FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	**CG Docket No. 17-59**
	)	
	)	
Call Authentication Trust Anchor	)	**WC Docket No. 17-97**
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act	)	**CG Docket No. 02-278**
	)	
	)	
Dismissal of Outdated or Otherwise Moot Robocalls Petitions	)	**CG Docket No. 25-307**

Comments of

National Consumer Law Center
on behalf of its low-income clients

Electronic Privacy Information Center (EPIC)

and

National Association of Consumer Advocates

Table of Contents

Comments

Introduction and Summary

These Comments, submitted by the National Consumer Law Center (NCLC) on behalf of its low-income clients, and joined by the Electronic Privacy Information Center (EPIC) and the National Association of Consumer Advocates (NACA), are submitted in response to the Further Notices of Proposed Rulemaking and Public Notice released by the Federal Communications Commission (Commission or FCC) on October 29, 2025,[1] and published in the Federal Register on December 5, 2025.[2]

We appreciate the fact that in this combined rulemaking, as well as in the recently adopted Third Report and Order and Further notice of Proposed Rulemaking regarding VoIP numbering authorization,[3] the Commission is paying attention to the continuing problem of unwanted and illegal telephone calls plaguing the American telephone system. However, it must be recognized that billions of calls made every month are dangerous scam calls which cumulatively cost an estimated 52 million people more than $25 billion every year.[4] It is essential that the FCC prioritize solving this problem with aggressive requirements to shut down these calls.

As explained in **Section I**, the most important thing the FCC can do to stop scam calls is to *require* that terminating voice service providers use effective analytics to block calls that are deemed

---

[1] FCC, Ninth Further Notice of Proposed Rulemaking in CG Docket No. 17-59; Seventh Further Notice of Proposed Rulemaking in WC Docket No. 17-97; Further Notice of Proposed Rulemaking in CG Docket No. 02-278; Public Notice in CG Docket No. 25-307 (adopted October 28, 2025, released October 29, 2025) (Further Notice) https://docs.fcc.gov/public/attachments/FCC-25-76A1.pdf.

[2] https://www.govinfo.gov/content/pkg/FR-2025-12-05/pdf/2025-22063.pdf

[3] FCC, Third Report and Order and Third Further Notice of Proposed Rulemaking, WC Docket Nos. 13-97, 07-243, 20-67 (adopted December 18, 2025, released December 19, 2025) https://docs.fcc.gov/public/attachments/FCC-25-86A1.pdf

[4] https://publicinterestnetwork.org/wp-content/uploads/2024/10/US-SpamScam-Report_2024_0307.pdf

likely to be scams. Requiring terminating providers to block calls transmitted by complicit upstream providers will change the entire network for the better. It will incentivize legal callers and all providers in the call path to ensure that their calls are not mixed with those sent by providers who are transmitting the scam calls.

In **Section II,** we explain our concerns about relying on the Commission's proposal to "give consumers accurate caller name and other information that enables them to regain control of their phones by ensuring they no longer have to guess whether a call is one they want to pick up."[5] We agree that consumers should have full and accurate caller name information to decide whether to answer a call. Providing call recipients with caller name information can help them to avoid wasting time on unwanted calls. And it could—*if it was accurate*—help call recipients avoid scam calls. However, given the ease with which scammers can falsify caller name information, requiring caller name information is more likely to give called parties a false sense of security, giving scammers an additional edge. While we support the idea of transmitting call name information, we urge the Commission not to put a new rule into effect until there are stronger protections against scam calls and falsification.

In **Section III** of these Comments, we support the Commission's proposal to prohibit calls originating from outside the United States from spoofing into U.S. phone numbers under the North American Numbering Plan. Gateway carriers should be responsible for accurately reporting the geographic regions from which the traffic they transmit originates. The Commission should require that gateway carriers block all foreign originated calls that use numbers assigned to the United States under the North American Numbering Plan, with only limited exceptions such as calls placed by U.S. consumers roaming on foreign wireless networks.

[5] Further Notice at ¶ 2.

