
Direction des études
et de la prospective

Centre national
de la musique



Study : Stream manipulation

2021

CONTENTS

AIMS OF THE STUDY

TIMELINE

PARTICIPANTS

01. OVERVIEW

Overview and process

Different packages available and different methods used

Types of music projects and artists concerned

02. RISKS AND FRAUD DETECTION

Associated risks

Fraud detection in action

03. EXTENT OF FRAUD DETECTED

Fraud detection methods and indicators of the overall volume

Fraud detected on the top 10,000 most-listened to tracks on the platforms

Deezer's figures with additional data from distributors

04. LEGAL ACTION

Criminal and civil liabilities

05. RECOMMENDATIONS

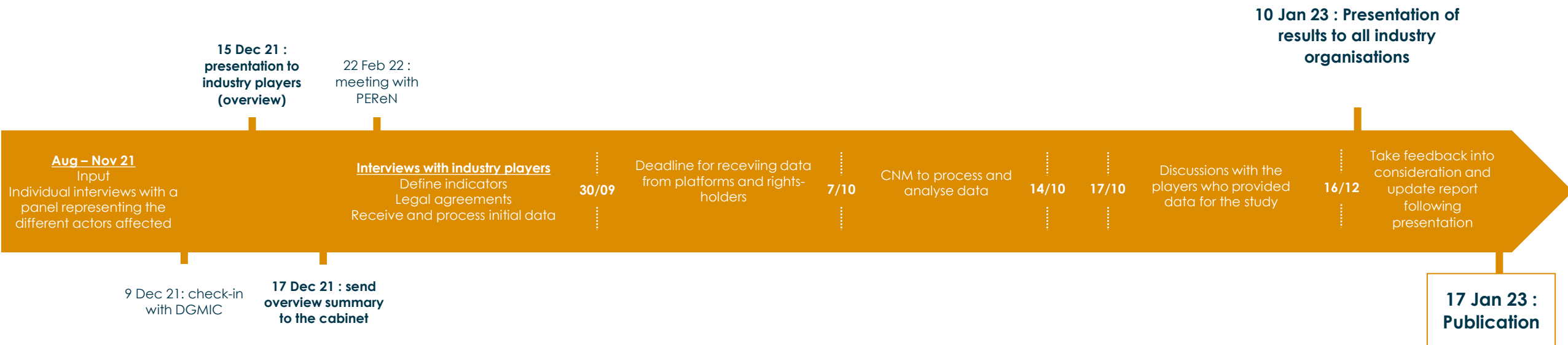
Summary of the aims of this study

At the French parliament's request, as part of the examination of the draft bill relating to the French law on the regulation and protection of access to cultural works in the digital age, the Minister of Culture, Roselyne Bachelot-Narquin, tasked the Centre national de la musique with executing a study on stream manipulation on online music streaming platforms.


The aim of the study is to establish:

- an analysis of the practice of stream manipulation, study **its impact** in terms of **royalty distributions to rights-holders**, as well as in terms of **safeguarding music diversity**;
- **recommendations** aimed at better detecting and redressing these practices, and limiting their spread.

Timeline



Participants in the study

 Platforms	 Producers/Distributors	 CMO	 Federations	 Agencies
Deezer Spotify Qobuz Apple Music YouTube Amazon Music	Universal Music Sony Music Warner Music Wagram Stories Believe IDOL	SACEM	UPFI* SNEP** BVMI*** FELIN**** SMA*****	OdAce Music
 Music Publishers	 Artists/Management	 Audit/Lawyers	 Media	 Other
Warner Chappell Lalouline Publishing Premiere Music Group	Anonyme	Nomos Paris Anonyme Legitary Beatdapp	LesJours VentesRap	Expert in cybercrime Music Tomorrow

**Union des producteurs phonographiques français indépendants* (Independent French producers union)
 ***Syndicat national de l'édition phonographique* (French national federation of phonographic publishing)
 ****Bundesverband Musikindustrie* (German national music industry association)
 *****Fédération nationale des labels indépendants* (French national federation for independent labels)
 ******Syndicat des musiques actuelles* (Popular music union)

01 . OVERVIEW

Definition

With a business model based on revenue sharing, a streaming platform considers a single stream as genuine and **valid** when a streamed song has been listened to for **at least 30 consecutive seconds**. A legitimate stream would result from a voluntary act by a human user whose intention is to listen to the song they've chosen independently or via a recommendation.

Stream manipulation of online plays can be defined as the **artificial creation of online plays or views by human and non-human means with the aim of generating income, improving chart position and/or swaying a recommendation system (playlists, search)**. Stream manipulation can be performed without the consent of the artist or their professional entourage.

Different types of stream manipulation



Fake streams

Commonly referred to as fake streams, these are streams that, for the purposes of royalties distribution, are considered illegitimate, i.e. operated by bots or individuals for compensation.



Fake uploads

Concerns uploading fake songs on an artist's page, repackaging old or unreleased tracks, or platform takedowns.



Manipulation via the ISRC*

A type of manipulation that is yet to be recognised by industry players.



Fake playlist creation

A fake playlist is a playlist followed by fake accounts (and possibly real accounts) and on which bots stream content repeatedly on a loop.

Identified process**Actor initiating the request**

Due to lack of evidence, the initiator remains unidentified and unidentifiable by platforms

Actor operating the artificial creation of fake streams

Offers to purchase streams available on the internet
Independent operator (hacker)

Track impacted by artificial increase in its streams

Purchasing fake streams

Stream purchasing services can be found through **traditional search engines**, which **optimise the ranking of search results**. Others services available through **word of mouth** also exist.

Indexing websites offer to increase the position of its customers' product(s) on the platforms on which they are broadcast.

Marketplaces are websites that allow individual entrepreneurs to offer their services in various packages.

Promotion agencies offer an external promotion service of including tracks in a playlist (real or fake) to increase the number of streams.

Vues YouTube gratuites

Voulez-vous des vues YouTube gratuites de vraies personnes ? Cherchez pas plus loin. GoVira fournit rapidement et facilement des vues YouTube gratuites, des likes, des commentaires et des abonnés de vraies personnes comme vous. Développer votre chaîne n'a jamais été aussi simple, sérieusement !

Obtenez des vues YouTube gratuites maintenant!

Views exchange which offer free services for increasing the number of views on YouTube, and paid growth services with Spotify or SoundCloud.

Anonymat et sécurité

Les écoutes Deezer qui seront livrées sont des vraies écoutes. C'est pourquoi c'est entièrement sécurisé pour votre compte Spotify. Il n'y a aucun risque. De plus, nous vous garantissons un anonymat total. Personne ne saura que vous avez acheté des écoutes. Vous pouvez payer par carte bancaire et par PayPal. Le paiement est sécurisé.



1000 ÉCOUTES DEEZER	5000 ÉCOUTES DEEZER	10 000 ÉCOUTES DEEZER	20 000 ÉCOUTES DEEZER
24,90€	89€	199€	299€

Pour tester nos services. Service clients 7j/7.

Pour passer à la vitesse supérieure. Service clients 7j/7.

Pour se démarquer de la concurrence. Service clients 7j/7.

Pour faire accéder sa carrière d'artiste. Service clients 7j/7.

Questions Fréquentes

Different methods used

Stream farming

Generate a large number of streams

Stream raid

Generate a large amount of streams, but in a detectable way

Account takeover

Take ownership of existing online accounts on a platform.

Device farms

- via free user accounts
- via personas (real fake accounts): accounts opened using expired, stolen or virtual credit cards; premium accounts dedicated to stream manipulation; hacked accounts (account takeover)

Zombies (botnets): takeover of a group of computers by installing a virus
hacked devices: listening launches on platforms

- hacked devices: launch listens on platforms
- click fraud: opens a pop-up that involuntary executes an action

Affiliate scams:

- sending a malicious link (of fake websites) to a loyal community

Credential stuffing: cyberattacking accounts by collecting stolen account credentials

- account takeover via a database of millions of emails/passwords already used

Artist identity takeover:

- uploading fake tracks on an artist's page
- reuploading unreleased tracks or takedown

Artists potentially concerned

Artists that regularly generate a significant volume of streams



To maintain their chart position

- To reach a certain stream threshold in the first week of release

Emerging artists



Image benefit

- Improved search engine optimisation on streaming platforms
- Better considered by music recommendation algorithms
- Playlist placements
- A negotiation lever for signing a commercial contract

Music projects specifically designed to generate income



To generate income by creating songs that last 35 or 45 seconds, that would not necessarily be identifiable and would loop through hacked accounts.

To harm competitors



To remove a competitor from the charts or a platform takedown

02 .

RISKS AND FRAUD DETECTION

Risks associated with stream manipulation

Market distortion

- A sharp increase in the number of streams recorded on a platform, without a proportional increase in the number of paying subscribers, automatically leads to a **drop in the unit value of a stream** and therefore a drop in the amount of royalties paid to rights-holders.
- It impacts distributors' market shares.

Affects consumer trust in the streaming market

- Consumers trust the market less thus use the service less (impact on charts and recommendations).
- Users trust platforms' security systems less and fear that their account will be hacked.

Negative impact on artists

- Music industry professionals now have the tools **to spot inorganic activity** and prefer to sign an artist with lower fan engagement numbers, but who will be more authentic.
- Artist's image tainted (reputational damage)
- **Fake streams disrupt artists' algorithmic profiles:** (i) they weaken engagement rates thereby reducing an artist's "recommendability", and (ii) also disrupt the recommendation algorithm by providing misleading information, since fake users don't behave like normal music fans.

Fraud detection

The platforms interviewed as part of the study indicated that they have the technological resources necessary to identify fraud. Some are more active on the issue than others. A few distributors have developed alert systems to detect abnormal streaming activity on their catalogues, but the majority of players don't use the same fraud detection tools.

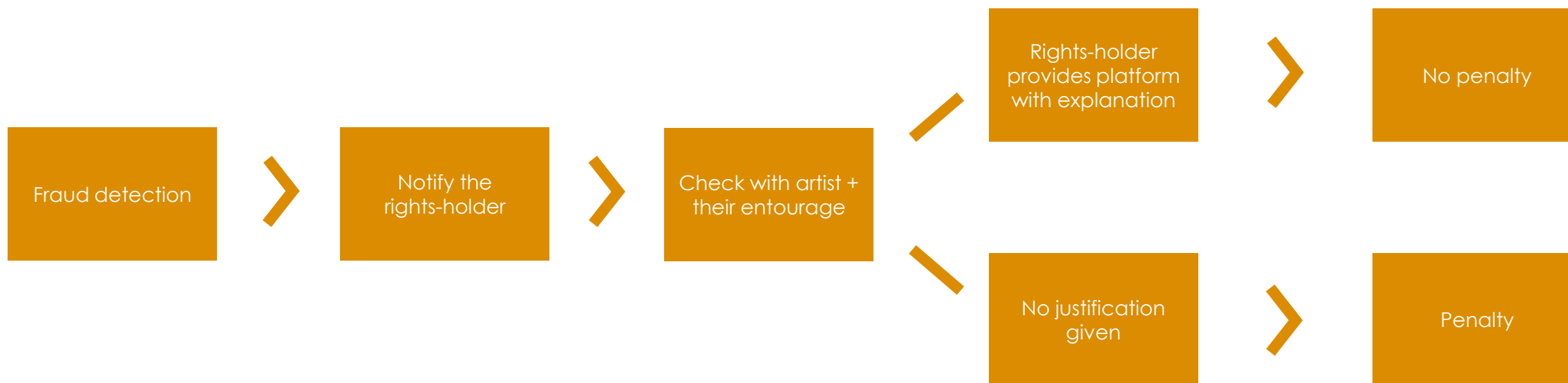
Fraud detection and deletion

- Identify activity considered abnormal: **consumption untypical of human behaviour** (listening time, repeat streams, type of device used, etc.).
- Development of **machine learning tools and algorithms** to track fraud through statistical signal detection models, which are installed on user profiles, artist profiles, etc.

Warn rights-holders

- **Royalty statements** and other indicators developed internally, such as stream source, market share on platforms, etc.
- Rights-holders have limited access to data (particularly concerning users) compared to platforms, but have the advantage of being able to **analyse performance from one platform to another**.

Impact post-identification



Platforms: the penalty differs, depending on the platform.

Some opt to remove streams that they consider to be fake, suspend promotion on the platform, remove the track in question from playlists, stop royalty distribution to rights-holders, or even a takedown (remove the track from the platform).














Producers / distributors: communicate with and inform the artist, or may even go as far as terminating the contractual relationship with the artist.

03 . EXTENT OF FRAUD DETECTED

Scope of analysis

In order to measure and analyse the volume of fraud detected, data was collected from three platforms (Qobuz, Spotify and Deezer), as well as from distributors, according to the methods detailed in the table opposite.

YouTube, Apple Music and Amazon Music were approached to take part in the study, but were either unable or unwilling to provide the data requested for the study.

			
 Time period	2021	2021	2021
 Geographic scope	All streams made in France Including content from all countries	All streams made in France Including content from all countries	All streams made in France Including content from all countries
 Data provided	(i) The top 10,000 most-listened to tracks on the platform, including CNM observation parameters (ii) Overall volume and certain indicators analysed by the CNM	(i) The top 10,000 most listened to tracks on the platform, without CNM observation parameters (ii) Overall detection	(i) The top 10,000 most listened to tracks on the platform, including CNM observation parameters (ii) Overall volume and certain indicators analysed by the CNM
 Supplementary data from panel of distributors		     	
		All tracks in the top 10,000 which have undergone detection for abnormal streaming activity, including the CNM observation parameters, in order to strengthen the validity of the top 10,000 tracks sent by the platform.	All tracks in the catalogue which have undergone detection for abnormal streaming activity, including the CNM observation parameters, to lead to a more global analysis of the platform.
		The panel represents 90.8% of Spotify's top 10,000 most-streamed tracks	The panel represents 75.3% of the overall volume of streams on Deezer.

