FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 1

[CG Docket Nos. 17-59 and 02-278; FCC 26-27; FR ID 347476]

Enhancing Know-Your-Customer Requirements

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) proposes actions to provide additional clarity to fill the gap between its current Know Your Customer (KYC) requirement and the types of rigorous KYC steps necessary to protect consumers. Specifically, the Commission seeks comment on customer identification requirements for new and renewing customers, requirements for verifying, retaining, and re-verifying customer information, requiring more information from certain customers such as high-volume customers, and on how these efforts can complement call branding and caller name requirements the Commission may adopt. The Commission also proposes to assess penalties for violations of the KYC requirement on a per call basis. With this inquiry, the Commission aims to make it more difficult for scammers to originate illegal calls and easier to enforce against them when they do get onto the network.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** and reply comments are due on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Pursuant to §§ 1.415 and 1.419 of the Commission's rules, 47 CFR 1.415, 1.419, interested parties may file comments and reply comments identified by CG Docket No. 17-59 and CG Docket No. 02-278 by any of the following methods:

- *Electronic Filers*: Comments may be filed electronically using the Internet by accessing the Electronic Comment Filing System (ECFS): *https://www.fcc.gov/ecfs*. *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).
- *Paper Filers*: Parties who choose to file by paper must file an original and one copy of each filing.
    - Filings can be sent by hand or messenger delivery, by commercial courier, or by the U.S. Postal Service. **All filings must be addressed to the Secretary, Federal Communications Commission.**
    - Hand-delivered or messenger-delivered paper filings for the Commission's Secretary are accepted between 8:00 a.m. and 4:00 p.m. by the FCC's mailing contractor at 9050 Junction Drive, Annapolis Junction, MD 20701. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
    - Commercial courier deliveries (any deliveries not by the U.S. Postal Service) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
    - Filings sent by U.S. Postal Service First-Class Mail, Priority Mail, and Priority Mail Express must be sent to 45 L Street NE, Washington, DC 20554.
- *Accessible formats*. To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format) or to request reasonable accommodations (e.g. accessible format documents, sign language interpreters, CART), send an e-mail to *fcc504@fcc.gov* or call the Consumer and Governmental Affairs Bureau at (202) 418-0530 (voice).

FOR FURTHER INFORMATION CONTACT: For further information about the Further Notice of Proposed Rulemaking (*FNPRM*), contact Richard Smith of the Consumer and Governmental Affairs Bureau at (202) 418-2854 or *Richard.Smith@fcc.gov*.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Further

Notice of Proposed Rulemaking (*FNPRM*) in CG Docket No. 17-59; and Further Notice of Proposed Rulemaking (*FNPRM*) in CG Docket No. 02-278, document FCC 26-27, adopted on April 30, 2026 and released on May 1, 2026. The full text of this document is available online at https://docs.fcc.gov/public/attachments/FCC-26-27A1.pdf.

Paperwork Reduction Act Analysis: The *FNPRM* may contain proposed new and revised information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on the information collection requirements described in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104–13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, see 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

Providing Accountability Through Transparency Act: Consistent with the Providing Accountability Through Transparency Act, Public Law 118–9, a summary of this document will be available on *https://www.fcc.gov/proposed-rulemakings*.

Ex Parte Rules: The proceeding the *FNPRM* initiates shall be treated as a ‘‘permit-but-disclose’’ proceeding in accordance with the Commission’s ex parte rules. Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter’s written comments, memoranda or other filings in the proceeding, the presenter

may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during ex parte meetings are deemed to be written *ex parte* presentations and must be filed consistent with § 1.1206(b) of the Commission's rules. In proceedings governed by § 1.49(f) of the Commission's rules or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must, when feasible, be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.*, .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

SYNOPSIS

I. DISCUSSION

Criminals continue to leverage the anonymity provided by phone calls and texts to defraud Americans and exploit communications networks to further other crimes. To bring illegal callers out of the shadows, we seek comment on making our KYC rules more robust by specifying information originating providers must obtain from customers before they are granted access to its service to make calls, how they should verify that information, and how we can assess enforcement penalties that are proportionate to the harms that unwanted and illegal calls cause. Through this proceeding, the FCC aims to make it more difficult for scammers to originate illegal calls and to enforce against them when they do get onto the network. In addition, we aim to clarify and reduce the regulatory uncertainty of KYC compliance for originating providers. This proceeding complements our broader work attacking illegal calls at all points in their lifecycle, including access to numbers, blocking, and call branding.

