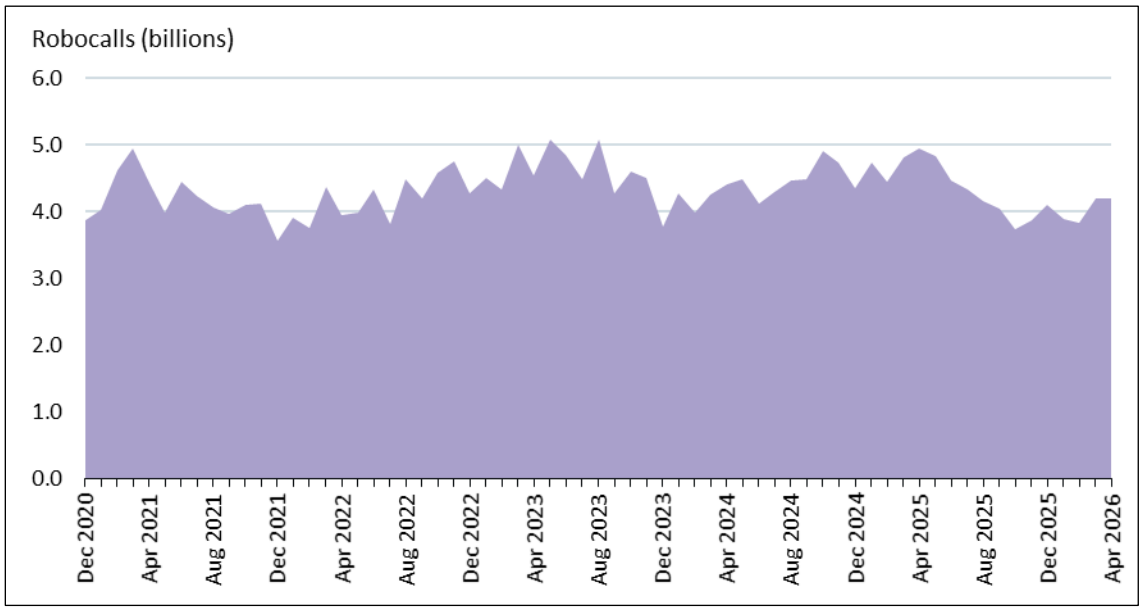
[8] FCC, "Unlawful Communications," August 8, 2025, https://www.fcc.gov/enforcement/bureau-priorities/unlawful-communications.

[9] FCC, "Stop Unwanted Robocalls and Texts," March 3, 2025, https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts.

[10] FTC Consumer Sentinel Network, "Imposter Scams, 2025, Q4," updated April 16, 2026, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts.

Figure 1. U.S. Monthly Robocalls

December 2020-April 2026



Source: Historical data provided by email from YouMail, the organization that produces the Robocall Index, https://www.robocallindex.com. Data beginning March 2026 are from the Robocall Index website.

Often, when a major scam is stopped or a new countermeasure is introduced, the total number of robocalls may decrease, but numbers often rebound as robocallers overcome or work around preventative measures (e.g., by using new originating numbers).[11] Many fraudulent robocalls originate overseas and are thus beyond the reach of U.S. enforcement activity, which adds to the complexity of stopping these campaigns. Although about 90% of all robocalls (both legal and illegal) appear to originate from within the United States, research indicates that a "significant proportion, if not the majority, of illegal robocalls originate overseas."[12]

FCC Regulatory Authority Over Robocalls

The TCPA, the Truth in Caller ID Act, and the TRACED Act (which amended the TCPA) collectively are the primary basis for the FCC's authority to regulate robocalls. The FCC has adopted numerous rules governing robocalls on the basis of these laws.

The Telephone Consumer Protection Act

The TCPA (P.L. 102-243) was signed into law on December 20, 1991. This law restricts the use of autodialers, the use of prerecorded/artificial voice messages, and unsolicited advertisements both by voice phone call and by fax. Restrictions are tightest when such calls or texts are made to

[11] Teresa Murray et al., *Ringing in Our Fears 2025: Robocalls Hit 6-Year High,* U.S. Public Interest Research Group (U.S. PIRG) Education Fund, December 2025, https://pirg.org/edfund/resources/ringing-in-our-fears-2025-robocalls-hit-6-year-high.

[12] Federal Trade Commission (FTC), "FTC Ramps Up Fight to Close the Door on Illegal Robocalls Originating from Overseas Scammers and Imposters," press release, April 11, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-ramps-fight-close-door-illegal-robocalls-originating-overseas-scammers-imposters.

mobile phones or protected destinations, such as emergency lines, hospital rooms, or care facilities. The TCPA also led to the creation of the National Do Not Call Registry in 2003.[13]

The FCC and FTC both have jurisdiction to enforce laws related to robocalls. Each may impose civil fines on parties who break the law. If fraud involving robocalls violates a criminal statute, other federal agencies may investigate and prosecute the criminal case. Individual states also have certain enforcement authority under the TCPA and may have additional enforcement authority under applicable state laws. Although the FCC (and FTC) may impose fines, parties making illegal robocalls rarely pay their fines.[14] The FCC does not have the authority to pursue collection through the courts; the agency must refer those cases to the Department of Justice (DOJ) for litigation. Only a portion of cases are pursued by DOJ, which often cannot find the parties in question or determines that other cases are of higher priority. For example, in 2023, neither the FCC nor DOJ collected any of the penalties imposed during that calendar year. Of the nine cases referred by the FCC to DOJ between January 2018 and November 2023, DOJ actively pursued collection for two of them.[15] In 2024, DOJ recovered a $9.9 million penalty from an Idaho resident for thousands of unlawful spoofed robocalls[16] and filed a stipulated order[17] against a company for facilitating billions of illegal robocalls.[18] The latter case resulted in a $10 million civil penalty, but payment was suspended because the company was unable to pay.[19]

The TCPA and the FCC's associated implementing regulations generally prohibit prerecorded advertising calls to residential landline numbers unless the called party has given prior express written consent. If the residential landline number is in the Registry, all advertising calls—including live ones—are prohibited unless the called party has an established business relationship with the caller or the called party has given prior express written consent. The TCPA does not restrict non-advertising prerecorded or autodialed calls to landlines.

The act prohibits all nonemergency autodialed and prerecorded calls to mobile phones unless the called party has given prior express consent. Consent must be in writing if a prerecorded or autodialed call contains an advertisement. If the mobile phone number is in the Registry, all advertising calls—including manually dialed and live ones—are prohibited unless the called party

[13] As noted earlier, the National Do Not Call Registry is a free, centralized list where consumers register their home and mobile telephone numbers to reduce unwanted telemarketing calls. The registry is managed by the FTC and enforced by the FCC and FTC. Once an individual submits their name to the registry, telemarketers must stop calling that person within 31 days. See the Do-Not-Call Implementation Act (P.L. 108-10).