Methodological precautions



- **Territory:** The data provided by the platforms and distributors and analysed as part of this study only concerns the French market. The data is in no way representative of the trend at an international level.
- **Detection method:** Each platform has its own detection method. As such, the data provided can neither be aggregated, nor compared.
- **Top 10,000 most-streamed tracks:** The data provided by Spotify relating to the top 10,000 tracks has been supplemented with data from distributors' financial reports. This action was authorised by Spotify. The panel applied to the Top 10,000 includes: Universal Music, Sony Music, Warner Music, Believe and Wagram, representing more than 90% of the top 10,000 tracks.
- **Global indicators:** Some of the platforms participating in the study did not provide the global volume indicators defined by the CNM.
- **“Catalogue type” indicator:** The catalogue type (local/international) is identified in two ways: the data collected from the platforms made the distinction on the basis of the track's ISRC (ISRCs starting with FR for France are considered as local catalogue), and the data coming from the distributors is based on the repertoire owner.

QUANTITATIVE OBSERVATIONS

Detection method and indicators on overall volume detected by the platforms.

Data requested from platforms



Data

Overall volume of streams detected as fraudulent in France in 2021

Indicator	Description
Total number of detections	Number of streams detected as fake by the platform, according to its detection method.
Breakdown by device	Volume of streams detected by the platform, broken down according to the type of device used.
Breakdown by streaming plan	Volume of streams detected by the platform, broken down according to the type of streaming plan.
Breakdown by type of stream	Volume of streams detected by the platform, split according to the platform's users listening behaviour.

Quantitative analysis (Spotify's data)

The platform's detection method

The platform developed processes to detect **abnormal streaming activity on albums, EPs and tracks**. A combination of indicators are observed, including, amongst others: the breakdown of streaming figures by user type, abnormal variations, skip data, geolocation, subscription type, and type of device, etc.

When fraudulent activity is identified, several actions are immediately undertaken to undo the impact of the fraud (removal of fake streams, royalties frozen, charts corrected), the rights-holders concerned are informed and follow-up procedures implemented. According to the platform, the removal of such artificial activity has no impact on the platform's performance indicators and financial results.

Amount of fraud detected on Spotify in France in 2021



Percentage of top 10,000 tracks detected as fake out of the overall share

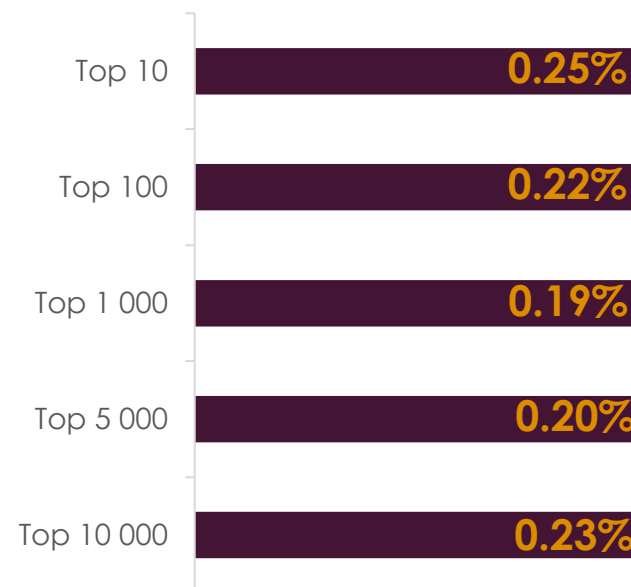
Based on the data provided by the platform, **the overall share of streams considered fake by the platform and detected in France in 2021 amounts to 1.14% of its total streams**. Of all these streams, 14.6% come from the top 10,000 most-listened to tracks. This means that **85.4% of streams detected as fake come from the long-tail**.

14.6%

A horizontal bar chart with a light orange bar representing 14.6%. The percentage value is written in white inside a dark orange box at the start of the bar.

Breakdown of fraud detected in Spotify's 2021 charts in France

(data supplemented by distributors' data)



In the top 10 most-streamed tracks, the platform detected 0.25% streams considered as fake, and 0.23% in the top 10,000.

Quantitative analysis (Qobuz's data)

The platform's detection method

Streaming fraud detection is based on looking for **abnormally strong periods of activity for each user**, such as abnormally long periods of continuous streaming and an abnormally high number of streams per label/artist/distributor.

When one of these controls is activated, the user is suspected of having attempted to defraud during the noted period.

In this case, the user's streams corresponding to these periods are labelled as fraud.

Amount of fraud detected on Qobuz in France in 2021



qobuz

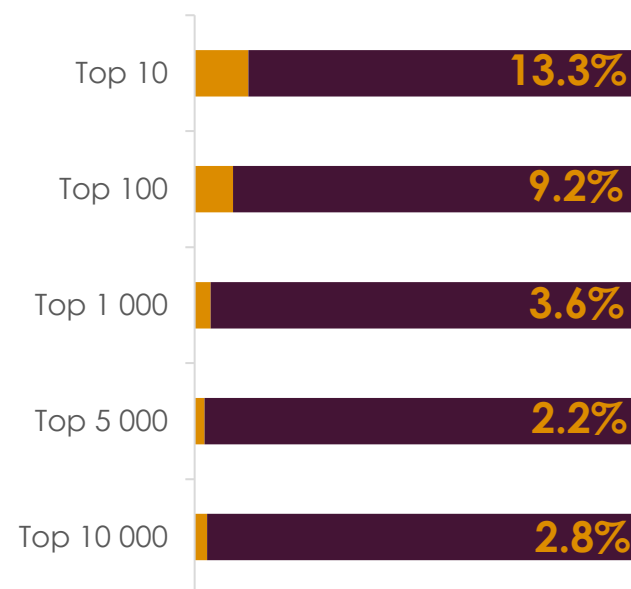
1.6%

Percentage of top 10,000 tracks detected as fake out of the overall share

Based on the data provided by Qobuz, **the overall share of streams considered fake by the platform and detected in France in 2021 amounts to 1.6% of its total streams**. Of all these streams, **43.5% come from the top 10,000 most-listened-to tracks**.



Breakdown of fraud detected in Qobuz's 2021 charts in France

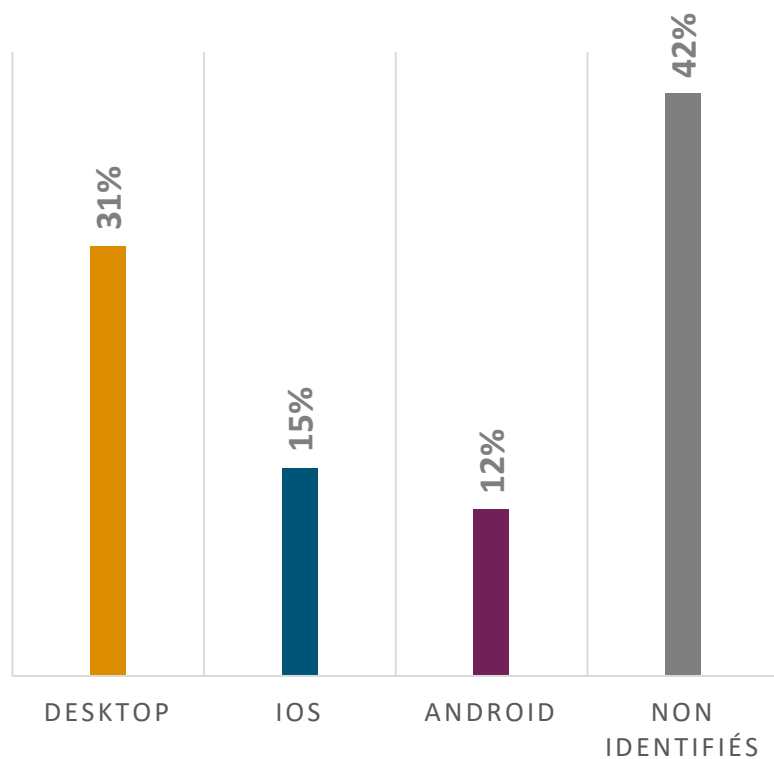


In the top 10 most-streamed tracks, more than 13% of streams were detected by the platform as fake, meanwhile the top 10,000 is at 2.8%.

According to the data received, streaming fraud on the platform is more concentrated on the most-listened to tracks.

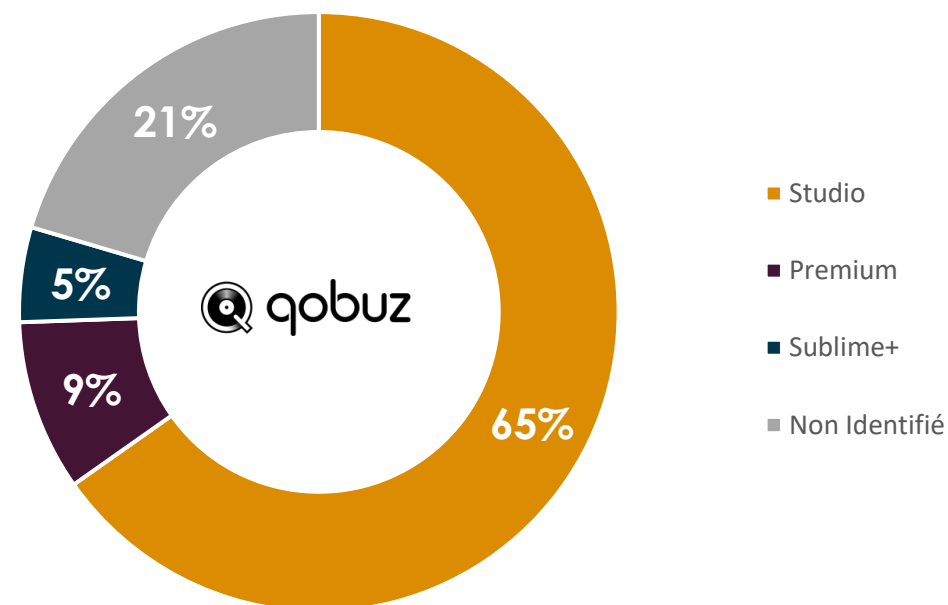
Indicators observed on the overall volume detected by Qobuz

Breakdown by device



31% of fraud detected comes from a computer

Breakdown by streaming plan



65% of fraud detected comes from the Studio plan and **13%** from the free-trial plan

Quantitative analysis (Deezer's data)

The platform's detection method

Algorithms analyse all platform activity **to detect potential fraudulent users**. According to the platform, these algorithms run daily and are updated weekly.

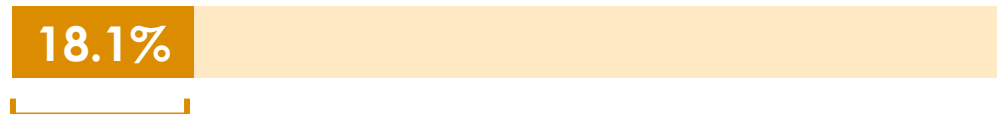
Many criteria are analysed, and the sum of the indices is used to help define the user's status. If the platform considers the status as fraudulent, all streams made on the day of detection are removed.

Amount of fraud detected on Deezer in France in 2021

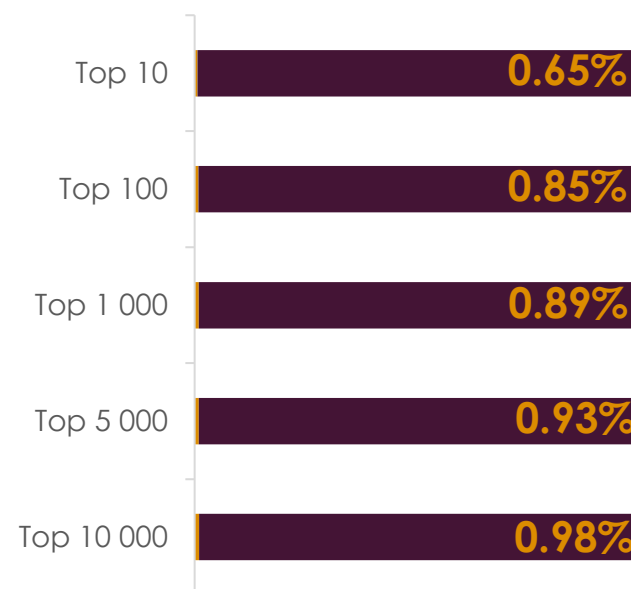


Percentage of top 10,000 tracks detected as fake out of the overall share

Based on the data provided, **the overall share of streams considered fake by the platform and detected in France in 2021 amounts to 2.6% of its total streams**. . Of all these streams, 18% come from the top 10,000, this means that **the majority of streams detected and considered as fake come from the long-tail (81.9%)**.



Breakdown of fraud detected in Deezer's 2021 charts in France

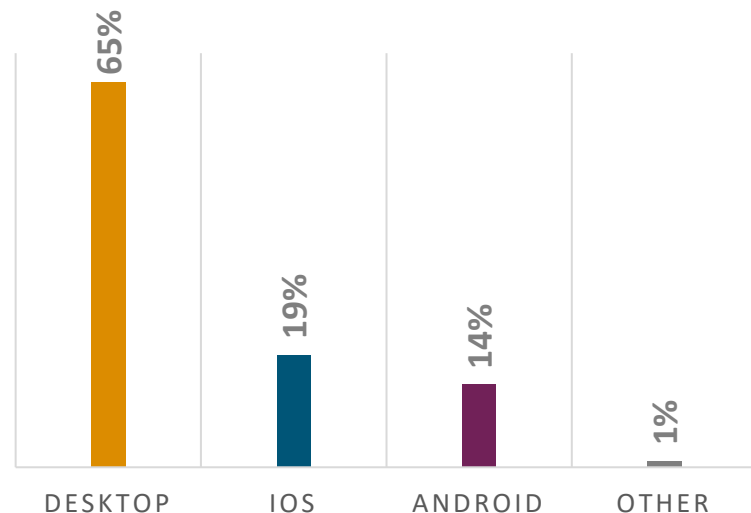


In the top 10 most-streamed tracks, more than 0.6% were detected as fake by the platform, while the top 10,000 is close to 1%.

