Before the
Federal Communications Commission
Washington, D.C.

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 of 1991	)	CG Docket No. 02-278
	)	
Dismissal of Outdated or Otherwise Moot Robocalls Petitions	)	CG Docket No. 25-307

COMMENTS OF THE AMERICAN BANKERS ASSOCIATION, AMERICAN FINANCIAL SERVICES ASSOCIATION, AMERICA'S CREDIT UNIONS, BANK POLICY INSTITUTE, CONSUMER BANKERS ASSOCIATION, DEFENSE CREDIT UNION COUNCIL, MORTGAGE BANKERS ASSOCIATION, AND STUDENT LOAN SERVICING ALLIANCE TO THE 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

Jonathan Thessin
Vice President/Senior Counsel
American Bankers Association
1333 New Hampshire Avenue, NW
Washington, DC 20036
(202) 663-5016

Philip Bohi
General Counsel
American Financial Services Association
1750 H St NW Suite 650
Washington, DC 20006
(202) 466-8605

James Akin
Head of Regulatory Advocacy
America's Credit Unions
99 M Street, SE
Washington, DC 20003
(800) 356-9655

Greg Williamson
Senior Vice President, Fraud Reduction
Bank Policy Institute
1300 Eye Street, NW
Washington, DC 20005
(202) 289-4322

Brian Fritzsche
Vice President, Associate General Counsel
Consumer Bankers Association
1225 New York Ave., NW
Washington, DC 20005
(202) 552-6381

Jason Stverak
Chief Advocacy Officer
Defense Credit Union Council
1627 Eye Street, NW, Suite 935
Washington, DC 20006
(202) 734-5007

Alisha Sears
Director, Regulatory Counsel
Mortgage Bankers Association
1919 M Street, NW, 5th Floor
Washington DC 20036
(202) 557-2930

Scott Buchanan
Executive Director
Student Loan Servicing Alliance
2210 Mt. Vernon Avenue
Suite 207
Alexandria, VA 22301
(202) 955-6055

January 5, 2026

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY

The American Bankers Association (ABA), American Financial Services Association, America's Credit Unions, Bank Policy Institute (BPI), Consumer Bankers Association, Defense Credit Union Council, Mortgage Bankers Association, and Student Loan Servicing Alliance[1] (the Associations) appreciate the opportunity to comment on the Federal Communications Commission's (Commission or FCC) Ninth Further Notice of Proposed Rulemaking (Proposal).[2]

Fraud is a pervasive problem that often takes an extraordinary financial and emotional toll on consumers. In a December 2025 report, the Federal Trade Commission estimated that 2024 fraud losses totaled a staggering $196 billion.[3] Increasingly, criminals perpetrate fraud by impersonating banks and other legitimate companies through voice calls, text messages, and advertisements on social media websites. Criminals illegally "spoof" the number used in the caller ID – i.e., to cause a call recipient's caller ID to display the name, or solely the number, of a legitimate company instead of the name and number of the actual caller – with the intent to defraud the consumer.

The financial services industry spends billions of dollars each year to protect consumers from fraud, investigate potential criminal activity, and help affected consumers recover their

---

[1] A description of each Association is in Appendix A.

[2] *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Dismissal of Outdated or Otherwise Moot Robocalls Petitions*, 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, and Public Notice in CG Docket No. 25-307 (rel. Oct. 29, 2025) [hereinafter, *Ninth Further Notice*].

[3] Fed. Trade Comm'n, Protecting Older Consumers 2024-2025: A Report of the Federal Trade Commission 28 (Dec. 1, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf.

hard-earned money.[4] But financial institutions cannot do this work alone. We need a whole-of-government strategy to address this serious problem,[5] and the FCC has a critical role to play. Currently, fraud committed through voice calls and text messages continues unabated because, unlike banks and credit unions that have customer identification obligations, wireless providers take few steps to stop fraudsters from impersonating legitimate companies and gaining consumers' trust. That must end.

We commend the Commission for proposing enhancements to the "STIR/SHAKEN" call authentication framework that promise to keep bad actors off calling networks and promote consumers' confidence that the calls they receive are legitimate. But the Commission should go further. We urge the Commission to finalize rules that specify the steps that voice service providers that originate calls (originating providers) must take to comply with an existing rule that requires providers to take effective steps to ensure that it does not transmit illegal calls. We also urge the Commission to require providers to verify the caller has the legal right to the number that will be displayed in the recipient's caller ID.

We also support the Commission's efforts to advance the use of "Rich Call Data" (RCD), which uses encrypted tokens to securely transmit the caller's name, logo, and/or website to the recipient's caller ID display.[6] However, RCD will be successful only if originating providers

---

[4] *See, e.g.,* Joseph Ibitola, *Overcoming the Hidden Costs of AML Compliance*, Flagright (updated July 1, 2025), https://www.flagright.com/post/overcoming-the-hidden-costs-of-aml-compliance#:~:text=AML%20compliance%20has%20become%20an,a%20financial%20firm's%20annual%20revenue (reporting that, globally, banks and fintech companies spend an estimated $206 billion per year on financial crime compliance).

[5] *See, e.g., ABA Banking Journal*, *Nichols Renews Call for National Strategy on Fraud* (Apr. 8, 2025), https://bankingjournal.aba.com/2025/04/abas-nichols-renews-call-for-national-strategy-on-fraud/ (describing ABA's campaigns to education consumers on fraud risks and the association's call for a "whole-of-government" approach to combating fraud).

[6] *Ninth Further Notice*, *supra* note 2, ¶ 51.

carefully verify the caller. Otherwise, bad actors will take advantage of RCD to impersonate legitimate companies by displaying their names, logos, or websites. Thus, the Commission should require providers that use RCD to verify that a caller has the legal right to use the number that will be displayed on the recipient's caller ID display and that the logo and website to be displayed belong to the caller.

In addition, we support the Commission's efforts to combat illegal calls placed by organizations outside the United States. However, before moving forward, we urge the Commission to study the effectiveness of its proposals in stopping illegal calls and study the proposals' impact on lawful companies that employ customer service representatives located abroad to respond to customer inquiries and requests.

We also support the Commission's landmark, commonsense proposed reforms to outdated Telephone Consumer Protection Act[7] (TCPA) rules. Congress enacted the TCPA to combat abusive telemarketing practices[8] – and not to create "a barrier to the normal, expected or desired communications between businesses and their customers."[9] In 2021, the Supreme Court in *Facebook v. Duguid* confirmed that the TCPA's restrictions apply only to the abusive telemarketing practices targeted by the Act – i.e., telemarketers' practice of calling randomly or sequentially drawn numbers of consumers – and they do not apply to calls placed by legitimate businesses to stored lists of customer numbers.[10]

---

[7] 47 U.S.C. § 227 *et seq.*

[8] *See* Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, § 2(1), 105 Stat. 2394 (2012) (observing the "increased use of cost-effective telemarketing techniques"); S. Rep. No. 102-178, at 1 (1991) ("The use of automated equipment to engage in telemarketing is generating an increasing number of consumer complaints."); H.R. Rep. No. 102-317, at 6 (1991) (observing that automatic dialing systems permit telemarketers to provide a message to potential customers "without incurring the normal cost of human intervention").

[9] H.R. Rep. No. 102-317, at 17.

[10] *See Facebook v. Duguid*, 592 U.S. 395, 401 (2021).

Despite clear congressional intent and the *Facebook* precedent, certain TCPA rules impair businesses' ability to place consumer-benefitting calls and messages. The Associations have long called for the Commission to revise its TCPA rules,[11] and we commend the Commission for reexamining these rules through this rulemaking, including its rules governing revocation of consent.

In a Report and Order issued in 2024 (Order, or 2024 Order), the Commission stated that, once a consumer revokes consent to receive autodialed or prerecorded voice calls or text messages under the TCPA, the caller may no longer send the consumer *any* calls or text messages that require consent, including fraud alerts, low-balance alerts, multi-factor authentication (MFA) messages, or utility calls – even if that was not the consumer's intent (the "revoke all rule").[12] This past September, ABA and the National Consumer Law Center (NCLC) jointly expressed concern that the Order may undermine their shared goal that consumers' revocations of consent under the TCPA be processed accurately and efficiently.[13] The Associations urge the Commission to modify the revoke all rule, as described in Appendix B, or rescind the rule.

---

[11] *See, e.g., In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 & Delete, Delete, Delete*, CG Docket Nos. 02-278 & 25-133, Comments of Am. Bankers Ass'n *et al.* (filed Apr. 11, 2025), https://www.fcc.gov/ecfs/document/104122423211014/1 [hereinafter, Financial and Utility Trade Associations Delete Comments]; *id.*, Comments of ACA Int'l (filed Apr. 11, 2025), https://www.fcc.gov/ecfs/document/1041181591094/1.

[12] *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order and Further Notice of Proposed Rulemaking, ¶¶ 29-32 (2024) [hereinafter, *2024 Order*].

[13] Letter from Jonathan Thessin, Am. Bankers Ass'n, & Patrick Crotty, Nat'l Consumer L. Ctr., to Brendan Carr, Chairman, Fed. Commc'ns Comm'n (Sept. 18, 2025), https://www.fcc.gov/ecfs/document/1091883314600/1 [hereinafter, ABA/NCLC Letter].

The Associations also urge the Commission, without delay, to extend the effective date of the revoke all rule to the later of April 11, 2027, or six months after adoption of an order resolving the revocation rules proposed in the Proposal. As noted in the ABA/NCLC letter, "further, limited extension of the effective date of this rule would promote the public interest by providing time for the Commission to assess these issues" and would "relieve banks and other callers of the requirement to design and implement complex processes to comply with the rule while the Commission is engaged in rulemaking to reconsider the rule."[14] We urge the Commission to issue an extension without delay.

In addition, the Associations urge the Commission to remove, from its 2015 order, the condition that permits a caller to place an exempt fraud alert or data reach notification only if the call is placed to a number that was provided by the customer.[15] As described in greater detail below, this condition greatly reduces the value of the exemption, and institutions may feel compelled to place fraud alerts only with the prior express consent of the called party.

The Commission has proposed to eliminate two other rules concerning call abandonment rates and the provision of a callback number for artificial and prerecorded voice calls. We agree with the Commission that these rules are outdated, have not been enforced for a substantial amount of time, and should be eliminated. We appreciate that the Commission proposes to eliminate its requirement that a caller that makes artificial or prerecorded voice calls must include a telephone number other than a 900 number. We ask the Commission to eliminate the

---

[14] *Id.* at 2.
[15] *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Declaratory Ruling and Order, ¶¶ 138-145 (2015) [hereinafter, *2015 Order*].

broader requirement that a caller leave a call-back number when placing an artificial or prerecorded voice call.