In **Section IV** we urge the Commission to revise its rules on the revocation of consent. The Commission should specify several easy, automated methods for revoking consent, and provide that if one of those methods is fully described in the call or text message itself, then the caller may designate it as the exclusive means of revocation. However, a caller that does not satisfy these requirements must be required to honor all reasonable methods of revoking consent.

Finally, in **Section V** we urge the Commission not to alter the rule regarding call abandonment or the rule requiring telemarketers provide a toll-free or low-cost phone number for do-not-call requests. We also urge the Commission to make limited modifications to the exception that allows financial institutions to send fraud alerts to phone numbers that have not been provided by their customers.

I. Terminating providers should be required to block suspicious calls.

Scam calls are extremely damaging to consumers, directly causing reported losses of billions of dollars every year.[6] When combined with their close cousins—unstoppable telemarketing calls—these calls significantly undermine the reliability and usefulness of the American telephone system.[7]

[6] Data from the Federal Trade Commission shows that reported losses to fraud climbed from $10 billion in 2023 to $12.5 billion in 2024, with phone calls and text messages among the most common contact methods for scams. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024; FTC Consumer Sentinel Network, Fraud Reports by Contact Method, Reports and Amount Lost by Contact Method, *Consumer Sentinel Network Data Book 2024*, at pg. 12 (2024 figures). Data from 2023 is available at https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf. The Consumer Sentinel Network is a "unique investigative cyber tool" that contains millions of reports on fraud including impostor scams and telemarketing scams. https://www.ftc.gov/enforcement/consumer-sentinel-network.

[7] See e.g., FCC, Second Report and Order, Second Further Notice of Proposed Rulemaking in CG Docket Nos. 02-278 and 21-402, adopted December 13, 2023, released December 18, 2023, at ¶¶ 5-11 (stating that unwanted and illegal calls and text messages harm consumers and noting FCC actions to address the problem). Available at https://docs.fcc.gov/public/attachments/FCC-23-107A1.pdf.

In response to the scourge of unwanted and illegal calls, the Commission has undertaken "a new campaign to tackle illegal robocalls at every point in the call path."[8] We applaud the Commission for recognizing the problem and embarking on a fresh, comprehensive approach. However, the most effective way to stop scam calls is to require, not just allow, providers to block illegal calls. We urge the Commission to make strengthening call blocking its primary focus.

In 47 C.F.R. § 64.1200(k), the Commission has promulgated a comprehensive system that *allows* providers to block voice calls that are unwanted. However, subsection (k) does not *mandate* that providers employ all the available tools at their disposal to determine which calls are likely illegal and then block them. Continuing volumes of consumer complaints and the magnitude of consumer losses to scam calls show that the current permissive blocking rules set forth in subsection (k) are not sufficient. And as explained in section II, *infra,* requiring additional information to be included in caller-ID is insufficient to protect subscribers from dangerous calls.

The gold standard for protecting subscribers from unwanted—or at least dangerous—calls is to require terminating providers to use all available tools to determine which calls are likely to be illegal and then block those calls. It is time for the Commission to employ this gold standard.

Ideally, the Commission should require all providers, regardless of their role in the call path, to a) determine that call traffic does not contain high volumes of scams or otherwise illegal robocalls, and b) block call traffic where substantial portions of the calls are illegal or of unknown legality. However, this requirement should be most emphatically imposed on terminating providers who should have an affirmative duty to protect their own customers, the telephone subscribers, from likely scam calls. As we explain, even if the duty to use reasonable analytics and to block calls is

[8] FCC Takes First Major Step in Fresh Approach to Combatting Illegal Robocalls, October 28, 2025. https://docs.fcc.gov/public/attachments/DOC-415139A1.pdf

only imposed on terminating providers, that requirement will create significant incentives on all other providers in the call path to deploy analytics to block scam calls.

Requiring terminating providers to use reasonable analytics and block likely illegal calls would cause all providers in the call path to be more careful about what calls they transmit. Not only might upstream providers lose revenue when terminating providers block call traffic that fails analytics tests, but by transmitting those "dirty" calls terminating providers will be more likely to block all traffic from that upstream provider, making it expensive for a provider to have a bad reputation.[9] As a result, requiring that terminating providers use reasonable analytics, including analytics incorporating information about how often upstream providers in the call path have sent illegal traffic, to determine which calls are likely scam calls and block those calls, creates more cops on the beat: all the providers in the telecommunications network will be enforcers against illegal calls. This will be a win-win for the entire system.