From the data provided, it seems that the share of streaming fraud increases as you scale-up the top charts.

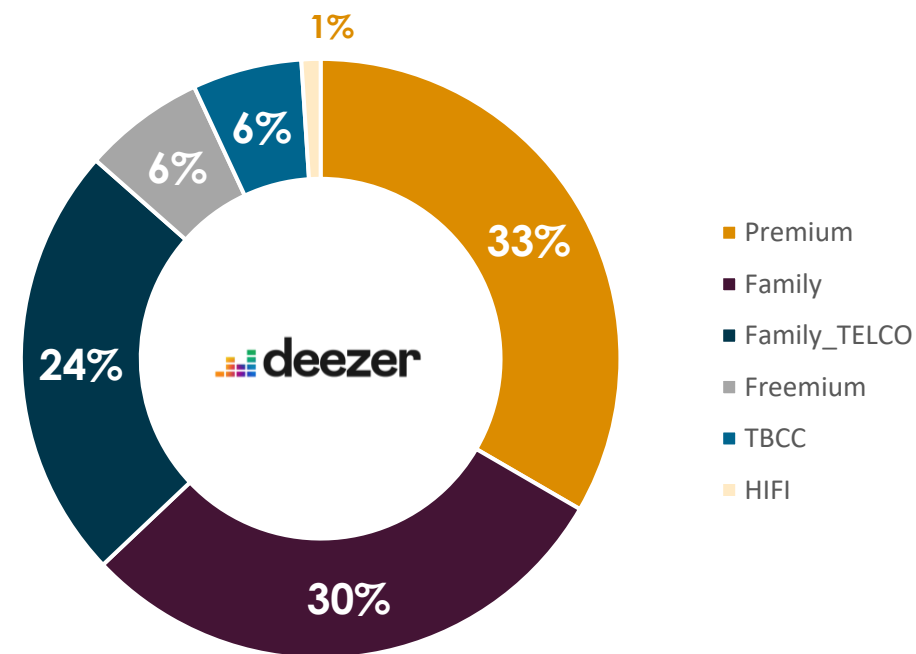
Indicators observed on the overall volume detected by Deezer

Breakdown by device



65% of fraud detected comes from a computer

Breakdown by streaming plan



54% of fraud detected comes the Family plan and **6%** from the free-trial plan

Breakdown by type of stream

74% of fraud detected comes from streaming **albums (37.4 %)** and **playlists (37,1%)**

QUANTITATIVE OBSERVATIONS

Fraud detection on the top 10,000 most-listened to tracks in France in 2021, on each of the platforms.

Data requested from platforms



Data

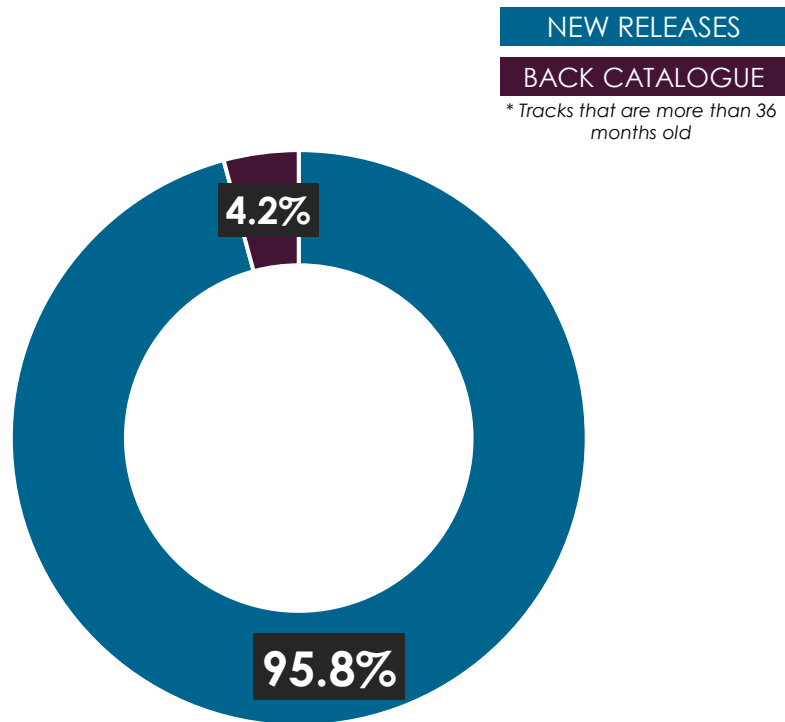
The top 10,000 most-listened to tracks on the platform

Parameters	Description
Track ID	Anonymised track name
Artist ID	Anonymised artist name
Genre	Music genre associated with the track
Catalogue	Origin of the track (local/international), based on the track's ISRC
Release date	Date the track was first released on the platform in order to analyse whether it's a new release or part of back catalogue
Total streams	Total number of streams over the requested period (2021)
Total fake streams	Total number of streams identified and considered as fake by the platform, over the requested period (2021)

Indicators observed on Spotify's top 10,000 most-listened to tracks

(supplemented with distributors' data)

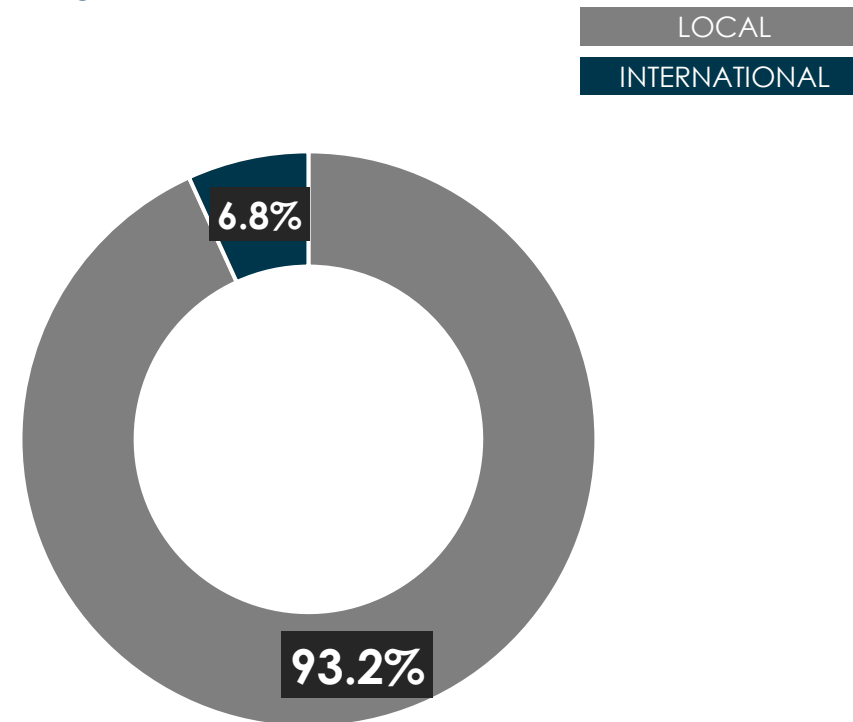
Breakdown by release date



96% of fraud detected comes from new releases

The amount of fraud detected on all new releases would come to 0.3% compared to 0% on all back catalogue.

Breakdown by catalogue



93% of fraud detected comes from local catalogue

The amount of fraud detected on the entire local catalogue is 0.3% compared to 0% on the international catalogue.

Indicators observed on Spotify's top 10,000 most-listened to tracks

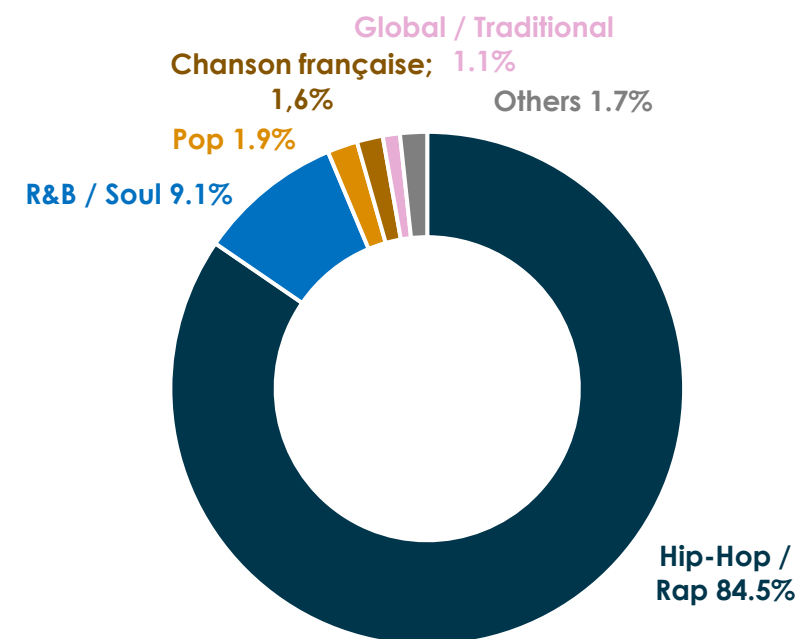
(supplemented with distributors' data)

The hip-hop/rap genre is predominantly consumed on the platform (at over 51%). The amount of streams considered as fake is **0.4% in hip-hop/rap** and in the **R&B/soul** genre.

	Overall share	Amount detected within each genre
HIP-HOP / RAP	51.4%	0.4%
POP	15.5%	0.0%
CHANSON FRANÇAISE	7.3%	0.1%
ROCK / METAL	6.7%	0.0%
DANCE / ELECTRO	6.6%	0.0%
R&B / SOUL	5.4%	0.4%
ALTERNATIVE / INDIE	2.3%	0.0%
GLOBAL / TRADITIONAL	1.6%	0.2%
UNIDENTIFIED	0.8%	
SOUNDTRACK	0.7%	
REGGAE	0.5%	
CLASSICAL / LYRICAL	0.3%	
JAZZ / BLUES	0.2%	
COUNTRY / FOLK	0.2%	

Breakdown by music genre (1)

In terms of breakdown, 84.5% of the streams detected and considered to be fake come from the hip-hop/rap genre. It is the most popular genre in the top 10,000 most-listened to tracks and therefore represent a higher volume of streams on the detection.



Indicators observed on Spotify's top 10,000 most-listened to tracks

(supplemented with distributors' data)

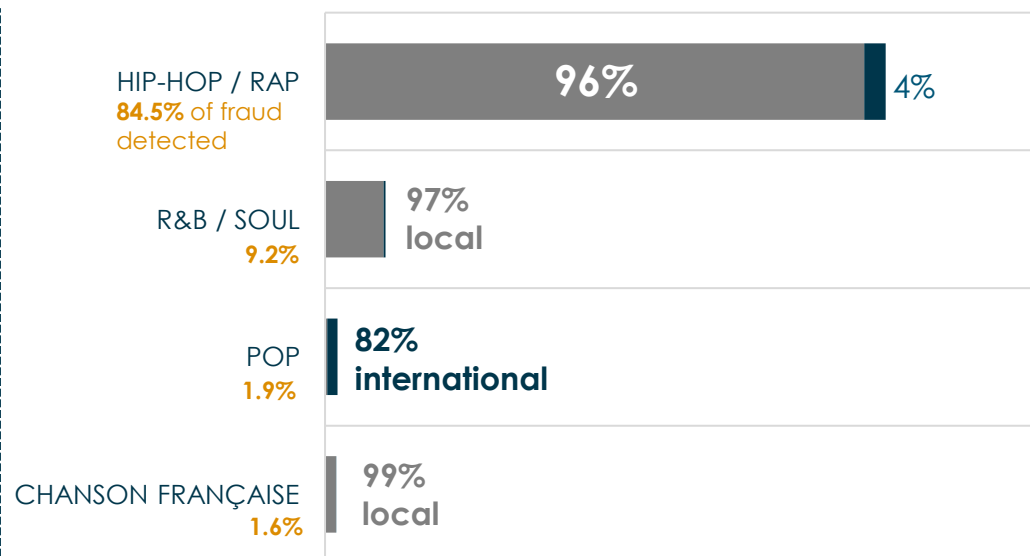
Breakdown by music genre (2)

Catalogue type detected within music genre

LOCAL

INTERNATIONAL

Within the hip-hop/rap (96%), R&B/soul (97%) and chanson française (99%) genres, the majority of fraud detected comes from the local catalogue. Fraud predominates in the international catalogue in pop (82%).

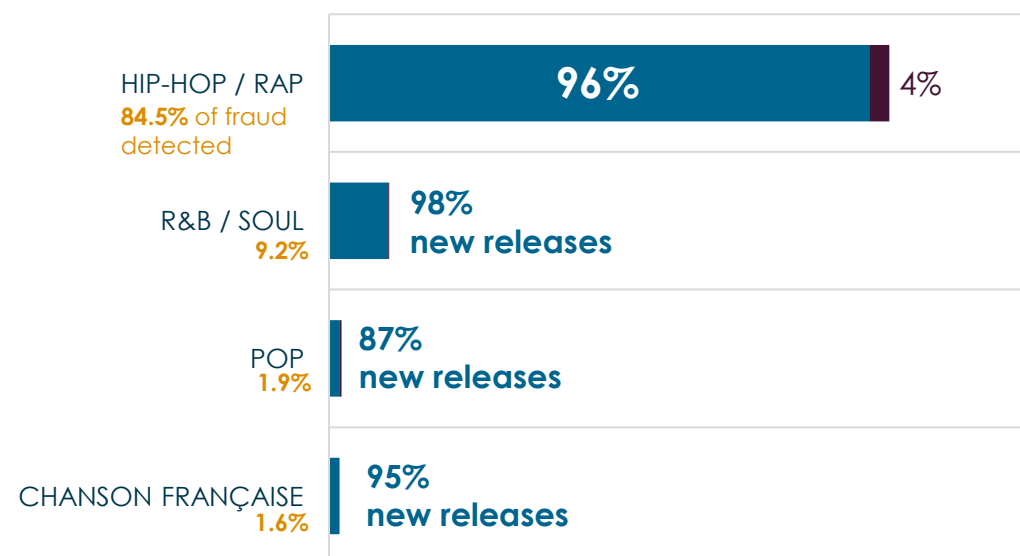


Release date detected within music genre

NEW RELEASES

BACK CATALOGUE

In all the genres observed, fraud predominates in new releases (87%+).