ARGUMENT

I. THE COMMISSION SHOULD REVISE THE REVOCATION OF CONSENT ORDER

a. The Commission Should Rescind or Modify the "Revoke All" Requirement

The Associations' members respect and carry out customer requests to opt out of receiving autodialed or prerecorded voice calls or text messages. But the revoke all rule could create unintended consequences, leading a company to opt its customer out of a broader set of messages than the consumer intended. Applying this provision, if a consumer replies "stop" to revoke consent to receive one type of message – for example, future autodialed past-due text messages – the caller must stop sending all future communications by phone or text on unrelated matters, such as warnings about unusual credit card transactions (fraud alerts), low-balance alerts, multi-factor authentication (MFA) messages, or utility calls – even if that was not the consumer's intent. Fraud alerts and MFA messages are important tools that banks and other financial institutions use to safeguard their customers. Disenrolling customers from fraud alerts – thereby reducing customers' awareness of fraudulent, or potentially fraudulent, activity on their account – is inconsistent with the work by the Administration and industries to reduce fraud and protect consumers. MFA is a critical tool to prevent fraud on customers' accounts; it prevents unauthorized access by requiring the customer to enter a code, typically received by text, prior to gaining access to the account. If customers are opted out of receiving these texts, MFA could only be enabled via email or a phone call, options rarely chosen by a consumer. Without MFA protecting the account, the customer is exposed to significant risk.

The revoke all rule also could be interpreted to require a revocation request to be honored across business and consumer accounts. For example, if a customer used the same phone number to sign up for alerts on a business account and a personal account, then a revocation request received in response to an alert on a business account may need to be applied to alerts sent on a personal account, and vice versa. This is unlikely to reflect the customer's intent in many cases.

The revoke all rule should be modified or eliminated because its costs outweigh its benefits.[16] The Commission's cost-benefit analysis failed to consider the significant operational changes necessary to implement the Rule.[17] As described in the Associations' *ex parte* filings and in the Edison Electric Institute's comments,[18] institutions with many business units typically have separate calling systems that will need to be integrated to comply with the rule. Under the revoke all rule, when a revocation is placed with one business unit (such as a bank's deposit account unit), the institution must communicate the revocation to all other business units (such as the bank's mortgage and short-term lending divisions) and with third parties hired by a specific business unit to communicate with customers on specific issues. This is costly and burdensome work. Smaller businesses will likely need to adopt manual processes to comply with the Rule.

Measured against these costs, the benefits of the revoke all provision are questionable. The Commission has provided no evidence that a consumer who replies "stop" to one type of

---

[16] *See In re: Delete, Delete, Delete*, GN Docket No. 25-133, Public Notice, 2-3 (Mar. 12, 2025) (observing that the "costs and benefits of a rule are relevant to retrospective review" of a rule) [hereinafter, *Delete Public Notice*].
[17] *See 2024 Order*, *supra* note 12 (App. B, Final Regulatory Flexibility Analysis, ¶ 17).
[18] *See In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Comments of Am. Bankers Ass'n et al. (filed July 31, 2023), https://www.fcc.gov/ecfs/document/108011664508910/1 [hereinafter, Financial Trades 2023 Comments]; *id.*, CG Docket No. 02-278, Reply Comments of Edison Electric Institute and National Rural Electric Cooperatives Association 6, 14-15 (July 31, 2023), https://www.fcc.gov/ecfs/document/10731229016571/2 [hereinafter, EEI/NRECA Comments].

text message seeks to stop receiving all future communications from the institution. To the contrary, in a poll of consumers conducted in October 2025, 62% of respondents stated they are concerned that the revoke all rule will negatively impact them by requiring their bank to stop sending all messages, including fraud alerts.[19]

Finally, the Commission should modify or eliminate the revoke all rule because it is not consistent with President Trump's recent executive orders.[20] Executive Order 14219 requires all agencies, including the Commission, to review all regulations to identify regulations not based on the "best reading of the underlying statutory authority," regulations that "impose significant costs upon private parties that are not outweighed by public benefits," and regulations that "impose undue burdens on small business . . . .."[21] The revoke all rule fits each of these classifications. It is not based on the best reading of the TCPA. The statute was not intended "to be a barrier to the normal, expected or desired communications between businesses and their customers."[22] The rule creates a "barrier" between an institution and its customers by requiring the institution to interpret a consumer's revocation as applying to all communications between the institution and the consumer, not solely to the category of communications to which the

[19] Press Release, Am. Bankers Ass'n, *National Survey: U.S. Consumers Rank Banks Above Other Industries for Fraud Protection, Support Consistent Rules for Data Sharing* (Oct. 20, 2025), https://www.aba.com/about-us/press-room/press-releases/fall-2025-morning-consult-survey-results-consumer-satisfaction. The poll was conducted by Morning Consult on behalf of ABA from October 1-6, 2025, among a national sample of 4,403 adults.

[20] *See Delete Public Notice*, *supra* note 16, at 2 ("encourage[ing] commenters to consider certain policy factors," including the "recent Presidential orders as well as statutory and regulatory retrospective review standards" when providing comment on Commission regulations that should be eliminated).

[21] Executive Order 14,219, Ensuring Lawful Governance and Implementing the President's "Department of Government Efficiency" Deregulatory Initiative, 90 Fed. Reg. 10,583, 10,583, § 2 (Feb. 25, 2025), https://www.federalregister.gov/documents/2025/02/25/2025-03138/ensuring-lawful-governance-and-implementing-the-presidents-department-of-government-efficiency.

[22] H.R. Rep. No. 102-317, at 17.

revocation was directed. And as described above, the provision also "impose[s] significant costs upon private parties" – both upon the consumers who are opted out of communications they wish to receive and the institutions who must implement these requirements, including small businesses. These costs are not "outweighed by public benefits," as there is no public benefit to applying a consumer's revocation more broadly than the consumer intended.

The Associations urge the Commission to rescind or modify the revoke all rule and have offered proposed revisions in Appendix B. The proposed revisions allow the caller to interpret a revocation request as applying only to the category of messages to which the revocation was directed, while also requiring the caller to provide a means for the consumer to revoke consent with respect to all messages requiring consent. We believe this language addresses the intent behind the revoke all rule while better ensuring consumers are not inadvertently cut off from all communications from the companies with whom they do business based on sending a single "stop" message in response to one type of message from that company.

b. The Commission Should Extend the Effective Date of the Revoke All Rule

Last April, the Consumer and Governmental Affairs Bureau granted a waiver delaying implementation of the revoke all rule to April 11, 2026.[23] Good cause exists to further extend this deadline in light of the Commission's proposal to modify the rule. Although the Commission may act before the current April 11, 2026 implementation deadline, businesses must begin deploying resources to comply by that date. These resources will be wasted if the Commission eliminates or modifies the rule.

---

[23] *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Order, DA 25-312 (Apr. 7, 2025).

Additionally, this past September, ABA and NCLC jointly requested a further extension of the deadline until April 11, 2027 should the Commission initiate a rulemaking as it has now done.[24] In light of the foregoing, the Associations respectfully request that the Commission include an order extending the deadline to the later of April 11, 2027, or six months after adoption of an order resolving the revocation rules.

c. The Commission Should Permit Callers to Designate the Exclusive Means by which Consumers May Revoke Prior Express Consent

The Commission proposes to amend its regulations to permit callers to designate the exclusive means by which consumers may revoke prior express consent. In the 2024 Order, under prior leadership, the Commission stated, with the Associations' support,[25] that a revocation request made using the words "stop," "quit," "end," "revoke," "opt out," "cancel," or "unsubscribe" that is sent in reply to an incoming text message constitutes a revocation.[26] However, the Commission also stated that if a consumer uses words other than those listed above, the caller must treat the reply text message as a valid revocation request "if a reasonable person would understand those words to have conveyed a request to revoke consent."[27] We support the Commission's revised proposal that permits a caller to designate the exclusive means by which a consumer may revoke consent instead of requiring callers to honor all revocation requests that are "reasonable."

The provision should be rescinded because allowing revocations through non-standardized terms is unnecessary and creates significant operational challenges and costs. The only benefit of the provision is to allow individuals to use a broader set of words to express a

[24] ABA/NCLC Joint Letter, *supra* note 13, at 2.
[25] *See* Financial Trades 2023 Comments, *supra* note 18, at 13; EEI/NRECA Comments, *supra* note 18, at 12.
[26] *See 2024 Order*, *supra* note 12, at 20 (Appx. A) (*to be codified at* 47 C.F.R. § 64.1200(a)(10)).
[27] *Id.*

revocation of consent. But this benefit is *de minimis*. Text messages sent by banks, credit unions, other financial services providers, and electric utility companies are clear that the recipient can revoke consent to receive additional texts if they reply "STOP."[28] There is no need for consumers to use a term that is not one of the Commission's seven standardized terms.

