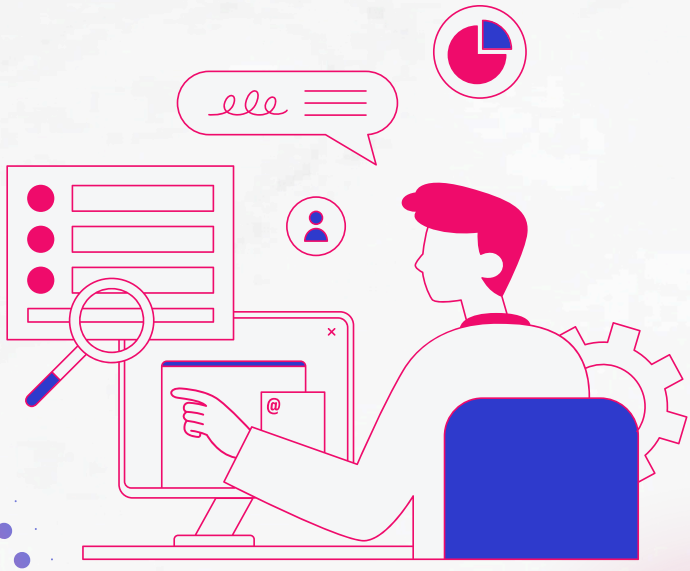
FIVE - POINT PLAN

FOR RESPONDING TO AI-GENERATED MUSIC UPLOADS



In response to the growing issue of unsolicited AI-generated music being uploaded to artists' profiles without consent, we have compiled this guidance to help prevent and address such activity. As these practices become more prevalent, it is increasingly important for artists and their teams to take proactive steps to protect their identity, catalogue, and audience across digital platforms.

As recently reported by Rolling Stone, Time, and BBC, AI voice and identity cloning is a growing threat the music industry can no longer ignore. We encourage you to take a moment to refresh your understanding of the steps needed to protect your artists' identities and catalogues. As this is an everchanging issue, the below advice is based on current recommendations from our community.

1. Secure Artist Profiles, Access Rights & Pre-Approval Controls

Fraud often exploits weak access controls or outdated permissions. Always ensure your profiles are secure.

1.1 Audit all DSP access

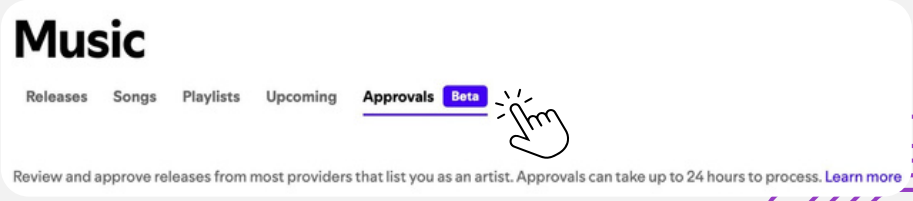
Remove:

- Former managers
- Former labels
- Ex-band members
- Anyone who no longer represents the artist
- Many artists do not realise old teams still have access.

1.2 Enable Spotify's new profile-protection code

- Your artist may or may not be eligible to use this tool. To find out if your artist is eligible, go to the Music tab in Spotify for Artists, and it will appear next to Upcoming Releases - the tab is called Approval (beta).

- This tool is currently in beta. If available, this code can be provided to distributors before uploads can be approved.



- It prevents unauthorised uploads but:
- Spotify has not clarified what happens to offending tracks
- It does not retroactively protect against existing fraud

1.3 Consider enabling YouTube's new Likeness Management tool

- Likeness detection helps creators find content on YouTube where their face appears to be altered or generated by AI.

1.4 Ensure all legitimate releases have correct metadata

Some takedowns are triggered by:

- Metadata conflicts
- Contributor name collisions
- Mis-matched rights information
- Keep agreements and split sheets organised and accessible.

1.5 Monitor profiles weekly

Especially for:

- Independent artists
- Deceased artists
- Retired artists
- Artists with dormant catalogues
- Scammers rely on low-activity profiles.

2. Long-Term Fraud Prevention, Policy Pressure & Industry-Wide Safeguards

Fraudulent AI-generated uploads are increasing rapidly, and systemic solutions are needed.