Filter applied to select local catalogue and new releases broken down by music genre (top 10,000)

(supplemented with distributors' data)



Amount of streams detected

When broken down by music genre, the overall share of fake streams and the filtered data show roughly the same trend, both always remaining below 1%. The R&B/soul genre goes from 0.4 to 0.7%.

Breakdown by music genre

After applying the filter, the top 5 genres remain the same, but their positions vary. In terms of distribution, almost 90% of streams detected as fake come from hip-hop/rap, followed by almost 10% in the R&B/soul genre. Fake streams detected in the pop genre fell from 1.9% to 0.3%.

0.23% Share detected

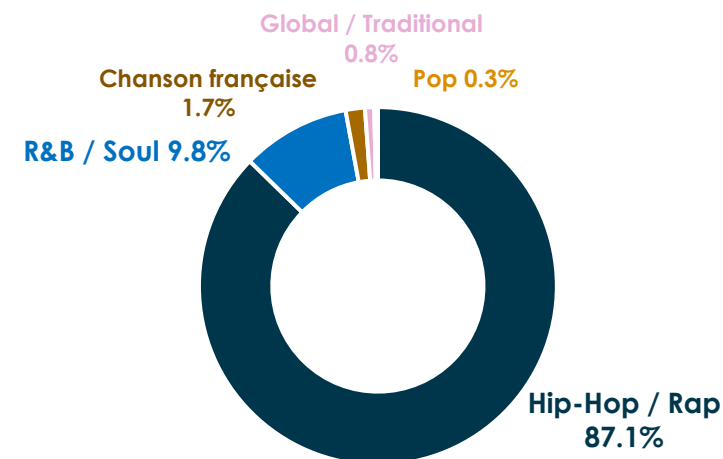
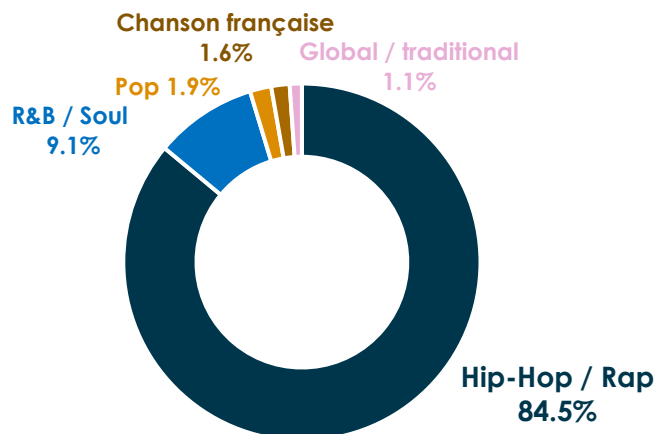
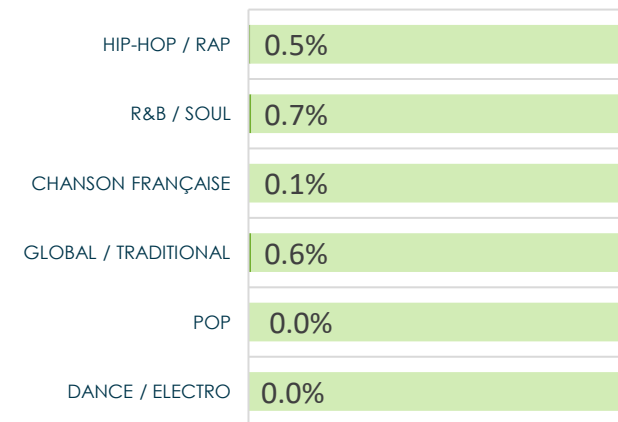
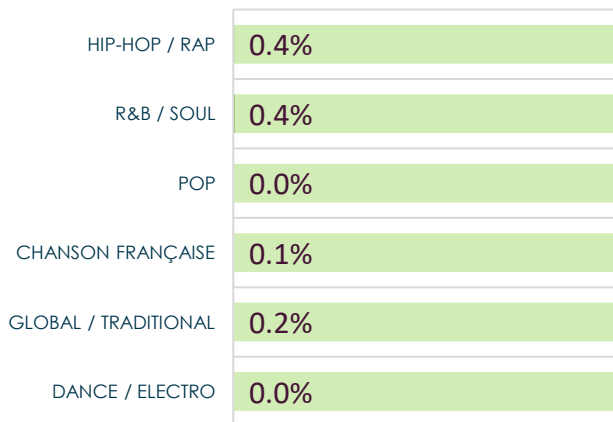
For comparison overall share

0.46% Share detected



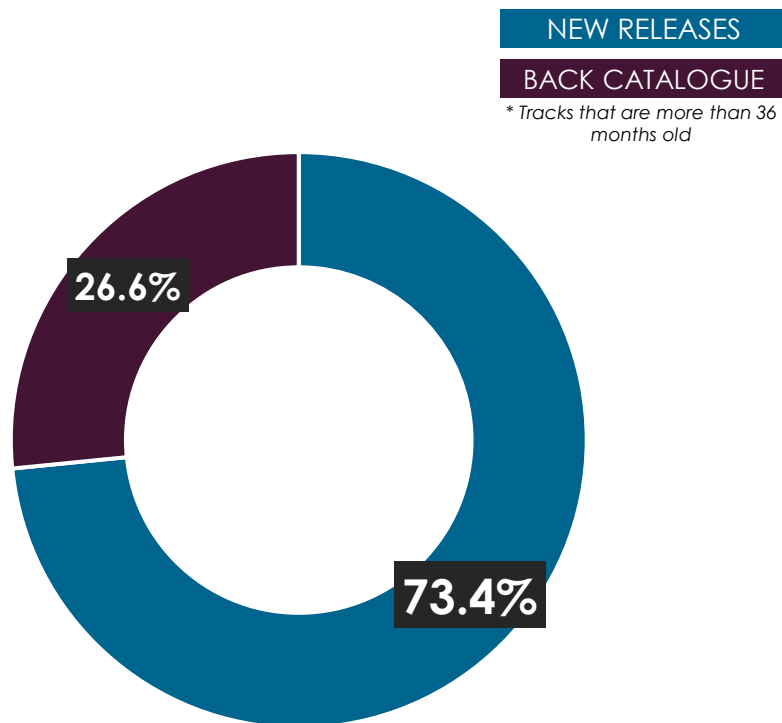
LOCAL

NEW RELEASES



Indicators observed on Qobuz's top 10,000 most-listened to tracks

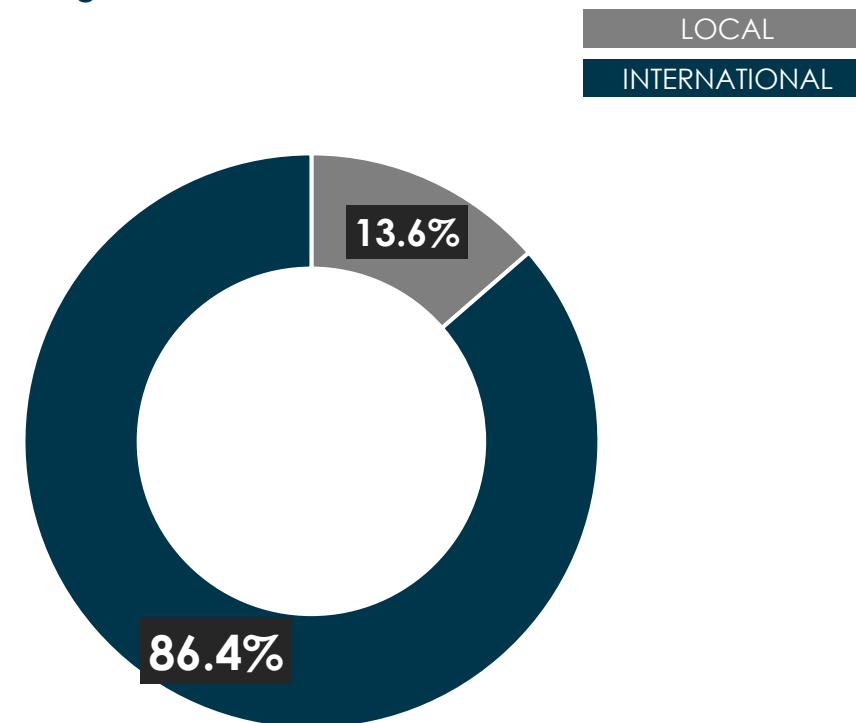
Breakdown by release date



73% of fraud detected comes from new releases

The amount of fraud detected on all new releases would come to 4.2% compared to 1.5% on all back catalogue.

Breakdown by catalogue



86% of fraud detected comes from international catalogue

The amount of fraud detected on the entire local catalogue is 1.6% compared to 3.2% on the international catalogue.

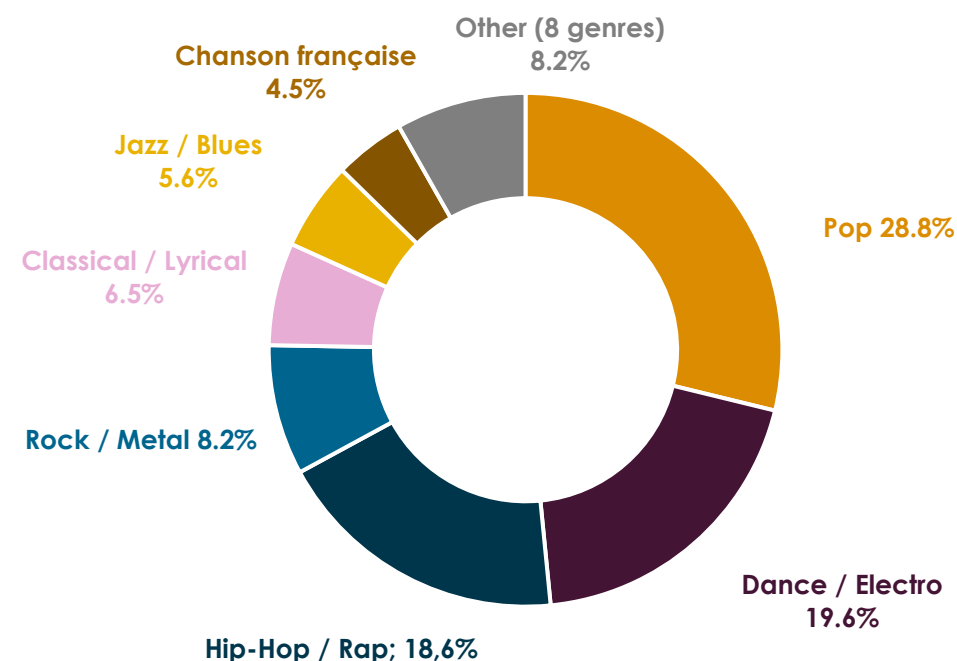
Indicators observed on Qobuz's top 10,000 most-listened to tracks

The amount of streams considered as fake is **15.2% in the hip-hop/rap genre**, followed by **ambient/chillout music at 12.3%**.

	Overall share	Amount detected within each genre
ROCK / METAL	30.4%	0.8%
POP	16.2%	5.0%
JAZZ / BLUES	14.8%	1.1%
CHANSON FRANÇAISE	10.3%	1.2%
R&B / SOUL	8.7%	0.8%
DANCE / ELECTRO	6.0%	9.3%
CLASSICAL / LYRICAL	5.6%	3.3%
HIP-HOP / RAP	3.5%	15.2%
SOUNDTRACK	1.6%	0.6%
GLOBAL / TRADITIONAL	1.3%	3.2%
REGGAE	0.7%	8.4%
RELIGIOUS / SPIRITUAL	0.5%	3.2%
CHILDREN'S MUSIC	0.4%	6.9%
UNIDENTIFIED	0.0%	3.8%
AMBIENT / CHILLOUT	0.0%	12.3%

Breakdown by music genre (1)

In terms of breakdown, **28.8%** of the streams detected and considered to be fake come from **pop**, then **dance/electro (19.6%)**.