A. Obtaining Customer Identification Information

We seek comment on requiring originating providers to obtain certain identification information from both new and renewing customers. Specifically, we seek comment on requiring originating providers to, at a minimum, 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 its services. For high-volume customers, including business and foreign customers, we seek comment on requiring originating providers to also collect the intended use of the service (e.g., marketing, education, political campaign) and the customer's IP address from which each call will be placed (if applicable). We believe that requiring originating providers to gather this basic identification information will have two benefits. First, it will deter some scammers from getting onto the network. Second, enforcers will be better able to identify the scammers when they do. Gathering such information is the standard to prevent money laundering, and given the misuse of networks by bad actors such as organized criminal groups, we believe it provides a good model for our work.

We seek comment on our views. Can enhanced KYC prevent misuses of U.S. communications networks and numbering resources? Would requiring the collection of this information help cut down on illegal calls? Is the information we describe above sufficient to enable originating providers to identify malicious actors before they originate illegal calls? Is any of this information not needed to verify the identity of new and renewing customers? What privacy concerns may arise from such a collection of personally identifiable information (PII) and how can we mitigate them? Should we require more information, such as date of birth, like the Treasury CIP rule? Is such information useful in identifying malicious actors before they make illegal calls and locating them after they make illegal calls? We seek comment on whether AI and other automated technologies are being used by originating providers for KYC compliance purposes to detect bad actors and prevent illegal calls? What types of information do automated tools gather and validate for KYC compliance purposes? If so, how does the effectiveness of these technologies compare to more traditional approaches that involve

acquiring and verifying identification documents? How do we ensure that any enhanced KYC requirements do not inhibit the development and deployment of AI and automated KYC systems? Are there specific networking protocols or layers that we should seek targeted information about given that IP addresses can change, VPNs may be used and there are a variety of ways to tunnel and port IP-based traffic? How can we minimize burdens on consumers so they are not unduly hindered in gaining access to voice services? Do enhanced KYC requirements impose burdens on smaller providers? If so, are there ways to minimize such burdens?

How should we define "physical address" for these purposes? Should we exclude the use of virtual addresses, shared office locations without a dedicated suite or floor, P.O. boxes, mail forwarding services, and hosted servers because such addresses are inadequate to confirm the identity of a customer and often used by bad actors to conceal its identity? We also seek comment on whether foreign customers use domestic U.S. providers to originate large volumes of calls. Are there ways in which we can address any KYC issues relating to foreign-based callers?

We seek comment on how we should define "new" and "renewing" customers for these purposes. Should new customers be only those new to the originating provider? Or are those switching to different plans offered by the current provider considered "new" for purposes of the KYC requirement? Should "renewing" customers be only those who are merely continuing an existing plan for a new contract period? Should contracts that contain automatic renewal clauses be considered a renewal in this context? How often do customers renew contracts for voice services? If infrequently, should we consider as an alternative to renewing customers requiring re-verification of existing customer identity information on a periodic basis such as after a specified number of years?

Risk-Based Differences. Should we require originating providers to collect more information about customers that are more likely to make illegal calls, e.g., those subscribing to

high volume services or those that may be difficult to locate based on being foreign-based, or other factors? For example, should we consider a tiered approach where KYC requirements become more stringent for high-volume callers, callers using specific types of calling equipment associated with robocalling, or callers engaged in certain traffic patterns? If so, what additional information should we require originating providers to collect from higher-risk customers? How should the Commission establish a threshold for what constitutes a "high-risk" and/or "high volume" caller? For example, the *Lingo Consent Decree* required the collection of an Employer Identification Number (EIN) or Business Registration Number for business accounts. Should we impose similar requirements for all new and renewing high-volume customers? To what extent would this assist in confirming the identity of the high-volume customers seeking to obtain access to the network? Is the distinction between a "high volume" and "low volume" customer sufficiently clear for KYC purposes or are there industry standards that should guide any such distinction, e.g., "high volume" being more than an individual caller or small business would typically make? Should all business customers accounts be subject to the same KYC requirements regardless of their call volume? Beyond call volume, are there other risk based call behaviors that should trigger enhanced KYC requirements for new or renewing customers? Would a risk-tiered approach be useful for smaller voice providers that may not typically have customers that generate high volume calls? Should we require originating providers to collect more information from customers that utilize lead generators or dialing platforms that may lack strong KYC requirements? Should we require originating providers to consult lists of terrorists and terrorist organizations and criminal persons maintained by law enforcement entities?