Against the provision's *de minimis* benefit are substantial costs to banks and other callers. To comply, businesses need to develop a system to identify a revocation that uses non-standard terms. Some of ABA's members have reported that, with each outbound texting campaign, they must build a system for identifying reply texts that use non-standard terms, at substantial cost. Other members have reported they must manually review all text messages received using non-standard terms in order to identify revocations, also at substantial cost. Because non-standardized revocation requests must be processed manually, the caller may be delayed in processing the request – as compared with a request that uses standardized terms – to the detriment of the consumer.[29]

In addition to these compliance costs, businesses face litigation risk with processing non-standard – and often ambiguous – expressions of revocation. Plaintiffs' law firms may counsel bank customers to reply to banks' text messages with "creative" revocation messages in order to generate lawsuits.[30] Although a court may ultimately determine that these means of revocation are not reasonable, the Commission's rules allow for litigation of the "reasonableness" of a revocation request, requiring companies to expend time and resources to litigate and potentially settle cases that do not have merit. Indeed, one bank reported that it manually reviews all non-

[28] *See* Financial and Utility Trade Associations Delete Comments, *supra* note 11, at 11.
[29] *See id.* at 11-12.
[30] For a detailed description of plaintiffs' efforts to use creative expressions of revocation to generate TCPA lawsuits, see Financial Trades 2023 Comments, *supra* note 18, at 8-9.

standard text messages sent in response to the bank's outbound collections texts to reduce this litigation risk.[31]

II. THE COMMISSION SHOULD REMOVE THE "PROVIDED NUMBER" CONDITION TO THE EXEMPTION FOR FRAUD ALERTS AND OTHER SPECIFIED MESSAGES

In its 2015 Declaratory Ruling and Order, the Commission granted ABA's request for an exemption from the TCPA's requirements for time sensitive messages concerning (1) suspected fraud; (2) breach of personal information; (3) remediation action customers can take; and (4) actions needed to arrange for receipt of pending mobile money transfers (Exemption).[32] ABA petitioned for this Exemption because our members desire to contact *all* affected consumers quickly and efficiently to provide these pro-consumer messages, but fear of TCPA class action liability limited their ability to do so absent the Exemption. These calls are free to the customer—as is required by the TCPA for any calls exempted under the Commission's exemption authority provided in section 227(b)(2)(C) of title 47.[33]

In granting the Exemption, the Commission imposed certain conditions that undermine the Exemption. Most significantly, the Commission required financial institutions to send alerts *only* to a wireless number *provided by* the customer of the financial institution (the provided number condition). We applaud the Commission for proposing to eliminate the provided number condition and strongly support its rescission.[34]

---

[31] *See* Financial and Utility Trade Associations Delete Comments, *supra* note 11, at 12.
[32] *2015 Order*, *supra* note 15, ¶¶ 138-39.
[33] The exemption authority provided in 47 U.S.C. § 227(b)(2)(C) provides the Commission with authority to exempt from the TCPA calls to wireless numbers "that are not charged to the called party."
[34] In 2015, ABA filed a Petition for Reconsideration that seeks removal of this unnecessary condition. *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991,* CG Docket No. 02-278, Pet. for Reconsideration of the Am. Bankers

The provided number condition significantly reduces the value provided by the Exemption. In many cases, a bank may have acquired a customer's number through reliable means, but still cannot satisfy the "provided number" condition, including through the following means:

- The bank acquired the customer's account from another institution, such as through a merger, and there is no record of how the predecessor institution obtained the customer's number.
- The bank obtained the customer's number through the customer's incoming call to the bank. If the customer used the bank's automated systems, or otherwise did not speak with a bank representative, the customer may not have had an opportunity to provide his or her number to the bank.
- The customer's spouse provided the customer's number to the bank.

In addition, during an "account takeover" situation – i.e., where a bad actor gains access to a customer's account – a bank may wish to call a number belonging to the customer that the bank cannot demonstrate was provided by the customer. The provided number condition discourages the bank from taking this potentially critical step to protect its customer.

Even when a bank's records show that it acquired a number from the customer, this provided number condition shifts to the bank the burden of proving that fact in the event of a challenge, increasing litigation risk. During the rulemaking proceeding, neither consumer advocacy groups nor any other party supported the condition as appropriate or necessary. Indeed, in a joint letter in 2020, ABA and NCLC asked the Commission to modify the Exemption to permit fraud alerts placed to numbers obtained by the institution through one of the three means described above.[35]

Ass'n (filed Aug. 13, 2015), https://www.aba.com/archives/tcpa-petition-reconsideration. The Commission has not acted on the Petition.

[35] *See* Letter from Margot Saunders, Nat'l Consumer L. Ctr., & Jonathan Thessin, Am. Bankers Ass'n, to Marlene Dortch, Sec., Fed. Commc'ns Comm'n 3-4 (Apr. 23, 2020),

Largely as a result of the provided number condition, ABA understands that few banks are utilizing the Exemption. And for the few banks that use it, removal of the provided number condition would encourage them to place a greater number of exempted calls, as removal of the condition would reduce banks' litigation risk. We urge the Commission to finalize its proposal to remove the provided number condition.

We also ask the Commission to make other modest modifications to the Exemption. Specifically, we ask the Commission to modify the limitation that a financial institution may send no more than three exempted messages per event over a three-day period to the customer of an affected account.[36] We ask the Commission to permit three exempted messages to each authorized user on the account. In the event of a data breach or suspicious activity on a customer's account, banks seek to contact the customer through all available means, including by contacting all authorized users on the account and all phone numbers associated with the account. The existing three-call limitation may prevent banks from contacting all users on the account, or to contact users at a frequency needed to reach a live party.

We also ask the Commission to clarify that a message that protects the consumer from fraud or identity theft may exceed the Exemption's 160-character limit.[37] In certain instances, this limitation makes it difficult, if not impossible, for banks and other businesses to compose messages that include all information that the sender seeks to convey through the message (and that would benefit the customer who receives the message), without truncation. For example, much of the text in an exempted fraud alert is consumed by content that is necessary in order for

---

https://www.aba.com/advocacy/policy-analysis/aba-consumer-group-urge-fcc-to-act-expeditiously-to-facilitate-covid-19-related-bank-calls.

[36] *2015 Order*, *supra* note 15, ¶ 138(5).

[37] *Id.*, ¶ 138(4).

the customer to understand why he or she is receiving the text message, such as the name of the institution placing the message, the merchant where the transaction was attempted, the amount of the transaction, the means by which the recipient may opt out of future texts, and punctuation and spaces.

These requests are described in greater detail in ABA's 2020 comment letter to the Commission.[38]

III. THE COMMISSION SHOULD ELIMINATE OTHER RULES THAT ARE NOT NECESSARY

The Commission seeks comment on whether two other rules – concerning call abandonment rates and identification rules for artificial and prerecorded voice calls – should be eliminated because they are outdated and have not been enforced for a substantial amount of time.[39] We agree that the Commission should eliminate these rules.

First, the Commission asks whether it should eliminate its rules that prohibit callers from disconnecting an unanswered telemarketing call before at least 15 seconds has elapsed or four rings (whichever comes first),[40] and from abandoning more than 3% of all telemarketing calls.[41] We agree with the Commission that these rules are no longer needed because advances make it very unlikely that any calling technology would result in a caller disconnecting an unanswered telemarketing call before at least 15 seconds has elapsed or four rings, or from abandoning more than 3% of all telemarketing calls. Moreover, these rules create an opportunity for a plaintiff in a

---

[38] *See* Letter from Jonathan Thessin, Am. Bankers Ass'n, to Marlene H. Dortch, Sec., Fed. Commc'ns Comm'n 9-14 (Oct. 26, 2020), https://www.fcc.gov/ecfs/document/1027676027558/1.
[39] *Ninth Further Notice*, *supra* note 2, ¶¶ 97-100.
[40] 47 C.F.R. § 64.1200(a)(6).
[41] *Id.* § 64.1200(a)(7).

class action lawsuit to allege that the bank or other business did not abide by these rules, no matter how unsupported that contention may be.

Second, the Commission asks whether it should eliminate its identification rules for artificial and prerecorded voice calls. Current FCC rules require a caller that is making artificial or pre-recorded voice calls to include a telephone number other than a 900 number (or any other number for which a charge would apply to the caller). The FCC proposes to replace this requirement with one that requires callers to provide a number that accepts "do-not-call" requests during normal business hours.

Our members do not provide a 900 number (or other number that results in charges to the consumer) when placing an artificial or prerecorded voice call, and we agree with the Commission that this rule is not necessary. We ask the Commission to eliminate the broader requirement that a caller leave a call-back number when placing an artificial or prerecorded voice call. Today, banks that place artificial or prerecorded voice calls may do so using artificial intelligence (AI) that will process a consumer's request not to receive additional consented-to calls. Moreover, our members are reluctant to leave a callback number, as that may suggest to the consumer that the business' call is fraudulent. Our members prefer to direct the consumer to contact the business using the phone number on the back of the consumer's credit or debit card.

IV. THE COMMISSION SHOULD REQUIRE WIRELESS PROVIDERS TO TAKE SPECIFIC STEPS TO STOP BAD ACTORS FROM IMPERSONATING LEGITIMATE COMPANIES AND GAINING CONSUMERS' TRUST

In addition to proposing rules that facilitate the ability of legitimate businesses to contact their customers, the Commission also proposes rules to combat bad actors who seek to defraud consumers through illegal calls. These proposals are a vital complement to the work that our members do every day to protect their customers and other consumers from fraud. We strongly support the Commission's work to stop fraudsters but, as described in greater detail below, we believe the Commission must require telecommunications companies to take specific steps to keep criminals from using our nation's calling infrastructure to defraud consumers.

The Commission's work to combat fraud has centered on a requirement that voice service providers adopt the "STIR/SHAKEN" call authentication framework – an industry-developed framework whereby calls are "signed" at origination with different levels of "attestation." That attestation is then verified through the call pathway until the call is delivered to the consumer. A call that receives an "A-level" attestation – the highest form of attestation – means the voice service provider originating the call (originating provider) knows the caller and knows the caller has the legal right to the number that will be displayed in the recipient's caller ID.[42] If a call receives A-level attestation, it is eligible for vendors' call branding designed to signal that the call is from a legitimate source, such as green "checkmark."

But STIR/SHAKEN has not lived up to its promise. Bad actors have found ways to place A-level-attested calls that illegally spoof the names and phone numbers of banks, credit unions, other financial services providers, electric utility companies, and other legitimate companies. We support the Commission's proposals to stop these criminals, but we also propose additional steps to strengthen the STIR/SHAKEN call authentication framework.[43]

---

[42] *See In the Matter of Call Authentication Trust Anchor*, WC Docket No. 17-97, Eighth Report and Order ¶ 10 (2024), https://docs.fcc.gov/public/attachments/FCC-24-120A1.pdf (describing attestation levels). B-level attestation means that the originating provider knows the caller but does not know if the customer has lawful access to the number used to place the call. C-level attestation means the originating provider does not know the caller or whether the caller has lawful access to the number. *Id.*

[43] At the outset, we observe that STIR/SHAKEN only works over IP networks. If a call passes through a non-IP network, which is often the case, the STIR/SHAKEN attestation is dropped. We continue to urge the Commission to establish a firm deadline for the transition of legacy TDM and other non-IP networks to IP. *See, e.g., id.*, Comments of ACA Int'l *et al.* (filed Nov.

a. The Commission Should Ensure Callers Have the Legal Right to Use the Number that Will Be Displayed in the Recipient's Caller ID Display When Providing A-Level Attestation to a Call

We appreciate that the Commission proposes new requirements intended to promote the reliability of an A-level attestation. Specifically, the Commission proposes to require providers that are delivering A-level calls to consumers to transmit only verified caller identity information.[44] We agree with the Commission that current requirements for A-level attestation do not provide sufficient assurance that the caller is a legitimate business. Available data show that too many A-level-attested calls are in fact illegally spoofed calls. In one analysis conducted for ABA of 12,900 calls that illegally spoofed telephone numbers belonging to 47 large banks, retailers, and healthcare providers, more than half of the calls received an A-level or B-level attestation.[45] In another example, fraudsters placed six waves of illegal imposter calls (where the fraudster claimed to be a bank) to consumers over eight weeks between mid-September and mid-November; each wave consisted of over 500,000 illegal calls, for a total of 15 million estimated illegal calls.[46] Significantly, over two-thirds of these calls received A- or B-level attestation.[47] In another example provided to BPI, a large bank determined that over 30% of the calls terminated using its number were spoofed.