Indicators observed on Qobuz's top 10,000 most-listened to tracks

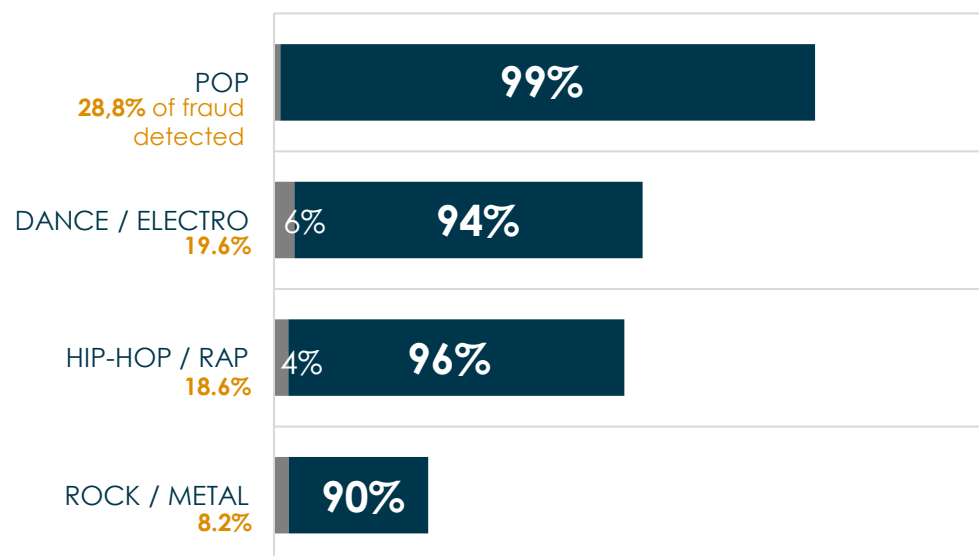
Breakdown by music genre (2)

Catalogue type detected within music genre

LOCAL

INTERNATIONAL

Fraud is largely predominant (more than 90%) in the international catalogue across all the genres observed.

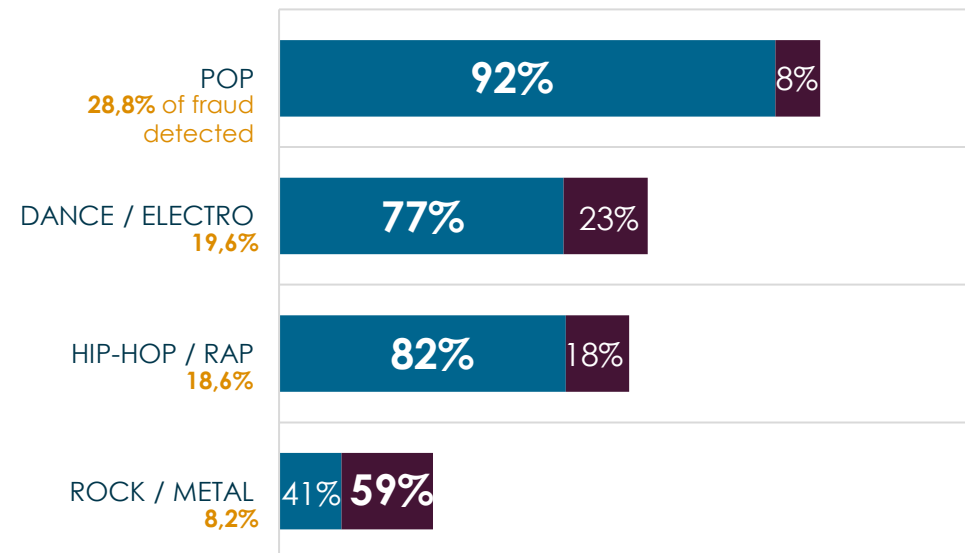


Release date detected within music genre

NEW RELEASES

BACK CATALOGUE

Within pop (92%), dance/electro (77%) and hip-hop/rap (82%), the majority of fraud detected comes from new releases. However, stream fraud predominates in the back catalogue in rock/metal (59%).



Filter applied to select local catalogue and new releases broken down by music genre (top 10,000)



Amount of streams detected

The amount of fake streams detected in the hip-hop/rap genre has seen a considerable drop, from 15.2% to 1%.

Breakdown by music genre

The top 5 genre positions have shuffled. In terms of distribution, 38.7% of streams considered as fake come from chanson française when the filter is applied, while overall they represent 4.5%.

It's followed by classical/lyrical (18%), and jazz/blues (11.8%). Hip-hop/rap (7%) comes in fifth behind rock/metal (9.2%).

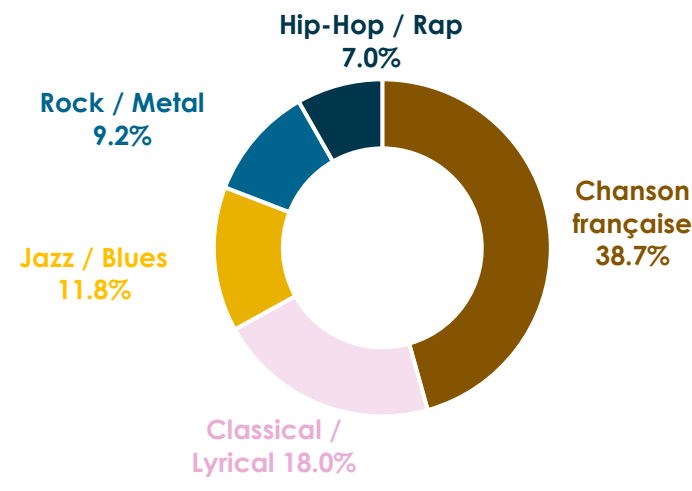
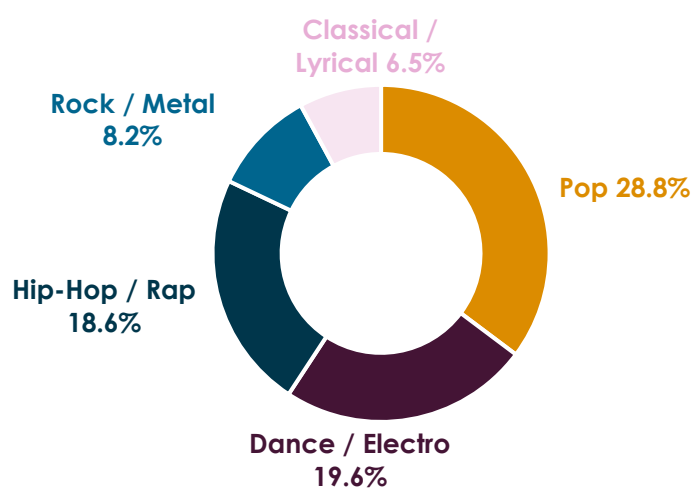
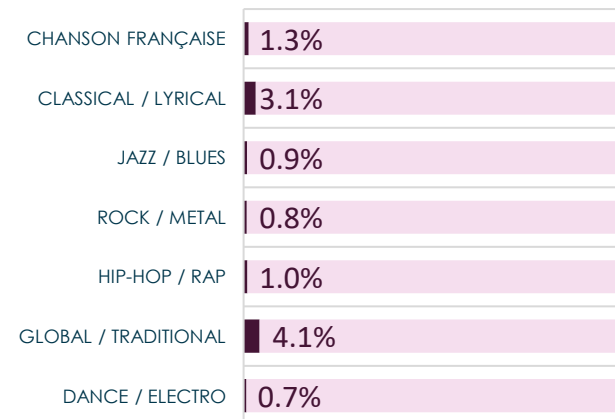
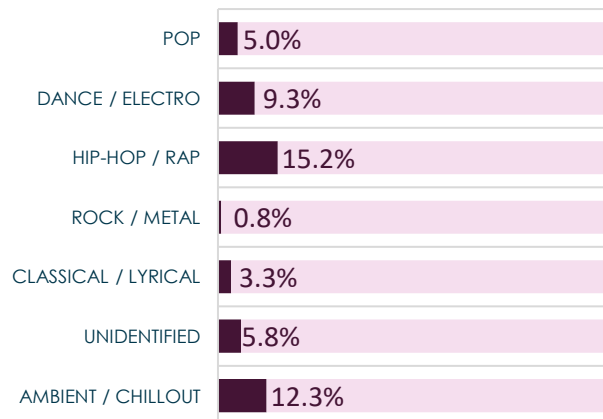
2.82% Share detected

For comparison overall share

1.18% Share detected

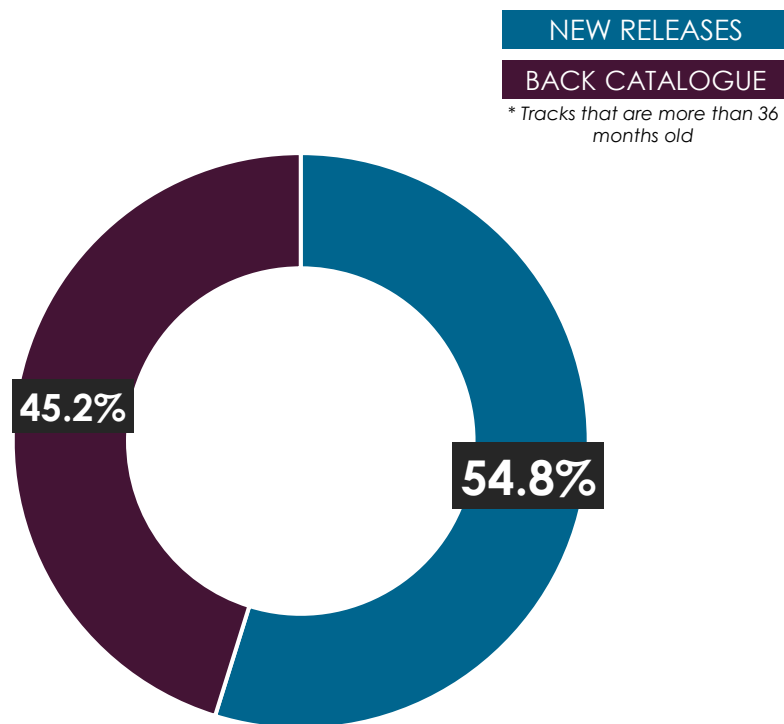


LOCAL
NEW RELEASES



Indicators observed on Deezer's top 10,000 most-listened to tracks

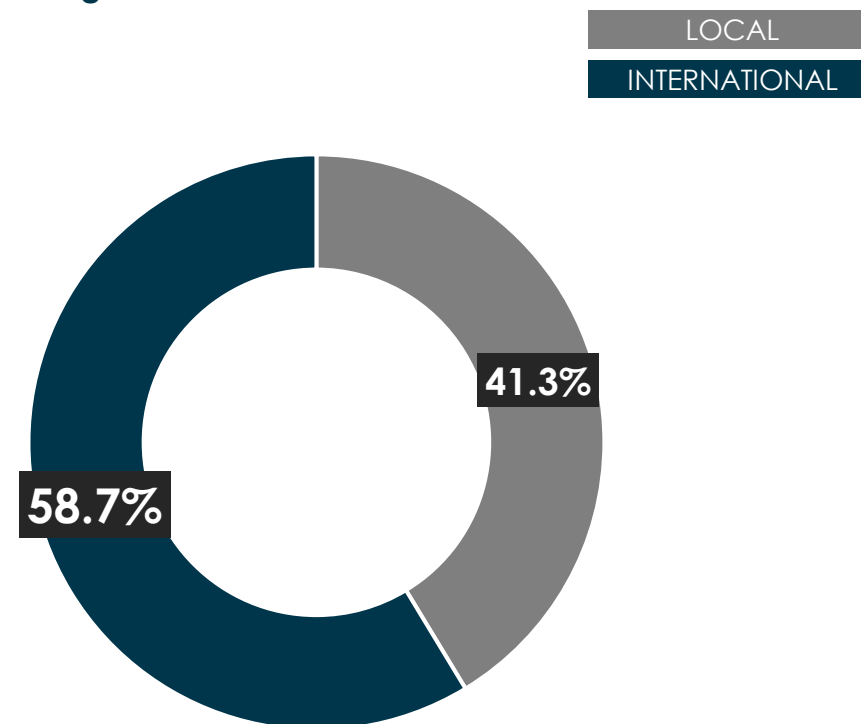
Breakdown by release date



55% of fraud detected comes from new releases

The amount of fraud detected on all new releases amounts to 0.9% compared to 1.1% for back catalogue.

Breakdown by catalogue



59% of fraud detected comes from international catalogue

The amount of fraud detected on the entire local catalogue amounts to 0.8% compared to 1.2% on the international catalogue.

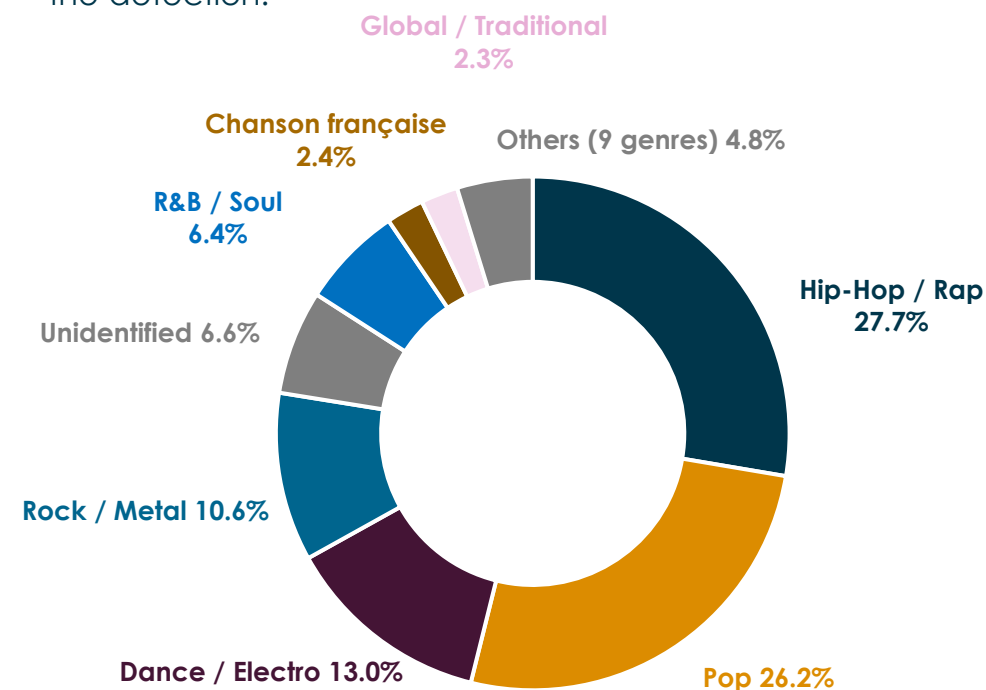
Indicators observed on Deezer's top 10,000 most-listened to tracks

Ambient music (4.8%) and **non-music tracks (3.5%)** record the highest share of abnormal streaming activity. For hip-hop/rap and pop, fraud detected represents 0.7% and 1.2% respectively.