[14] See §§IV.D and IV.E, in FCC, *Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information*, DOC-408475A1, December 27, 2024, https://docs.fcc.gov/public/attachments/DOC-408475A1.pdf (hereinafter FCC, *Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information*, §§IV.D and IV.E).

[15] FCC, *Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information*, §§IV.D and IV.E. See also Eric Priezkalns, "FCC Withheld Data from 2024 Robocall Report to US Government," *Commsrisk*, January 31, 2025, https://commsrisk.com/fcc-withheld-data-from-2024-robocall-report-to-us-government/.

[16] Department of Justice (DOJ), "Federal Court Enters $9.9M Penalty and Injunction Against Man Found to Have Caused Thousands of Unlawful Spoofed Robocalls," March 22, 2024, https://www.justice.gov/archives/opa/pr/federal-court-enters-99m-penalty-and-injunction-against-man-found-have-caused-thousands.

[17] A "stipulated order" is the same as a "consent decree." It is a binding, negotiated agreement between the FCC (often through its Enforcement Bureau) and a company or individual under investigation, which is subsequently approved and entered by a court or administrative law judge to resolve alleged violations of regulations.

[18] DOJ, "United States Settles Suit Against Telecommunications Service Provider for Assisting and Facilitating Illegal Robocalls," January 2, 2024, https://www.justice.gov/archives/opa/pr/united-states-settles-suit-against-telecommunications-service-provider-assisting-and (hereinafter DOJ, "United States Settles Suit Against Telecommunications Service Provider").

[19] DOJ, "United States Settles Suit Against Telecommunications Service Provider."

has an established business relationship with the caller or the called party has given prior express written consent.

The Truth in Caller ID Act

The Truth in Caller ID Act of 2009 (P.L. 111-331) was signed into law on December 22, 2010, to deter illegal caller ID spoofing. The law prohibits any person, in connection with any voice service or text messaging service, to "cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value." Telecommunications carriers are required to implement measures to prevent spoofing and to take reasonable measures to ensure the accuracy of caller ID information. The FCC enforces the provisions of the Truth in Caller ID Act.[20]

The Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act

The TRACED Act (P.L. 116-105) was signed into law on December 30, 2019. The law amended the TCPA to expand the actions the FCC can take to counter illegal robocalls. The law increased monetary forfeitures for TCPA violations and extended the statute of limitations for certain intentional violations. The law also required the FCC to (1) initiate a rulemaking to help protect subscribers from receiving unwanted calls or texts from a caller using an unauthenticated number; (2) assemble, in conjunction with DOJ, an interagency working group to study and report to Congress on enforcing the prohibition of certain robocalls; and (3) initiate a proceeding to determine whether the FCC's policies regarding access to number resources could be modified to help reduce access to numbers by potential robocall violators. The TRACED Act is the basis for many of the tools used today to fight illegal robocalls.

Classification of Robocalls

Under FCC rules, robocalls and robotexts are generally illegal if they are made to any mobile phone without the recipient's prior express written consent; robocalls are also generally illegal if they are made to any nonbusiness landline under the same circumstances.[21] Examples of these rules are summarized in **Table 1**.

Table 1. Legal Versus Illegal Robocalls and Robotexts

Category	Examples of Legal Uses	Examples of Illegal Uses
Consent	Commercial calls and texts: called party gave written permission to receive automated messages from a specific company, such as opting in via a website or text. Informational texts: for texts that are not telemarketing, oral consent is sufficient.	Commercial calls and texts: an entity sends automated sales calls or texts without specific written consent. "Opt-out" violation: a called party replies "STOP" to a robotext from a political campaign or other sender, but the sender continues to send automated messages.

[20] FCC, "Caller ID Spoofing," November 13, 2024, https://www.fcc.gov/consumers/guides/spoofing.

[21] For detailed information about the FCC's robocall-related actions, see FCC, "Stop Unwanted Robocalls and Texts," March 3, 2025, https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts.

Content	Examples of informational content include • a school notifies parents about a closing due to weather; • a pharmacy sends a reminder that a prescription is ready for pickup; • a utility company informs customers of an area service outage; and • an airline sends automated flight status updates. Legitimate debt collectors can use autodialed calls to make contact, but they must follow specific rules under the Fair Debt Collection Practices Act (P.L. 95-109).	Examples of fraudulent activity include • impersonating a government agency, such as the Internal Revenue Service or Social Security Administration, to demand money or personal information; • attempting to sell a fake "extended vehicle warranty"; • impersonating a tech company, such as Apple or Amazon, to get account details; • engaging in student loan or credit card debt relief scams; and • promoting fake prizes, sweepstakes, or free offers that require consumers to pay a fee or provide personal information.
Caller identity	Example of legitimate spoofing: a doctor calls from a personal phone but displays the office number for privacy, or a business displays its toll-free number for callbacks.	Example of misleading spoofing: a scammer uses "neighbor spoofing" to falsify their caller ID, making the call appear to come from a local number or a trusted government agency to mislead the called party into answering.
Campaigns	Political campaigns and charities: Political campaigns and nonprofit organizations can use robocalls and texts, though the rules differ depending on the type of phone and message. For autodialed messages to mobile phones, callers must have prior consent. All prerecorded calls must identify the caller. Surveys and polls: legitimate market research and polling calls are generally permitted.	Telemarketing campaigns without consent: a company uses an autodialer to send a prerecorded sales pitch without prior written permission. Harassment: even if a call is otherwise permitted, repeated, threatening, or harassing messages are illegal.
Contact rules	Calling within legal hours: telemarketers must follow the legal time frame for making calls (typically 8 a.m. to 9 p.m. local time).	Contacting numbers on the Do Not Call Registry: Legitimate telemarketers who call a number on the registry without prior written consent can face penalties. Scammers often ignore this list.

Source: Compiled by CRS.

Tools in the Fight Against Illegal Robocall and Robotext Scams

In addition to the laws and implementing regulations discussed above, multiple tools exist to stop or reduce robotexts, including industry-developed technologies and procedures, built-in phone features, carrier services, and third-party apps. FCC regulations have provided the framework through which the telecommunications industry has developed network-based tools to stop robocalls from reaching customers. The telecommunications industry—both service providers and equipment manufacturers—has also created end-user tools for consumers (i.e., using third-party apps to block suspected robocalls). Using a combination of these methods likely provides a more effective defense against spam and scam text messages than using any single tool.

The tools described in the following section can be thought of as components of a layered protection stack that work together to keep the telephone network secure and help protect consumers from illegal and fraudulent robocalls. **Table 2** lists the layers and components of the stack, along with their key functions, how they are used to protect consumers, and whether they apply to robocalls or robotexts. It also lists the regulation or standard and the organization responsible for the oversight of each component. The tools in the table are presented in the order in which they function within the stack, from initial customer vetting through post-detection enforcement. The discussion that follows leads with call authentication—the most significant and widely implemented tool—and proceeds thematically rather than in stack order, so the sequence of topics in the text will not correspond to the sequence of rows in the table.