18, 2025), https://www.fcc.gov/ecfs/document/111858134339/1; *id.*, Comments of Am. Bankers Ass'n *et al.* (filed July 16, 2025), https://www.fcc.gov/ecfs/document/107161568110562/1.

[44] *Ninth Further Notice*, *supra* note 2, ¶¶ 30-42.

[45] App. C, at 3-5. For ABA, a consultant identified 12,900 calls placed between January 1, 2025 and December 18, 2025, that illegally spoofed 47 financial institutions and other leading U.S. companies. Of those calls, 80.2% received A- or B-level attestation.

[46] *Id.* at 6-10. Each illegal call had the following script: "Hello, this is an automated alert from [BANK NAME]. A purchase was declined for $328.99 at [RETAILER/SITE]. Press 5 if you recognize this purchase. If you do not recognize this purchase, call our fraud department immediately at (800) XXX-XXX. To repeat this message, please press 1." *Id.* at 7.

[47] *Id.* at 8.

Our Associations have long called for the Commission to require telecoms to confirm a caller's name and phone number before permitting it to appear on a caller ID display.[48] Therefore, we support the Commission's proposal to require terminating providers to transmit ***verified*** caller identity information when it assigns an A-level attestation to a call. If the terminating provider does not have verified caller identity information, the provider should not be able to represent to the recipient that the call is from a legitimate source by giving the call an A-level attestation.

We support the Commission's proposal to require originating providers that transmit caller identity information to employ "reasonable measures" to verify the accuracy of the information transmitted.[49] We urge the Commission to define "reasonable measures" in a manner that (1) requires voice service providers to follow robust and specific know your customer procedures before allowing a caller to place calls on the provider's network, as discussed *infra* on pages 23-24; and (2) requires the caller to demonstrate to the provider that the caller has the legal right to use the number that will be displayed in the recipient's caller ID display when the caller seeks to place an A-level attested call.

Today, bad actors are able to place illegally spoofed calls with A-level attestation in large part because originating providers do not regularly engage in meaningful diligence of the caller before granting A-level attestation to its calls. Existing FCC rules, however, require each originating provider to take "affirmative, effective measures" to prevent callers from

---

[48] *See In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor,* CG Docket No. 17-59, WC Docket No. 17-97, Comments of Am. Bankers Ass'n *et al.* 17 (Aug. 9, 2023), https://www.fcc.gov/ecfs/document/108100286505590/1.
[49] *Ninth Further Notice*, *supra* note 2, ¶¶ 43-49.

"originat[ing] illegal calls, including knowing its customers . . . ."[50] Similarly, in 2023, the Commission required every provider in the call's pathway to take "reasonable and effective steps" to ensure that it does not transmit illegal calls, even if the provider did not originate the call (the Effective Measures Rule).[51] But the Commission has "not mandate[d] specific measures to comply with" these rules,[52] which we urge the FCC to do now to promote accountability and combat the proliferation of illegal calls. An analysis conducted for ABA identified a fraudulent originating provider that increased its calling operations from originating no calls in July 2025 to more than 136 million calls by September 2025.[53] Further analysis showed that the majority of calls originated by this provider consisted of illegal calls. Clearly, the provider did not conduct diligence of the (bad actor) companies on whose behalf the provider originated calls.

For example, a more robust "Know Your Customer" requirement could require voice service providers to confirm that the business is bonded, has a legitimate physical address (i.e., one that does not raise red flags such as being shared with dozens of other entities), offers a real product or service; and that the person operating the business has not previously been charged with violating telemarketing laws. Providers also could be required to understand the nature of

---

[50] 47 C.F.R. § 64.1200(n).

[51] *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor,* Seventh Report and Order in CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59, ¶¶ 49-51 (rel. May 19, 2023), https://docs.fcc.gov/public/attachments/FCC-23-37A1.pdf.

[52] *In the Matter of Telnyx LLC*, File No. EB-TCD-24-00037170, FCC 25-10, ¶ 2 (Feb. 4, 2025), https://docs.fcc.gov/public/attachments/FCC-25-10A1.pdf (summarizing 47 C.F.R. § 64.1200(n)(4)); *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order ¶ 34 (Dec. 30, 2020), https://docs.fcc.gov/public/attachments/FCC-20-187A1.pdf (promulgating regulation that gave voice service providers "flexibility" in meeting KYC requirements).

[53] App. C, at 12-13. As further evidence that this originating provider was transmitting fraudulent calls, the provider had a Delaware address shared by approximately one hundred other entities and had a primary contact number in a foreign country.

the caller's business. If a caller seeks access to thousands of phone numbers to place millions of calls, the provider should investigate why the caller seeks access to so many numbers.

As a second step to ensure originating providers do not originate calls on behalf of bad actors, the Commission should require originating providers – when they provide A-level attestation – to verify that the caller has the legal right to use the phone number that will be displayed in the recipient's caller ID. As described above, our research found that originating providers currently do not verify that the caller has the legal right to use the number displayed in the recipient's caller ID display before providing an A-level attestation for the call.[54] That must change. The Commission should require this verification step in order for a provider to satisfy the Commission's proposed requirement that originating providers employ "reasonable measures" to verify the accuracy of the information transmitted in the call.[55]

To ensure that voice service providers follow the requirements listed above, the Commission should propose, in a separate notice of proposed rulemaking, two actions:

(1) The Commission should propose establishing a verification system that ensures callers have the legal rights to originate calls using the caller's telephone numbers and an auditing process that allows verification of compliance.[56]

(2) The Commission should propose creating a database of the phone numbers that have been assigned to individual callers, so that originating providers can more easily

---

[54] *See supra* page 21.
[55] *Ninth Further Notice*, *supra* note 2, ¶ 43.
[56] This verification system could be modeled after the Global Legal Entity Identifier Foundation (GLEIF). GLEIF is a supra-national, not-for-profit organization that was tasked by the Financial Stability Board in the aftermath of the 2008 financial crisis to manage an open, non-proprietary legal entity identification system. *See* GLEIF – Global Legal Entity Identifier Foundation, https://www.gleif.org/en (last visited Dec. 30, 2025). The Commission should establish a structure modeled after GLEIF to ensure voice service providers engage in robust vetting of callers.

verify that a caller has the legal right to place calls from a certain phone number. The Commission should explore requiring originating providers to consult with the reassigned numbers database to verify that a caller has the legal right to place calls from the number that will be displayed in the call recipient's caller ID display before providing an A-level attestation to the call.[57]

Imposing these requirements on originating providers will facilitate the Commission's enforcement of the existing STIR/SHAKEN standards. We appreciate that the Commission in recent months has prohibited over 1,200 voice service providers from originating or transmitting calls because the provider failed to stop illegal calls, and has issued orders and cease-and-desist letters to require other providers to stop transmitting illegal calls.[58] If originating providers are required to take specific steps to ensure callers are legitimate, then the Commission can take more effective enforcement action against providers that violate these rules – before the illegal calls are placed. Commission enforcement actions are critical because only the Commission – and not the Federal Trade Commission or another federal agency – can bring actions against voice service providers that originate or transmit illegal calls.[59]

---

[57] In 2021, the Commission created a database of reassigned numbers to assist callers with determining whether the number belonging to their customer had been reassigned to another consumer unbeknownst to the caller. *See* Fed. Commc'ns Comm'n, Reassigned Numbers Database, https://www.fcc.gov/reassigned-numbers-database (last visited Jan. 5, 2026).

[58] *See In the Matter of Robocall Mitigation Database Filers*, DA 25-737 (rel. Aug. 25, 2025), https://docs.fcc.gov/public/attachments/DA-25-737A1.pdf; *In the Matter of China Telecom Global Limited*, DA 25-1022 (rel. Dec. 8, 2025), https://docs.fcc.gov/public/attachments/DA-25-1022A1.pdf; Letter from Patrick Webre, Acting Chief, Enforcement Bureau, Fed. Commc'ns Comm'n, to SK Teleco LLC, DC-415638 (Dec. 2, 2025), https://docs.fcc.gov/public/attachments/DOC-415638A1.pdf; Robocall Enforcement Notice to All U.S.-Based Voice Service Providers, DA 24-1081 (rel. Oct. 18, 2024), https://docs.fcc.gov/public/attachments/DA-24-1081A1.pdf.

[59] *See* 15 U.S.C. § 45(a)(2) (exempting, from the Federal Trade Commission's authority over unfair or deceptive acts or practices, common carriers).

b. The Commission Should Address Barriers to Efficient and Cost-Effective Use of Rich Call Data

To ensure that caller identity information is securely transmitted from the originating provider to the terminating provider, the Commission seeks comment on whether to require providers to use "Rich Call Data" (Rich Call Data or RCD) whenever they transmit caller identity information.[60] Through Rich Call Data, the caller's identity information is placed into an encrypted token with a digital signature, which the terminating provider then decrypts and verifies.[61] RCD allows the caller to display its name, logo, and/or website on the recipient's caller ID display.[62]

We agree that use of RCD has the potential to enhance the reliability of caller identity information by preventing alteration in transit, which will empower consumers to make informed decisions about whether to answer a call. The Commission should require all originating providers to implement RCD to securely transmit caller identity information, similar to the existing requirement that all providers must implement the STIR/SHAKEN call authentication framework. This would allow callers to use the functionality provided by RCD. However, as described below, challenges exist that currently prevent the efficient and cost-effective use of RCD. Consequently, the Commission should address these challenges before mandating that callers use RCD.