	Overall share	Amount detected within each genre
HIP-HOP / RAP	41.3%	0.7%
POP	21.4%	1.2%
DANCE / ELECTRO	9.2%	1.4%
ROCK / METAL	8.3%	1.2%
UNIDENTIFIED	7.1%	0.9%
R&B / SOUL	4.6%	1.4%
CHANSON FRANÇAISE	2.4%	1.0%
GLOBAL / TRADITIONAL	2.2%	1.1%
ALTERNATIVE / INDIE	1.1%	1.3%
SOUNDTRACK	0.9%	1.1%
REGGAE	0.8%	1.1%
JAZZ / BLUES	0.3%	1.8%
COUNTRY / FOLK	0.1%	1.5%
CLASSICAL / LYRICAL	0.1%	1.3%
AMBIENT / CHILLOUT	0.1%	4.8%
NON-MUSIC	0.0%	3.5%
RELIGIOUS / SPIRITUAL	0.0%	2.1%

Breakdown by music genre (1)

In terms of distribution, **27.7% of the streams detected** and considered to be fake come from the **hip-hop/rap** genre, followed by **pop at 26.2%**. These are the most popular genre in the top 10,000 most-listened to tracks and therefore represent a higher volume of streams on the detection.



Indicators observed on Deezer's top 10,000 most-listened to tracks

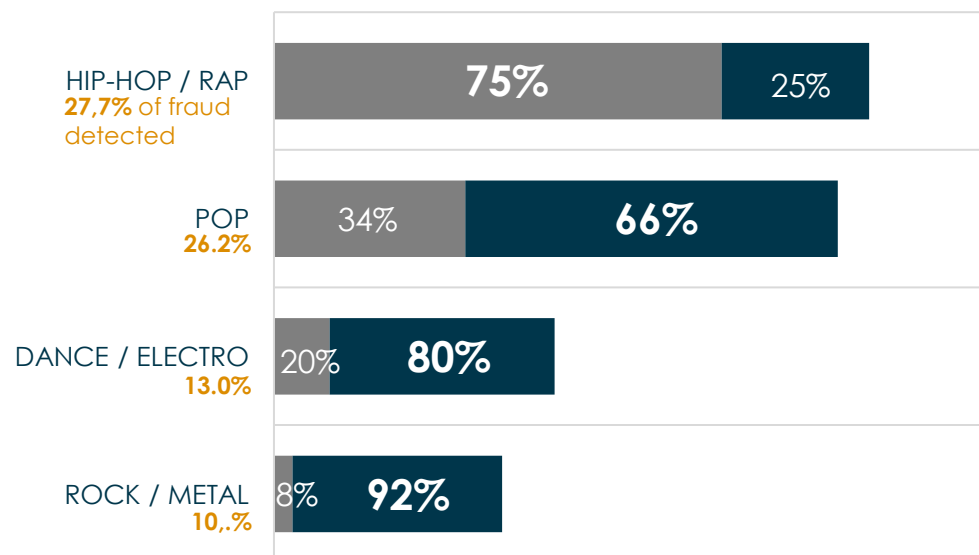
Breakdown by music genre (2)

Catalogue type detected within music genres

LOCAL

INTERNATIONAL

Within pop (66%), dance/electro (80%) and rock/metal (92%), the majority of fraud detected is in the international catalogue. Fraud predominates in the local catalogue in hip-hop/rap (75%).

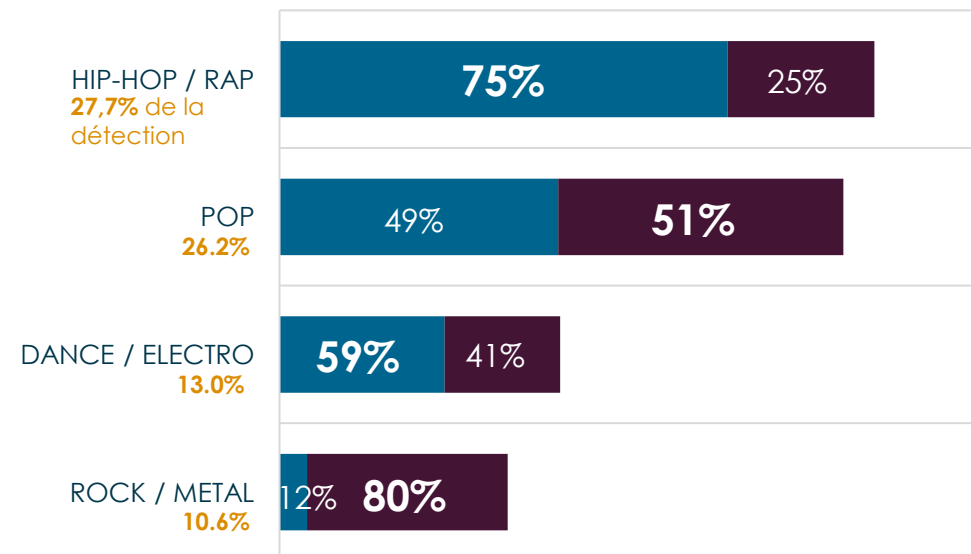


Release date detected within music genre

NEW RELEASES

BACK CATALOGUE

Within hip-hop/rap (75%) and dance/electro (59%) the majority of fraud is detected amongst new releases. For pop (51%) and rock/metal (80%), it predominates in the back catalogue.



Filter applied to select local catalogue and new releases broken down by music genre (top 10,000)



Share of fake streams detected

When broken down by music genre, the overall share of fake streams and the filtered data show roughly the same trend. Tracks identified as ambient /chillout generate the largest share (4.8%).

Breakdown by music genre

When the filter is applied, the share of fake streams allocated to hip-hop/rap increases to 56%, while its overall share represents nearly 28%.

When comparing filtered data with overall data, fake streams in pop are down to 16%, when overall they exceed 26%. Finally, in the filtered data, chanson française (6%), comes in ahead of dance/electro (5.6%).

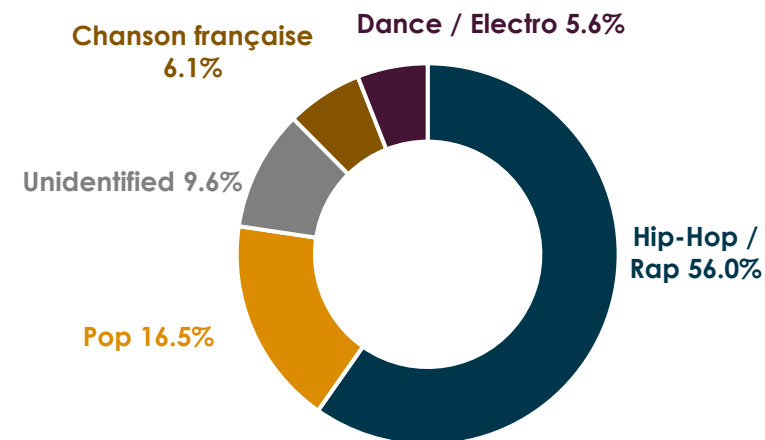
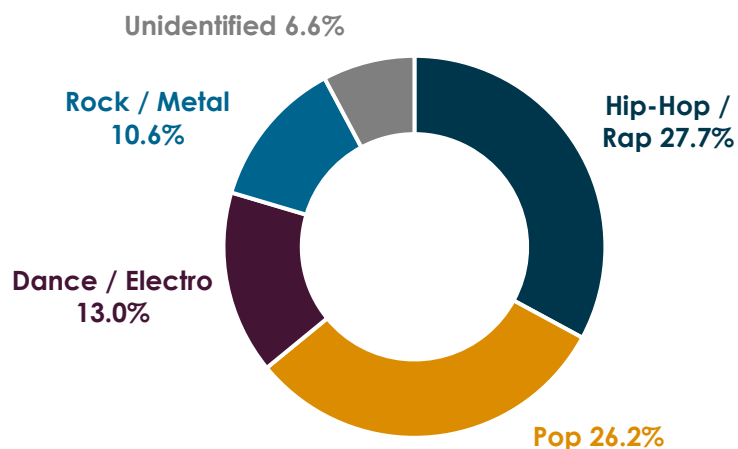
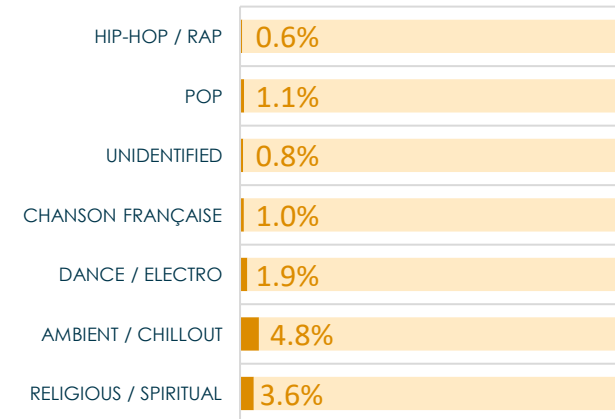
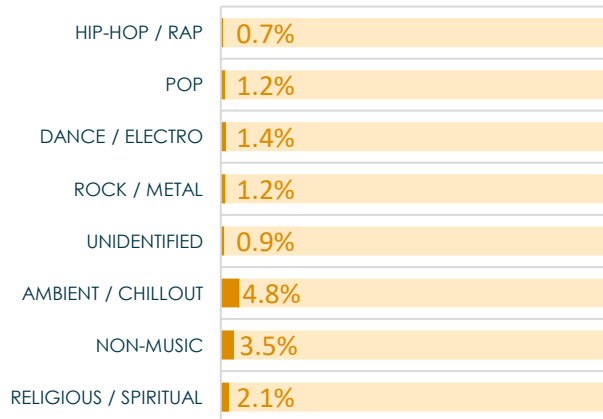
0.98% Share detected

For comparison overall share

0.75% Share detected



LOCAL
NEW RELEASES



QUANTITATIVE OBSERVATIONS

On DEEZER's figures based on additional data provided by distributors

Data requested from distributors



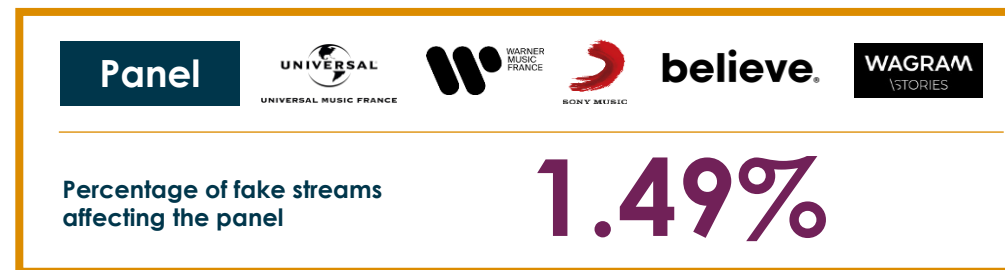
Data

All tracks in the catalogue that have been detected for abnormal streaming activity.

Parameters	Description
Track ID	Anonymised track name
Artist ID	Anonymised artist name
Genre	Music genre associated with the track
Catalogue	Origin of the track (local/international)
Release date	Date the track was first released on the platform in order to analyse whether it's a new release or part of back catalogue
Total streams	Total number of streams over the requested period (2021)
Total fake streams	Total number of streams identified and considered as fake by the platform, over the requested period (2021)

Quantitative analysis (distributors' data)

The data analysed comes from the **distributors' financial reports** and concerns all the tracks in their catalogue for which abnormal streaming activity has been detected by Deezer. The data was aggregated in order to establish an overall volume. This panel does not include data from aggregators that are subsidiaries of distributors.



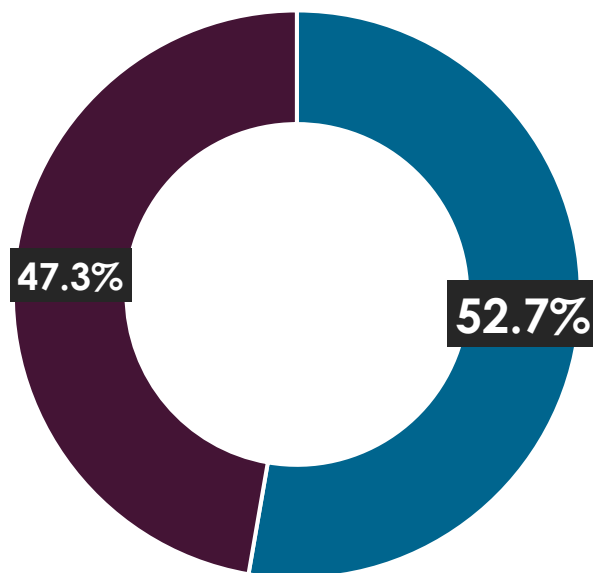
NEW RELEASES

BACK CATALOGUE

* Defined as track over 3 years old

The majority of streaming activity identified as abnormal comes from **new releases (nearly 53%)**.

For all streams related to new releases, the amount of abnormal streaming activity amounts to 1.3%, compared to 1.8% for back catalogue.