Differences Based on Prepaid and Postpaid Service. We seek comment on whether customer information requirements should vary depending upon whether the customer is seeking a prepaid or postpaid service plan. Are there differences in current industry KYC information collections based upon whether the customer is seeking prepaid or postpaid plans or whether the customer purchases a prepaid plan at a retail store or online? Are there KYC measures we can

impose for prepaid service purchased through third-party vendors such as prepaid SIM cards? What, if any, customer information do wireless providers obtain from customers who purchase prepaid SIM cards? What percentage of prepaid plans are purchased in person at retail stores? What steps do providers currently take to validate KYC for prepaid services purchased at third-party retailers? Do prepaid customers have the same ability to make high volumes of illegal calls as postpaid customers, or are there inherent limitations on prepaid plans? To what extent are bad actors using prepaid service to make illegal calls? Are current KYC standards associated with prepaid services being exploited by criminals committing other types of crime, such as human trafficking?

For example, fraudulent Short Messaging Service (SMS) text messages can originate from Subscriber Identity Module (SIM) boxes. What steps have Mobile Network Operators (MNO) and Mobile Virtual Network Operators (MVNO) taken to address bulk purchases of SIM cards or bulk account activation? Have these measures proven effective at reducing the number of illegal calls being made using SIM boxes? If not, are there ways we should address this issue in the KYC framework that would not otherwise hinder access to affordable phone service to millions of Americans?

How do the KYC requirements discussed herein compare to existing industry practices and guidelines designed to satisfy the KYC requirement? To the extent these requirements create new burdens on originating providers, how can we minimize those burdens, including those on smaller originating providers such as non-nationwide service providers, while still promoting the objective to identify customers that pose the greatest risks to make illegal calls and to locate them if they do make such calls? For example, companies in the financial services industry need not directly collect KYC information in certain circumstances when they can obtain it from alternative sources such as credit reports. Should we adopt a similar exemption in this context? If so, which alternative sources should qualify for this exemption? Should we use any existing industry best practices to set baseline KYC compliance standards, including for

smaller providers? We also seek comment on whether such KYC requirements would provide sufficient flexibility to account for different services and customers with varying risk profiles in a manner that allows providers to continue to adapt to the evolving tactics used by bad actors to gain access to voice services.

We also seek comment on how we can ensure any new KYC requirements complement any Call Branding or Caller Name requirements we may adopt. For example, how can we ensure we do not duplicate burdens on originating providers? Is there a direct connection between the customer identity information originating providers would gather if we adopt enhanced KYC requirements and the caller identity information terminating providers would deliver to handsets? Are there other considerations raised in the *Call Branding FNPRM* proceeding that should be coordinated with any enhanced KYC requirements to better promote the objectives of both proceedings? We seek comment on these and any other issues relevant to this matter.

B. Verifying and Retaining Customer Information

An effective KYC regime must confirm the accuracy of the information customers provide. We seek comment on requiring originating providers to take specific measures to verify, re-verify, and retain collected customer identification information. Bad actors may submit fake or stolen information to conceal their identity to gain access to the network and avoid accountability for making illegal calls. Originating providers that conduct a thorough verification of their customers' information can discover the use of such fake information before allowing bad actors to originate calls and stop illegal calls before they occur. By better knowing their customers, providers can also help facilitate the Commission and other law enforcement agency efforts to locate such callers by ensuring that the information provided is accurate. Verification measures also ensure originating providers' compliance with the obligation to exercise due diligence to ensure that its network is not used to originate illegal traffic. Periodic review or ongoing re-verification of KYC information is essential to ensure that bad actors have not gained access to the network and to enable the Commission to hold them accountable.

Verification. We seek comment on requiring originating providers to obtain supporting records to verify the customer's identity, such as copies of government-issued identification. For customers seeking access to services that enable origination of high volumes of calls (e.g., a number of calls above what an individual caller would make using a personal account), we seek comment on requiring verification of customer information using supporting records such as corporate formation records, proof of good standing such as a state-issued certification, confirmation that the telephone number provided is the customer's current active telephone number, third-party records of a customer's physical address, and verification of commercial presence (e.g., website, social media, store front) when applicable before being granted access to the network. We anticipate that most high-volume callers will be businesses or similar entities that have such supporting records. To the extent, however, that they are individuals seeking access to high-volume service, what additional verification measures should we require?