Another part of an effective system to stop scam calls is to strengthen know-your-customer rules. We strongly support the Commissions' plan, noted in ¶49 of the Further Notice, to open a separate proceeding on these requirements. Know-Your-Customer rules which require providers to determine and monitor metrics for their customer's call traffic, such as the average call duration and the average number of unique phone numbers used to place calls, will greatly facilitate effective call blocking. Providers should know what type of call traffic their customers will transmit and be ready to investigate and potentially block call traffic when it changes unexpectedly.

[9] As described further below, the current rules have not resulted in a provider's reputation for transmitting illegal calls leading to financial consequences. See Section II, *infra*.

II. Requiring Caller Name Information can help consumers but should not be required until stronger safeguards against falsification are in place.

We agree with the Commission's assertion that "[i]f consumers have trustworthy caller identity information, they can make better informed decisions about whether to answer a call, which is likely to lead to higher answer rates and engagement."[10] In theory, caller-ID information can enable subscribers to screen their calls and refuse scam and other unwanted calls. But, even with the suggested improvement in caller-ID information, bad actors will still be able to send false or misleading caller identity information. Relying on potentially inaccurate caller identity information as a primary means to protect subscribers from dangerous calls will not stop the harms caused by these calls. Indeed, it is likely to give called parties a false sense of security, making them more rather than less vulnerable to scams.

One of the gaps in regulation that makes misleading caller ID information possible is that callers can "rent" large quantities of telephone numbers to deliberately evade the Commission's requirements for callers to identify themselves properly.[11] This practice, frequently called "number rotation," already facilitates sending consumers misleading information under the guise of an A-level attestation. By purchasing a temporary right to use a phone number, callers can place calls with the highest attestation level while using a phone number that does not accurately represent their identity. There is no reason to believe that callers who already use rented numbers to provide misleading caller IDs will not also use misleading pseudonyms to make A-attested calls with inaccurate caller ID and name information. Before mandating that terminating providers transmit caller name information whenever they transmit an indication that a call has an A-level attestation, the

[10] Further Notice at ¶32.
[11] NCLC and other groups have previously commented on this issue. See Reply Comments of National Consumer Law Center et al., received December 22, 2023. Available at https://www.fcc.gov/ecfs/document/122235773414/1.

Commission should ban the practice of manipulating attestation levels by renting telephone numbers.

Additionally, some providers habitually transmit scams or otherwise illegal calls with false attestations, and these providers can often go years without facing consequences. As other commentators have pointed out, some providers flout or ignore the rules and routinely transmit calls with false attestations.[12] The STIR/SHAKEN framework ultimately leaves it to the provider to determine whether a caller has a legitimate right to use a telephone number and assumes that the reputational damage a provider should suffer from originating calls with false attestations will ensure that it will be diligent in making accurate attestations.[13] This assumption has proven unjustified, as currently provider reputation does not appear to mitigate the transmission of illegal calls. The Commission need look no further than its own enforcement actions to verify this is the case. For example, in its recent Cease-and-Desist Letter to SK Teleco LLC, the Commission noted that "[a]ccording to STIR/SHAKEN data, the Company was responsible for signing over 97% of all Walmart pre-authorized [scam] calls identified by YouMail between May 2024 and March 2025."[14] Thus it appears that the company was almost exclusively responsible for bombarding consumers with a widespread type of illegal imposter scam robocall for almost a year while it openly attested that it was putting those calls on the network. Downstream providers were continuously apprised of SK Teleco's role in originating scam robocalls through the numerous tracebacks conducted on these calls, yet downstream providers continued to allow SK Telco's scam calls through their networks.

---

[12] See Comments of ZipDX at pg. 3, received October 9, 2025. Available at https://www.fcc.gov/ecfs/document/1009348017728/1.