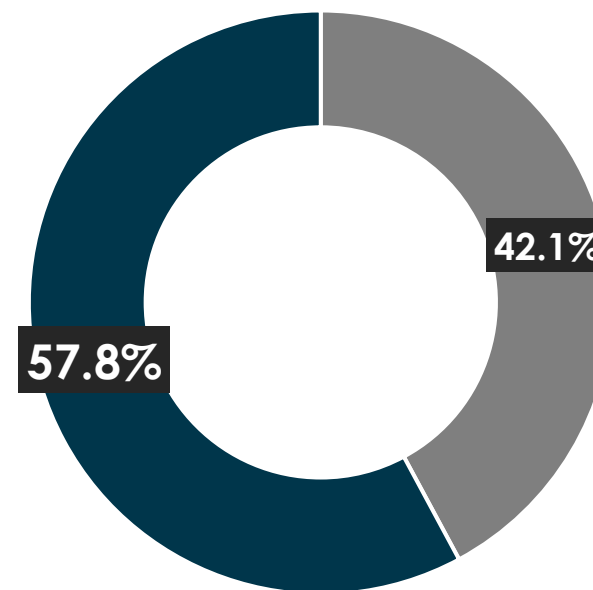


LOCAL

INTERNATIONAL

The majority of streaming activity identified as abnormal comes from the **international catalogue (nearly 58%)**.

The **amount of abnormal streaming activity on the local catalogue amounts to 1.2%**, compared to 1.9% on the international catalogue.



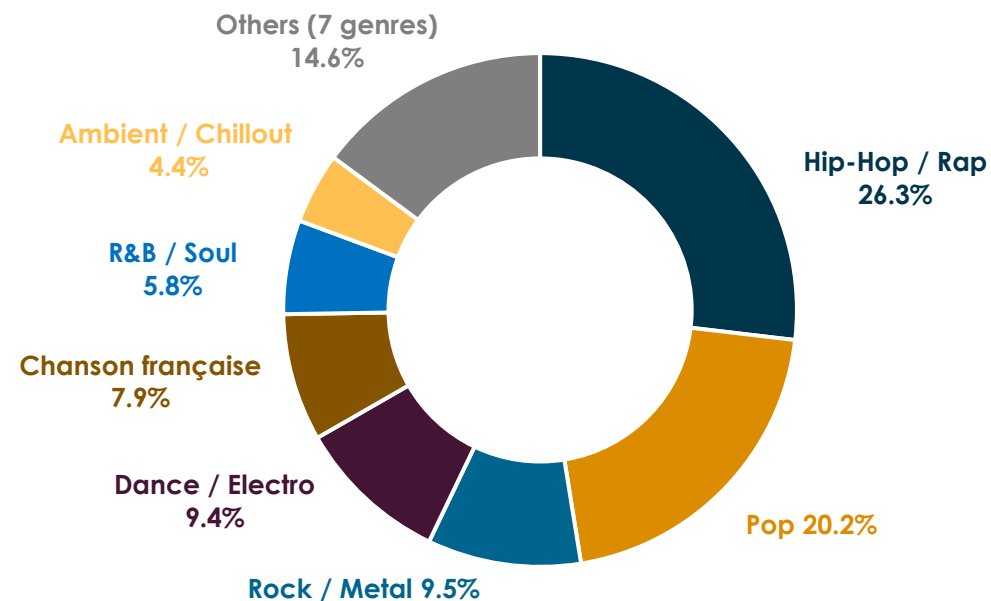
Indicators observed from distributors' data

Ambient music records the highest share of abnormal streaming activity (22.5%). For hip-hop and pop - genres which have the majority overall share, fraud detected represents 1.1% and 1.7% respectively.

	Overall share	Amount detected within each genre
HIP-HOP / RAP	36.8%	1.1%
POP	18.4%	1.7%
CHANSON FRANÇAISE	9.7%	1.2%
ROCK / METAL	9.6%	1.5%
DANCE / ELECTRO	6.8%	2.1%
R&B / SOUL	5.5%	1.6%
ALTERNATIVE / INDIE	3.2%	1.6%
GLOBAL / TRADITIONAL	2.3%	2.0%
SOUNDTRACK	1.8%	1.5%
UNIDENTIFIED	1.2%	2.3%
CLASSICAL / LYRICAL	1.2%	1.8%
JAZZ / BLUES	1.0%	3.5%
REGGAE	0.9%	1.6%
COUNTRY / FOLK	0.4%	2.0%
CHILDREN'S MUSIC	0.4%	2.6%
AMBIENT / CHILLOUT	0.3%	22.5%

Breakdown by music genre (1)

In terms of distribution, **26.3% of streams detected** and considered to be fake are classed as **hip-hop/rap**, followed by **pop at 20.2%**. These are the most popular genre in the top 10,000 most-listened to tracks and therefore represent a higher volume of streams on the detection.



Indicators observed from distributors' data

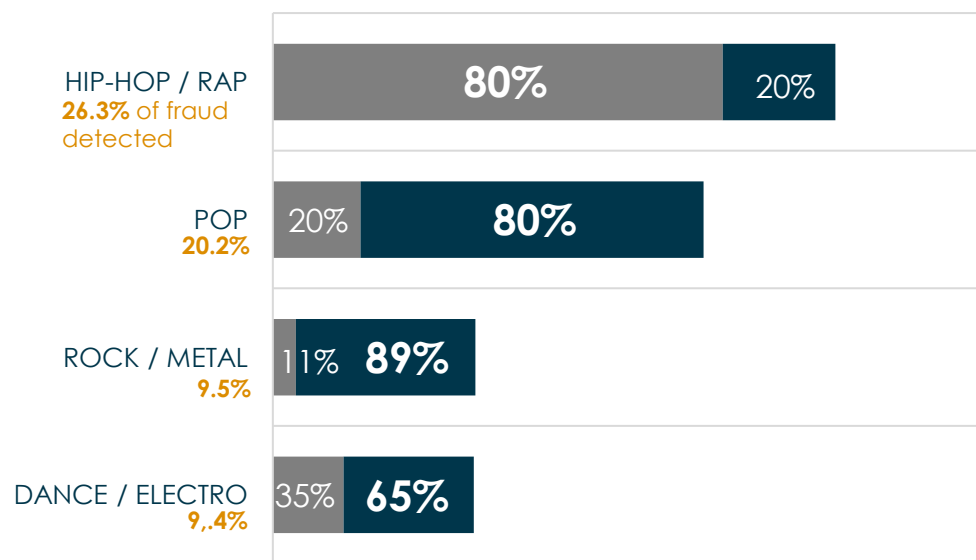
Breakdown by music genre (2)

Catalogue type detected within music genres

LOCAL

INTERNATIONAL

Within pop (80%), dance/electro (65%) and rock/metal (89%), the majority of fraud detected comes from the international catalogue. Fraud predominates in the local catalogue for hip-hop/rap (80%).

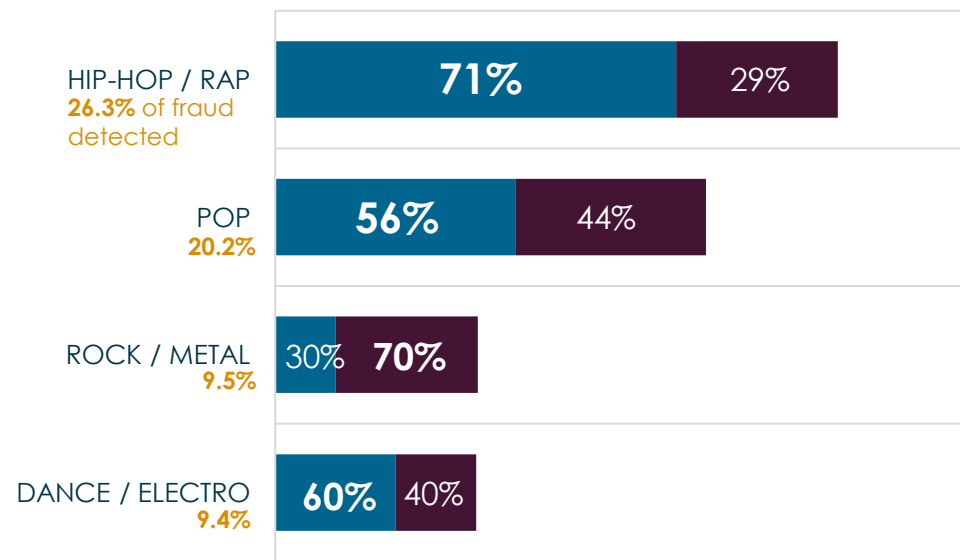


Release date detected within music genre

NEW RELEASES

BACK CATALOGUE

In hip-hop/rap (71%), pop (56%) and dance/electro (60%), the majority of fraud is detected amongst new releases. The only genre for which the back catalogue holds the majority is rock/metal (70%).



Filter applied to select local catalogue and new releases broken down by music genre



Share of fake streams detected

After applying the filter, the share of fake streams detected is between 1 and 2%, with the exception of jazz/blues (2.6%), tracks for which no genre is identified (2.2%), and ambient/chillout - the latter of which generates the highest share of abnormal streaming activity (4.7%).

Breakdown by music genre

After applying the filter, hip-hop/rap goes from 26.3% to 58.4%. It's followed by chanson française, which moves up three places (11.6%), then by pop (11%). R&B/soul enters the top 5 genres, with 5.5% of abnormal streaming activity.

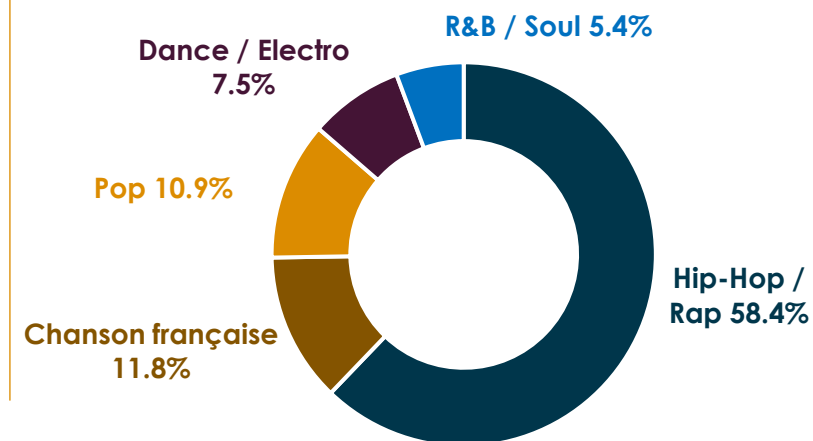
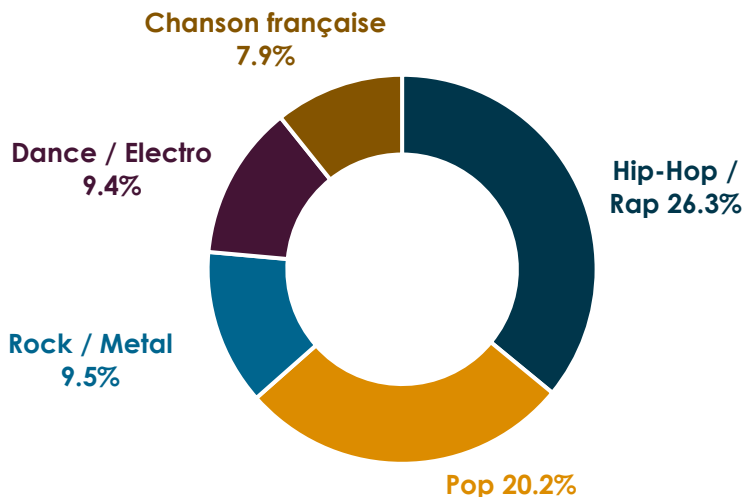
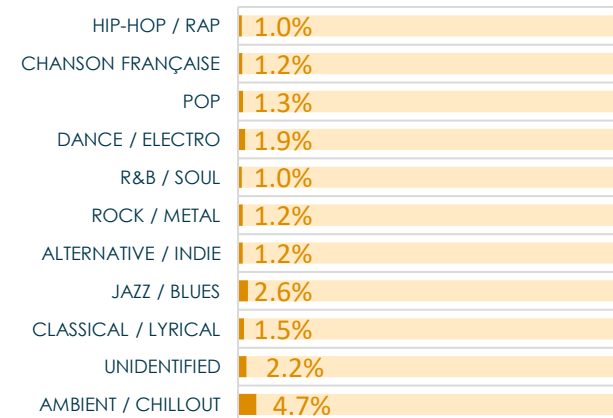
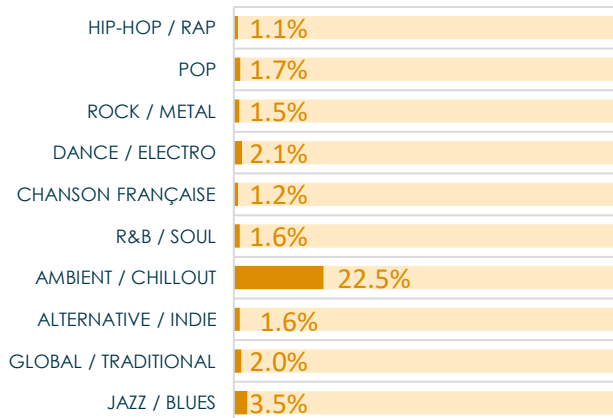
1.49% Share detected

For comparison overall share

1.09% Share detected



LOCAL
NEW RELEASES



Summary: observations on Deezer

Overall volume on Deezer in France in 2021

The panel represents 75.3% of the overall volume of streams



1.5% The amount of fake streams affecting the panel

Fraud detected on Deezer in France in 2021

 deezer

2.6%

Panel 44.8%

Others 55.2%

Share of streams detected

The distributors who participated in the study represent more than 75% of streaming on Deezer. The share of abnormal streaming activity detected amongst the panel of distributors is 1.49%.

Breakdown of fraud detection

From the data received from the panel of distributors, a calculation by the difference was made.

Of all the abnormal streaming activity detected by Deezer, less than 45% comes from the panel of distributors.