First, RCD will only be effective if originating providers verify the identity of the caller who places a call that will use RCD. Otherwise, bad actors will obtain access to RCD and place

---

[60] *Ninth Further Notice*, *supra* note 2, ¶¶ 51-55; *see also* Signature-based Handling of Asserted Information Using toKENS (SHAKEN): Calling Name and Rich Call Data Handling Procedures, ATIS-100094.2 (Apr. 30, 2025) (providing standards for Rich Call Data).
[61] *Ninth Further Notice*, *supra* note 2, ¶ 51.
[62] *Id.*

calls with the indicia of legitimacy – just as bad actor callers are doing today when they improperly obtain A-level attestation for their calls.[63] If the Commission mandates use of RCD, it should require providers to verify that a caller has the legal right to use the number that will be displayed on the recipient's caller ID display and that the logo displayed belongs to the caller.

Second, RCD and other branded calling technology requires end-to-end IP connectivity to function. TDM network infrastructure – the legacy "copper" wires – removes authentication information and cannot support the transmission of RCD. Thus, for RCD to be deployed widely, legacy TDM equipment must be replaced by IP. We continue to urge the Commission to require providers utilizing legacy TDM networks to transition to IP by a date certain.[64] Without a clear and enforceable timeline for IP migration, branded calling through RCD will remain limited to a subset of calls, undermining its potential to prevent fraud.

Third, the Commission should recognize that RCD and other call-branding services today are cost-prohibitive for many callers. This cost creates a barrier for broader adoption of RCD. The Commission should be mindful of this reality as it promotes RCD.

Rich Call Data represents a promising next step in the evolution of call authentication and the fight against illegal robocalls. But the Commission must ensure that the information transmitted through RCD is verified, and that barriers to broader adoption are addressed. Without these steps, the promise of RCD will not be realized.

---

[63] *See* Letter from Keith Buell, General Counsel & Head of Global Pub. Policy, Numeracle, to Marlene Dortch, Sec., Fed. Commc'ns Comm'n 2-3 (Oct. 21, 2025), https://www.fcc.gov/ecfs/document/10210742510712/1 (asserting that Commission must ensure that caller information used in RCD is verified).

[64] *See supra* note 43 (describing Associations' past advocacy urging Commission to require providers utilizing legacy TDM networks to transition to IP by a date certain).

V. THE COMMISSION SHOULD STUDY THE IMPACT ON ILLEGAL CALLS AND ON LAWFUL COMPANIES OF THE COMMISSION'S PROPOSED NEW OBLIGATIONS ON FOREIGN-ORIGINATED CALLS

A clear majority of illegal calls are placed by organizations outside the United States.[65] In recognition of the significant problem posed by these foreign-originated calls, the Commission proposes several measures to identify them for call recipients. Specifically, the Commission:

- Proposes to require voice service providers that use reasonable analytics to block calls to consider, as a factor in their analytics, whether a call originated from outside of the U.S.
- Asks whether it should establish a specific area code for all foreign-originated calls to identify these calls to consumers. If the Commission establishes a specific area code for foreign-originated calls, the agency asks if it should require gateway providers to block any foreign-originated calls that will display a U.S. phone number on the recipient's caller ID display.
- Asks whether it should continue to permit callers to spoof U.S. telephone numbers for calls originated outside of the U.S. for calls made by a business, such as a bank, that has a call center located outside the U.S.

The Associations agree with the Commission that calls placed by organizations outside the United States are a significant problem, and we support the Commission's efforts to combat these calls. At the same time, it is critical that U.S. businesses be able to allocate their human resources in the most efficient way possible – whether through call centers located domestically or abroad – so that businesses can serve their customers promptly and economically. If

[65] *See, e.g.,* Aspen Institute Financial Security Program, Elevating Fraud and Scams as a National Security Threat (Oct. 27, 2025), https://fraudtaskforce.aspeninstitute.org/scams-as-national-security-threat.

regulations force businesses to misallocate resources, it will lead to greater costs to consumers, less efficient service, and reduced economic output. We also are concerned that the Commission's proposals to address illegal foreign-originated calls, though well-intentioned, would discourage consumers from answering calls placed by legitimate companies that employ customer service representatives at locations outside of the United States.

In addition, the Commission's proposals may not be effective at stopping illegal calls placed by organizations outside the United States. Data obtained by ABA's consultant shows that most illegal calls originate inside the United States because illegal callers typically have established U.S.-based originating telecommunications companies to initiate the calls. Once the call is connected, the bad actor uses Voice Over Internet Protocol (VOIP) to initiate a secondary call to connect the first call to the overseas center where the scammer speaking on the phone is located.

We ask the Commission, before moving forward with its proposals, to conduct a study of their impact on U.S. businesses and on stopping organizations operating illegal calls.

VI. THE COMMISSION SHOULD ISSUE A SEPARATE NOTICE OF PROPOSED RULEMAKING THAT PROPOSES ADDITIONAL ACTIONS TO STOP BAD ACTORS WHO SEEK TO DEFRAUD CONSUMERS

The Associations appreciate that the Commission has taken significant steps in our collective fight to stop bad actor callers who seek to defraud consumers. However, as the Associations have recommended previously, there are additional steps that the Commission can and should take to stop these illegal calls. We urge the Commission to propose the following actions in a separate notice of proposed rulemaking.

- **Create a database of reported "SCAM" messages.** We urge the Commission to establish a centralized database of customer-reported "SCAM" messages – i.e., suspected fraudulent or spam messages that customers report to their voice service provider or messaging provider through the "Report Junk" feature on iPhones and "Block and report spam" option on Android devices. The database should allow registered companies, including our members, to review the submissions for brand impersonation so that they can identify ongoing scams targeting the company's customers and take action to mitigate the impact. Additionally, a centralized portal with contributions from voice service providers and all significant messaging providers would provide real-time intelligence to companies in ongoing scam activities, allowing affected industries to better respond with tailored mitigation measures. Importantly, all messaging providers – e.g. voice service providers, Apple, WhatsApp, etc. – should be required to submit customer-reported "spam/scam texts/messages" to the database.[66] In designing the database, we encourage the Commission to take steps to ensure access to the database is not cost-prohibitive. The database would contain data that is freely provided by consumers, and callers using the database would expend additional resources to act on the information they obtain from the database to protect consumers.

[66] The Commission has authority under section 251(e) of the Communications Act to require voice service providers and messaging providers to report customer-reported "SCAM" messages to a centralized database. The Commission previously concluded that the agency's exclusive jurisdiction over numbering policy provides authority for the agency to require voice service providers to implement the "STIR/SHAKEN" call authentication framework to prevent the fraudulent abuse of the phone numbers that are administered under the North American Numbering Plan. *In the Matter of Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order ¶ 153 (rel. Oct. 1, 2020), https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf; *In the Matter of Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 & 20-67, Report and Order and Further Notice of Proposed Rulemaking ¶ 42 (rel. Mar. 31, 2020) [hereinafter, *First Caller ID Authentication Report and Order and Further Notice*], https://docs.fcc.gov/public/attachments/FCC-20-42A1.pdf. A database of reported SCAM messages is similarly intended to prevent the fraudulent abuse of phone numbers administered under the NANP.

- **Require subscribers to opt into "email-to-text" before receiving these messages:** Criminals distribute large volumes of "smishing" messages (a "phishing" attack through text message) from e-mail addresses, which convert the e-mail message to an SMS text message. Criminals often send these "e-mail to SMS" messages from telephone numbers that cannot accept incoming calls. These numbers are not uniquely assigned to an e-mail address, and therefore they cannot easily be reported and shut down. Requiring mobile wireless providers to offer email-to-text as an opt-in service would significantly reduce the use of this technology to send illegal text messages. We commend the Commission for including this provision in a draft Report and Order issued last September 5, 2024.[67] We urge the Commission to finalize this provision.
- **Require a voice service provider – when it blocks a call in the network – to send the required SIP Code 603+ notification to the responsible organization (i.e., the legitimate company that has been assigned the phone number from which the call purported to originate), not to the caller, if those two entities are different.** This past March, the Commission required voice service providers exclusively to use "SIP Code 603+" to communicate to the caller that its call was blocked in the network based on analytics.[68] We commend the Commission for requiring use of SIP Code 603+. However, criminals who illegally spoof legitimate companies may receive notification when their illegal call is blocked in the network, tipping them off. The notification should instead be

---

[67] *See In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls and Targeting and Eliminating Unlawful Text Messages*, Eighth Report and Order in CG Docket No. 17-59 & Third Report and Order in CG Docket No. 21-402, ¶¶ 71-73 (pub. draft rel. Sept. 5, 2024).

[68] *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Eighth Report and Order, ¶¶ 15-25 (rel. Feb. 28, 2025).

sent to the company whose number is being illegally spoofed, so they can be made aware that a criminal is spoofing their phone number.

- **Ban SIM boxes.** SIM boxes allow the use of multiple SIM cards simultaneously. Each SIM card allows a criminal to send calls or text messages that purport to originate from a different phone number.[69] An organization with a SIM box thus is capable of placing thousands of fraudulent texts or calls to consumers at once. Because the calls purport to originate from different numbers, it is very difficult to track the calls' origin. The Commission should ban the possession or supplying of SIM boxes.[70]

- **Make clear that "number renting" is prohibited by the Commission's existing rules.** Bad actors may obtain hundreds of thousands of phone numbers from which to place outbound calls, use those numbers for a short duration of time, and then return those numbers and seek new numbers from which to originate calls. We agree with the National Consumer Law Center that, to our knowledge, there is no legitimate reason why a caller would want to use a number for a short duration of time.[71] To the contrary, our

---

[69] *See* App. C, at 16 (describing growth of prepaid SIM card-enabled scam calls and text messages).

[70] The United Kingdom banned the possession or supplying of SIM boxes in April 2025.

The Commission has legal authority to ban SIM boxes under its long-standing authority to regulate "all facets of numbering administration in the United States." Second Report and Order and Memorandum Opinion and Order, 11 FCC Rcd 19392, 19512, ¶ 271 (1996). As referenced above, in 2020, under this authority, the Commission required voice service providers to implement the STIR/SHAKEN caller ID authentication framework to "prevent the fraudulent exploitation of numbering resources." *First Caller ID Authentication Report and Order and Further Notice*, *supra* note 66, ¶ 42; *see also id.*, ¶¶ 3, 68. A ban on SIM boxes similarly is intended to prevent criminals from fraudulently exploiting our nation's numbering resources by placing calls that purport to originate from a phone number that is different than the number from which the call actually originated.

