# Comments of Box Commons on the Notice of Inquiry: Music Streaming Fraud

**Re: U.S. Copyright Office, Docket No. 2026-6**

**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:** regulations.gov (COLC-2026-0166-0001)

**Notice:** Music Streaming Fraud, Notice of Inquiry, 91 Fed. Reg. 64188 (Oct. 7, 2026), FR Doc. 2026-20537

---

## I. Executive Summary

Box Commons thanks the Copyright Office for this inquiry. The Notice takes care to describe what platforms, distributors, rights owners, and law enforcement are already doing. We write on one narrow point where we have standing: the role of provenance and consent records in preventing streaming fraud.

**Our observation.** Streaming fraud runs on recordings whose origin no one in the payment chain can verify. A royalty pool pays for plays. It cannot tell who made a recording, whether a person or a model generated it, or whether the uploader holds the rights. Detection tools work hard to spot fake *listening*. The supply of unverifiable *recordings* is what lets a scheme spread its plays thin enough to evade them. The defendant in the first U.S. criminal prosecution for AI-assisted streaming fraud put it plainly: "We need to get a TON of songs fast to make this work around the anti-fraud policies these guys are all using now."[1]

**Our recommendation.** Detection, clawbacks, fines, and removal remain essential. They act after money moves. We recommend that Congress and the Office also support a complementary layer that acts before money moves: a minimum, verifiable provenance record attached to each recording when it enters the supply chain. Specifically:

1. **A minimum provenance record at ingestion.** Congress should ask the Office to convene the industry's existing standards bodies. Their task: define, on a voluntary basis, the few facts every delivered recording should carry. Those are a verified party, a content identifier bound to the audio, a structured disclosure of how the recording was made, and the basis of the uploader's rights.

[1] Email of Dec. 26, 2018, quoted in Sealed Indictment, *United States v. Smith*, No. 24-cr-504 (S.D.N.Y. Sept. 4, 2024), cited in the Notice at nn.10, 51.

2. **Protected information sharing with due process.** Congress should consider a safe harbor for sharing fraud indicators, modeled on the one the Notice cites from FinCEN.[2] It should include notice and appeal rights for artists and labels wrongly flagged.
3. **Factual labels, kept separate from legal eligibility.** Machine-readable labels should record facts (origin, rights basis, verification status). Whether a given recording qualifies for statutory royalties remains a legal judgment for the Office and the collectives.
4. **Independent verification of voluntary baselines.** Industry commitments such as the new Streaming Integrity Initiative of the International Federation of the Phonographic Industry (IFPI) set a strong common floor. Congress should encourage, without mandating, independent and technology-neutral assessment of conformance to them.
5. **A path that works for independents.** Any framework should offer low-cost verification and fair appeals, so that independent artists, labels, and stations do not carry the cost of fraud they did not commit.

**Why it matters now.** Generative tools have made recordings nearly free to produce. As of July 2026, Deezer reports that fully AI-generated tracks exceeded half of its daily new deliveries on peak days. They draw 1 to 3 percent of streams, and up to 85 percent of the streams those tracks generated in 2025 were fraudulent.[3] Fraud detection has to scale with every play. A provenance record at ingestion has to happen only once per recording.

---

## II. Who We Are and What We Address

Box Commons is a Wyoming nonprofit corporation organized as a Section 501(c)(6) standards body and data cooperative for independent audio: radio, podcasts, and music. We develop technology-neutral standards for consent, provenance, and chain-of-custody records for audio, so that independent creators can document their rights and audio buyers can rely on that documentation.

We answer **Questions 4, 6, 7, 8(a), and 10**, and address information-sharing rules (Question 8(c)) within our response to Question 7(a). We do not have prevalence, economic, or live-event data and do not address Questions 1, 2, 3, or 5. We take no position on Question 8(b) or on the legislation cited in footnote 59 of the Notice, and we leave Question 9 to law enforcement and those with prosecutorial experience.

---

## III. Question 4: AI-Generated Music, Fraud, and Royalties

We agree with the Congressional Request that "there is nothing inherently wrong with using AI as a creative tool in music development."[4] The issue for royalty integrity is not AI. It is *undisclosed and unverifiable* origin at scale.