[13] See ATIS 1000074 .v003 at pg. 12, n. 2 ("Ultimately it is up to service provider policy to decide what constitutes 'legitimate right to assert a TN' but the service provider's reputation may be directly dependent on how rigorous they have been in making this assertion.") Available at https://access.atis.org/apps/group_public/download.php/67436/ATIS-1000074.v003.pdf

[14] Letter to SK Teleco LLC, dated December 2, 2025 at pg. 2. Available at https://docs.fcc.gov/public/attachments/DOC-415638A1.pdf.

The Commission's SK Telco order illustrates that even where a provider has earned a bad reputation, that fact does nothing to prevent that provider from continuing to bombard consumers with scams and other illegal calls. When originating providers can put scam calls on the network for months or years without consequences, it is not helpful, and may be harmful, to require terminating providers to transmit caller name information supplied by these bad actors. We encourage the Commission to change this dynamic by strengthening 47 C.F.R. § 64.1200(k) to require providers, and particularly terminating providers, to block suspected illegal calls based on reasonable analytics, including an upstream provider's history of transmitting illegal calls. Trusting providers to voluntarily block calls from providers with a bad reputation has not worked, and it is time to address this reality.

There is no reason to believe that the currently available methods for circumventing STIR/SHAKEN, such as number rotation, will not undercut the Commission's proposed call labeling rule. Furthermore, while accurate caller name information could help consumers avoid wasting time answering unwanted calls, asking consumers to protect themselves from illegal calls, even if they have reliable caller name information, is at best an incomplete approach to the robocall problem.

A better approach to solving the robocall problem would be to focus on promulgating strong rules requiring providers at all points in the call path to know their traffic and block calls of unknown legality. The Commission should direct its attention to rulemakings that will strengthen call blocking requirements and stop illegal calls before they ever reach consumers. This effort, particularly if undertaken in conjunction with measures to address the short-term rental of telephone numbers and to quickly shut down providers who habitually transmit illegal calls, will have a greater impact than rules requiring the transmission of caller name information.

III. The Commission should adopt its proposal to prohibit foreign calls using U.S. numbers.

We applaud the Commission's proposals to require that gateway providers determine when a call originates outside of the United States and prohibit spoofing of United States telephone numbers on foreign originated[15] calls.[16] Consumers should be able to trust that a caller who uses a United States phone number is in the United States and can be held accountable under U.S. law. Consumers, and even enforcement authorities like state attorneys general, face significant difficulties in establishing jurisdiction in a U.S. court over foreign entities who place illegal calls or attempt illegal schemes using telephone calls. A foreign originated call that uses a United States phone number inherently misleads the called party about the caller's location and consequentially about the availability of effective legal remedies against the caller.

Consumers generally understand that if they purchase a product or service from a person or company located outside of the United States they may have more difficulty holding the seller liable if it breaks its word. For this reason, consumers generally want and expect to know when they are doing business with someone who is located outside of the United States. For instance, many e-commerce websites inform consumers when they are purchasing from a foreign business or if their order will ship from outside of the United States. Allowing foreign callers to spoof into United States phone numbers undermines consumers' reasonable expectation that a U.S. phone number means the caller is domestic. Prohibiting foreign callers from spoofing into United States phone numbers will help consumers know when they are speaking to someone who isn't in the U.S. and

[15] We use the term "foreign originated" to mean a voice or text call where the entity that took the physical steps necessary to initiate transmission of the call for completion on a United States network is within the territorial limits of a jurisdiction other than the United States, its territories, and possessions.

[16] Further Notice at ¶¶ 70-76 & 86.

may not be subject to our laws, which will help to restore consumers' trust in the safety of our phone networks.

Exceptions to the general principle that foreign calls should not use U.S. phone numbers will create enforcement difficulties and should be strictly limited. For this reason, companies that have off-shored their call centers, or otherwise place foreign calls into the United States, should be required to use phone numbers that correspond to the jurisdiction in which their call center or other calling business unit is located. Otherwise, foreign service providers could simply claim that their call traffic originates from U.S. businesses with foreign call centers and gateway providers would have few options to verify the truth of that assertion. The only exceptions to the rule should be for calls which generate a billing record which leads directly to a U.S. network, such as a call from a U.S. subscriber roaming on a foreign network. Strictly limiting exceptions will ensure that gateway providers can more easily identify foreign calls illegally spoofing into U.S. numbers and block those calls.