2.1 Strengthen your own internal processes

Create a fraud-response checklist including:

- Evidence to gather
- DSP forms to submit
- Distributor contacts
- Expected timelines

Maintain a **central folder** with:

- Agreements
- Split sheets
- Rights documentation
- Past takedown correspondence

2.2 Choose distributors with strong KYC

Prioritise distributors that:

- Use identity verification
- Require government ID
- Operate on royalty-based models (more incentive to prevent fraud)

Avoid distributors with:

- Subscription-based models
- No KYC
- High volumes of low-quality uploads

2.3 Push DSPs for stronger protections

MMF can advocate for:

- Mandatory **Know Your Customer** requirements for all distributors
- Clear DSP policies on:
- What happens to fraudulent tracks
- Whether revenue is clawed back
- Whether offending accounts are banned

Transparency on:

- Distributor information
- AI-generated content declarations
- Upload source metadata

2.4 Encourage DSPs to improve reporting tools

- Faster takedown pathways
- Ability to report multiple tracks at once
- Ability to flag suspicious labels

Better visibility of:

- ISRC
- Distributor
- Label
- Upload date

2.5 Share intelligence within the MMF community

Sharing the below helps protect artists:

- Label names
- Distributor accounts
- Upload patterns
- Scam techniques

3. Verification, Evidence Capture & Internal Triage

When a suspicious “prepare for your release” email or unexpected upload appears on any Streaming Service, confirm the fraud and preserve evidence.

3.1 Verify the release across all DSP dashboards

- Check Spotify for Artists → Upcoming tab (fraudulent releases may appear 12–48 hours after the email).
- Check Apple Music for Artists, Amazon Music for Artists, YouTube Studio, Deezer for Creators, Tidal Artists

Confirm whether the release is:

- Incorrectly mapped to the legitimate artist profile, or
- Placed on a newly created duplicate profile (common when Spotify tries to “resolve” conflicts).

3.2 Capture all available evidence

Screenshots of:

- Packshot/cover art
- Release metadata (title, artist name, release date)
- ISRC and UPC if visible
- Distributor or label name (if any DSP displays it - Songstats may display more detailed information, so worth checking there).
- The release appearing on the artist’s profile
- Save the original email from Spotify or any DSP.

3.3 Log the timeline

- Note when the email arrived, when the release appeared, and when you submitted reports.
- DSPs often dispute timelines; a clear log strengthens escalation.

3.4 Assess potential risk

Check whether:

- The track is AI-generated (common in these scams).
- The same label has uploaded multiple fraudulent releases (often 10–20 at once).
- The artist is being targeted because they are independent, inactive, or have limited team oversight.

4. Identify the Distributor and Source of the Fraud

DSPs generally refuse to disclose distributor information “for security reasons”, which forces managers to investigate independently.

4.1 Use metadata-visible DSPs

- Qobuz displays label information, including clickable links to check other releases from the same label.
- Click the label name to see:
- Other releases
- Upload patterns
- Whether the label is pushing multiple AI-generated tracks on the same day

4.2 Use SongStats or similar tools

Enter the ISRC to identify:

- The distributor
- The uploader's account
- Other releases from the same source
- This is currently the most reliable method for tracing fraudulent uploads.

4.3 Contact the distributor directly

Use senior contacts where possible.

Provide:

- ISRC
- Screenshots
- Evidence of fraud
- Many distributors will:
- Remove the release
- Ban the user
- Confirm whether they are seeing similar patterns (some report **a dozen cases per week)**

4.4 Monitor for repeat offenders

Fraudulent labels often:

- Upload in batches
- Target artists in similar genres
- Target artists with moderate but not major-label profiles
- Keep a list of suspicious labels.

5. Rapid Takedown Actions Across All DSPs

Because DSPs do not share distributor information and have inconsistent reporting tools, if there is no distributor on-board to help action takedowns, managers must act **platform by platform.**

5.1 Escalate through your distributor (if you have one)

- Ask them to issue a **multi-DSP takedown request**.
- Some distributors will refuse unless they are the distributor of record, so be prepared to act independently

5.2 Spotify

- For Upcoming Releases (Artists): Log into Spotify for Artists, go to Music → Upcoming, click the three dots next to the release, and select "Report incorrect release" to launch the mismatch form.
- Submit a Spotify for Artists support ticket with screenshots and ISRCs.
- Note: Spotify quotes 10–15 days, but escalations can result in removal within hours.

Monitor for:

- The release being removed from the profile but reappearing on a new profile.
- Spotify removing visibility but leaving the fraudulent profile “in the system”.

5.3 Apple Music, Amazon, YouTube, Deezer, Qobuz, Tidal

- Submit individual takedown forms for each DSP: Apple, Amazon, YouTube, Deezer, Qobuz, Tidal

Provide:

- Screenshots
- ISRC
- A statement that the release is fraudulent and unauthorised

Expect:

- Apple and Amazon to act relatively quickly
- YouTube to require additional verification
- Qobuz to be the most transparent about label/distributor metadata

5.4 Track all submissions

Maintain a spreadsheet of:

- DSP
- Form submitted
- Date/time
- Response
- Removal confirmation
- Fraud cases often require **10–20 separate actions.**

NOTES