**AI removes the cost constraint on fraud.** A fraud scheme needs many recordings so that no single track draws enough plays to trip a detector. Before generative tools, that catalog was costly to build. The Smith case shows the shift. The defendant reportedly obtained AI-generated songs

[2] Notice n.60 (citing FinCEN, Section 314(b) Fact Sheet (June 12, 2026)).

[3] Deezer, *AI music has surpassed 50% of new music uploads for the first time* (July 21, 2026), https://newsroom-deezer.com/2026/07/ai-music-exceeds-50-percent-daily-uploads-deezer/.

[4] Notice n.51 (quoting Letter from Rep. Scott Fitzgerald to Shira Perlmutter, Register of Copyrights (May 21, 2026), at 2).

from a supplier, at one point thousands per week, and streamed them with bot accounts. He was sentenced on October 6, 2026, to 18 months in prison and ordered to repay roughly $8.1 million.[5]

**Platforms are seeing the same pattern at scale.** Deezer's figures above show a large and growing share of uploads drawing a small share of genuine listening, with much of that listening found to be fraudulent. Deezer has responded by tagging albums with fully AI-generated tracks, excluding those tracks from algorithmic and editorial recommendations, and excluding detected fraudulent streams from royalty payments.[6] [7] We commend this work.

**Royalty eligibility now depends on facts the supply chain does not record.** The Office has concluded that AI-generated material is protectable only where a human author has determined sufficient expressive elements, and that prompts alone do not suffice.[8] The D.C. Circuit has held that the Copyright Act requires human authorship.[9] We do not ask the Office to resolve here how these principles apply to statutory royalties. We note only that *whatever the answer*, it cannot be administered at scale unless each recording carries a reliable record of how it was made. Today, the industry's disclosure tools rely on what the uploader declares, and that declaration travels separately from the audio.

---

## IV. Question 6: Effectiveness of Current Methods

### A. What is working

Industry has acted on many fronts, and the record should reflect it:

- **Streaming services.** Since April 2024, Spotify charges labels and distributors per track when it detects flagrant artificial streaming, and requires at least 1,000 streams in the previous 12 months before a track generates recorded royalties.[10] In September 2025 it announced a music spam filter, a policy against unauthorized vocal impersonation, and support for an AI disclosure standard for music credits developed through DDEX. It reported removing over 75 million spammy tracks in the prior 12 months.[11] The Notice also describes Apple Music's sliding scale of fines.
- **Distributors and rights owners.** Distributors have built know-your-customer (KYC) and trust-and-safety programs. In September 2026, IFPI launched the Streaming Integrity Initiative, in which participating distributors commit to rights verification and KYC, content vetting, detection and action against repeat offenders, intelligence sharing where legally

[5] WUNC/WFAE, *NC man receives 18-month sentence in first-ever music stream fraud case* (Oct. 7, 2026), https://www.wfae.org/2026-10-07/nc-man-receives-18-month-sentence-in-first-ever-music-stream-fraud-case. The defendant pleaded guilty on March 19, 2026, to conspiracy to commit wire fraud. Notice n.52.

[6] Deezer, *Deezer launches world's first AI tagging system for music streaming* (June 20, 2025), https://newsroom-deezer.com/2025/06/deezer-launches-worlds-first-ai-tagging-system-for-music-streaming/.

[7] Deezer, *AI music has surpassed 50% of new music uploads for the first time* (July 21, 2026), https://newsroom-deezer.com/2026/07/ai-music-exceeds-50-percent-daily-uploads-deezer/.

[8] U.S. Copyright Office, *Copyright and Artificial Intelligence, Part 2: Copyrightability* (Jan. 29, 2025); see NewsNet No. 1060, https://copyright.gov/newsnet/2025/1060.html.

[9] *Thaler v. Perlmutter*, 130 F.4th 1039 (D.C. Cir. 2025), *cert. denied* (Mar. 2, 2026).

