FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	**WC Docket No. 17-59**
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	**WC Docket No. 02-278**

Reply Comments of

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

National Association of Consumer Advocates

Consumer Action

Consumer Reports

and

National Consumers League

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

Table of Contents

Reply Comments

Introduction and Summary

These Reply Comments, submitted by the National Consumer Law Center (NCLC) on behalf of its low-income clients, and joined by the National Association of Consumer Advocates, Consumer Action, Consumer Reports and National Consumers League, are in response to the Further Notice of Proposed Rulemaking (FNPRM) released by the Federal Communications Commission (Commission or FCC) on May 1, 2026,[1] and published in the Federal Register on May 26, 2026.[2] Anonymous access to the U.S. phone network has fueled an epidemic of fraud. In 2025, the Federal Trade Commission (FTC) reported that text messages and phone calls were the first and third most common contact method for fraud attempts.[3] Even worse, scam calls and texts are the most effective contact method for scams. Median losses reported to the FTC in 2025 from fraudulent calls and texts were $1,835 and $1,000 respectively – substantially higher than any other contact method.[4] Commission action to combat fraudulent calls is urgently needed and we support the Commission's efforts to block criminals from accessing the U.S. phone network through stronger know-your-customer requirements.

The Commission has proposed an array of initiatives to combat illegal calls, and we applaud the Commission's vigorous approach. These Reply Comments focus on:

---

[1] FCC, Further Notice of Proposed Rulemaking, In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59; Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278 (adopted April 30, 2026, released May 1, 2026), https://docs.fcc.gov/public/attachments/FCC-26-27A1.pdf.
[2] Enhancing Know-Your-Customer Requirements, https://www.federalregister.gov/documents/2026/05/26/2026-10407/enhancing-know-your-customer-requirements.
[3] FTC Consumer Sentinel Network, Payment & Contact Methods, all quarters 2025, Reports and Amount Lost by Contact Method. Available at: https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts
[4] Id.

- The types of voice service which should be subject to enhanced "Know-Your-Customer" (KYC) requirements;
- The type of customer identifying information which voice service providers should collect and verify; and
- Appropriate enforcement measures for providers who disregard the Commission's KYC rules and knowingly originate illegal call traffic.

In section I of these Reply Comments, we describe how the Commission's proposal to require additional KYC information will deter fraudulent or otherwise illegal calls for some but not all forms of voice service. Enhanced KYC requirements for voice service providers[5] offering Voice over Internet Protocol (VoIP) service will make it more difficult for criminals to obtain network access for fraudulent robocall campaigns. Also, voice service providers generally already collect significant amounts of customer identifying information in the sale of postpaid cellular plans to mitigate the risk of non-payment. An enhanced KYC requirement for postpaid cellular service would support enforcement efforts without negatively impacting consumers.

However, we urge the Commission not to extend KYC requirements for small-scale sales of prepaid cellular plans to individuals and small businesses, which could harm some consumers. For example, individuals who are fleeing domestic violence need to be able to obtain cellular service without the risk that their abusers will trace them. In any event, KYC requirements for small-sale retail sales are unlikely to have a meaningful impact on fraud. We also urge the Commission not to

[5] In this Reply Comment, we use the same definition of "voice service provider" as the Commission sets forth in the FNPRM. "Specifically, 'voice service provider' means any entity originating, carrying, or terminating voice calls through time-division multiplexing (i.e., 'traditional' voice service), Voice over Internet Protocol (VoIP), or commercial mobile radio service (CMRS), unless otherwise noted." FNPRM at ¶2, fn. 1.

impose KYC requirements on switched access voice service subscriptions, which do not have many of the features that facilitate illegal calling.

In Section II of these Reply Comments, we recommend that the Commission adopt risk-based KYC requirements. For the riskiest forms of service, where a prospective customer can access voice service capable of supporting high-volume robocall campaigns, the Commission should require collection of customer information that is sufficient to support enforcement actions to redress consumer harm caused by illegal calling campaigns. Additionally, a KYC requirement should include an obligation for providers to know their customers' expected call traffic so that providers can effectively monitor their networks. This will ensure that voice service providers can look for and investigate discrepancies between expected and actual traffic on their networks, enabling the provider to detect and shut down illegal robocall campaigns as early as possible.