Is this list comprehensive? Should we require more or fewer verification measures; should any additional steps vary depending on whether the customer is deemed higher or lower risk? And should we require that originating providers complete all steps successfully before allowing the customer to use its network? If the customer is renewing, what period of time should the provider have to complete its verification before suspending access to the network? What existing tools and practices do providers use to verify customer information? Are there commercially available resources that originating providers can use to accurately verify the identity and location of a customer? If so, should we find use of these resources sufficient to satisfy any enhanced KYC verification requirement? Are there other industries and/or other countries with successful KYC verification requirements? If so, are their models applicable to U.S. communications services? What privacy issues related to the collection and retention of such information should we consider?

We believe that there are red flags that should raise concerns for closer verification such as providing a registered agent or virtual office as a physical address; registering a corporate

address using a residential address or random commercial location that is unaffiliated with the customer; lacking a commercial presence or operating a suspicious website (e.g., a newly created website); using a suspicious email address (e.g., a recently created email address, template website with little information unique to the company); not being registered in the state in which it purports to be located or incorporated; or paying for service in non-traceable ways such as the use of cryptocurrency. We tentatively conclude that these red flags should alert an originating provider as to a customer's potential intention to use its service to make illegal calls and seek comment on this conclusion. Are there additional red flags that raise concerns with a customer's access to the network that should result in originating providers exercising more stringent verification measures?

Risk-Based Re-verification. Should we require originating providers to re-verify KYC customer information in response to changes in traffic patterns or other red flags that may suggest illegal calls? If so, what types of changes in traffic patterns? We expect that originating providers will monitor traffic on their networks to determine if there are customer information inconsistencies such as a domestic U.S. company transmitting traffic from a foreign-based IP address or dormant accounts suddenly reappearing and sending large volumes of calls. In such instances, we seek comment on whether re-verification methods should include contacting the customer directly; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with financial institutions; or obtaining a financial statement. We seek comment on what resources, databases, or third-party tools originating providers could use to verify customer identity. Are there privacy, cost, or operational concerns that we should consider when determining which verification resources are appropriate?

Alternatively, should we require originating providers to periodically re-verify customer information on an ongoing basis, such as annually? How would the compliance burdens of this

approach including for smaller providers compare to a re-verification process triggered only by a red flag or unusual activity on the customer's account? Should any re-verification requirements be identical to the original verification measures when initiating service or, in the absence of any reasonable basis for concern or red flags, be less stringent? We seek comment on the current practices and guidelines that originating providers take in this context including how often and under what circumstances they re-verify customer information to ensure that it remains accurate and what actions they take to ensure that their services are not being used to originate illegal traffic.

Retention. We seek comment on requiring originating providers to retain KYC information and supporting records for the entirety of any potential statute of limitation period relating to misuse of their services to make illegal calls. In the case of spoofing or intentional violations of section 227(b) of the Communications Act, that statute of limitations period is four years. As a result, originating providers would be required to retain KYC customer information and supporting records for four years following termination of the customer relationship and we seek comment on this approach. We seek comment on industry customer information retention periods including whether this approach imposes any new burdens on smaller providers by differing from those practices. What steps does the industry take to protect such information from unauthorized access, and would those steps offer enough protection to an expanded collection and retention of PII or would heightened security be necessary? Should we consider an alternative retention timeframe?

C. Enforcement

We propose to codify a base forfeiture amount for violations of § 64.1200(n)(4) on a per call basis to best correlate penalties to the volume of illegal calls made, and thus the harm caused by any one caller. Specifically, we propose to codify a $2,500 per call base forfeiture amount. Alternative approaches, such as assessing fines on a "per customer" basis, would result in a single base forfeiture regardless of the number of illegal calls made by the customer. The

Commission has confirmed that the responsibility imposed by § 64.1200(n)(4) for originating providers to know their customers is a critical aspect of protecting Americans from illegal and harmful calls. In that regard, we emphasize that § 64.1200(n)(4) requires that originating providers take "affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls," which includes both "knowing its customers," and "exercising due diligence in ensuring that its services are not used to originate illegal traffic." Originating providers that fail to satisfy either obligation will be deemed in violation of the rule. We believe that our proposed approach would better encourage compliance with the rule. We seek comment on this and any other issues relevant to this proposal including whether and how to expedite the provision of customer information to the Commission or law enforcement upon any notification to the originating provider that one of its customers is under investigation for using the provider's network to make illegal calls.