[71] *See* Letter from Chris Frascella, Electronic Privacy Info. Ctr., & Margot Saunders, Nat'l Consumer L. Ctr., to Marlene Dortch, Sec., Fed. Commc'ns Comm'n (Mar. 25, 2024), https://www.fcc.gov/ecfs/document/10325387525062/1; *In the Matter of Numbering Policies for Modern Communications, Telephone Numbering Requirements for IP-Enabled Service*

members seek to advance their brand and deepen their relationship with consumers by using a consistent set of phone numbers from which to place calls.

CONCLUSION

We commend the Commission for issuing a proposal that, if adopted, will take important steps forward in the fight against illegal calls spoofing by strengthening our nation's call authentication framework. The proposal also would make important updates to the Commission's telecommunications rules, including modifying the revoke all rule. To prevent companies from needlessly expending resources while the Commission reconsiders the rule, we urge the Commission to extend the effective date of the rule to the later of April 11, 2027, or six months after adoption of an order resolving the revocation rules proposed in the Proposal.

Respectfully submitted,

s//Jonathan Thessin
Jonathan Thessin
Vice President/Senior Counsel
American Bankers Association
1333 New Hampshire Avenue, NW
Washington, DC 20036
(202) 663-5016

s//Philip Bohi
Philip Bohi
General Counsel
American Financial Services Ass'n
1750 H St NW Suite 650
Washington, DC 20006
(202) 466-8605

s//James Akin
James Akin
Head of Regulatory Advocacy
America's Credit Unions
99 M Street, SE
Washington, DC 20003
(800) 356-9655

s//Greg Williamson
Greg Williamson
Senior Vice President, Fraud Reduction
Bank Policy Institute
1300 Eye Street, NW
Washington, DC 20005
(202) 289-4322

Providers, Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources, WC Docket Nos. 13-97, 07-243, & 20-67, Reply Comments of National Consumer Law Center et al. (filed Dec. 22, 2023), https://www.fcc.gov/ecfs/document/122235773414/1.

s//Brian Fritzsche
Brian Fritzsche
Vice President, Associate General Counsel
Consumer Bankers Association
1225 New York Ave., NW
Washington, DC, 20005
(202) 552-6381

s//Jason Stverak
Jason Stverak
Chief Advocacy Officer
Defense Credit Union Council
1627 Eye Street, NW, Suite 935
Washington, DC 20006
(202) 734-5007

s//Alisha Sears
Alisha Sears
Director, Regulatory Counsel
Mortgage Bankers Association
1919 M Street, NW, 5th Floor
Washington DC 20036
(202) 557-2930

s//Scott Buchanan
Scott Buchanan
Executive Director
Student Loan Servicing Alliance
2210 Mt. Vernon Avenue, Suite 207
Alexandria, VA 22301
(202) 955-6055

January 5, 2026

APPENDIX A

The American Bankers Association is the voice of the nation's $25.1 trillion banking industry, which is composed of small, regional and large banks that together employ over 2 million people, safeguard $19.7 trillion in deposits and extend $13.2 trillion in loans.

The American Financial Services Association (AFSA) is the national trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with closed-end and open-end credit products including traditional installment loans, mortgages, direct and indirect vehicle financing, payment cards, and retail sales finance.

America's Credit Unions is the national trade association for consumers' best option for financial services: credit unions. America's Credit Unions advocates for policies that allow credit unions to effectively meet the needs of their nearly 142 million members nationwide.

The Bank Policy Institute is a nonpartisan public policy, research and advocacy group that represents universal banks, regional banks, and the major foreign banks doing business in the United States. BPI produces academic research and analysis on regulatory and monetary policy topics, analyzes and comments on proposed regulations, and represents the financial services industry with respect to cybersecurity, fraud, and other information security issues.

The CBA is a member-driven trade association, and the only national financial trade group focused exclusively on retail banking—banking services geared toward consumers and small businesses. As the recognized voice on retail banking issues, CBA provides leadership, education, research, and federal representation for its members. CBA members operate in all 50 states. They include the nation's largest bank holding companies as well as regional and supercommunity banks. Eighty-three percent of CBA's members are financial institutions holding more than $10 billion in assets

The Defense Credit Union Council (DCUC) is the trusted resource for credit unions on all military and veteran matters.

The Mortgage Bankers Association (MBA) is the national association representing the real estate finance industry that works to ensure the continued strength of the nation's residential and commercial real estate markets, to expand homeownership, and to extend access to affordable housing to all Americans.

The Student Loan Servicing Alliance (SLSA) is the nonprofit trade association that focuses exclusively on student loan servicing issues. Our membership is responsible for servicing all federal student loans and the vast majority of private loans, and our membership is a mix of companies, state agencies, non-profits and their service partners. Our servicer members and affiliate members provide the full range of student loan servicing operations, repayment support, customer service, payment processing, and claims processing for tens of millions of federal and private loan borrowers across the country.

APPENDIX B

Proposed Revisions to 47 C.F.R. 64.1200(a)(10)-(12)

Bold = language to be added

~~Strike out~~ = language to be deleted

***

(10) A called party may revoke prior express consent, including prior express written consent, to receive calls or text messages made pursuant to paragraphs (a)(1) through (3) and (c)(2) of this section ~~by using any reasonable method to clearly express a desire not to receive further calls or text messages from the caller or sender~~. Any revocation request made using **(i)** an automated, interactive voice or key press-activated opt-out mechanism on a call; **(ii)** using the words "stop," "quit," "end," "revoke," "opt out," "cancel," or "unsubscribe" sent in reply to an incoming text message; or **(iii)** pursuant to a website or telephone number designated by the caller to process opt-out requests constitutes a ~~reasonable means~~ per se ~~to revoke~~ **revocation of** consent**, provided that a caller may specify the scope of calls and text messages to which a revocation sent using one of these means would apply as long as the caller informs the recipient of an option to revoke consent with respect to all calls and text messages requiring consent.** ~~If a called party uses any such method to revoke consent, that consent is considered definitively revoked and the caller may not send additional robocalls and robotexts. If a reply to an incoming text message uses words other than "stop," "quit," "end," "revoke," "opt out," "cancel," or "unsubscribe," the caller must treat that reply text as a valid revocation request if a reasonable person would understand those words to have conveyed a request to revoke consent.~~ Should the text initiator choose to use a texting protocol that does not allow reply texts, it must provide a clear and conspicuous disclosure on each text to the consumer that two-way texting is not available due to technical limitations of the texting protocol, and clearly and conspicuously provide on each text reasonable alternative ways to revoke consent. All requests to revoke prior express consent or prior express written consent made in ~~any reasonable manner~~ **the manner described above** must be honored within ~~a reasonable time not to exceed~~ ten business days from receipt of such request. ~~Callers or senders of text messages covered by paragraphs (a)(1) through (3) and (c)(2) of this section may not designate an exclusive means to request revocation of consent.~~

~~(a)(11) The use of any other means to revoke consent not listed in paragraph (a)(10) of this section, such as a voicemail or email to any telephone number or email address intended to reach the caller, creates a rebuttable presumption that the consumer has revoked consent when the called party satisfies their obligation to produce evidence that such a request has been made, absent evidence to the contrary. In those circumstances, a totality of circumstances analysis will determine whether the caller can demonstrate that a request to revoke consent has not been conveyed in a reasonable manner.~~

(12) A ~~one-time~~ text message confirming a request to revoke consent ~~from receiving any further calls or text messages~~ **or informing the called party of the option to revoke consent with respect to all calls and text messages requiring consent,** made pursuant to paragraph (a)(10)**,**

does not violate paragraphs (a)(1) and (2) of this section as long as the confirmation text**(s)** ~~merely confirms the text recipient's revocation request and~~ does not include any marketing or promotional information~~, and is the only additional message sent to the called party after receipt of the revocation request~~. ~~If the confirmation text is sent within five minutes of receipt, it will be presumed to fall within the consumer's prior express consent. If it takes longer, however, the sender will have to make a showing that such delay was reasonable.~~ To the extent that the text recipient has consented to several categories of text messages from the text sender, the confirmation message may request clarification as to whether the revocation request was meant to encompass all such messages~~; the sender must cease all further texts for which consent is required absent further clarification that the recipient wishes to continue to receive certain text messages~~.

Appendix C

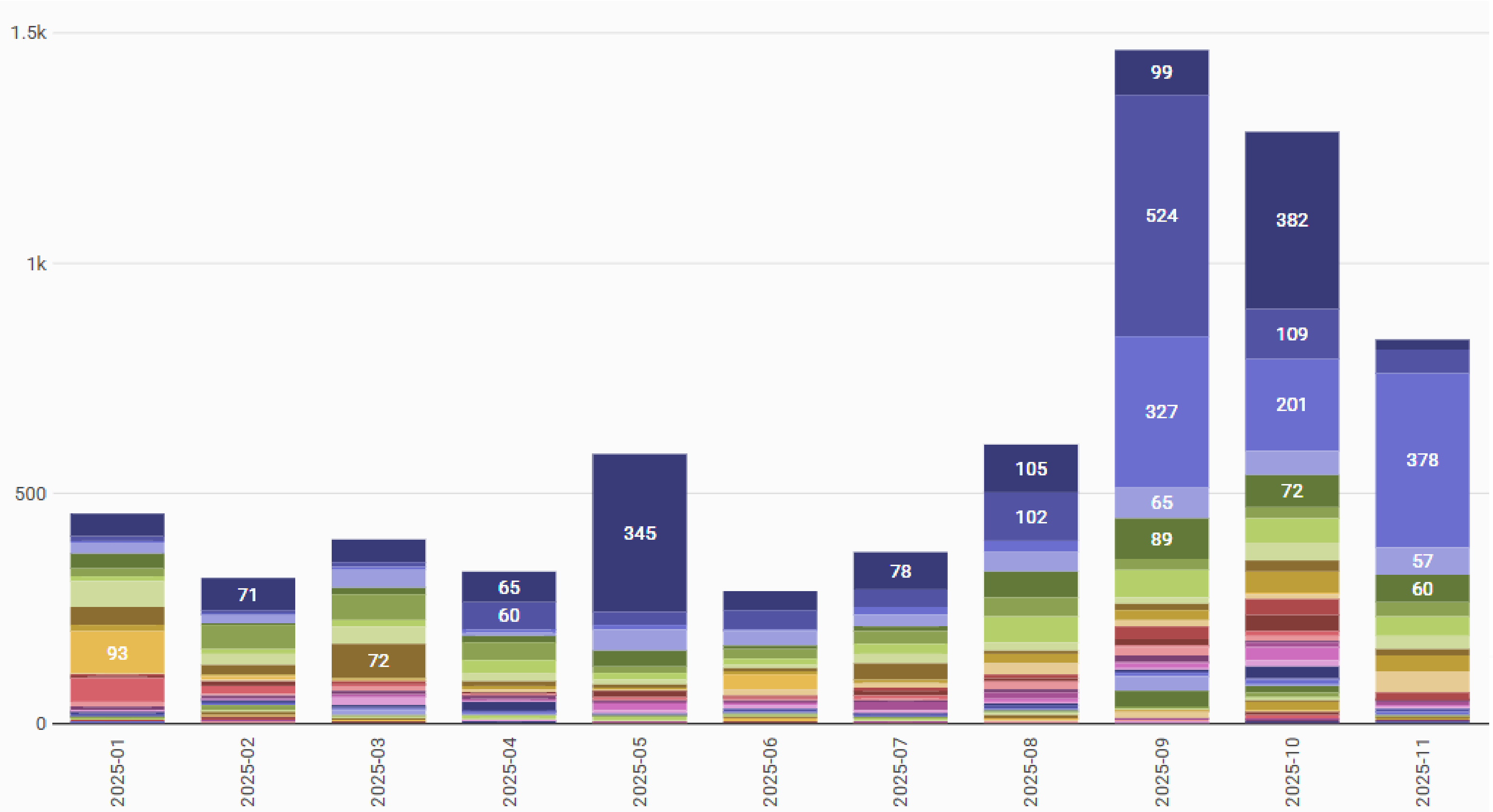
2025 Study of Financial Institution Owned Toll-Free Number Spoofing