Table 2. The Robocall Enforcement Ecosystem

Layer	Tool	Core Function	Impact on the Caller	Robocalls	Robotexts	Regulation/ Standard	Oversight Organization
Vetting[a]	Know Your Customer (KYC)	Verifying the legal identity of the entity buying the phone service	Blocks fraudulent traffic through verification	Regulatory mandate: voice providers must validate customers before allowing outbound call traffic.	Carrier-enforced practice: text aggregators and providers similarly vet business senders before granting messaging access.	47 C.F.R. §64.1200(n)(4); 47 C.F.R. §64.6305	Federal Communications Commission (FCC); CTIA; carriers
Compliance	Robocall Mitigation Database (RMD)	A central FCC registry certifying the provider's anti-robocall program	Blocks traffic from noncompliant providers	Regulatory mandate: all voice providers must file robocall mitigation plans and register in the RMD.	Not applicable: the RMD is a voice-specific registry with no text messaging equivalent.	47 C.F.R. §64.6305; ATIS-1000074[b]	Secure Telephone Identity Governance Authority (STI-GA); FCC
Validation	Reassigned Numbers Database (RND)	Determining whether a phone number has changed owners since consent was given	Prevents "wrong-person" calls and reduces legal liability for businesses	Regulatory mandate: callers must query the RND before placing autodialed or prerecorded calls to mitigate calls to consumers who have not given their consent.	No mandatory query requirement: the FCC has issued a narrow waiver permitting mobile providers to use the RND to verify whether a number subject to a blocking order has been permanently disconnected, but general pre-text RND queries are not required.	47 C.F.R. §64.1200(l)	FCC
Identity authentication	STIR/SHAKEN	Digitally signing the call to prove the caller ID is not spoofed	Validates the call; assigns attestation level	Regulatory mandate: STIR/SHAKEN is a voice-call framework that cryptographically authenticates the calling number on internet protocol-based networks.	Not applicable: the FCC explicitly declined to adopt text authentication requirements, finding that authentication solutions for text messages were preliminary and required more study.	47 C.F.R. §64.6301; 47 C.F.R. §64.6302; 47 C.F.R. §64.6303; ATIS-1000074	STI-GA; FCC

Layer	Tool	Core Function	Impact on the Caller	Robocalls	Robotexts	Regulation/ Standard	Oversight Organization
Security	Do Not Originate (DNO) Lists	Blacklisting "high-risk" numbers that should never make outbound calls (e.g., 911)	Drops calls claiming to be from "high-risk" spoofed sources	Regulatory mandate: all voice service providers must block calls from numbers on a reasonable DNO list.	Regulatory mandate: DNO blocking requirements apply to text and multimedia messaging. A gap remains because the framework does not cover "over-the-top" (OTT) messaging services such as iMessage, WhatsApp, or Rich Communication Services (RCS).	47 C.F.R. §64.1200(o); 47 C.F.R. §64.1200(p)	FCC; Industry Traceback Group (ITG)
	Red Flags	Triggering analytics-based review of suspicious patterns	Triggers "spam" label or further review; does not result in an immediate block	Voluntary: carriers use analytics-based red flags to identify suspicious call patterns but are not required to do so.	Voluntary: red-flag guidance does not apply to OTT messaging services.	Analytics-based blocking is permitted under 47 C.F.R. §64.1200(o)	FCC, carriers
Enforcement	Traceback	Identifying the source of illegal traffic after it has been detected	Holds providers accountable and enables FCC/state fines	Regulatory mandate: the ITG traceback process was developed primarily to trace illegal robocall campaigns to their originating provider.	Regulatory mandate (notification-triggered): the FCC and ITG have extended traceback authority to illegal robotext campaigns, enabling enforcement against text-spam originators.	47 C.F.R. §64.6305	FCC; ITG

Source: Compiled by CRS.

Notes: STIR/SHAKEN = Secure Telephone Identity Revisited and Signature-Based Handling of Asserted Information Using Tokens.

a. KYC vetting applies to both robocalls and robotexts, but the obligations differ in origin and strength. For robocalls, vetting is a direct FCC regulatory requirement: voice service providers must verify the legal identity of customers before granting access to the network for outbound call traffic. For robotexts, no equivalent FCC-mandated vetting requirement exists. Instead, sender vetting in the text messaging ecosystem is primarily a carrier and industry practice, and the FCC has encouraged these efforts. However, the FCC has stopped short of mandating the practice, meaning that the robotext vetting framework rests on voluntary industry compliance rather than on a regulatory obligation comparable to that governing voice providers.

b. Standards developed by the Alliance for Telecommunications Industry Solutions (ATIS) and cited in this table are industry developed and voluntary unless incorporated by reference into FCC rules.

Industry and FCC Efforts

Together, the telecommunications industry and the FCC have created a set of tools that complement one another in their joint efforts to stop illegal robocalls.

Call Authentication

STIR/SHAKEN—short for Secure Telephone Identity Revisited and Signature-Based Handling of Asserted Information Using Tokens—is a call authentication technology designed to limit the completion of illegal robocalls to consumers and prevent caller ID spoofing by verifying that a call is from a legitimate source. The STIR/SHAKEN framework uses digital certificates to ensure that the phone number displayed on a caller ID has not been modified. STIR/SHAKEN is used to authenticate caller ID information for voice calls, not for text messages.[22] STIR/SHAKEN reviews only a call's routing data, so it cannot be employed to determine the purpose of a call, whether a call is part of a scam, or whether AI will be used once the call is connected.

The STIR/SHAKEN system creates a "chain of trust" by digitally validating a call as it moves through different phone networks.[23] When a call is initiated, the caller's phone company (the originating service provider) digitally signs the call's information. This signature verifies the caller's identity and confirms that the caller is authorized to use that phone number. On the basis of its knowledge of the customer and the customer's right to use the number, the originating provider assigns one of three levels of trust or "attestation" levels to the call. The company that delivers the call to the recipient's phone (the terminating service provider) then verifies the signature and uses the attestation level to inform its blocking and labeling decisions.

- Full attestation: the highest level of trust, indicating that the caller and the caller's phone number are both verified. This level of attestation is called "fully signed," and these calls often show a "verified" checkmark or label on mobile devices.
- Partial attestation: a lower level of trust, indicating that the caller is known, but the caller's association with the number is unverified. This level of attestation is called "partially signed."
- Gateway attestation: the lowest level of trust, for unverified calls, such as those from outside the network. This level of attestation is called "gateway signed."

The terminating provider's call analytics then use the attestation level to decide whether to complete the call, label it as "spam likely," or block it entirely. Calls that are fully signed are more likely to be completed; those that are not fully signed are more likely to be labeled as "spam likely" or blocked.

Status and Impact of STIR/SHAKEN Implementation

The first rules requiring STIR/SHAKEN caller ID authentication were promulgated by the FCC on March 31, 2020, as required by the TRACED Act. The rules mandated that originating and terminating large voice service providers implement the framework in internet protocol (IP)

[22] FCC, *Call Authentication Trust Anchor and Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources: Report and Order and Further Notice of Proposed Rulemaking*, WC Dockets 17-97 and 20-67, March 31, 2020, https://docs.fcc.gov/public/attachments/FCC-20-42A1.pdf.