Lastly, in Section III we urge the Commission to adopt robust enforcement measures. Providers should be subject to per-call forfeiture penalties for willfully failing to obtain identification information from their direct customers and transmitting anonymous, illegal calls. Also, we strongly oppose any regulatory safe harbor. A safe harbor will encourage pro forma compliance while disincentivizing providers from actively investigating and adapting to the ever-changing tactics criminals use to exploit their victims. Finally, we suggest that the Commission extend 47 C.F.R. § 64.6305 to require KYC related certifications and a commitment to respond to law enforcement requests for customer identification information within twenty-four hours, unless the provider can demonstrate good cause for a delay in responding.

I. The Commission should require KYC information for certain types of voice service.

A. Collecting customer identifying information will deter fraud, but KYC requirements are not appropriate for all types of voice service.

In paragraphs 9 to 17 of the FNPRM the Commission seeks comments on requiring originating providers to obtain certain identification information from both new and renewing customers. We support the Commission's proposal to require voice service providers to obtain customer identification information before they start providing certain forms of service and to verify customer information at regular intervals thereafter. Criminals understand that the less identifying information they divulge, the more difficult they are to prosecute. Strong KYC requirements will deter some scammers from seeking network access. Even illegal callers that would have no scruples against using falsified information to gain network access may be deterred by the increased operational costs and heightened risk of criminal penalties entailed in fabricating credentials and constructing fictious identities. These illegal callers will also face disruptions to their operations if their voice service provider determines they have lied and terminates service.

A KYC requirement can help to keep bad actors off the network and will make it easier to hold voice service providers accountable if they violate the requirement and knowingly assist criminals. We support KYC requirements for voice service providers because they can help prevent criminals from gaining an anonymous on-ramp to the U.S. phone network to hunt for people to defraud.

However, voice service is offered in multiple ways, including through switched access lines,[6] cellular networks, and voice over internet protocol ("VoIP") technology. Subscribers also purchase

---

[6] We use the term "switched access line" to refer to a service connection between an end user and the local telephone company's switch, the basis of plain old telephone service ("POTS"). See FCC, *Voice Telephone Services: Status as of June 30, 2025* at pg. 16, Industry Analysis Division Office of Economics and Analytics May 2026. Available at: https://docs.fcc.gov/public/attachments/DOC-421558A1.pdf

phone service in different ways, including through prepaid plans sold in person or over the internet, or through postpaid subscription plans. Each of these different ways of connecting to the U.S. network and different ways of purchasing service present different risks of abuse by criminals and there is no one-size-fits-all KYC requirement that will be effective across the entire communications system. KYC requirements should be tailored to the unique aspects of different service arrangements and sales channels. We urge the Commission to balance the risks posed by different types of phone service with the benefits to consumers of being able to obtain service or transfer to a new provider quickly, easily, and inexpensively.

Requiring all originating providers obtain and retain the name, physical address, government issued identification number, and an alternate telephone number of any new and renewing customer before granting access to voice services is overly broad. Some low-income consumers who rely on inexpensive, easily obtainable services, such as prepaid cellular service purchased through retailers, do not have a permanent physical address and may have difficulty obtaining or keeping government-issued identification. Also, few low-income consumers are likely to have an alternate telephone number. Locking all forms of phone service behind a restrictive KYC requirement will effectively kick unhoused consumers who cannot provide a physical address off the U.S. phone network, preventing them from accessing emergency services or connecting with employers and loved ones.

Also, several commentors point out that survivors of domestic violence may be substantially adversely impacted by a blanket KYC requirement that involves the collection of physical address and government issued identification.[7] Rather than impose a blanket requirement to collect customer identification information for all forms of phone service sold through any channel, the Commission should target the types of service and sales channels that scammers exploit. As further detailed

[7] See e.g., Comments of National Network to End Domestic Violence, Submission ID26109882043, available at: https://www.fcc.gov/ecfs/document/26109882043/1.

below, we urge the commission to require VoIP providers collect customer identifying information in all circumstances and mandate collection of KYC information for all bulk sales of prepaid subscriber lines but we do not believe it is appropriate to require KYC information for retail sales of prepaid cellular phone plans.

