Reply Comments of Box Commons

In the Matter of Improving the Effectiveness of the Robocall Mitigation Database; Call Authentication Trust Anchor; Advanced Methods To Target and Eliminate Unlawful Robocalls

Re: FCC 26-49, WC Docket Nos. 24-213 and 17-97; CG Docket No. 17-59

Submitted by:
Box Commons
c/o Northwest Registered Agent LLC
30 N Gould St Ste N
Sheridan, WY 82801
Contact: Brice Love, Founding Catalyst
Email: info@boxcommons.org
Web: boxcommons.org

Date: October 13, 2026

Submitted via: ECFS (Electronic Comment Filing System)

Docket: Further Notice of Proposed Rulemaking, FCC 26-49 (rel. July 23, 2026); 91 FR 57454 (September 9, 2026), Document No. 2026-18366

I. Summary

The initial record confirms two verification gaps that the Robocall Mitigation Database (RMD) cannot close on its own. The first is a **program gap**: the RMD holds providers' descriptions of their mitigation programs, not evidence that those programs work. The second is a **content gap**: STIR/SHAKEN verifies the right to use a number, not the voice on the call, and major industry commenters agree that networks cannot judge call content in real time. Box Commons proposes a way to close each gap without new mandates. First, a voluntary, independent assessment pathway for mitigation programs. Second, caller-originated authenticity information about call audio that travels with the call, built on existing standards and visible through structured RMD fields.

Box Commons respectfully recommends that the Commission:

1. **Recognize a voluntary independent-assessment pathway** for mitigation programs, recorded in structured RMD fields;
2. **Treat a current assessment as an objective low-risk indicator** in risk-based review, never as the sole basis for any action;
3. **Accept one assessment of shared controls** and list assessment among available reinstatement criteria;
4. **Add an optional RMD field** for call-audio authenticity measures a provider originates, preserves, or verifies;
5. **Open a technical inquiry** into caller-originated call-audio credentials; and
6. **Invite non-public reporting of wrongful-blocking error rates** within the assessment pathway.

II. The Program Gap: From Self-Description to Evidence

A. What the Record Shows

The FNPRM reports that staff "frequently identify robocall mitigation plans with minimal information" (¶ 58). Commenters go further. Numeracle observes that "[e]very one of them is a self-assertion with no independent verification."[1] Sonera notes that a certification is not a fail-safe "because a certification does not independently establish that a provider is actually complying."[2] A longer self-description is still a self-description.

B. Box Commons' Proposal: Independent Program Assessment

As we proposed in our initial comments, the Commission should recognize independent assessment of mitigation programs against published, version-controlled criteria.[3] Accredited bodies would conduct the assessments. The RMD would record the result in structured fields: criteria version, scope, assessor, and date.

This proposal differs from, and complements, the identity verification Numeracle proposes for the RMD's front door.[4] Identity verification asks *who* a filer is. Program assessment asks *whether the filer's program works*. Both are needed, and one accreditation framework could serve both.

For providers that choose it, a current assessment would serve as an objective low-risk indicator, the kind of "objective criteria" NCTA asks the Commission to use in deciding when audits are warranted.[5]

C. Design Requirements the Pathway Meets

Skeptical commenters raise fair concerns. We treat them as requirements:

- **Voluntary.** TextNow opposes "a mandatory third-party audit regime,"[6] and ACA Connects warns against routine independent audits at providers' expense.[7] No provider would need an assessment.
- **Evidence, not decision.** Ridgeway insists that "every decision to accept, reject, suspend, remove, or reinstate a filing must remain with" the Bureaus.[8] An assessment is evidence the Bureau weighs, rebuts, or disregards.
- **Pinger's three conditions.** Third-party data should never be "the sole basis for any action against a filing," should carry weight "only on a documented methodology with a correction process," and its absence should support no inference.[9] We adopt all three. A provider without an assessment faces no adverse inference.
- **Shared controls, assessed once.** Affiliates "often rely on centralized compliance functions, shared analytics platforms, and common vendor relationships."[10] One assessment of a shared

[1] Numeracle at 3.
[2] Sonera at 3.
[3] Box Commons Comments, Section V.
[4] Numeracle at 6 (proposing verification of filers' identity by the Commission, an RMD Administrator, "or an accredited independent verifier operating under Commission oversight").
[5] NCTA at 3.
[6] TextNow at 45.
[7] ACA Connects at 8–9.
[8] Ridgeway at 32.
[9] Pinger at 32.
[10] CTIA at 21.

program can support each accountable entity's filing.
- **Re-entry.** Independent assessment should be among the reinstatement conditions the Commission considers (¶ 107). It tests whether a removed provider's program has actually changed.