[23] FCC, "Combating Spoofed Robocalls with Caller ID Authentication," https://www.fcc.gov/call-authentication (hereinafter FCC, "Combating Spoofed Robocalls with Caller ID Authentication").

networks by June 30, 2021;[24] smaller, non-facilities-based providers were given extensions until June 30, 2022, or June 30, 2023.[25] Foreign providers processing international calls (known as "gateway providers") have been required to implement STIR/SHAKEN since June 30, 2023.[26] As of December 31, 2023, all providers, minus limited exceptions, are required to have implemented the framework in their IP networks.[27]

STIR/SHAKEN has not been fully implemented. As of early 2026, large U.S. carriers have achieved over 95% STIR/SHAKEN implementation. The minority (about 21%) of calls from smaller, non-facilities-based providers are made on IP-based networks, a situation that contributes to the amount of total call traffic that is fully signed—about 45%. This level of implementation is caused by the reliance of these carriers on non-IP legacy (i.e., analog) infrastructure, high costs for smaller providers, and technical challenges with international traffic at gateway providers.

Despite the relatively lower levels of attestation, STIR/SHAKEN is credited with decreasing the number of spoofed, illegal, and high-volume robocalls—a decline of about 11% from 2021 to 2022. The telecommunications industry is working to implement STIR/SHAKEN for text messages.[28] There has been a significant increase in robotexts, from an average of 7.3 billion per month in 2021 to 19.2 billion in December 2023.[29] Overall, it is difficult to pinpoint the effect STIR/SHAKEN has had on the total number of robocalls received by consumers, as the call volume varies over time.

The FCC assesses the efficacy of the framework independently of its implementation status, focusing instead on the usefulness of the technology itself. In its triennial report to Congress, the FCC asserted that the STIR/SHAKEN framework is effective at authenticating caller ID information when implemented as designed.[30] However, the agency noted that some stakeholders have raised concerns regarding the consistency and ubiquity of the framework's implementation; they assert that these concerns undermine the value of the STIR/SHAKEN framework.

[24] FCC, "Combating Spoofed Robocalls with Caller ID Authentication."

[25] The STIR/SHAKEN implementation extension for services scheduled for §214 discontinuance ended on June 30, 2022, and the implementation extensions for non-facilities-based and facilities-based small voice service providers ended on June 30, 2022, and June 30, 2023, respectively. See 47 C.F.R. §§64.6304(a)(1), (c). A complete list of the proceedings establishing and amending these deadlines is available at FCC, "Combating Spoofed Robocalls with Caller ID Authentication."

[26] FCC, "Wireline Competition Bureau Announces Deadlines for Gateway Provider Robocall Mitigation Requirements and Additional Compliance Dates and Filing Instructions," WC Docket no. 17-97, December 12, 2022, https://docs.fcc.gov/public/attachments/DA-22-1303A1.pdf.

[27] 47 C.F.R. §§64.6301, 64.6302; and FCC, "Public Notice: Wireline Competition Bureau Reminds Non-Gateway Intermediate Providers of STIR/SHAKEN Implementation Deadline," WC Docket no. 17-97, https://docs.fcc.gov/public/attachments/DA-23-1158A1.pdf.

[28] This figure does not take into account gateway providers, as they were not required to implement STIR/SHAKEN until June 30, 2023. Transaction Network Services, "2023 Robocall Investigation Report," press release, March 2023, https://tnsi.com/resource/com/tns-2023-robocall-investigation-report-milestone-10th-edition-out-now-press-release.

[29] Robokiller, "2023 United States Robotext Trends," https://www.robokiller.com/spam-text-insights. Data for 2024 and 2025 are more difficult to assess. Robokiller ownership changed in 2024, and the company has not collected data since the sale.

[30] FCC, *Triennial Report on the Efficacy of the Technologies Used in the STIR/SHAKEN Caller ID Authentication Framework*, DOC-416732A1, December 19, 2025, https://docs.fcc.gov/public/attachments/DOC-416732A1.pdf.

Robocall Mitigation Database

Created by the FCC in 2021,[31] the Robocall Mitigation Database (RMD) is a public database where voice service providers self-certify their robocall mitigation efforts, as required by law.[32] The RMD allows intermediate and terminating providers to verify that originating carriers have implemented STIR/SHAKEN or are taking other steps to stop unwanted robocalls, and the RMD supports FCC oversight and enforcement against noncompliant providers. Voice service providers must keep their filings updated to avoid having their certifications revoked, which would prevent other providers from accepting their network traffic. The RMD does not apply to robotexts. Although there is an accountability framework to stop robotexts, it is not as robust as the framework for robocalls because there is no RMD-equivalent registry for the text messaging ecosystem.

Traceback

Robocall *traceback* is a cooperative effort by telecommunications providers to trace illegal or fraudulent robocalls back through the telecommunications network to their point of origin. The TRACED Act mandated that the FCC designate a private consortium to coordinate telecommunications industry traceback efforts. That group is the Industry Traceback Group (ITG), which USTelecom (an industry trade group) established in 2015.[33] The group consists of hundreds of telecommunications service providers, such as AT&T, Verizon, and T-Mobile.

The ITG does not monitor all calls—it initiates traceback investigations selectively in response to evidence of illegal or harmful call campaigns. Triggers include consumer complaints, reports from telecommunications providers and law enforcement agencies and calling patterns that suggest large-scale fraud, spoofing, or other regulatory violations. When the ITG receives reports of suspicious call campaigns, the ITG enters the information into the Secure Traceback Portal (STP), a website used to coordinate the investigation with voice service providers. The ITG contacts the terminating service provider; that provider then identifies the most immediate upstream provider and enters that information into the STP. This process is repeated, with each provider identifying the provider before it in the call path. The traceback continues until the originating service provider is identified or a dead end is reached. Once the originating provider is found, it must investigate whether its customer violated the law. If so, the provider must take steps to stop the illegal calls, which can include terminating the customer's account.[34] Carriers that fail to cooperate risk being removed from the RMD, which would effectively halt their operations by requiring other providers to refuse their traffic. The FCC requires all voice service providers to cooperate with ITG traceback requests within 24 hours.[35]

STIR/SHAKEN records support the traceback process by generating authentication records, including attestation levels and originating provider information. Investigators can use that information to trace illegal call campaigns back to their sources. STIR/SHAKEN authenticates

[31] The TRACED Act (P.L. 116-105), §4(b)(5), directed the FCC to require voice service providers to implement a robocall mitigation program. The FCC implemented that requirement through the Robocall Mitigation Database (RMD), which became operational in 2021.

[32] FCC, *Call Authentication Trust Anchor: Second Report and Order*, WC Docket 17-97, September 29, 2020, https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf.

[33] Industry Traceback Group (ITG), https://tracebacks.org/.