B. VoIP services should be subject to an enhanced KYC requirement.

Enforcement actions have demonstrated that bad actors frequently gain access to the U.S. phone network through VoIP service providers.[8] VoIP service allows criminals to inexpensively place large numbers of simultaneous calls and to falsify or "spoof" the calling phone number – features which enable scam robocall campaigns. KYC requirements can help to make VoIP service more difficult and expensive for scammers to utilize, which will help to protect all voice service subscribers from spoofed robocall campaigns and other criminal exploits. Importantly, VoIP's technical requirements mean an enhanced KYC requirement is unlikely to harm consumers or prevent them from accessing necessary communications services. Since every VoIP customer necessarily has a separate broadband connection, they don't need to rely on voice service as their exclusive communication service either for normal communications or for anonymous ones. We urge the Commission to require all interconnected VoIP service providers to collect customer identifying information.

Requiring KYC measures for all interconnected VoIP service will not negatively impact individuals who require anonymous communications services or face difficulty producing identifying information, such domestic violence survivors or unhoused individuals. All interconnected VoIP services require a high-speed data connection: a broadband internet connection is literally a defining

---

[8] *See State Attorneys General & Privacy: Enforcement Trends 2020-2024*, Electronic Privacy Information Center, https://epic.org/wp-content/uploads/2025/10/EPIC-State-AG-Enforcement.pdf (documenting numerous enforcement measures taken by state attorneys general against VoIP providers for facilitating illegal robocalls).

characteristic of interconnected VoIP service.[9] As a result, a domestic violence survivor who uses VoIP as a primary communication method will also have access to other internet-based communications services, such as over-the-top messaging and calling services like Signal, Telegram, and WhatsApp. Many of these services are free and feature privacy protections, such as end-to-end encryption, that can satisfy a survivor's need for anonymity. Others with a legitimate need for anonymity, such as journalists who need to confer with anonymous sources or whistle blowers who wish to unveil waste, fraud, and abuse without risking detection and retaliation, will also be able to use these services. Allowing anonymous access to VoIP services facilitates harmful illegal robocall campaigns, and because over-the-top services are necessarily available to VoIP customers and satisfy legitimate needs for anonymous communications services, we support extending KYC obligations for all VoIP voice service providers.

Nor will a universal KYC requirement for all interconnected VoIP service have a negative effect on unhoused consumers. Subscribing to a broadband service is impossible for most unhoused consumers or others who do not have a permanent physical address, since broadband connections are generally hardwired to a property or require an expensive receiver or other specialized equipment that is generally beyond the means of low-income consumers. As discussed in section I(D) of these comments, prepaid cellular service is a better solution for these consumers. In other words, if the Commission imposes a KYC requirement on VoIP providers, it will never result in consumers being wholly unable to access communications services either on an anonymous basis or otherwise.

---

[9] An "Interconnected VoIP Service" is defined at 47 C.F.R. § 9.3 as: "a service that:
(i) Enables real-time, two-way voice communications;
(ii) Requires a broadband connection from the user's location;
(iii) Requires internet protocol-compatible customer premises equipment (CPE); and
(iv) Permits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network." (emphasis supplied).

Also, a KYC obligation for VoIP services is clearly warranted because VoIP calling has many features that facilitate large-scale fraud and has been used extensively by criminal scammers in the past. VoIP technology allows callers to transmit spoofed calling phone numbers and easily interfaces with automated dialing equipment and artificial or prerecorded voice equipment. VoIP providers have been implicated in numerous recent enforcement actions targeting illegal robocalls, including:

- *Arizona v. Michael D. Lansky L.L.C.*, an ongoing enforcement action by over fifty state attorneys general against a VoIP provider that allegedly facilitated a "barrage of unwanted robocalls sent to millions of American consumers that are harassing, annoying, threatening, and malicious."[10]
- *State of North Carolina ex rel. Joshua H. Stein v. Articul8, LLC et al.*, an enforcement action by the North Carolina attorney general alleging that an intermediate VoIP provider knowingly "allows scammers and fraudsters to access the U.S. telephone network and bombard U.S. consumers with fraudulent and illegal telemarketing calls and robocalls."[11]
- *Indiana v. Startel Commc'n LLC*, a suit against intermediate and originating VoIP providers that allegedly transmitted hundreds of millions of foreign illegal robocalls into the United States.[12]
- *Ohio ex rel Yost v. Jones*, an enforcement action by the Ohio Attorney General alleging that a Panamanian company placed billions of illegal robocalls to U.S. consumers through numerous VoIP providers that facilitated the traffic.[13]
- *State of Vermont v. Telecom carrier Access, LLC, et al.*, a suit by the Vermont Attorney General against TCA VoIP, a gateway VoIP alleged to have "knowingly brought thousands--if not hundreds of thousands--of illegal and fraudulent phone calls into the State of Vermont, and hundreds of millions nationwide."[14]
- *Off. of Att'y Gen. v. Smartbiz Telecom LLC*, a federal district court decision granting summary judgment to the Florida Attorney General on TSR claims in an enforcement action against an intermediate VoIP provider for facilitating illegal robocalls.[15]

VoIP telephone service's well documented history of abuse by scammers, its facilitation of harmful illegal calls, and the fact that all VoIP users necessarily have access to other communications options

[10] No. CV-23-00233-TUC-CKJ, 2024 WL 3657129 (D. Ariz. May 8, 2024)..
[11] Case No.: 1:22-cv-00058 (MD NC Jan. 2025) https://ncdoj.gov/wp-content/uploads/2022/01/FILED-Complaint_NC-v-Articul8_22-cv-00058-MDNC-2022.pdf.
[12] No. 321CV00150RLYMPB, 2022 WL 22702954, (S.D. Ind. Sept. 9, 2022).
[13] No. 2:22-CV-2700, 2025 WL 316331 (S.D. Ohio Jan. 28, 2025).
[14] https://ago.vermont.gov/wp-content/uploads/2022/03/TCA-VOIP-Complaint.pdf
[15] No. 22-23945-CIV, 2024 WL 4251895 (S.D. Fla. Sept. 19, 2024).

including anonymous options, all militate in favor of a strong KYC requirement to help keep illegal callers from using interconnected VoIP services to access the U.S. phone network.

C. Postpaid cellular service should be subject to KYC requirements.

Cellular service is typically sold through either prepaid or postpaid service plans. Postpaid cellular plans, where the subscriber pays only after gaining access to voice service, generally require a credit check, which in turn means that the cellular service provider must collect customer identification information sufficient to ensure that they are checking the correct subscriber's credit worthiness. This is frequently accomplished by requiring the potential customer to submit government issued identification, like a social security number or photo ID. There are certain exceptions--for instance, mobile network operator T-Mobile allows customers with a history of at least 12 months of timely prepaid cellular plan payments to convert to a postpaid service plan without a credit check.[16] However, in general the risk of non-payment associated with postpaid cellular plans has motivated voice service providers to collect significant customer identification information before providing service.

Given that postpaid cellular plans are already subject to a *de facto* KYC requirement, we support a formal requirement that voice service providers collect customer identification information in connection with the initial sale of postpaid cellular service plans. A KYC requirement will benefit enforcement efforts by deterring providers from ignoring illegal traffic coming from their postpaid customers. Cellular service providers who become aware that their customers have lied about their identities and are making illegal calls could be held accountable for violating a KYC requirement. These providers should not be permitted to make a cynical determination that allowing scammers to anonymously use postpaid cellular service plans to send illegal robocalls is sufficiently profitable that they do not need to collect customer identification information.

---

[16] https://www.t-mobile.com/offers/smartphone-equality-program

D. The Commission should not impose KYC requirements for prepaid cellular service except bulk sales.

In contrast to postpaid plans, prepaid cellular service plans, where the customer pays in advance for access to voice services for a specific term, do not present a risk of nonpayment. As a result, providers frequently do not collect customer identification information before activating this form of cellular service plan. We do not, however, support a blanket requirement that voice service providers collect customer identifying information before providing voice service through prepaid cellular plans.