We seek comment on whether the Commission should, as an alternative to adopting specific KYC requirements, issue baseline KYC guidance or expectations that act as a regulatory safe harbor. Specifically, should we deem compliance with any enhanced KYC obligations or baseline KYC expectations a safe harbor from any enforcement action against the originating provider? Should using an accredited third party to verify customer identity trigger a safe harbor? Should we establish a safe harbor for originating providers that employ effective AI or automated systems that satisfy KYC objectives by identifying bad actors and preventing illegal calls? Would such a safe harbor approach sufficiently incent better KYC practices while giving originating providers flexibility to develop innovative KYC protections and react to evolving tactics used by bad actors to gain access to voice networks? Does such an approach promote innovation and competition among originating providers leading to better KYC compliance and fraud prevention across the ecosystem of voice calling customers?

We seek comment on other enforcement measures we should consider to deter illegal calls. For example, are our existing rules sufficient to ensure that originating providers provide

assurance of their compliance with KYC rules? If not, should we require a specific certification regarding KYC compliance as part of the Robocall Mitigation Database (RMD) filings? It might also include requiring originating providers to obtain independent verification of their compliance, e.g., via an independent auditor using generally accepted standards for providing such assurance. Should we consider broadening our downstream provider blocking requirements so that any provider downstream of an originating provider that fails to comply with our KYC requirements must block that originating provider's traffic? Would that be technically feasible, e.g., can all downstream providers (not just the immediate downstream provider) identify the originating provider?

D. Deterring Other Criminal Use of the Network

We seek comment on whether enhanced KYC requirements can prevent or deter criminal use of communication networks that do not involve illegal calls. Enhanced KYC information can assist law enforcement to more easily identify callers that use the network to perpetuate crimes by ensuring that voice providers have accurate and complete customer information. The KYC information gathered and verified would help ensure that law enforcement gets accurate information in response to subpoenas when investigating crimes. For example, can enhanced KYC rules assist law enforcement in investigating organized criminal groups that use the network to facilitate illegal activities? Can they be used to deter or detect trafficking operations that use communication networks to buy and sell illicit goods? Would enhanced KYC measures for originating providers also address abuse in text messaging networks? Would such rules assist law enforcement in the investigation of fraud, espionage, or influence operations that undermine national security? Are there enhancements we could make that would better assist law enforcement investigations?

E. Implementation

We seek comment on whether to make any rules we adopt pursuant to this *FNPRM* applicable primarily only to new and renewing customers that originating providers acquire after

the effective date of any new rules and to any customers that renew service with such providers after the effective date. We also seek comment on whether any new KYC rules should take effect six months after OMB approval of any applicable Paperwork Reduction Act requirements. Would extending the effective date for smaller providers further minimize compliance burdens?

We seek comment on whether we should adopt a different implementation timeline for KYC requirements that would apply to existing customers that use high-volume services if we were to adopt heightened KYC requirements for such customers seeking to obtain such services. Or should existing customers that use high-volume services have to undergo heightened KYC measures only at service renewal? How should we define renewal for this purpose?

We seek comment on these issues and whether they best balance the need for enhanced KYC requirements with the legitimate business requirements of providers, particularly small and rural providers.

F. Legal Authority

Consistent with our approach in the *Fourth Call Blocking Order*, we believe sections 201(b), 227(e), and 251(e) of the Communications Act of 1934, as amended, give us authority to implement affirmative measures requiring originating providers to know their customers and exercise due diligence in ensuring that their services are not used to originate illegal calls. Section 201(b) grants us broad authority to adopt rules governing just and reasonable practices of common carriers. Our section 251(e) numbering authority provides separate authority to prevent the fraudulent abuse of North American Numbering Plan (NANP) resources; this particularly applies where callers spoof caller ID for fraudulent purposes and therefore exploit numbering resources, regardless of whether the originating voice service provider that places the calls onto the U.S. network is a common carrier.

Similarly, the Truth in Caller ID Act grants us authority to prescribe rules to make unlawful the spoofing of caller ID information with the intent to defraud, cause harm, or wrongfully obtain something of value. Taken together, section 251(e) and the Truth in Caller ID

Act grant us authority to prescribe rules to prevent the unlawful spoofing of caller ID and abuse of NANP resources by callers, and the proposed amendments to our existing KYC requirements would take a further positive step toward stopping such illegal calling. Consistent with our existing § 64.1200(n)(4) rule, we find that it is essential that any rules apply to all originating providers including VoIP providers. Absent broad application, VoIP would remain a potential safe haven for malicious actors to make illegal calls to consumers. We seek comment on these views.