[34] ITG, *Policies and Procedure*, revised August 2025, https://tracebacks.org/wp-content/uploads/2025/09/ITG_Policies-Procedures_Aug_2025.pdf; and 47 C.F.R. §64.1200(n).

[35] 47 C.F.R. §64.1200(n).

calls rather than blocks them; carriers use the attestation data to make downstream blocking and labeling decisions. Attestation rates remain incomplete, limiting the framework's reach.

Traceback can also be used to stop robotexts, but no equivalent authentication framework exists for text messages. Identifying illegal text campaigns depends heavily on consumer complaints and provider reports; once the FCC receives a complaint, it notifies the carrier, and a traceback may be manually initiated.

Reassigned Numbers Database

The FCC created the Reassigned Numbers Database (RND) in December 2018 as a means of consent verification to prevent consumers from getting unwanted calls or texts intended for someone who previously held their phone number.[36] The RND, which became operational on November 1, 2021, is used by legitimate marketers to determine whether a telephone number may have been reassigned so they can avoid contacting consumers who have not given consent to receive calls or texts.

The RND operates differently for robocalls and robotexts. For robocalls, callers using an autodialer or prerecorded voice are strongly incentivized to query the RND before contacting consumers where prior express consent is required: a query showing the number has not been reassigned provides a legal safe harbor against TCPA liability for inadvertent contact with a non-consenting consumer, though the query itself is not strictly mandated.[37]

For robotexts, no equivalent mandatory pre-text query requirement exists. The FCC has issued a narrow waiver allowing mobile providers to use the RND to verify whether a number subject to a blocking order has been permanently disconnected—primarily to prevent over-blocking of lawful texts sent to new subscribers of a reassigned number—but the absence of a general mandatory query requirement for texts makes enforcement in this area largely reactive.[38]

Do Not Originate Lists, Red Flags, and Know Your Customer

Do Not Originate (DNO) lists, red flags, and Know Your Customer (KYC) are defensive measures in fighting robocalls and robotexts.[39] DNO lists allow automated "rules-based" blocking of certain calls and texts.[40] Red flags indicate to providers that additional information about a call or text may be required to determine whether it is fraudulent or not. Finally, KYC places a due diligence obligation on service providers to investigate the legitimacy of their customers and the

[36] FCC, *Advanced Methods to Target and Eliminate Unlawful Robocalls: Second Report and Order*, CG Docket 17-59, December 12, 2018, https://docs.fcc.gov/public/attachments/FCC-18-177A1.pdf. The Reassigned Numbers Database (RND) can be found at https://www.reassigned.us/.

[37] FCC, "Reassigned Numbers Database," April 4, 2025, https://www.fcc.gov/reassigned-numbers-database.

[38] FCC, *Targeting and Eliminating Unlawful Text Messages: Second Report and Order*, CG Docket 21-402, December 13, 2023, https://docs.fcc.gov/public/attachments/FCC-23-107A1.pdf (hereinafter FCC, *Targeting and Eliminating Unlawful Text Messages*).

[39] The text equivalent is sometimes referred to as DNOT—Do Not Originate Text—and applies only to SMS and MMS providers. Messaging services such as WhatsApp, Signal, and Telegram (called over-the-top or OTT apps) are explicitly exempt because they are not considered telecommunications services. These messaging services are also outside the scope of the red flag rules.

[40] The scope of Do Not Originate (DNO) is narrower for robotexts than for robocalls. The FCC permits analytics-based blocking for robocalls and has proposed studying such blocking in the case of robotexts. See FCC, *Targeting and Eliminating Unlawful Text Messages*, December 13, 2023; FCC, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991: Second Report and Order*, CG Docket 02-278; and FCC, *Advanced Methods to Target and Eliminate Unlawful Robocalls: Waiver Order*, CG Docket 17-59, December 13, 2023, https://docs.fcc.gov/public/attachments/FCC-23-107A1.pdf.

traffic those customers generate before harm occurs. **Table 3** compares DNO lists, red flags, and KYC.

DNO Lists

DNO lists contain phone numbers that should never place outbound calls. The FCC first authorized telecommunications carriers to use DNO lists to block unwanted calls in 2017[41] and has required their use since December 15, 2025.[42] The FCC began requiring the use of a DNO list for text messages on May 11, 2023.[43] The rules require that three categories of numbers be included in DNO lists:

- Inbound-only numbers: should never originate calls. For example, many government agencies, banks, utility providers, emergency helplines, and medical facilities use these numbers.
- Unused or unassigned numbers: can be used by robocallers to circumvent authentication methods.
- Flagged numbers linked with previous fraud: have been identified as illegitimate by industry fraud specialists or law enforcement agencies.

Unlike in the RMD, no single, official DNO list exists, and the FCC does not maintain or endorse any list. Carriers can create their own list or use a third-party list. The FCC requires carriers use a "reasonable" list that includes the three categories above, as well as numbers for which subscribers have requested blocking.

Red Flags

Red flags[44] are warning signs or suspicious patterns identified by telecommunications providers using analytics systems often driven by AI. Although tracking red flags is voluntary (i.e., the FCC does not require carriers to do so), carriers use them to identify potential illegal or unwanted calls. Unlike numbers on a DNO list, red flags trigger an analysis or potential spam label on a call or text rather than an immediate and automatic block. This tool can be used to complement automatic blocking based on DNO lists, which tend to be more static in nature. Some indicators used include a high volume of calls from a single number in a short period; calls originating from multiple locations using the same caller ID; and unusual calling patterns, such as a large number of outbound calls without connections.

[41] FCC, *Advanced Methods to Target and Eliminate Unlawful Robocalls: Report and Order and Further Notice of Proposed Rulemaking*, CG Docket 17-59, November 16, 2017, https://docs.fcc.gov/public/attachments/FCC-17-151A1.pdf.

[42] FCC, "FCC Announces Effective Date for Providers to Block with a DNO List," September 29, 2025, https://www.fcc.gov/document/fcc-announces-effective-date-providers-block-dno-list; and FCC, *Advanced Methods to Target and Eliminate Unlawful Robocalls: Eighth Report and Order*, CG Docket 17-59, February 27, 2025, https://docs.fcc.gov/public/attachments/FCC-25-15A1.pdf.

[43] FCC, *Targeting and Eliminating Unlawful Text Messages: Report and Order and Further Notice of Proposed Rulemaking*, CG Docket 21-402, March 16, 2023, https://docs.fcc.gov/public/attachments/FCC-23-21A1.pdf. This mandate does not cover "over-the-top" messaging services such as iMessage, WhatsApp, or Rich Communication Services (RCS) because they are not regulated as telecommunications services.

[44] FCC, *Targeting and Eliminating Unlawful Text Messages*.

Know Your Customer

KYC is a set of tools that businesses, including the telecommunications industry, use to verify the identities of their customers, among other things.[45] KYC is both an initial step and an ongoing process to protect consumers from becoming victims of scams and illegal robocall activity. KYC is a mandatory obligation with flexible implementation, meaning the FCC requires customer vetting but does not prescribe the specific steps a company must take to achieve that obligation. This process is intended to answer questions such as "Is this a legitimate customer?," "Are they who they claim to be?," and "Are they going to utilize the network and services for appropriate and legal reasons?"