[10] Spotify for Artists, *Modernizing Our Royalty System to Drive an Additional $1 Billion toward Emerging and Professional Artists* (Nov. 21, 2023) (policies effective Apr. 1, 2024), https://artists.spotify.com/en/blog/modernizing-our-royalty-system.

[11] Spotify, *Spotify Strengthens AI Protections for Artists, Songwriters, and Producers* (Sept. 25, 2025), https://newsroom.spotify.com/2025-09-25/spotify-strengthens-ai-protections/.

permissible, and continuous measurement.[12]

- **Cross-industry coordination.** The Music Fights Fraud Alliance works with the National Cyber-Forensics and Training Alliance on a shared database of identified fraud markers.[13]

### B. Where the gap remains (Question 6(b))

Each method listed in Question 6(b) is effective at what it is designed to do. Taken together, they leave one gap:

| Method | What it verifies | What it cannot verify |
|---|---|---|
| Customer verification (KYC) | The uploader is a real, identified party | Whether that party made or owns *this* recording |
| Content verification | A recording does not match known works | Whether a novel recording is human-made or generated, and by whom |
| Clawbacks, fines, removal | Money can be recovered after detection | Losses already paid out; fraud designed to stay under detection thresholds |

Customer verification confirms the *person*. Content matching catches *copies*. Neither establishes the *origin and rights basis of a new recording*. That is the input a volume-based scheme needs, and generative tools now supply it at almost no cost.

**After-the-fact tools also carry a cost for honest independents.** When enforcement relies on detecting suspicious listening, legitimate artists can be caught by fraud they did not commit, for example when a third party buys fake streams for their track. Trade reporting in 2024 described independent artists having music removed in exactly this way.[14] A verifiable provenance record would give such artists evidence to present on appeal.

### C. How stakeholders are positioned (Question 6(a))

Distributors sit at the point of ingestion, which makes them the natural place to *capture* a provenance record. The Streaming Integrity Initiative rightly places its commitments there. Streaming services and collectives are best placed to *check* that record at payment. What no single participant can do alone is *define* a record that every other participant will trust. That calls for a shared, neutral specification, which is the role standards bodies play.

We made a parallel observation to the Federal Communications Commission (FCC) in September: call authentication verifies the *signal*, not the *content* of a call.[15] Streaming has the same split.

[12] *Music companies unite on IFPI-led Streaming Integrity Initiative to tackle fraudulent content*, Music Week (Sept. 14, 2026), https://www.musicweek.com/labels/read/music-companies-unite-on-ifpi-led-streaming-integrity-initiative-to-tackle-fraudulent-content/094977; see also Notice n.47.

[13] *Merlin joins Music Fights Fraud Alliance as part of united industry front against streaming fraud*, Music Week (May 1, 2025), https://www.musicweek.com/digital/read/merlin-joins-music-fights-fraud-alliance-as-part-of-united-industry-front-against-streaming-fraud/091859.

[14] *Artists Are Seeing Their Music Removed From DSPs for Streaming Fraud They Didn't Commit*, RightsTech (Apr. 10, 2024), https://rightstech.com/2024/04/artists-are-seeing-their-music-removed-from-dsps-for-streaming-fraud-they-didnt-commit/; see also Notice n.38.

[15] See Comments of Box Commons, *Improving the Effectiveness of the Robocall Mitigation Database*, WC Docket Nos. 24-213 and 17-97, CG Docket No. 17-59 (filed Sept. 24, 2026).

Detection verifies the *plays*. Nothing yet verifies the *recording*.

---

## V. Question 7: Using Ownership and Usage Data

Question 7 describes, in the Office's own words, the infrastructure that would close this gap. We address each part.

### A. Suspicious-activity sharing (Question 7(a))

We support structured sharing of fraud indicators among streaming services, distributors, and collectives. The Notice's reference to FinCEN's Section 314(b) safe harbor is apt.[16] Any safe harbor for music should include three protections:

- **Data minimization:** share indicators, not full listener records.
- **Notice:** tell an affected artist or label when a flag leads to withheld royalties or removal.
- **Appeal:** give them a defined, timely path to contest it, with provenance records accepted as evidence.