First, it is important that prepaid cellular plans remain an option for domestic violence survivors who need access to telecommunications without risking disclosure of their identity or location. Second, the easy access associated with prepaid cellular service means this may be the only form of voice service that low-income and unhoused consumers can obtain. Access to phone service can be a lifeline to an unhoused consumer, who may not have government identification documents at hand, will not have a fixed address, and may not be in the credit reporting system.

Even if the Commission imposed KYC requirements on prepaid cellular service providers, it is unlikely that those requirements would be effective at preventing criminals from anonymously obtaining prepaid cellular service plans. These plans are widely available at brick-and-mortar retail outlets where sales staff may not check identification, and even if they do, those retail outlets will have difficulty transmitting customer identifying information to the mobile network operator who is responsible for providing the service. Applying a KYC requirement to retail sales of prepaid SIM cards could result in these products being removed from store shelves, making voice service difficult or impossible for unhoused or other low-income consumers to obtain. Even if stores chose to collect customer identification information on behalf of voice service providers to continue selling prepaid SIMs, scammers would still be able to obtain these products anonymously by simply paying a third-party to make the purchase or by using false credentials.

For the forgoing reasons, we urge the Commission not to impose a blanket KYC requirement on all prepaid cellular plans; however, we believe the Commission should adopt a targeted KYC requirement for bulk sales of prepaid SIM cards. Criminals increasingly gain access to U.S. cellular networks using SIM farms – large numbers of physical SIM cards or virtual eSIMs controlled in tandem by specialized equipment and used to make high volumes of calls through cellular networks. Publicly available information suggests that criminals have leveraged bulk purchases of prepaid SIM cards to build SIM farms. For example, the Secret Service disrupted a SIM farm in late 2025 and released pictures of confiscated equipment.[17] These pictures included stacks of branded SIM card holders that showed the name of a mobile virtual network operator ("MVNO") that had apparently provided a large quantities of SIM cards which were used to build the SIM farm.[18] Though it is unclear whether the criminals who built and operated this SIM farm obtained the SIM cards directly from the MVNO, it is clear that the operation purchased SIM cards in bulk – potentially as many as the 100,000 SIM cards the Secret Service confiscated.

Bulk sales of prepaid cellular service plans sold without collecting customer identification information facilitate the construction and operation of SIM farms. A KYC requirement would make it more difficult for criminals to remain anonymous when using bulk sales of prepaid SIM cards to construct SIM farms. Therefore, we believe the Commission should require the collection of customer identification information for all bulk sales of SIM cards or eSIMs associated with prepaid cellular service plans. We suggest that the Commission establish a specific threshold for the

---

[17] U.S. Secret Service dismantles imminent telecommunications threat in New York tristate area, September 23, 2025, U.S. Secret Service Media Relations. Available at: https://www.secretservice.gov/newsroom/releases/2025/09/us-secret-service-dismantles-imminent-telecommunications-threat-new-york. ("[P]rotective intelligence investigation led to the discovery of more than 300 co-located SIM servers and 100,000 SIM cards across multiple sites. In addition to carrying out anonymous telephonic threats, these devices could be used to conduct a wide range of telecommunications attacks.").

[18] https://www.secretservice.gov/sites/default/files/2025-09/20250922_equipment_02.jpg

number of prepaid SIM cards or eSIMs which can be sold to a single purchaser without collecting and retaining customer identification information. This would provide clarity to retailers or voice service providers who may be concerned that they will inadvertently violate the KYC requirement by furnishing a purchaser with prepaid SIM cards. While anonymous retail sales still present a risk that criminals could buy SIM cards or eSIMs piecemeal and construct a SIM farm, retail sales are limited to the number of cards the retailer has in stock, which complicates efforts to obtain the high volumes of SIM cards needed to build large SIM farms that can support the widespread illegal calling campaigns.

Also, we suggest that the Commission establish a requirement to monitor call traffic associated with prepaid cellular accounts to ensure that it conforms to reasonable patterns of individual or family use. Providers should not be permitted to turn a blind eye to prepaid accounts that originate high volumes of calls that are inconsistent with individual or small business use. We recommend that the Commission conduct further rulemaking to determine appropriate metrics for monitoring prepaid cellular traffic and providing notice to customers of account restrictions which will limit scammers' ability to use this type of account in SIM farms.