The Commission's existing regulations require a provider to "[t]ake affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic."[17] The Commission should clarify that "knowing its customers" includes taking reasonable steps to determine what portions of an upstream provider's call traffic originates inside or outside of the United States.

Indeed, the Commission's regulations already require that providers disclose whether they are a foreign voice service provider in their Robocall Mitigation Database filings,[18] and gateway providers are required to "implement an appropriate robocall mitigation program with respect to

[17] 47 U.S.C. § 64.1200(n)(4).
[18] 47 C.F.R. § 64.6305(d)(4)

calls that use North American Numbering Plan resources that pertain to the United States in the caller ID field."[19] These requirements have been in place for years, suggesting that gateway providers have been able determine their call traffic contains foreign originated calls. Given that providers are already required to know the origin of their traffic to an extent that allows them to self-certify as a gateway provider, there is no reason that they should not also be required to transmit information about foreign originated calls through the call path, either by providing this information to their immediate downstream partner or by including the information in the call's signaling header as is done with the attestation level and other information required by STIR/SHAKEN.

All providers have ample opportunities to discern whether call traffic contains foreign originated calls. Downstream providers generally formalize their business arrangements with upstream providers in contracts. There is no reason why these contracts could not obligate an upstream provider to collect and disclose information about the jurisdiction in which call traffic using U.S. phone numbers originates. Providers generally know when they are dealing with foreign upstream customers, as payments from these customers will often come through foreign financial institutions and the IP-address(es) the upstream provider uses to interconnect with the provider are suggestive of whether the customer is foreign or domestic. In short, providers have multiple mechanisms to determine whether call traffic is likely originating from outside the United States and there is no reason that they cannot block calls that likely originated abroad but use U.S. phone numbers.

Lastly, some other countries already require providers to treat foreign originated calls differently than calls that originate domestically, indicating that it is possible to comply with a prohibition such as the Commission proposes. For example, on December 1, 2022, Germany

[19] 47 C.F.R. § 64.6305(b)(1)

implemented regulations requiring providers to hide the calling phone number for calls that attempt to use German numbering resources but originate on foreign networks, with a narrow exception for German subscribers roaming on foreign networks.[20] Other countries' experiences indicate that the FCC's proposal to prohibit the use of U.S. phone numbers for foreign originated calls is an achievable safeguard against harmful spoofing.

IV. Callers must provide clear information about the scope and method of revocation.

As part of the proposed amendments, the Commission proposes to repeal 47 C.F.R. § 64.1200(a)(10), which sets standards for subscribers' revocation of consent, and has called for comments on whether it should allow callers to designate an exclusive means by which subscribers can revoke consent.[21]

We strongly support consumer choice and consumer control over calls and text messages. There is widespread agreement that consumers have the right to revoke consent at any time, in any reasonable way.[22] However, we think that, in this instance, allowing callers a carefully circumscribed ability to mandate that the consumer use a particular method to revoke consent in certain circumstances could promote that goal, by incentivizing callers to make simple, automated, easily-understood methods available and making it easier for consumers to revoke consent

We therefore encourage the Commission to revise 47 C.F.R. § 64.1200(a)(10) to require a caller to honor any reasonable revocation request, except that if the caller informs the called party of

[20] Bundesnetzagentur, Press Release, November 29, 2022. Available at: https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/PressReleases/2022/20221129_NumberManipulation.pdf?__blob=publicationFile&v=1

[21] Further Notice at ¶¶ 101-104.

[22] See e.g., Gager v. Dell Fin. Servs., L.L.C., 727 F.3d 265 (3d Cir. 2013); Osorio v. State Farm Bank, 746 F.3d 1242 (11th Cir. 2014); Van Patten v. Vertical Fitness Grp., 847 F.3d 1037, 1047–1049 (9th Cir. 2017); Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02278, WC Docket No. 07-135, Declaratory Ruling and Order, 30 FCC Rcd 7961, 7989-90, ¶ 47 ("we clarify that a called party may revoke consent at any time and through any reasonable means.").

an easy, automated method of revocation by clearly and conspicuously disclosing it in the call or message itself, then that method may constitute the exclusive means of revocation.