To enhance the existing KYC requirement, the FCC is seeking comment on the specific information originating providers must obtain from customers before they can make calls, how they should verify that information, and how it can enforce violations proportionate to the harms they cause. The intention is to provide additional clarity to fill any gaps between general KYC requirements and the types of rigorous steps necessary to protect consumers from illegal robocalls.[46]

Table 3. Comparison of Do Not Originate Lists, Red Flags, and Know Your Customer

Feature	DNO Lists	Red Flags	KYC
Mechanism	Blacklist of specific numbers that should never originate calls	Indicators of suspicious patterns or activities	Ongoing due diligence obligation requiring providers to verify the legitimacy of customers and the traffic they generate
Action taken	Automatic blocking of the call	Triggers analysis, potential blocking, or labeling as "spam likely"	Investigation of suspicious customers or partners
Basis	Static, predefined numbers (e.g., inbound only, invalid numbers)	Dynamic, behavior-based analytics and patterns (e.g., call volume, origin)	Initial and ongoing monitoring of customers; risk-based
Certainty	High certainty that a call is fraudulent if the number is on the list	Indicates a possibility of fraud; requires further assessment	Indicates a possibility of fraud; requires further assessment
Applies to Robocalls?	Mandatory as of 5/11/23 (47 C.F.R. §64.1200(o))	Voluntary (FCC does not require carriers to track; carrier discretion)	Mandatory obligation, flexible implementation (47 C.F.R. §64.1200(n)(4) requires affirmative measures; specific steps not prescribed)
Applies to Robotexts?	Mandatory as of 12/11/23 (47 C.F.R. §64.1200(p)); does not apply to "over-the-top" (OTT) messaging such as iMessage, WhatsApp, or Rich Communication Services	Voluntary (explicitly outside the scope of FCC red-flag rules for OTT apps; voluntary for SMS/MMS providers)	Voluntary/industry-enforced practice

Source: Compiled by CRS. DNO = Do Not Originate; KYC = Know Your Customer.

[45] 47 C.F.R. §64.6305. See also U.S. Bank, "Why Know Your Customer (KYC)—for Organizations," https://www.usbank.com/corporate-and-commercial-banking/insights/risk/compliance/why-kyc-for-organizations.html.

[46] FCC, Advanced Methods to Target and Eliminate Unlawful Robocalls; Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991: Further Notice of Proposed Rulemaking, CG Dockets 17-59 and 02-278, April 9, 2026, https://docs.fcc.gov/public/attachments/DOC-421205A1.pdf.

Consumer Options

In addition to the rules created by the FCC and the tools used at the network level, several consumer options may also be used to reduce unwanted calls and texts. These include built-in phone features, carrier-provided tools, and third-party apps.

Built-In Phone Features

Most smartphones offer free, built-in features to help manage and filter unwanted text messages. See the following two examples:

- The Android Messages app includes an option to enable spam protection. It uses Google technology to detect, flag, and block suspected spam texts.[47]
- iPhone users can send texts from any number not in their contacts list into a separate Unknown Senders folder in the Messages app.[48]

Both Android and iPhone allow consumers to manually block specific phone numbers; however, spammers frequently change numbers.

Carrier-Provided Tools

Major mobile carriers provide their own services and apps to help protect their customers from spam texts and calls, often using advanced filtering on the network level. See the following three examples:

- AT&T offers the ActiveArmor app, which helps block fraud and spam texts.[49]
- T-Mobile provides the Scam Shield app to block and identify scam texts and calls.[50]
- Verizon has the Call Filter service for screening and blocking unwanted messages and calls.[51]

Consumers can also report spam by forwarding the message to their carrier using the short code 7726 (which spells "SPAM"). Carriers can then use that information to investigate and block similar messages in the future.

Third-Party Apps

Many third-party apps provide more advanced filtering and blocking features, often with a monthly or yearly subscription. See the following five examples:

- Hiya provides spam blocking and caller ID services. It uses a database to identify and block millions of spam calls and texts daily.[52]

[47] Consumers can turn on this option by opening the Messages app, tapping the profile icon or the three-dot menu, and enabling Spam Protection through Settings.

[48] Users will not receive notifications for these messages, and they can review them or delete them in bulk. To enable this, users can go to Settings, then Messages, and turn on Filter Unknown Senders.

[49] AT&T, "ActiveArmor," https://www.att.com/security/active-armor/.

[50] T-Mobile, "ScamShield," https://www.t-mobile.com/benefits/scam-shield.

[51] Verizon, "Call Filter," https://www.verizon.com/solutions-and-services/add-ons/protection-and-security/call-filter/.

[52] Hiya, https://www.hiya.com/.

- Nomorobo offers tools for blocking robotexts and calls. It filters them into a spam folder, preventing alerts.[53]
- Robokiller uses Answer Bots (recorded messages) to engage with the caller (with the intention of wasting their time), in addition to blocking text messages using predictive algorithms.[54]
- Truecaller identifies unknown calls and automatically blocks spam. Its community-sourced database may flag potential scammers.[55]
- YouMail provides call blocking, smart visual voicemail, and virtual phone numbers to manage privacy.[56]

Selected FCC Robocall Activities, 2024-2026

The FCC has taken a range of steps to stop illegal robocalls, including removing noncompliant carriers from the RMD and regulating the use of AI in robocalls. These and other actions are discussed below.

Removal of Noncompliant Carriers from the RMD

In December 2024, the FCC ordered 2,411 providers to cure deficient filings or provide a reason why they should not have their RMD certification revoked, which would trigger removal from the RMD.[57] In early August 2025, the FCC revoked RMD certification for 185 providers and removed them from the database; all had appeared in at least one traceback as an originating, gateway, or nonresponsive provider.[58] Later the same month, the FCC revoked RMD certification for over 1,200 additional providers and removed them from the database.[59] These were among the most sweeping instances of the FCC removing carriers from the RMD.

In August 2025, a bipartisan group of 51 state attorneys general launched Operation Robocall Roundup, which sent warning letters to 37 voice providers; the letters demanded that they stop illegal robocalls from being routed through their networks.[60] The letters were sent to providers that the attorneys general noted had not complied with FCC rules requiring traceback support, RMD certification, and robocall mitigation plans.[61]

[53] Nomorobo, https://www.nomorobo.com/.

[54] Robokiller, https://www.robokiller.com/.

[55] Truecaller, https://www.truecaller.com/.

[56] YouMail, https://www.youmail.com/.

[57] FCC, "FCC EB Orders 2,411 Companies to Cure RMD Deficiencies or Risk Removal," December 10, 2024, https://www.fcc.gov/document/fcc-eb-orders-2411-companies-cure-rmd-deficiencies-or-risk-removal.

[58] FCC, "FCC Removes Non-Compliant Providers from Robocall Mitigation Database," August 6, 2025, https://www.fcc.gov/document/fcc-removes-non-compliant-providers-robocall-mitigation-database.