E. KYC requirements are unnecessary for switched access voice service subscriptions.

Finally, voice service is also provided through switched access lines. The Commission has published data indicating that, although the number is steadily declining, there were still approximately 15 million end-user switched access lines in service as of June 2025.[19] This form of service is commonly referred to as POTS or plain old telephone service, and it does not support many of the features that facilitate illegal calling campaigns, like caller ID spoofing. POTS service is

[19] FCC, *Voice Telephone Services: Status as of June 30, 2025* at pg. 2, Industry Analysis Division Office of Economics and Analytics May 2026. Available at: https://docs.fcc.gov/public/attachments/DOC-421558A1.pdf

provided to a physical location, unlike services such as nomadic VoIP service that can be utilized from anywhere in the world through the internet. Given these facts, a KYC requirement for POTS service is unnecessary. POTS telephone service has not been implicated in recent enforcement actions targeting illegal calls, it is associated with a physical address that can be investigated if the service is abused, and a KYC requirement could complicate legitimate uses of POTS service, such as switched access lines dedicated to security alarm monitoring. We do not believe that it is necessary for the Commission to require providers of switched access lines to collect customer identification information before starting service.

We generally support the Commission's proposal to require originating provider to obtain certain identification information for new and renewing customers. However, as noted above, we do not believe it is appropriate to extend this requirement to switched access lines or to sales prepaid cellular plans, except for bulk sales of prepaid SIM cards or eSIMs.

II. KYC Requirements Should Be Based on Risk and Require Periodic Verification

Different forms of voice service present different risks of enabling illegal robocalling. For instance, an individual mobile subscriber line does not natively support multiple separate, simultaneous calls, making it difficult to use these lines for robocalling. On the other hand, a dedicated SIP trunk used for transmitting VoIP calls can support massive calling campaigns that can harass and defraud consumers on an industrial scale. An enhanced KYC requirement should be based on the service's ability to facilitate illegal robocalling.

For voice services provided for individual or small business use that do not natively support high volume calling, we support the Commission's proposal to require originating providers to, at a minimum, obtain and retain the name, physical address, government issued identification number, and if available an alternate telephone number, from new customers. This customer identifying information should be sufficient to support service of legal action should the customer use the service for illegal calling.

Therefore, in response to the Commission's question posed in paragraph 11 of the FNPRM, the physical address required should be where the customer usually resides, or for businesses, the location of the business's headquarters or another location which can accept service of process. Maildrops, virtual offices, and other locations where an individual is not available to accept service should not satisfy a KYC requirement.

All originating voice service providers should also be required to take reasonable steps to verify the accuracy of customer identifying information collected to satisfy a KYC requirement. For example, voice service providers could check government identification numbers and address information against public records databases, like a state department of motor vehicles database, or collect corroborating information such as official correspondence addressed to the individual or business subscriber. If a business provides the address of a registered agent, the voice service provider should collect and maintain a current contract for the registered agent service to ensure that the business can be served at that location. Voice service providers should periodically re-verify customer identification information by either re-checking public records databases or requesting updated corroborating documentation.

For postpaid cellular customers, this reverification should be largely self-executing, because a consumer's periodic payment for services from a linked bank account or credit card in the customer's own name provides a strong form of verification of the customer's identity. A history of payments from an account at a U.S. based financial institution should satisfy a KYC re-verification requirement, making the burden of re-verification of KYC information for post-paid cellular customers minimal.

For the riskiest services, those that support high volume robocalling, voice service providers should also be required to collect information about the customer's intended use of the service. High-volume customers should provide both information demonstrating that their anticipated use of the service is legal, for instance examples of consumer consent to receive robocalls and sample call scripts, as well as expected traffic metrics such as the average call duration and daily call volume. Collecting this information will allow originating voice service providers to monitor their networks and investigate customer traffic that does not conform to the expected traffic profile. Sudden changes in call traffic can indicate that a customer's account has been hijacked by scammers. In such cases it is imperative that voice service providers suspend and investigate the suspicious traffic promptly. Similarly, collecting information like consent records and call scripts allows providers to monitor for complaints from terminating providers or law enforcement agencies which may indicate that the provider's customer has changed how it uses high-volume services or that it did not provide truthful information in the first instance. Originating voice service providers that offer high volume calling services should know their customers' identities as well as take affirmative steps to ensure that their services are not abused to perpetrate fraud on a large scale. We support the Commission's proposals in paragraphs 18 to 24 of the FNPRM, but urge the Commission to include traffic monitoring obligations in KYC verification requirements.