### B. A shared database (Question 7(b))

A shared "known-bad" list of fraud markers is valuable, and the work of the Music Fights Fraud Alliance deserves support. A list of bad actors has a known limit, however: a bad actor can open a new account, and the Notice describes fraudsters "bouncing from distributor to distributor."

We recommend pairing it with a "known-good" layer: a registry of recordings that carry verified provenance records. A new account is cheap to open. A verified chain of custody for each of thousands of recordings is not. The two databases complement each other. One flags risk, and the other lets clean catalogs move through the system with less friction.

Governance matters as much as design. A registry that determines who gets paid should be run under multi-stakeholder oversight, with published rules, independent review, and appeal rights, so that no single commercial participant controls access to the royalty pool.

### C. Metadata standardization and use (Question 7(c))

The industry already has strong building blocks. The gap is how they connect.

- **The International Standard Recording Code (ISRC) identifies the recording, not its rights.** IFPI, which administers the ISRC system internationally, states that an ISRC "identifies the recording rather than other factors such as ownership," and that "no elements of an ISRC should be used to infer the rights status of the recording."[17] ISRC is a necessary key, but by design it says nothing about who made a recording, how, or under what rights.
- **DDEX carries the supply chain's data.** Digital Data Exchange (DDEX) message standards move release and rights data between labels, distributors, and services. The new DDEX-developed AI disclosure standard for music credits is an important step.[18] Like other delivery metadata, it travels alongside the audio and depends on what the uploader declares.

[16] Notice n.60 (citing FinCEN, Section 314(b) Fact Sheet (June 12, 2026)).

[17] IFPI, International ISRC Agency, *Ownership*, https://isrc.ifpi.org/why-use-isrc/ownership.

[18] Spotify, *Spotify Strengthens AI Protections for Artists, Songwriters, and Producers* (Sept. 25, 2025), https://newsroom.spotify.com/2025-09-25/spotify-strengthens-ai-protections/.

- **Content credentials bind provenance to the file.** The open specification of the Coalition for Content Provenance and Authenticity (C2PA) attaches a cryptographically signed provenance record to a media file, and the open-source reference implementation supports common audio formats including MP3, WAV, FLAC, and M4A.[19] The "digital source type" vocabulary of the International Press Telecommunications Council (IPTC), including the value `trainedAlgorithmicMedia` ("created using generative AI"), offers a standard way to state that content was generated by a model.[20]

A minimum provenance record would connect these tools rather than replace them. It would contain:

1. a verified party, linked to the distributor's KYC record;
2. the ISRC, plus a content identifier bound to the audio itself;
3. a structured disclosure of how the recording was made, aligned with the DDEX AI disclosure vocabulary and the IPTC digital source types;
4. the basis of the uploader's rights (ownership, license, or consent from contributing performers); and
5. a signature, so that later changes are detectable.

**Usage data is only as good as the metadata at its source.** We see this firsthand. Working with an independent internet radio network, Box Commons captures and labels stream audio and metadata from 18 stations. Metadata quality varies widely across them. Some stations identify each song. Others carry a single title for an hour-long show. Station promotional breaks carry a slogan that automated tools read as a song title. Inconsistencies like these flow into play reports and royalty calculations everywhere. Standardizing a small set of required fields at the point of creation and delivery would improve both fraud detection and ordinary royalty accuracy.

### D. Labeling content ineligible for statutory royalties (Question 7(d))

Current rules already exclude manipulated plays. The regulations governing the statutory mechanical license exclude plays caused by "user manipulation."[21] Labels can make such exclusions easier to administer if they follow two principles:

- **Label facts, not conclusions.** A label should state verifiable facts: how the recording was made, what rights basis was declared, and whether the record has been independently verified. "AI-generated" is not the same as "ineligible," and a label should not make that legal judgment by default. The collectives and the Office should apply eligibility rules to those facts.
- **Attach labels at ingestion and update them.** Status should be set when a recording enters the supply chain, carried through existing DDEX messages to services and collectives, and updated as investigations conclude. The notice and appeal protections in Part V.A should apply.