National Security. We believe that the Commission's national security authority is another basis for the possible rules we discuss above. Illegal calls are more than an annoyance – bad actors can use them for denial-of-service attacks and also surveil and target government officials and sensitive infrastructure. We thus believe protecting networks with enhanced KYC requirements advances our responsibility to "make available, so far as possible, . . . a rapid, efficient, Nation-wide and world-wide wire and radio communication service . . . for the purpose of the national defense." With respect to international telecommunications services, do we have authority under Section 303(r) to adopt rules implementing the General Agreement on Trade in Services (GATS), which allows members, subject to certain conditions, to enforce measures necessary to secure compliance with laws or regulations relating to "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts" and "the prevention of deceptive and fraudulent practices"?

We seek comment on these possible bases of authority along with any others, including how our rights under other trade agreements, including free trade agreements, might serve as authority for any changes to our KYC requirements as discussed above.

G. Costs and Benefits

The Commission receives more complaints about illegal calls than any other issue. Illegal calls can annoy, defraud, and erode confidence in the telecommunications network while

costing consumers billions of dollars in fraud and wasted time. As noted above, the most effective way to prevent illegal calls from reaching American consumers is by ensuring they never enter the network. Originating providers are best positioned to stop illegal calls before they enter the network by screening new or renewing customers. When an originating provider fails to meet its obligations to properly scrutinize its customers before they commence using the provider's services to originate calls, it creates a risk that malicious actors will gain access to those services to make illegal calls and opens the door for foreign actors to exploit U.S. networks for fraud, espionage, or influence operations that undermine national security. In addition, a lack of accurate and complete customer information hinders the Commission's ability to identify and locate parties responsible for making illegal calls.

In the *Fourth Call Blocking Order*, the Commission required all originating providers to implement KYC obligations and exercise due diligence to ensure their services are not used to originate unlawful and illegal calls. In this *FNPRM*, we seek comment on specific actions that originating providers might take to comply with the existing KYC requirements. We anticipate that many originating providers already take KYC compliance measures and therefore tentatively conclude that any incremental compliance costs will be minimal. We expect that any changes to the rules will eliminate confusion and provide clear guidance to originating providers where ambiguity exists. As a result, any rule changes are likely to reduce regulatory uncertainty. We seek comment on the costs and benefits of changes to our rules, including the specific economic impact on small business entities and ways to minimize those impacts.

We believe that any potential rule changes discussed above will help consumers avoid illegal calls including scams, fraud, and otherwise unlawful calls and better protect U.S. telecommunications networks from foreign actors. In addition, we propose to codify the forfeiture amount for KYC violations on a per call basis, which we believe will create incentives for compliance and further reduce the origination of unlawful and illegal calls. We seek comment on whether there are additional costs and burdens on originating providers that we have

not identified including ways to minimize burdens for smaller voice service providers.

II. INITIAL REGULATORY FLEXIBILITY ANALYSIS

As. required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Federal Communications Commission (Commission) has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the policies and rules proposed in the *FNPRM* assessing the possible significant economic impact on a substantial number of small entities. The Commission requests written public comments on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments specified on the first page of the *FNPRM*. The Commission will send a copy of the *FNPRM* including this IRFA, to the Chief Counsel for the SBA Office of Advocacy. In addition, the *FNPRM* and IRFA (or summaries thereof) will be published in the Federal Register.

A. Need for, and Objectives of, the Proposed Rules

The Commission has prioritized combatting illegal calls as a top consumer protection. The Commission's goal is to stop illegal calls before they enter the network, thus requiring originating providers to block them, which would give consumers more information and ability to decide which calls they wish to receive. The Commission initiates this proceeding to further enhance its existing "Know-Your-Customer" (KYC) requirements to mandate better compliance and enforcement of the rule. The Commission seeks comment on specific actions originating providers must take to guard against the origination of illegal calls. In this *FNPRM*, the Commission notes that it receives more complaints about unwanted calls than any other issue. Unwanted and often illegal calls can annoy and defraud the consumer as well as lead to eroding confidence in the telecommunications network while costing consumers billions of dollars in fraud, wasted time, and nuisance.

The most effective way to prevent illegal calls from reaching American consumers is by ensuring that those calls never originate on or enter the U.S. network. The Commission seeks comment on ways to keep bad actors from gaining access to the network. The Commission

believes that originating providers are best positioned to stop illegal calls before they enter the network by screening new or renewing customers. When an originating provider fails to meet its obligations to properly scrutinize its customers before they commence using the provider's services to originate calls, it creates a risk that malicious actors will gain access to those services to make illegal calls and opens the door for foreign actors to exploit U.S. networks for fraud, espionage, or influence operations that undermine national security. In addition, the Commission's ability to identify and locate the parties that are responsible for making illegal calls is hindered when accurate and complete customer information is unavailable from the voice service provider.