Overall summary

Share of fraud detected

The three platforms participating in the study each used their own detection method. Qobuz and Deezer apply their detection algorithms at the user account level - which lead to some "false positives", and Spotify applies it at the track level.

Based on the data provided, the share of fraud detected on the platforms in France is shown between 1% and 3% in 2021. In view of market figures, this represents between 1 and 3 billion streams detected as being fraudulent.

On Deezer and Spotify, more than 80% of streaming fraud occurs on the services' long tail (outside the top 10,000), while on Qobuz fraudulent activity is mainly concentrated to the most-listened to tracks.

Global volume indicators

On the platforms that participated in the study, **between 6 and 13% of abnormal streaming activity was detected as coming from the trial-period plan.**

Streaming fraud is mainly identified as coming from a computer (65% on Deezer and 31% on Qobuz) and **the Family plan amasses 54% abnormal streaming activity on Deezer.**

Catalogue diversity (genres, track age, origin)

On Spotify and Deezer, **the most popular genre in the top 10,000 most-listened to tracks is hip-hop/rap (more than 50% on Spotify and 40% on Deezer).** In terms of distribution, the majority of streaming fraud detected therefore comes from this genre (84.5% and 27.7% respectively).

On Deezer, **the share of streaming fraud detected is higher for ambient music (4.8%) and non-music tracks (3.5%).** For hip-hop/rap and pop, fraud detected represents 0.7% and 1.2% respectively. The data from distributors confirm this trend, whereby **the share of streaming fraud detected on ambient music amounts to 22.5%.**

On Spotify's top 10,000 most-listened to tracks (supplemented with data from distributors), **96% of streaming fraud detected comes from new releases and 93% from the local catalogue. The share of streaming fraud detected on local new releases amounts to 0.46%.** This figure is at 1.18% on Qobuz's top 10,000, and 0.75% on Deezer.

Distributors data

The panel of distributors (Universal, Sony, Warner, Believe and Wagram) represents more than 90% of Spotify's top 10,000 and more than 75% of the overall volume of streams on Deezer. Less than 45% of streaming fraud detected on Deezer comes from this panel.

Industry view (qualitative research, 2021)

The quantitative analysis showed that there was **at least 1 to 3% of all streaming was identified as fraudulent** on the participating platforms in 2021. However, as part of qualitative research, some interviews conducted highlighted the **extent of streaming fraud that went undetected**, with participants communicating their concerns:

- The **methods used by fraudsters are evolving and continue to improve**. The practice seems to be becoming more widespread and some industry professionals are even approached directly by artificial streaming service to increase their streams figures.
- **Certain platforms have noticed an increase in fraud.**
- Several industry professionals reveal that they **cannot currently rely on an artist's platform performance** (for signing an artist to a label, booking them for a show, or getting them on a radio playlist). This leads to a lack of trust in the platform-distributor-label relationship.
- Some rights-holders and lawyers mentioned the **likelihood that this practice is part of a strategy to "launder"** income from illegal or even criminal activities.

Observations since the study began

A year after the start of the study, **industry players are increasingly mobilising their voices on the issue**. As for platforms and rights-holders, exchanges between industry professionals is increasing, vigilance over stream data is heightened, and some players are more cooperative in sharing data.

Information relayed from certain players

Apple Music

Is investing in new technology and recruiting a new team to identify and remove fake streams. A process for identifying and investigating so-called suspicious streaming activity has been put in place. Streams under investigation are no longer included in the regular reporting sent to distributors, nor in the charts. A daily report of suspicious streaming activity is sent to partners (record labels, distributors) and at the end of the investigation, fraudulent streaming activity is removed. A monthly report detailing the streams which have been removed is sent to partners (record labels, distributors).

deezer

Introduced a new algorithm at the beginning of 2022 which has significantly increased the amount of fraudulent streaming activity being detected. Inter-departmental collaboration has increased and their algorithms are regularly assessed and improved in order to quickly counter constantly-evolving fraudulent practices.



A multi-weekly procedure for monitoring streaming activity in order to exclude abnormal activity detected in charts, such as certifications (gold, platinum, diamond, etc.).

The Official Charts Company (OCC), appointed on behalf of SNEP as the provider of France's official music charts, receives data in daily reports from streaming platforms and industry players.

By analysing this information (based on a series of parameters provided to the service provider), it can now implement procedures from the first half of 2022. This is in addition to the detection work carried out upstream by the platforms and make it possible, through ongoing dialogue with the latter, to strengthen the fight against fraud and improve existing detection tools.

amazon music

Implemented a new detection system and increased its fraud detection team, enabling Amazon Music to provide the CNM with all the data necessary for this study, and for more recent observation perimeters (2022) which will offer the possibility of initiating future analyses. Amazon Music confirms that it is continually working to strengthen detection methods and tools, and continues to work closely with the CNM and the entire music industry in order to effectively combat these fraudulent practices.

Spotify

Developing informative tools for artists and labels. The platform informs them of the risks involved and makes them aware of the impact that buying streams can have on the income of other artists on the market. Spotify also indicates that it continues to invest heavily in current detection techniques and to carry out manual checks to prevent, detect and limit the impact of fraud on the platform.

04 . LEGAL ACTION

Legal classification – criminal liability

Anyone who considers themselves a victim can report it to the police in order to make the person who allegedly committed the offence criminally liable.

Fraud (article 313-1 of France's Penal Code)	Unauthorised access to automated data processing systems - STAD (article 323-1 of France's Penal Code)	Unfair commercial practices (article L. 121-1 of France's Consumer Protection Code)
<p>Obtaining property or money by fraudulent means. The statute of limitations begins to run from its commission (6 years).</p> <p>It can be committed:</p> <ul style="list-style-type: none"> - under the use of a false name or a false identity, - using fraudulent means and techniques. To qualify as a fraudster, the perpetrator of the offense must have had the clear and distinct intention to obtain the money or property from the victim. 	<p>Computer hacking, such as:</p> <ul style="list-style-type: none"> - offenses of fraudulently gaining and/or maintaining access to a computer system, - hindering or distorting the operation of a computer system, - fraudulently transferring, deleting or modifying data, - participating in a group formed or in an agreement established with a view to the preparation of one or more of these offences. 	<p>The concept of "commercial practice" is not defined in the Consumer Protection Code, but is defined in the European directive n° 2005-29 of 11 May, 2005 relating to unfair business-to-consumer commercial practices of companies:</p> <p>"any action, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers."</p> <p>The law distinguishes between two kinds of misleading commercial practices: misleading actions and misleading omissions. In both cases, the consumer is deceived, preventing them from making an informed and thus efficient choice, encouraging them to make a commercial decision that they would not have taken in other circumstances.</p>
<p>Punishable by a five-year prison sentence and a €37,000 fine.</p>	<p>Punishable by a two-year prison sentence and a €60,000 fine (gaining or maintaining access fraudulently, in all or part of a STAD), Punishable by a three-year prison sentence and a €100,000 fine (modifying the operation of this system).</p>	<p>Punishable by a two-year prison sentence and a €300,000 fine.</p>

Procedure: the person who considers themselves to be the victim of fraud, STAD offenses or misleading commercial practice, can **report it to the police**. Ideally, the person reporting the crime is to hand over all evidence in their possession that can be used to demonstrate the offense. It is up to the **justice system to legally qualify the facts** and to initiate proceedings. The final decision on the outcome of the complaint is made by the public prosecutor.

Illicit or abusive commercial practices can also be reported to the DGCCRF (the French General Directorate for Competition Policy, Consumer Affairs and Fraud Control), which ensures that the economy operates smoothly and that consumers are protected, by investigating infringements and breaches of consumer rights (misleading advertising, false discounts, abuse of weakness, etc.) and consumer safety.

Legal classification – criminal liability

	Fraud	Unauthorised access to automated data processing systems - STAD	Unfair commercial practices
Fraud techniques concerned	All techniques resulting in artificially increasing play counts	Account hacking on streaming platforms	Promotional agencies and SEO websites purchasing streams
Potential plaintiffs / complainants	Rights-holder	Streaming platform	Rights-holder
Potential respondents / defendants	Initiator / Service provider (legal entity or natural person)	Technical service provider (hacker)	Service provider (legal entity or natural person)
Difficulties	Burden of proof Demonstrating fraudulent intent Apprehension of the French jurisdiction	Prerequisite: existence of a STAD (no legal texts provide a definition of this expression) Identifying the service provider: since the practices are operated by bots, tracing the source of the operation is often impossible.	Burden of proof Demonstrating fraudulent intent

Legal classification – civil liability

Tort liability

Concerning the possible engagement of tort liability, article 1240 of the Civil Code provides that **“any human action whatsoever which causes harm to another creates an obligation in the person by whose fault it occurred to make reparation for it.”**

Non-compliance with contractual conditions or general conditions of use

Steps should be taken to determine whether or not a contractual relationship between several parties exists. In the event that a contractual relationship is established, it seems likely that a clause aimed at stream manipulation will be provided.

Moreover, some online music platforms provide account suspension clauses in the event of fraud detection.

Regarding the contracts concluded by the actors, certain clauses could specifically provide for the possibility of stream manipulation.

Trademark infringement

(articles L 713-2 and L 713-3 of the French Intellectual Property Code)

The unauthorised use of a trademark, to designate goods or services in respect of which a trade mark is registered, in the course of business, by a person other than its owner.

The use of a mark, even with the additional words, "in the manner of, system, imitation or formula", constitutes an infringement, because this practice aims to take advantage of the reputation of the mark.

Unfair competition

It refers to the abuse of commercial practice by one company over another and can be defined as a set of practices exercised by one or more companies in the context of a market in order to harm one of its players.

The legal regime of unfair competition is set by various laws. The source is found in articles 1240 and 1241 of the French Civil Code which provide for the general principle of extra-contractual liability. But the evolution of this regime is very largely based on case law. The different types of behaviour that can be sanctioned on this basis have thus been largely defined by the courts.

Procedure: to be implemented, personal liability requires an operative event, damage and a causal link. The operative event, otherwise known as “fault”, is the illicit behaviour of an individual. The damage corresponds to the damage suffered by the victim and which gives rise to the right to compensation. The causal link is the essential element for establishing the relationship between the offence and the damage caused to the victim. **If there is no evidence to establish that this disorder is the result of this fault, then the civil liability of its author cannot be engaged. However, it appears that a strong statistical anomaly could be considered as proof.**

Legal classification – civil liability

	Tort liability		Non-compliance with contractual conditions or general conditions of use		Trademark infringement	Unfair competition
Fraud techniques concerned	All techniques resulting in artificially increasing play counts		All techniques resulting in artificially increasing play counts	Device farms: opening accounts for manipulation purposes	Promotional agencies and SEO websites purchasing streams	Promotional agencies and SEO websites purchasing streams
Potential plaintiffs / complainants	Rights-holder	Streaming platform	Rights-holder	Streaming platform	Streaming platform	Rights-holder
Potential respondents / defendants	Streaming platform	Initiator / Service provider (legal entity or natural person)	Service provider or rights-holder (legal entity or natural person)		Service provider (legal entity)	Service provider (legal entity)
Difficulties	<p>Three conditions must be met to incur civil liability: an established fact (fault), damage must have been occurred, and the causal link between the two.</p>					

05 . RECOMMANDATIONS

Recommendations



Inter-professional charter for the prevention of and fight against stream manipulation

After consultation with the professional organisations representing online music publishers, phonographic distributors and producers, and authors, composers and performers, the CNM recommends implementing an interprofessional charter for the prevention of and fight against stream manipulation.

This document would help to (i) **define precisely what these practices are**; (ii) **clearly identify the chain of responsibilities** and thus make all industry professionals aware of the legal risks associated with such manipulation; (iii) **standardise and formalise warning processes** and graduate penalties.

The following commitments (amongst others) would be expected of artists, managers, producers, distributors and DSPs, including measures directly implemented by the CNM:

Never contribute directly or indirectly to an activity aimed at stream manipulation

Members must attend a **training session** on stream manipulation, in the year after joining

Alert all the parties concerned in the event of suspicion of fraud, abnormal streaming activity and suspicious user behaviour linked to potential stream manipulation.

Implement a **monitoring system subject to certain standards**

Undergo a **regular audit of control procedures**

Include a **standard contractual clause** stating that any party involved directly or indirectly in stream manipulation would breach their contractual obligations. This clause would state the **dissuasive penalties** if fraudulent streaming activity were detected (non-remuneration, breach of contract) and would state the legal proceedings.

Recommendations



Mobilise resources: a three-step strategy

Actions are envisaged at several levels: (i) an audit of data and detection methods; (ii) a transparency assessment; (iii) a policy of clampdown measures.

Audit and fraud detection software for streaming platforms and record labels

Launch of a call for tenders for choosing a company capable of auditing data and detection systems. **A working group would be set up by the CNM in the spring 2023** to draw up specifications adapted to sectoral needs, in collaboration with streaming platforms and distributors.

Objectives: for each of the platforms, to define their detection methods and ensuing results, implement a **single reporting method between the DSPs and rights-holders, on the basis of common indicators.**

PEReN - *Pôle d'expertise de la régulation numérique*
(Centre of expertise in digital regulation)

This national centre of expertise is attached to the *Directeur Général des Entreprises* (the French General Directorate for Enterprise) for its administrative and financial management, and is placed under the joint authority of the ministers in charge of the economy, culture and digital.

As part of the study, PEReN endeavoured to provide the CNM with **data transparency indicators**. The centre would support the auditing firm.

DGCCRF - General Directorate for Competition Policy, Consumer Affairs and Fraud Control

Within the Ministry of the Economy, the DGCCRF is a supervision authority that monitors compliance with competition rules, ensures the economic protection of consumers, and the safety and compliance of products and services.

The DGCCRF could be called upon to highlight the possible existing **clampdown measures** to implement or to define new ones, specific to the industry.

Centre national
de la musique

cnm