III. Robust Enforcement Measures are Essential

A. Per-call penalties are necessary

We support the Commission's proposed $2,500 per call forfeiture amount for voice service providers that violate KYC requirements and knowingly originate illegal calls. Per-call penalties are necessary so that voice service providers cannot treat penalties as merely a cost of doing business. A per-customer penalty would allow an originating voice service provider to treat forfeitures as a cost of doing business because forfeiture amounts would not scale with the scope of non-compliance.

Providers could make a cynical determination that if a potential customer promises sufficiently lucrative business, it could permit anonymous network access and large-scale fraud then simply pay a penalty if it is caught and prosecuted. Per-call penalties will scale to match the impact of fraudulent robocalling campaigns. This will ensure that courting criminal scammers isn't a sound business plan.

B. A regulatory safe harbor will undercut the effectiveness of a KYC Requirement

In paragraph 26 of the NPRM, the Commission asks whether it should, instead of adopting specific KYC requirements, issue baseline KYC guidance that acts as a regulatory safe harbor. We strongly oppose the creation of a regulatory safe harbor from liability for several reasons.

First, scammers are creative and will change their tactics to nominally comply with KYC requirements while hiding their identity to escape accountability. Criminals continually adapt their tactics and originating voice service providers cannot simply follow a checklist of compliance measures by rote. Technology, business processes, and consumer behavior will continue to change and evolve faster than the Commission will be able to issue new KYC guidance. No matter how bold or sophisticated the Commission's KYC safe harbor provisions are today, they will not remain effective in an ever-changing marketplace, leaving the Commission chasing scammers that stay one step ahead.

Additionally, there are many different types of voice service and it will be difficult or impossible to detail effective KYC guidance across the industry. The wide variety of calling technologies and use cases mean that providers will need to engage with their customers to ensure that their baseline KYC procedures are adequate for the particular circumstances. A cookie-cutter approach that merely satisfies a minimum KYC requirement will not be effective.

Also, the Commission will have no way of knowing that mandated KYC guidelines are effective in the circumstances. Techniques such as AI review are non-auditable and can obfuscate ineffective KYC review. Instead, the commission should continue to assess a provider's compliance with KYC requirements on a case-by-case basis considering the totality of the circumstances.

C. The Commission should require KYC certifications to support enforcement actions

We suggest that the Commission require additional certifications to improve the effectiveness of its KYC mandate. In particular, we recommend that the Commission amend 47 C.F.R. § 64.6305 to require all voice service providers to describe in their Robocall Mitigation Database (RMD) filings the specific steps they take to satisfy any enhanced KYC measures the Commission may impose, or to disclaim that they originate any voice call traffic subject to such requirements. The Commission already requires that providers describe their efforts to comply with the requirement to know their customers under 47 C.F.R. § 64.1200(n)(4), and any heightened KYC requirements should also be detailed in RMD filings.

Requiring this certification will make it easier for law enforcement to determine whether a provider has knowingly facilitated illegal traffic. If a provider does not follow the KYC program it discloses in its RMD filing, it is compelling evidence that the provider has willfully violated the Commission's rules and knowingly facilitated illegal robocalls. This will make it easier for enforcement authorities to bring enforcement actions against bad actor providers.

Additionally, we suggest that the Commission amend § 64.6305(a)(2) to enhance the requirement that all voice service providers "respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium" by adding that providers must also produce customer identifying information collected and maintained pursuant to KYC requirements, unless the provider can demonstrate good cause for a longer response time.

Conclusion

We thank the Commission for its commitment to using every tool at its disposal to fight fraudulent or otherwise illegal robocalls. We are grateful for the opportunity to provide comments on these important issues.

Respectfully submitted this 27th day of July 2026, by:

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