In this *FNPRM*, we: (1) seek comment on specific customer identification requirements for new and renewing customers; (2) seek comment on requirements for originating providers to verify, retain, and periodically re-verify customer information; (3) seek comment on whether any enhanced KYC requirements should include risk-based security controls to require higher levels of scrutiny for certain customers including foreign customers and high-volume customers based on the risks posed to make illegal calls; and (4) propose that the Commission will assess penalties for violations of the KYC rule on a per call basis.

B. Legal Basis

The proposed action is authorized pursuant to sections 1-4, 201(b), 227(e), and 251(e) of the Communications Act of 1934, as amended, and 47 U.S.C. 151-154, 201(b), 227(e), and 251(e).

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term

"small business" has the same meaning as the term "small business concern" under the Small Business Act (SBA). A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA. The SBA establishes small business size standards that agencies are required to use when promulgating regulations relating to small businesses; agencies may establish alternative size standards for use in such programs, but must consult and obtain approval from SBA before doing so.

Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe three broad groups of small entities that could be directly affected by our actions. In general, a small business is an independent business having fewer than 500 employees. These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses. Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and not dominant their field. While we do not have data regarding the number of non-profits that meet that criteria, over 99 percent of nonprofits have fewer than 500 employees. Finally, "small governmental jurisdictions" are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand. Based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 out of 90,835 local government jurisdictions have a population of less than 50,000.

The rules proposed in the *FNPRM* will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS) codes and corresponding SBA size standard. Based on currently available U.S. Census data regarding the estimated number of small firms in each identified industry, we conclude that the proposed rules will impact a substantial number of small entities. Where available, we also provide additional information regarding the number of potentially affected entities in the above identified industries.

Table 1. 2022 Census Bureau Data by NAICS Code

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms	Total Small Firms	% Small Firms
Wired Telecommunications Carriers	517111	1,500 employees	3,403	3,027	88.95%
Wireless Telecommunications Carriers (except Satellite)	517112	1,500 employees	1,184	1,081	91.30%

Table 2. Telecommunications Service Provider Data

2024 Universal Service Monitoring Report Telecommunications Service Provider Data (Data as of December 2023)	SBA Size Standard (1500 Employees)		
Affected Entity	**Total # FCC Form 499A Filers**	**Small Firms**	**% Small Entities**
Competitive Local Exchange Carriers (CLECs)	3,729	3,576	95.90
Incumbent Local Exchange Carriers (Incumbent LECs)	1,175	917	78.04
Local Exchange Carriers (LECs)	4,904	4,493	91.62
Wired Telecommunications Carriers	4,682	4,276	91.33
Wireless Telecommunications Carriers (except Satellite)	585	498	85.13
Wireless Telephony	326	247	75.77

D. Description of Economic Impact and Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

The RFA directs agencies to describe the economic impact of proposed rules on small entities, as well as projected reporting, recordkeeping and other compliance requirements, including an estimate of the classes of small entities which will be subject to the requirements and the type of professional skills necessary for preparation of the report or record.

The Commission seeks comment on specific actions originating providers should take to guard against unwanted and illegal calls. The *FNPRM* seeks comment on establishing new information collection, reporting, recordkeeping, or compliance requirements for small entities. Specifically, it seeks comment on requiring originating providers to obtain specific customer identification information from new and renewing customers. This may require originating providers to enhance their current practices for obtaining such customer information before granting access to their services.

The *FNPRM* also seeks comment on specific requirements for originating providers to verify, retain, and re-verify customer information. This may require affected small entities to establish or enhance existing verification procedures, maintain records of verification activities, and implement systems to ensure customer identification information is secure, accurate, and complete.

The *FNPRM* also seeks comment on whether KYC requirements should include risk-based security controls depending on an assessment of the risk that the customer poses to make large numbers of illegal calls. For example, greater levels of review for foreign and high-volume customers than for low-volume customers. To comply with this requirement, affected small entities may need to establish verification procedures when a customer indicates an intent to make a high volume of calls or is located in a country other than the United States.

Finally, the Commission invites comment on the costs and burdens of enhanced KYC requirements on small entity voice service providers. The Commission expects that information received in comments, including cost and benefit analyses where requested, will help the Commission identify and evaluate relevant compliance matters for small entities that may result if the proposals and associated requirements discussed in the *FNPRM* are ultimately adopted.