A Study In Toll Free Number Spoofing Of Financials

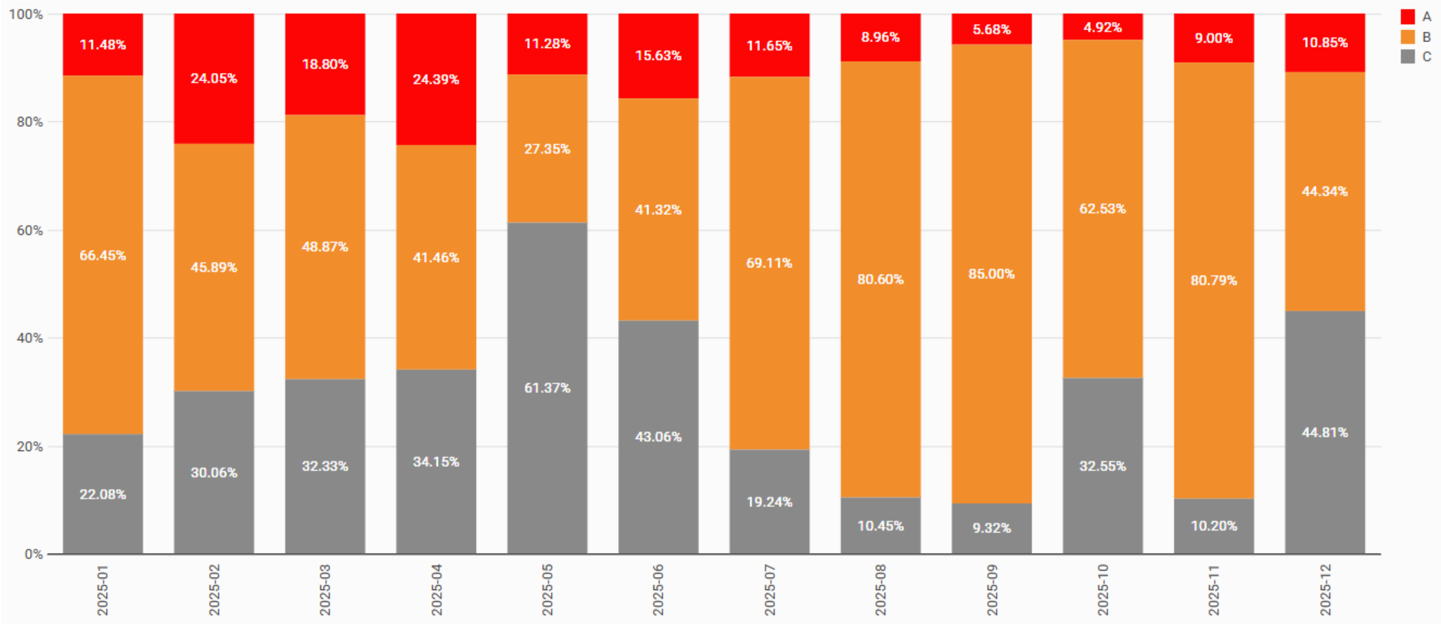
The study involved 47 top brands targeted by spoofing, including top banks, credit unions, payment networks and large retailers and healthcare providers. The analysis utilized:

- Over 12,900 calls with attestation data
- 206 toll-free numbers owned by
- 47 large, recognizable U.S. institutions
- 302 distinct telecom providers attesting calls

Incidents rising in volume & breadth



More Than Half is A or B Attested



A- Level attestation

Provider knows the caller **and** confirms they are **authorized to use the calling number**

B-Level Attestation

Provider knows the caller **but has not verified** they are authorized to use the calling number

C-Level Attestation

Provider **cannot verify** the caller or their authorization and only knows the call entered its network.

>> A & B attests could be used in Branded Calling as well

Retrospective Of Recent Vishing Incidents For Top US Bank

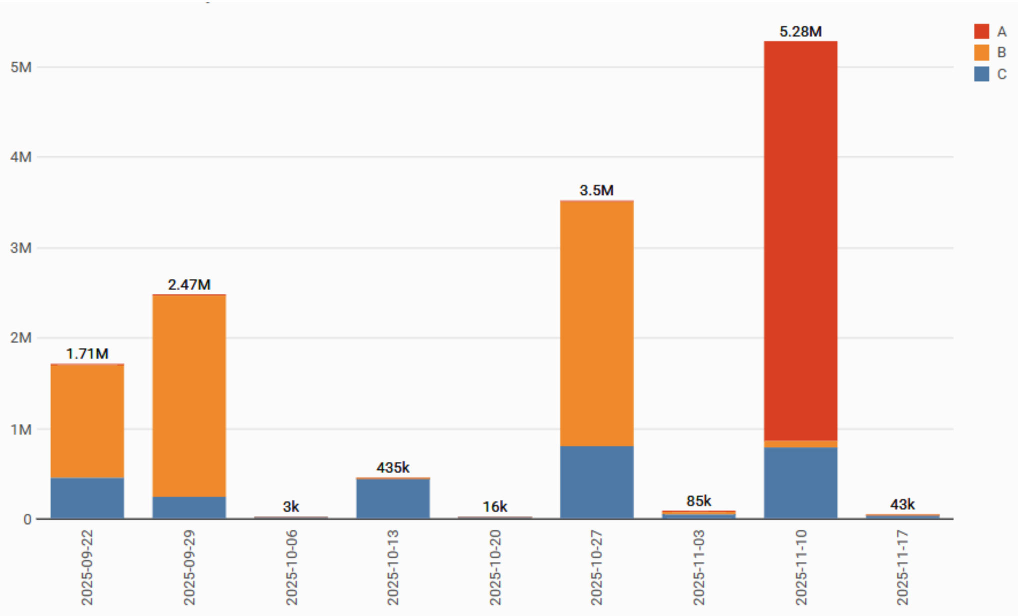
Top Bank Impacted By Over 10 Million Spoofed Calls In 8 Weeks

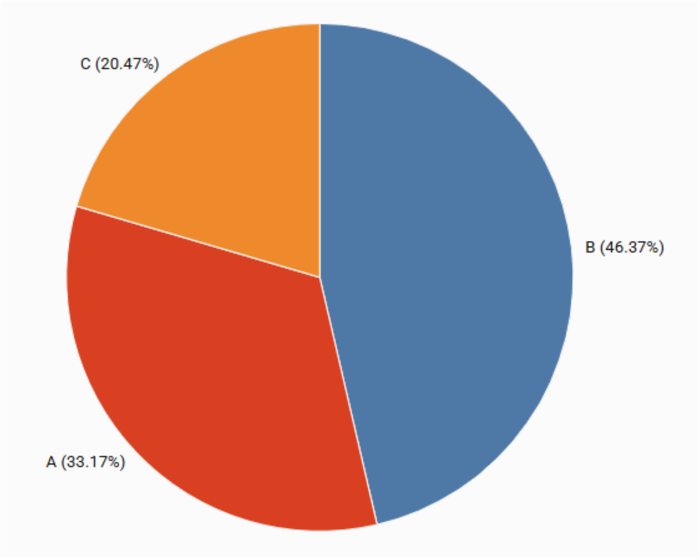
Hello, this is an automated alert from [BANK NAME]. A purchase was declined for $328.99 at [RETAILER/SITE]. Press 5 if you recognize this purchase. If you do not recognize this purchase, call our fraud department immediately at (800) XXX-XXX. To repeat this message, please press 1.