III. The Content Gap: STIR/SHAKEN Authenticates the Signal, Not the Voice

A. The Record Concedes the Gap

Our initial comments explained that STIR/SHAKEN operates on the signaling plane.[11] The baseline PASSporT token (RFC 8225) asserts the originating number, the destination, and the time of issuance. It makes no assertion about the audio. A call with full attestation can still carry a cloned or synthetic voice.

The initial record confirms that networks cannot fill this gap themselves. In opposing an extension of mitigation duties to all illegal calls, CTIA observes that "providers cannot analyze in real time the content of calls."[12] NCTA points to cases where "the illegality is limited to fraudulent representations made on the call itself."[13] ACA Connects notes that a call "may be unlawful in ways that a provider could not detect from signaling and traffic data."[14] Numeracle adds that impersonation by a live caller "is no less harmful than one placed by a machine or AI."[15]

Box Commons agrees that providers should not have to judge call content in real time. The answer is not to inspect conversations. It is to let the party that generates the audio make a verifiable statement about it.

B. Box Commons' Proposal: Caller-Originated Call-Audio Credentials

We proposed a three-part architecture in our initial comments, which we incorporate by reference.[16]

1. **A content credential from the caller.** The entity that generates the audio, such as an enterprise caller or its voice platform, signs a statement about it. The statement covers whether the voice is human or synthetic, who generated it, and whether any required disclosure was given. The C2PA content credential standard already supports this model. It defines manifests signed with COSE, "hard" bindings that hash the content, and "soft" bindings computed "from the digital content of an asset, rather than its raw bits."
2. **Delivery through existing call-authentication paths.** The credential can travel with the call in three ways:
   - a PASSporT extension, using the extension mechanism RFC 8225 already defines;
   - the Rich Call Data extension (RFC 9795), whose `rcdi` integrity digests protect referenced content;
   - out-of-band delivery through a Call Placement Service (RFC 8816), for calls that cannot carry SIP signaling end to end.

[11] Box Commons Comments, Section II.A.
[12] CTIA at 19.
[13] NCTA at 8.
[14] ACA Connects at 5.
[15] Numeracle at 10.
[16] Box Commons Comments, Sections III.A–C. Technical sources: IETF RFC 8225 (PASSporT), §§ 5, 8.1; IETF RFC 9795 (PASSporT Extension for Rich Call Data), §§ 5–6; IETF RFC 8816 (STIR Out-of-Band Architecture and Use Cases); C2PA Technical Specification v2.2, §§ 9.1, 10.3.

3. **Verification, not interpretation.** A terminating provider or its analytics checks a signature and a binding. It does not listen to the call. A valid credential is a positive signal; a missing one, consistent with Pinger's principle, supports no inference.

The RMD's role is modest: an optional structured field in which providers indicate whether they originate, preserve, or verify such credentials, at no cost to providers that have not adopted them. A technical inquiry, coordinated with the IETF STIR Working Group and ATIS, could then develop the details.

IV. Errors and Disclosure

Mitigation errors fall on lawful callers. INCOMPAS and the Cloud Communications Alliance describe "[t]he blocking and mislabeling of legitimate traffic by analytics companies and larger providers" as "a long-standing concern."[17] ClearCaptions reports that third-party analytics "appear to be identifying calls from new ClearCaptions customers as possible spam or fraud calls."[18] Its average customer is eighty years old and lives with moderate-to-profound hearing loss.