We suggest that the Commission maintain the current waiver of the effective date of subsection (a)(10) while it undertakes further rulemaking to determine the specific methods which could constitute an exclusive means of revoking consent; however, we suggest that methods of revocation already stated in the Commission's rules are the appropriate starting point. The Commission's rules at 47 C.F.R. § 64.1200(b)(3) set forth automated methods to make do-not-call requests during prerecorded or artificially voiced calls and for messages left on answering machines and voicemail services, and the current version of 47 C.F.R. § 64.1200(a)(10) describes an automated method to revoke consent in response to a text message. The Commission could adapt these provisions as the means by which callers can specify the exclusive method of revoking consent, if clearly and conspicuously disclosed to the called party in the voice call, voicemail, or text call.

We also agree that the current provisions about how to construe revocation requests when the caller makes multiple categories of calls would be better if simplified. When a consumer has consented to receive messages for several different purposes, for example appointment reminders as well as marketing communications, and then responds to one type of message by revoking consent, it will often be unclear both to the consumer and to the caller whether that revocation is intended to apply to only one type or all types of messages the consumer has consented to receive. The current version of the rule, requiring and back-and-forth between the consumer and the caller to resolve this ambiguity, is complicated for callers. It also means that in many cases opting out will be a multi-step process for the consumer, with more unwanted messages. And it creates the potential that consumers will mistakenly revoke acceptance regarding calls they want and need—such as a medical office's appointment reminders.

We therefore propose that the current requirements in 47 C.F.R. § 64.1200(a)(12) be revised. The Commission should allow callers to construe a revocation as applying to only the type of message that prompted the revocation--but only if the call or message clearly and conspicuously discloses that the revocation will apply just to that type of message, and provides an automated method to revoke consent for all types of messages for which consent is required.

V. The Commission should not alter or repeal other TCPA rules.

We urge the Commission to not move forward with the proposal to repeal its call abandonment rules or to modify its artificial and prerecorded voice identification rules. We support, with important modifications, the Commission's proposed revisions to the exception allowed for fraud alert calls.

Call Abandonment. In support of the proposed repeal of the call abandonment rule, the further notice posits that the evolution of technology "along with marketers' incentives to avoid negative consumer impressions via dead air and abandoned calls, may mean our rules are no longer necessary."[23] However, this logic breaks down if callers are using advanced technology to avoid leaving evidence of their illegal calls. Consumers cannot form negative impressions of a seller or marketer if they do not know their identity. The Commission should not repeal its call abandonment rules and in so doing encourage abusive tactics that obfuscate the caller's identity.

The Commission is correct that modern dialing equipment leverages advances in technology, including artificial intelligence (AI). However, these advances in technology have not necessarily reduced or eliminated dead air calls that frustrate consumers and waste their time. In fact, the opposite may be true because advances in technology lend themselves to algorithmic screening for live voices, often called answering machine detection, which can be used by illegal callers to avoid

[23] Further Notice at ¶ 98.

leaving incriminating voicemail recordings - instead leaving annoying silence as the computer listens to determine whether a live person has answered. Illegal callers know that leaving voicemails can be risky as they are used for tracebacks and other methods of identifying illegal calls and the providers that facilitate them. Callers can leverage AI to listen for a live voice answering the call and only play a prerecorded message if one is detected. These calls still harass consumers with prerecorded messages or dead air calls that violate the Commission's call abandonment rule, 47 C.F.R. § 64.1200(a)(7). Repealing this rule would in effect authorize use of answering machine detection as a method of evading illegal robocall enforcement efforts.