(all incidents use approximately similar messages)

Largest incident:
5.2 million robocalls week of Nov 10^{th} with over 80% of calls A-attested

Attestations for incidents (9/22 to 11/23)





>> During the incidents, majority of robocalls were A or B attested

Example Transcripts

Week	Example
Nov 10	**5.3 million robocalls like:** Hello, this is an automated alert from Bank XYZ. A purchase was declined for $328.99 at GameStop.com. Press 5 if you recognize this purchase. If you do not recognize this purchase, call our fraud department immediately at (800) 700-0564. To repeat this message, please press 1.
Nov 3	**85 thousand robocalls like:** Bank XYZ alerts. A purchase was declined for $128.99 at iga.com. Press 1 if you recognize this purchase. If you do not recognize this purchase, call our fraud department immediately at (800) 221-9093. That is (800) 221-9093. To repeat this message, press any key now.
Oct 27	***3.5 million robocalls like:*** *This is an automated message from **Bank XYZ** Alerts. We've detected a potentially suspicious transaction on your account. To hear the details of this activity, please press 1. If you would like to end this call now, press the star key. Again, press 1 to review the transaction, or press star to hang up. A purchase was declined for $122 **at Amazon.com.** Press 1 if you recognize this purchase. If you do not recognize this purchase, call our fraud department immediately at (833) 200-7521.*
Oct 13	**435 thousand robocalls like:** Bank XYZ, a purchase was declined for $319.55 at Target.com. Press 1 if you recognize this purchase. If you do not recognize this purchase, call our fraud department immediately at (800) 401-5414.
Sept 29	***2.5 million robocalls like:*** *Hello, this is Automated Message from **Bank XYZ** Telephone Banking. For your security, we monitor your account and have noticed some unusual activity related to your debit card. Please call us back at (844) 587-5633. Once again(844) 587-5633.*
Sept 22	***1.7 million robocalls like: Bank XYZ**, we noticed a recent attempted charge of **$228.15 at Amazon.com**. The transaction was declined for your protection. If you recognize this activity, press 1. If you do not recognize this activity, please call us at (833) 228-1690. I repeat(833) 228-1690.*

Timeline Of 6 Incidents In 8 Weeks

Week	Est Calls	Lifespan	Comments
Nov 10	5.3 million	6+ days (11/11-16*)	A-attested by 1 large provider
Nov 3	85 thousand	2 days (11/6-7)	Highly varied
Oct 27	3.5 million	4 days (10/28-31)	B-attested by 1 large provider
Oct 13	435 thousand	1 day (10/15)	C-attested by 1 large provider
Sept 29	2.5 million	1 day (10/2)	B-attested by 4 large providers
Sept 22	1.7 million	2 days (9/21-22)	B-attested by 1 large provider

** incident continues into the next week (Nov 17)*

Example of “Bad Actor” Telecom

Operations : 250M-2.5B Robocalls

Robocalls per month

Sum of Est Calls	Prd 2025-06	2025-07	2025-08	2025-09	2025-10	2025-11	Grand total
	213,744,000	309,264,000	504,205,000	409,464,000	420,301,000	409,335,000	2,266,313,000
	298,163,000	454,864,000	458,622,000	344,512,000		1,891,000	1,558,052,000
	435,817,000	377,849,000	202,215,000	189,851,000	198,031,000	141,993,000	1,545,756,000
	197,012,000	205,715,000	184,398,000	80,664,000	105,178,000	157,976,000	930,943,000
				120,688,000	345,500,000	317,744,000	783,932,000
			17,886,000	2,590,000			20,476,000
	172,513,000	205,135,000	107,430,000	47,429,000	45,009,000	44,346,000	621,862,000
	53,084,000	121,367,000	134,297,000	98,005,000	19,732,000	107,374,000	533,859,000
	42,804,000	84,413,000	83,682,000	93,840,000	71,537,000	74,540,000	450,816,000
			49,745,000	136,589,000	102,259,000	138,175,000	426,768,000
			77,195,000	189,157,000	86,899,000	54,265,000	407,516,000
	86,011,000	57,747,000	53,829,000	78,324,000	52,342,000	47,528,000	375,781,000
	83,535,000	63,933,000	47,232,000	92,975,000	80,321,000	4,534,000	372,530,000
		428,000	24,768,000	65,290,000	205,974,000	63,007,000	359,467,000
	72,092,000	110,955,000	86,964,000	71,258,000	16,637,000	1,119,000	359,025,000
				49,603,000	110,051,000	192,834,000	352,488,000

- Legitimate telecoms do not start from zero calls to 100M in a month

Example – Robocall Mitigation Database (RMD) Filing

Robocall Mitigation Database Filings

Number

RMD0023117

Provider Details

*FCC Registration Number (FRN)

0035751148

*Business Name

Business Address

1207 Delaware Ave #3348
Wilmington DE 19806

*Foreign Voice Service Provider

No

*Other FRNs (enter 'None' if you have none)

None

*Principals, Affiliates, Subsidiaries, and Parent Companies

None

*Other DBA Name(s) (enter 'None' if you have none)

None

*Previous Business Names (enter 'None' if you have none)

None

*Robocall Mitigation Contact Name

*Contact Title

CEO

*Contact Department

Admin

Contact Business Address

1207 Delaware Ave #3348
Wilmington DE 19806

*Contact Telephone Number

+92 313 4681297

Contact Phone Extension

*Contact Email

naeem@natechsol.com

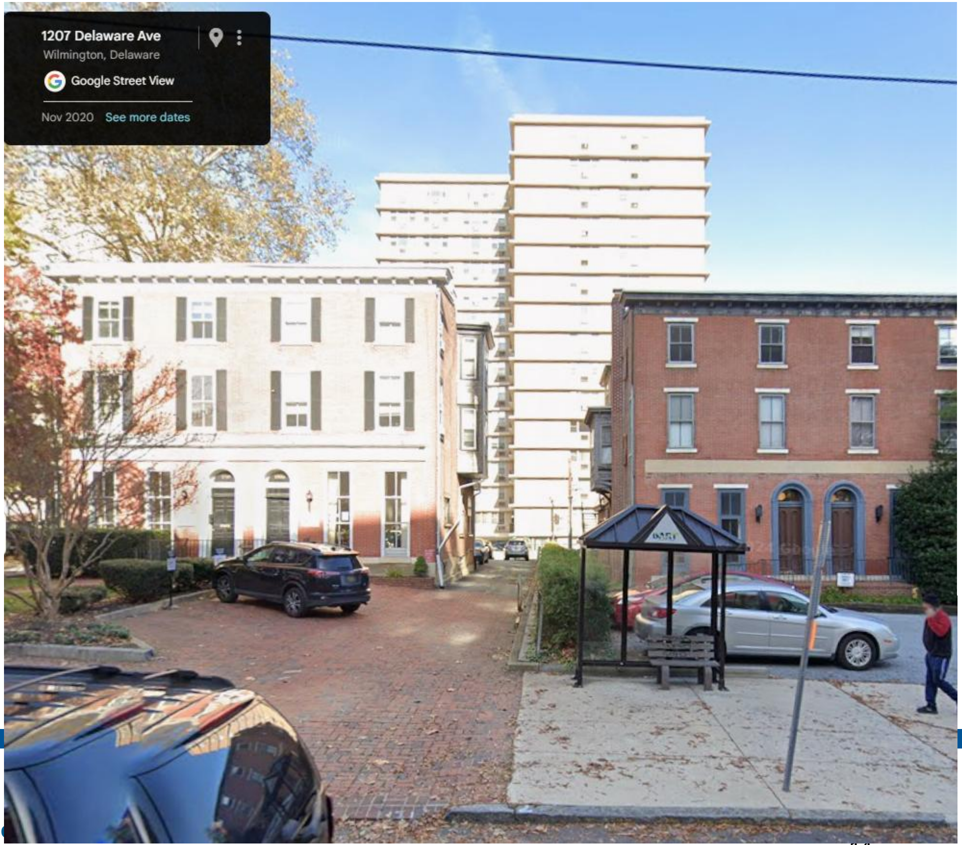
Telecoms Required to Register with RMD

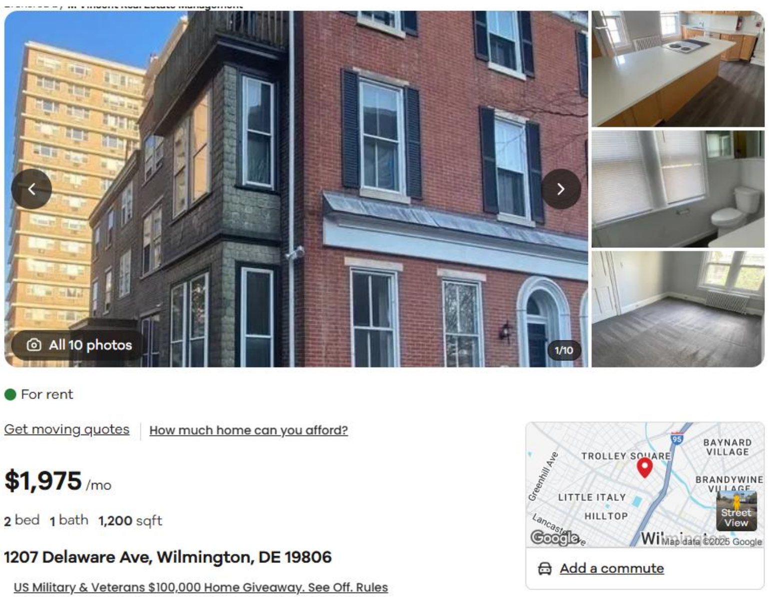
- FCC hosted database
- No checks of information submitted
- No check of required Robocall Mitigation plan
- Some facilitating telecoms don't even check to see if RMD was filed
- Foreign Nationals scamming Americans

Pakistan Phone Number

American Bankers Association®

Company's HQ – +400M Robocalls in Four Months

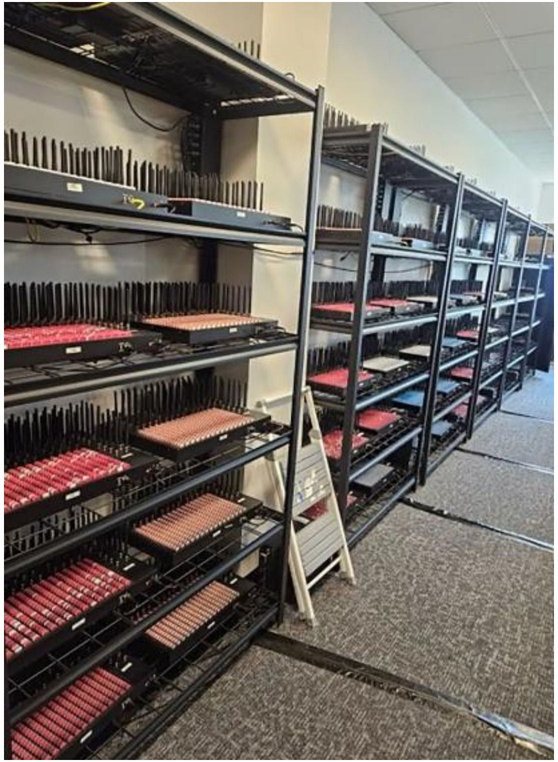




American Bankers Association

Growth of Pre-paid Sim Card Enabled Scam Calls/Texts

Growth of Pre-paid Sim Card Enabled Scam Calls/Texts



- Sim Farm
  - 100,000 sim cards
  - 300 servers
- mobileX sim cards
- Likely in operation for nearly a year

https://www.secretservice.gov/newsroom/releases/2025/09/us-secret-service-dismantles-imminent-telecommunications-threat-new-york

https://www.nytimes.com/2025/09/23/us/politics/secret-service-sim-cards-servers-un.html