[59] FCC, "FCC Bars Over 1,200 More Providers from Robocall Mitigation Database," August 25, 2025, https://www.fcc.gov/document/fcc-bars-over-1200-more-providers-robocall-mitigation-database.

[60] State of Indiana, "Attorney General Todd Rokita Launches Operation Robocall Roundup, Issuing Warnings to 37 Telecom Companies," August 11, 2025, https://events.in.gov/event/attorney-general-todd-rokita-launches-operation-robocall-roundup-issuing-warnings-to-37-telecom-companies.

[61] FCC, "FCC Bars Over 1,200 Providers from Network Access for Their Continued Non-Compliance with Robocall Protections," August 25, 2025, https://docs.fcc.gov/public/attachments/DOC-414073A1.pdf.

Consent Decree for Violating STIR/SHAKEN Rules

On August 21, 2024, the FCC announced a settlement to resolve an enforcement action against Lingo Telecom, a voice service provider that transmitted spoofed robocalls that used generative AI voice cloning technology. The company agreed to pay a $1 million civil penalty and implement a compliance plan requiring strict adherence to the STIR/SHAKEN caller ID authentication rules, including requirements that the company more thoroughly verify the accuracy of the information provided by its customers.[62]

Consumer Communications Information Services Threat Classification

On May 13, 2024, the FCC's Enforcement Bureau, for the first time, officially classified a group of entities and individuals that was facilitating ongoing robocall campaigns aimed at defrauding and harming consumers as a Consumer Communications Information Services Threat (C-CIST). This classification is intended to provide international partners with another means to identify known threats before they reach U.S. networks. The creation of the C-CIST classification is intended to build on the agency's "Spring Cleaning" enforcement actions against calls that facilitate the misuse of generative AI voice cloning and provide a means to name persistent bad actors.[63] The first C-CIST designation was for a group of entities and individuals known collectively as "Royal Tiger," which was classified as "C-CIST1." The FCC designated the group "Green Mirage" as C-CIST2 in January 2025 for perpetrating a mortgage relief scam targeting homeowners.[64]

Delay of Rules for Revoking Consent

On February 15, 2024, the FCC adopted rules to, among other things, require companies to offer consumers the ability to revoke their consent, using any "reasonable means," to be called or texted.[65] For example, the FCC would consider terms such as "stop," "end," "revoke," "cancel," and "unsubscribe" as being reasonable means for a consumer to revoke consent. The rules also clarified that if a consumer revokes consent, that revocation would apply to both robocalls and robotexts and would revoke consent from calls or texts from the entire company, not just for a specific campaign.

The FCC extended the effective date of certain requirements under Section 64.1200(a)(10) of Title 47 of the *Code of Federal Regulations*—including the "revoke-all" requirement—from April

[62] FCC, "FCC Settles Case Against Provider that Transmitted Spoofed AI-Generated Robocalls for Election Interference in New Hampshire," August 21, 2024, https://docs.fcc.gov/public/attachments/DOC-404951A1.pdf. The full settlement text is available at FCC, "FCC EB Settles with Lingo for Transmitting Illegal Robocalls," August 21, 2024, https://www.fcc.gov/document/fcc-eb-settles-lingo-transmitting-illegal-robocalls.

[63] FCC, "FCC Classifies Repeat Robocall Bad Actor as First 'C-CIST,'" May 13, 2024, https://www.fcc.gov/document/fcc-classifies-repeat-robocall-bad-actor-first-c-cist. This web page has links to the news release, public notice, advisory, and fact sheet, all containing slightly different information.

[64] FCC, "FCC Enforcement Advisory: FCC Enforcement Bureau Classifies 'Green Mirage' as Second Consumer Communications Information Services Threat (C-CIST2)," January 14, 2025, https://docs.fcc.gov/public/attachments/DA-25-41A1.pdf.

[65] FCC, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991: Report and Order and Further Notice of Proposed Rulemaking*, CG Docket 02-278, February 15, 2024, https://docs.fcc.gov/public/attachments/FCC-24-24A1.pdf.

11, 2025, to January 31, 2027.[66] The delayed requirements include the obligation to treat a revocation of consent made in response to one type of informational message as a revocation applicable to all future robocalls and robotexts from that caller. Until that date, businesses are required to stop only the specific type of communication in response to which the consumer revoked consent, rather than all communications. For example, if a consumer were to revoke consent via text message, the caller would be required only to stop texting the consumer; the caller could continue to make voice calls if the consumer had previously consented to voice calls. Similarly, until January 31, 2027, a revocation sent in response to communications from one business unit of a company will not necessarily cease calls or texts from another business unit of the same company.

Regulation of AI-Generated Robocalls

On February 2, 2024, the FCC declared that AI-generated voices are "artificial" under the TCPA.[67] The rule is intended to prevent the use of AI to deceive consumers, such as by impersonating public figures. This means that robocalls using AI-generated voices are generally illegal unless callers obtain explicit, documented consent from individuals before making such calls, as with other types of robocalls.

All prerecorded or artificial voice messages, including those using AI, must clearly identify the caller at the beginning of the message and provide a contact number. For telemarketing calls, an automated opt-out mechanism must also be available throughout the call. The FCC exempted calls made for emergency purposes (e.g., safety alerts). Under the updated rule, the FCC may issue substantial fines, and state attorneys general and individuals are allowed to pursue legal action and seek monetary compensation from parties making these calls.[68]

One-to-One Consent Rule Repealed

The FCC's one-to-one consent rule for marketing calls and texts was set to take effect on January 27, 2025. The rule would have closed what is referred to as the "lead generator" loophole by requiring telemarketers to obtain one-to-one consent from consumers for covered calls. In other words, the consumer would have to give prior express written consent to receive calls from each single seller, rather than a broad group of sellers from one lead generation form. On January 24, 2025, the U.S. Court of Appeals for the Eleventh Circuit vacated the rule, citing agency overreach, and the FCC formally repealed the rule on July 14, 2025.[69]

[66] FCC, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991: Order*, CG Docket 02-278, January 6, 2026, https://docs.fcc.gov/public/attachments/DA-26-12A1.pdf.

[67] FCC, *Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts: Declaratory Ruling*, CG Docket 23-362, February 2, 2024, https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf.

[68] Victims may receive $500-$1,500 per call or text, with higher amounts for willful violations.

[69] Insurance Marketing Coalition Limited v. FCC, 127 F.4th 303 (11th Cir. 2025); and FCC, "FCC Removes One-to-One Consent Rule Nullified by Court Decision," July 14, 2025, https://www.fcc.gov/document/fcc-removes-one-one-consent-rule-nullified-court-decision.

The Role of Artificial Intelligence in Enabling and Combating Robocalls

AI is being used both to create scam calls and assist consumers in identifying such calls. Recently, scammers have begun using generative AI (GenAI). GenAI is a "type of [AI] capable of generating new content—including text, images, or code—often in response to a prompt entered by a user."