E. Discussion of Significant Alternatives Considered That Minimize the Significant Economic Impact on Small Entities

The RFA directs agencies to provide a description of any significant alternatives to the proposed rules that would accomplish the stated objectives of applicable statutes, and minimize any significant economic impact on small entities. The discussion is required to include alternatives such as: "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."

In the *FNPRM*, the Commission seeks comment on several approaches that may minimize impacts on small entities. For example, we seek comment on whether originating providers should be exempted from acquiring direct KYC information when such information can be obtained from credible alternative sources such as a credit report. We also seek comment on current industry practices for obtaining, verifying, and retaining customer information including ways that we might tailor any enhanced KYC requirements to conform to these practices in a way that minimizes any new burdens. We seek comment on whether enhanced KYC requirements can be designed to complement any *Call Branding FNPRM* proposal to require originating providers that transmit caller identity information to employ reasonable measures to verify the accuracy of the information transmitted including mandating the collection and verification of specific customer information. In particular, we seek comment on whether there are ways in which enhanced KYC requirements can be coordinated to minimize burdens and promote industry compliance. Finally, we seek comment on whether any rules adopted pursuant to this *FNPRM* apply only to customers originating providers acquire after the effective date of any new rules and to any customers that renew service with the provider after the effective date. We also seek comment on whether any such rules should not take effect until six months after OMB approval of any applicable Paperwork Reduction Act requirement to

provide affected entities with an opportunity to take any measures necessary to ensure compliance with these requirements.

The Commission expects to more fully consider the economic impact and alternatives for small entities following review of comments filed in response to the *FNPRM* and this IRFA. The Commission's evaluation of this information will shape the final alternatives it considers, the final conclusions it reaches, and any final actions it ultimately takes in this proceeding to minimize any significant economic impact that may occur on small entities.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

None.

List of Subjects in 47 CFR Part 1

Administrative practice and procedure, Communications common carriers, Penalties, Reporting and recordkeeping requirements, Telecommunications, Telephone.

Federal Communications Commission.

Marlene Dortch,
Secretary.

Proposed Rules

For the reasons discussed in the preamble, the Federal Communications Commission proposes to amend 47 CFR part 1 as follows:

PART 1—PRACTICE AND PROCEDURE

1. The authority citation for part 1 continues to read as follows:

Authority: 47 U.S.C. chs. 2, 5, 9, 13; 28 U.S.C. 2461 note; 47 U.S.C. 1754, unless otherwise noted.

2. Amend § 1.80, by revising Table 1 to paragraph (b)(11) to read as follows:

*****

(b)***

(11) ***

TABLE 1 TO PARAGRAPH (b)(11)-BASE AMOUNTS FOR SECTION 503 FORFEITURES

Forfeitures	**Violation amount**
Misrepresentation/lack of candor	(1)
Failure to file required DODC required forms, and/or filing materially inaccurate or incomplete DODC information	$15,000
Construction and/or operation without an instrument of authorization for the service	10,000
Failure to comply with prescribed lighting and/or marking	10,000
Violation of public file rules	10,000
Violation of political rules: Reasonable access, lowest unit charge, equal opportunity, and discrimination	9,000
Unauthorized substantial transfer of control	8,000
Violation of children's television commercialization or programming requirements	8,000
Violations of rules relating to distress and safety frequencies	8,000
False distress communications	8,000
EAS equipment not installed or operational	8,000
Alien ownership violation	8,000
Failure to permit inspection	7,000
Transmission of indecent/obscene materials	7,000

Interference	7,000
Importation or marketing of unauthorized equipment	7,000
Exceeding of authorized antenna height	5,000
Fraud by wire, radio or television	5,000
Unauthorized discontinuance of service	5,000
Use of unauthorized equipment	5,000
Exceeding power limits	4,000
Failure to Respond to Commission communications	4,000
Violation of sponsorship ID requirements	4,000
Unauthorized emissions	4,000
Using unauthorized frequency	4,000
Failure to engage in required frequency coordination	4,000
Construction or operation at unauthorized location	4,000
Violation of requirements pertaining to broadcasting of lotteries or contests	4,000
Violation of transmitter control and metering requirements	3,000
Failure to file required forms or information	3,000
Per call violations of the robocall blocking rules	2,500
Per call Know Your Customer violations	2,500
Failure to make required measurements or conduct required monitoring	2,000
Failure to provide station ID	1,000
Unauthorized pro forma transfer of control	1,000
Failure to maintain required records	1,000

* * * * *

[FR Doc. 2026-10407 Filed: 5/22/2026 8:45 am; Publication Date: 5/26/2026]