---

## VI. Question 8(a): Voluntary Initiatives and Best Practices

The Streaming Integrity Initiative establishes a common baseline for distributors. A natural next step, used widely elsewhere, is independent verification that participants meet that baseline. In

[19] Content Authenticity Initiative, c2pa-rs, *Supported formats*, https://github.com/contentauth/c2pa-rs/blob/main/docs/supported-formats.md.

[20] IPTC, *Digital Source Type* NewsCodes vocabulary, https://cv.iptc.org/newscodes/digitalsourcetype/.

[21] 37 C.F.R. 385.2 (definitions of "Play" and "User Manipulation"); see Notice nn.15, 20.

information security, SOC 2 (System and Organization Controls) reports give customers independent assurance about controls that a provider would otherwise describe itself. The same approach could apply here. A published, technology-neutral set of criteria drawn from the Initiative's commitments and a minimum provenance record would let any qualified assessor attest, on a recurring basis, that a distributor's controls work. Streaming services could then give verified catalogs faster onboarding and fewer holds. That creates a market incentive to participate, with no new mandate.

Box Commons is building standards of this kind for independent audio and would welcome the chance to contribute to an industry-wide effort. Any such program should separate those who write the criteria from those who assess against them, and should include independent creators in its governance.

---

## VII. Question 10: Recommendations to Congress

We respectfully recommend that Congress:

1. **Request a provenance-at-ingestion working group.** Ask the Office to convene DDEX, C2PA, IFPI, the Mechanical Licensing Collective (MLC), SoundExchange, the Music Fights Fraud Alliance, streaming services, distributors, and independent creator representatives to define a voluntary minimum provenance record for delivered recordings.
2. **Enact a narrow information-sharing safe harbor** for fraud indicators among streaming services, distributors, and collectives, conditioned on data minimization, notice, and appeal rights.
3. **Direct a study of statutory-royalty status labels.** Ask the Office, with the MLC and SoundExchange, to study machine-readable status labels for statutory royalty administration that keep factual provenance labels separate from legal eligibility determinations.
4. **Encourage independent conformance assessment** of voluntary industry baselines, with technology-neutral criteria and no preference for any proprietary tool.
5. **Protect independent creators** by requiring that any framework include a low-cost path to verification and a fair, timely appeal process.

None of these steps requires government to build or operate new infrastructure. Each builds on standards and alliances the industry has already created.

---

## VIII. Standing Offer

Box Commons offers to take part, at no cost, in any working group, roundtable, or technical session the Office convenes on provenance, metadata, or labeling in connection with this inquiry, and to share what we learn from capturing and labeling independent radio streams.

---

## IX. About Box Commons

Box Commons is a Wyoming nonprofit corporation organized as a Section 501(c)(6) standards body and data cooperative focused on clean audio data: consent, provenance, chain of custody, and AI liability for independent audio. Our standards are technology-neutral and outcome-based. They address observable practices, not particular products. Our governance design gives equal weight

to three chambers (industry, civil society, and academic and research members) so that no single interest controls the standards process. Our intellectual property policy defaults to royalty-free terms.

Prior Box Commons filings include comments to the National Institute of Standards and Technology, the Federal Communications Commission, the National Highway Traffic Safety Administration, and the National Association of Insurance Commissioners.

---

**Respectfully submitted,**

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

---

*Methodology and AI disclosure: This comment was prepared by Box Commons using an AI-assisted research and drafting workflow. Research covered the Notice of Inquiry (91 Fed. Reg. 64188); the Office's January 2025 report on copyrightability;* Thaler v. Perlmutter*; public policy statements from Spotify, Deezer, and IFPI; reporting on United States v. Smith (S.D.N.Y.); ISRC, DDEX, C2PA, and IPTC documentation; and Box Commons' own stream capture records. The empirical data, policy analysis, and recommendations contained herein were directed, verified, and approved by Brice Love, Founding Catalyst. AI tools (Claude, Anthropic) were used for research synthesis and structural drafting. All factual claims have been independently verified against primary sources. Box Commons assumes full responsibility for the accuracy and substance of this submission.*