Within the assessment pathway, providers should report wrongful-blocking and labeling error rates alongside effectiveness measures. They should report them non-publicly, which answers TextNow's concern that public metrics "are themselves a roadmap."[19] The same principle resolves FNPRM ¶ 57: the assessor reviews detailed analytics under confidentiality, and the RMD shows only the result. Documented error management also supports the insurability of AI-based analytics, as our initial comments explained.[20]

V. Safeguards and Neutrality

Any recognized assessor should hold accreditation under ISO/IEC 17065 or an equivalent framework, keep standard-setting separate from assessment, and use published criteria available on royalty-free terms. It should favor no vendor or technology, maintain a public registry of current assessments, and have no affiliation with any provider it assesses. This tracks Ridgeway's standard that any external RMD administrator be "impartial, not aligned with any particular telecommunication industry segment, and not an affiliate of any RMD filer."[21]

In the interest of transparency, Box Commons develops certification criteria and could seek to act as an assessment body. Our recommendations are vendor-neutral and would apply equally to any qualifying body.

VI. Recommendations

Box Commons respectfully recommends that the Commission:

1. **Recognize a voluntary independent-assessment pathway** for mitigation programs, with results recorded in structured RMD fields (criteria version, scope, assessor, date).
2. **Treat a current assessment as an objective low-risk indicator** in risk-based audit selection and plan review, never as the sole basis for any action, and draw no adverse inference from its absence.

[17] INCOMPAS/CCA at 15.
[18] ClearCaptions at 1–2.
[19] TextNow at 43.
[20] Box Commons Comments, Section IV.
[21] Ridgeway at 32.

3. **Accept one assessment of shared controls** across commonly controlled entities, and **list independent assessment among available reinstatement criteria** (¶ 107).
4. **Add an optional RMD field** for call-audio authenticity measures a provider originates, preserves, or verifies.
5. **Open a technical inquiry** into caller-originated call-audio credentials, coordinated with the IETF STIR Working Group and ATIS, building on PASSporT extensions, RFC 9795, RFC 8816, and C2PA.
6. **Invite non-public reporting of wrongful-blocking and labeling error rates** within the assessment pathway.
7. **Apply the safeguards in Section V** to any recognized assessor.

VII. Standing Offer

Box Commons renews its offer to participate, at no cost, in any working group, pilot, or technical inquiry on program assessment criteria or call-audio authenticity.

About Box Commons

Box Commons is a Wyoming nonprofit corporation organized as a Section 501(c)(6) standards body. It develops technology-neutral, outcome-based certification standards for audio data, covering consent documentation, provenance, chain of custody, and audit-trail integrity. Its governance gives equal voting weight to industry, civil society, and academic/research chambers, so that no single interest controls the standards process. Its intellectual property policy defaults to royalty-free terms.

Respectfully submitted,

Brice Love
Founding Catalyst
Box Commons
c/o Northwest Registered Agent LLC
30 N Gould Street, Suite N, Sheridan, WY 82801
info@boxcommons.org
boxcommons.org

Methodology statement: This reply was prepared by Box Commons using an AI-assisted research and drafting workflow. The record analysis, policy positions, and recommendations herein were directed, verified, and approved by Brice Love, Founding Catalyst. AI tools were used for research synthesis and structural drafting. All quotations and factual claims were checked against the FNPRM (FCC 26-49), the filings cited, and the cited technical standards, as retrieved from their primary sources. Box Commons assumes full responsibility for the accuracy and substance of this submission.

Appendix: Filings Cited

Short-form citations ("[Filer] at [page]") refer to the initial comments below, filed in WC Docket Nos. 24-213 and 17-97 and CG Docket No. 17-59. Page numbers are the filer's printed page numbers.

Filer	Filed	ECFS ID
ACA Connects	Oct. 9, 2026	26110080320
ClearCaptions, LLC (ex parte)	Oct. 8, 2026	26110080172
CTIA	Oct. 9, 2026	26110080402
INCOMPAS and Cloud Communications Alliance (INCOMPAS/CCA)	Oct. 9, 2026	26110080368
NCTA	Oct. 9, 2026	26110080370
Numeracle, Inc.	Oct. 9, 2026	26110080332
Pinger, Inc.	Oct. 9, 2026	26110080415
Ridgeway Telecommunications LLC	Oct. 8, 2026	26110080165
Sonera LLC	Oct. 6, 2026	26110079705
TextNow, Inc.	Oct. 9, 2026	26110080416

Box Commons' initial comments: Comments of Box Commons (filed Sept. 24, 2026) (ECFS 26110078019) (Box Commons Comments).