Voice Cloning

Scammers are using GenAI to copy or "clone" voices of people a telephone call recipient might know. This technique replicates a person's voice using an existing set of audio clips, usually found online (e.g., TikTok or YouTube videos). For example, it has been used to create calls that sound like a family member in distress and in need of money.

For this scam, it is important to delineate which technologies are being used and how the combination of those technologies can be regulated and enforced. Although the content of these calls (i.e., the voice a call recipient hears) is created using AI technology, it would not legally be considered a robocall unless an autodialer were also used. Given the targeted nature of these types of scams, it is unlikely that an autodialer would be employed. If a spoofed number were used, it is possible that STIR/SHAKEN authentication could block the call from reaching the intended recipient. However, STIR/SHAKEN is not capable of determining the content of a call, only whether its origin is likely to be fraudulent.

Filtering and Screening Robocalls

Another way GenAI can be used to spot scams is by checking for grammatical errors or poor translations from a foreign language to English. One company, Truecaller, has created AI-based tools to identify spoofed robocalls and stop them from reaching consumers. For example, an "AI assistant" could be used to answer and filter calls so they do not reach the consumer. The same tool would be able to ensure that the user does not miss important calls, such as a reminder for a doctor appointment.

Legislation in the 119th Congress

Since the TRACED Act, which passed with broad support in the 116th Congress, lawmakers have pursued additional federal legislation to curb robocalls for the past several sessions. Four bills have been introduced in the 119th Congress that directly address robocall regulation, several of which were introduced in previous Congresses. No hearings specific to robocalls have been held in the 119th Congress as of the date of this report.

H.R. 6152/S. 2666, Foreign Robocall Elimination Act

The Foreign Robocall Elimination Act (H.R. 6152) would direct the FCC to establish a task force on unlawful robocalls originating overseas and submit a report to Congress not more than 360 days after the task force is established. Additionally, this legislation would require a provider to post a bond of not more than $100,000 before filing a certification to the RMD if such a bond is determined necessary by the FCC to preserve the integrity of the RMD. H.R. 6152 is similar to

legislation introduced in the House in the 117th and 118th Congresses. The current version introduced the bond requirement and longer-term surveillance of call data.

There is a similar version of this bill in the Senate, S. 2666. That bill would direct the FCC to establish a task force on unlawful robocalls and require the FCC to submit a report to Congress not more than 360 days after the task force is established to address issues related to robocalls originating overseas. S. 2666 also contains a bond requirement, though it differs from the House version in one respect: whereas H.R. 6152 would authorize the FCC to impose a bond through rulemaking if it determines one is necessary, S. 2666 would mandate that telephone companies post a $100,000 bond and register in the RMD before transmitting calls in the United States.

H.R. 1027, Quashing Unwanted and Interruptive Electronic Telecommunications (QUIET) Act

H.R. 1027 would establish a disclosure requirement for robocalls that use AI to emulate a human being and increase forfeiture and fine amounts for certain violations of the TCPA.[70] The bill also proposes doubling the maximum forfeiture penalty and criminal fine that may be imposed for certain violations of the TCPA involving the use of AI to impersonate an individual or entity with the intent to defraud, cause harm, or wrongfully obtain anything of value.

H.R. 334, Amending the Communications Act of 1934

H.R. 334 would provide "statutory authority for the application of standards to systems that transmit artificial or prerecorded telephone messages generated using AI." Specifically, the standards would require that

- such messages clearly identify and state the telephone number or address of the individual or entity initiating the call and that
- any system making such phone calls release a recipient's telephone line within five seconds of notification that the recipient has ended the call.

The FCC would develop and implement standards that would apply to any system used to transmit an artificial or prerecorded voice message by telephone.

Options for Congress

While Congress has provided the legal framework through which the FCC and the telecommunications industry have developed and implemented technical and procedural tools to combat illegal robocalls, some options for further action remain.

Congress may advance one or more of the bills targeting robocalls that have been introduced in the 119th Congress. For example, the Foreign Robocall Elimination Act (S. 2666) would shift the focus on fighting robocalls from technical and procedural tools to economic incentives. The legislation would require voice service providers to post a bond before they could register with the RMD. Since some service providers profit from high call volumes,[71] the bond requirement

[70] Specifically, any robocall that uses artificial intelligence (AI) to emulate a human being must include a disclosure at the beginning of the message indicating that AI is being used. Under the bill, robocalls are defined as calls made or text messages sent (1) using automatic dialing technology or (2) using an artificially generated message or an artificial or prerecorded voice. Calls or texts that are made or sent using equipment that requires substantial human intervention are excluded.

[71] U.S. PIRG, "Who's Calling?," February 6, 2025, https://pirg.org/edfund/resources/whos-calling.

would give insurers incentive to rigorously vet companies they cover. If providers allow illegal, spoofed, or other scam traffic to pass through their networks, insurers can forfeit these bonds to pay consumer damages. This would provide carriers an incentive to block fraudulent calls. Supporters argue that altering the financial landscape for call providers may prove more effective than trying to outpace scammers technologically.[72] While large providers may be able to absorb such a cost, smaller providers may find that such a requirement causes an undue financial burden or diverts funding from network upgrades needed to fully implement STIR/SHAKEN.

The FCC has the authority to impose civil fines for illegal calls and texts, but collection rates are low. If Congress were to provide the FCC with the authority to collect the fines it imposes, that authority could provide another financial incentive to deter would-be scammers (see discussion in "The Telephone Consumer Protection Act"). The FCC Legal Enforcement Act (S. 2095), introduced in the 118th Congress, would have given the FCC authority to pursue unpaid fines for violations of the TCPA via litigation. Under existing law, DOJ pursues unpaid fines for these violations. S. 2095 would have given DOJ a set period to pursue litigation to collect an unpaid fine, and, if it did not do so, the FCC would have been granted that authority. Executing this authority may require additional personnel (i.e., specialized attorneys) at the FCC to conduct litigation. If Congress chooses to pursue a similar piece of legislation to S. 2095, lawmakers may consider providing additional resources (such as through the appropriations process, authorization to substantially increase existing regulatory fees, or creation of new regulatory fees) to the FCC to support these new litigation activities. Congress may also consider directing DOJ to prioritize robocall enforcement without altering the FCC's authorities.

Congress may also continue its oversight of the FCC with respect to robocall enforcement without introducing new legislation, develop legislative solutions to options the FCC has decided not to pursue (e.g., one-to-one consent; see "One-to-One Consent Rule Repealed"), or take no action.

[72] National Consumer Law Center, "Strategies for Reducing Scam Calls and Texts by Holding Providers Accountable," September 30, 2025, https://www.nclc.org/resources/strategies-for-reducing-scam-calls-and-texts-by-holding-providers-accountable/; and Aaron Mak, "Congress Takes a New Swing at Robocalls," *Politico*, October 27, 2025, https://www.politico.com/newsletters/digital-future-daily/2025/10/27/congress-takes-a-new-swing-at-robocalls-00623971.

Author Information

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

Disclaimer