Modification of Pre-Recorded Voice Caller ID Rules. We urge the Commission to delete its proposal to modify its artificial and pre-recorded voice caller identification rules, 47 C.F.R. §§ 64.1200(a)(7)(i)(A), (b)(2), and (d)(4), to only require that callers identify themselves with their telephone number. This change would permit callers to use 900-numbers as their telephone numbers, which would burden consumers' right to revoke consent. While the Commission is correct that local and long-distance charges are uncommon in the modern telecommunications marketplace, the current regulation gives callers latitude to use ordinary (NPA-NXX-XXXX) numbers under the North American Numbering Plan. It is not necessary to change the current rule to allow callers to use ordinary telephone numbers for processing do-not-call requests. Modifying the current rule to remove the prohibition on 900 numbers or any other number for which charges exceed local or long-distance transmission charges and replacing it with only "a requirement that callers identify themselves with their telephone number to enable called consumers to know who is calling"[24] would allow callers to use pay-per-call numbers as their phone number. There is no reason to allow callers to provide call recipients with only a pay-per-call number to revoke consent or request to be added

[24] Further Notice at ¶ 100.

to a caller's internal do-not-call list. There is no reason to permit businesses to burden consumers' revocation rights by forcing them to pay to contact the caller and make a do-not-call request.

We do not interpret the Further Notice as proposing to eliminate the requirement in 47 C.F.R. § 64.1200(b)(3) that certain calls which leave an artificial or prerecorded-voice on an answering machine or voice mail must include a toll-free number that enables the called party to make a do-not-call request. If the Commission is considering repealing this rule, then we reiterate that the toll-free number requirement provides an important tool for law enforcement authorities to identify evidence of illegal robocalls from voicemail recordings. We urge the Commission to maintain this rule for the reasons articulated in the letter to the Commission dated October 16, 2025,[25] and ex parte presentation noticed on October 20, 2025.[26]

Finally, we understand the banks' request that the Commission's eliminate the requirement that financial institutions call only the number provided by the consumer when making a fraud alert or similar call pursuant to a TCPA exception.[27] We believe that the Commission can meet the banks' needs while protecting subscribers from unwanted wrong-number calls. This can be done by permitting the financial institution to use numbers obtained from a reliable source. The concern expressed by the American Bankers Association[28] that the condition imposed on the exemption limiting the alerts only to wireless numbers provided by the customer, can be addressed by expanding the permissible ways in which institutions can obtain numbers to be called for the fraud alerts exempted in the 2015 Order. Specifically, customer numbers obtained by the institution which were 1) supplied by a family member or other cardholder who has been explicitly authorized by that

[25] Available at https://www.fcc.gov/ecfs/document/10160346025643/1.
[26] Available at https://www.fcc.gov/ecfs/document/10211597300182/1.
[27] Further Notice at ¶ 105.
[28] See Comments of the American Bankers Association, et al., CG Docket No. 02-278, GN Docket No. 25-133, Received April 14, 2025. Available at: https://www.fcc.gov/ecfs/document/104122423211014/1.

customer to be on the account, 2) captured when the customer called the institution, or 3) included in records of accounts purchased from other institutions, can be reasonable means of obtaining numbers to which fraud alerts can be directed. In each of these three sets of circumstances, there is a very high likelihood that the number belongs to the customer, even though the customer did not directly provide the number to the institution.

The Commission should not, however, allow financial institutions to send fraud alerts and other communications excepted by 47 C.F.R. § 64.1200(a)(9)(iii) to numbers that are not reliably associated with their customer, such as numbers obtained from public records searches. Fraud alerts sent to wrong numbers are likely to cause significant alarm to the recipient, undercut the effectiveness of fraud alerts as a tool, and possibly facilitate fraud by making consumers less vigilant about scam text messages impersonating banks. We urge the Commission to recognize the above three methods for reliably obtaining numbers from non-customers instead of removing the customer-provided number requirement completely.

CONCLUSION

We applaud the Commission for continuing its work to reduce illegal and dangerous robocalls. American consumers are under siege by increasingly sophisticated scammers who continue to use the telephone network as their preferred means of identifying and defrauding victims. We urge the Commission to strengthen robocall rules to ensure that only safe, legal communications reach consumers.

Respectfully submitted this 5th day of January 2026, by:

Patrick Crotty
pcrotty@nclc.org
Margot Saunders
msaunders@nclc.org
National Consumer Law Center
1001 Connecticut Ave., NW
Washington, D.C. 20036