

We [may earn money](#) when you buy through our links. Join 7M+ viewers on our [YouTube channel >>](#) ✕

[Home Security](#)[Senior Safety](#)[Kid Safety](#)[Deals](#)[Awards](#)[News](#)[Home](#) | [News](#) | [What is Music Streaming Fraud?](#)

What is Music Streaming Fraud?

✓ Why you can trust SafeWise

For over 13 years, SafeWise experts have conducted independent research and testing to write unbiased, human reviews (not robots). [Learn more.](#)



By **Fergus Halliday**

Feb 10, 2025 ⌚ 4 min read ✓ Edited By Alina Bradford

For pretty much as long as people have been able to listen to music via streaming services like Apple Music and Spotify, scammers have been trying to take a cut of the money involved. These days, [Spotify isn't the only one stealing from artists](#). Some estimates have suggested that streaming fraud costs the industry [as much as \\$2 billion in profits a year](#).

As co-CEO of the startup Beatdapp, Andrew Batey works on the frontlines of trying to make that number go down. Speaking to SafeWise, he shared his definition of what streaming fraud looks like and shed light on the tools that Beatdapp uses to combat it.

"I define streaming fraud as anyone who has manipulated the stream," he explained.

What that manipulation looks like has changed over the years. Initially, it was just bots running 10,000 streams in a week. However, as Batey and others have grown more sophisticated in their efforts to stream fraud so too have scammers.

"Some streaming services would look at the last 28 days or first 28 days for fraud, so the first or last three days you'd see a ton of fraud go through," Batey explained.

Learning to spot that manipulation is the name of the game here. Most people don't realize just how much data that streaming apps like Apple Music hold on to, nor how companies like Beatdapp use it to flag fraudulent streams.

"We work a lot with first-party data with the streaming services themselves. We have everything from the gyroscope, battery life, the orientation of the phone, everything you've done in-app before you've played something," he explained.

Batey said that the company takes that data and then uses over 600 machine-learning models to identify patterns that suggest when a user's account has been hacked and is being used differently.

"We have hundreds of machine learning models to detect who's real, who's not real, who's streams count, who's streams shouldn't count," he said.

Rarely, there's one specific red flag that separates frauds from fans. Batey said that Beatdapp errs on the side of letting fraud through so that we don't accidentally penalize a superfan or artist. If it calls something fraud, it's usually because they're 99.99% sure it is.

"It's normally like these 47 flags are true and it would be impossible for this to be a real person," he said.

Like the scammers the company targets, Beatdapp's arsenal of anti-fraud tech starts with the simple stuff. If they detect more than 5,000 streams from a given user in a given week, it gets flagged. Realistically, the most that even a dedicated fan might be able to stream caps out at around 3,200 and that's without accounting for stuff like sleep.

"When you see someone with 8,000 streams, it's obviously fraud," Batey said.



Stay Safe and become a SafeWise Insider!

Sign up for our free weekly newsletter to get the best safety news, product info, and deals.

By signing up, you agree to our [Terms and Conditions](#) and [Privacy Policy](#).

This rules-based approach works for the easy stuff. For everything else, there's Beatdapp's R&D team. Their job is to develop new models, backtest those models and double-check for any potential biases.

"When we build custom models, we not only check to see if the model is correct but we introduce data that we know not to be fraud to see if our models accidentally flag it. We're not only testing the model but backtesting the model," Batey explained.

The company even worked with various “superfan” apps to develop models for what that behavior looks like, and every month, the company goes back and reconfirms its models.

Compared to other types of fraud, Batey said that the vagaries of how streaming music gets paid out make it harder to crack down on than something more traditional like bank fraud.

“With music, it’s a bit different because it’s a pool of capital being paid out and you don’t have a real user who knows they should have been paid so we have to be really careful not to penalize artists who come up with creative ways to do marketing or have fans that are hyper-engaged with their content or even penalize artists who aren’t doing the wrong thing.”

The other thorny thing is that while the basic mechanics of streaming fraud remain constant, what it looks like can often change shape. In the past, [white noise tracks](#) have been proven to be a popular vehicle for scammers looking to rack up fake streams.

Nowadays, as with seemingly every part of the tech world, [AI](#) has become a growing concern.

“AI is a little scary because as AI gets better, it creates a lower barrier to entry for fraudsters to enter the market, but there’s always going to be a way to enter the market, and they will try to figure that out,” Batey said.

More sophisticated schemers are actually looking to the past for inspiration, digitising CDs and albums from regions like Africa and other content that isn’t necessarily available on streaming platforms.

“Nobody is paying attention because nobody has uploaded the DSPs, and so then they upload it, and then they’re the first person to own the digital fingerprint, so they can have lots of high-quality music that’s not theirs, and then they stream manipulate it,” Batey said.

Another honeypot for scammers is user-generated or upload sites like Soundcloud. Since an artist might only push out one of every hundred songs they record, these sites represent a trove of potential music that scammers can use to launder their illegitimate listens.

“There’s a really good chance that if you can target those platforms where that stuff is aggregated, you can steal a bunch of that music [and] upload it and the artist has no clue because you’re putting it under a different name, different album, different ISRC and you’re loading it up,” Batey said.

As the CEO of Beatdapp puts it, streaming fraud and scammers are like water. They tend towards the path of least resistance. Even if companies like Batey’s can’t necessarily eliminate streaming fraud entirely, they can push the opportunity cost for scammers upwards over time.

Success is less about getting fraudsters to face the music and more about turning up the volume until they get put off and leave for greener pastures.

“At some point, it becomes too difficult and they give up and move on,” he said.

As that happens, the money siphoned by streaming will make its way back into the coffers of legitimate artists. The war on streaming fraud likely won't address the fundamental issues faced by those who make their livelihoods from platforms like Spotify, but it can't hurt either.

Related articles on SafeWise

- [Mysterious Package on your Doorstep? Make Sure It's Not a Brushing Scam](#)
- [What Are Phishing Scams?](#)
- [Rental scams: Everything you need to know](#)
- [Lost Money to Scammers? Take Action with These Recovery Tips](#)

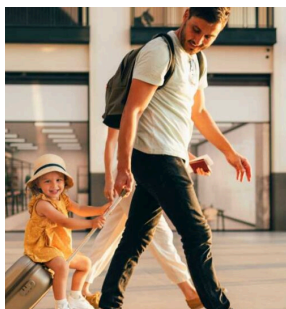
Share Article



Written by
[Fergus Halliday](#)



Recent Articles



By
Rebecca
Edwards

**Tack GPS Tracker
Review**

02/18/2026



By
Alina Bradford

**How to Install the
Ring Battery Doorbell
Plus**

02/17/2026



By Cathy Habas

**LogicMark Freedom
Alert Max Review**

A refreshing take on
medical alert systems, the

02/13/2026



By John Carlsen

**Vivint Cameras 2026
Guide**

Vivint has some of the
most advanced cameras

02/04/2026

The budget-friendly Tack GPS tracker works in 120 countries and costs just \$3 to \$7...

Learn how to install and set up the Ring Battery Doorbell Plus with our step-by-step...

LogicMark Freedom Alert Max proved to be...

in any security system. Find out what...

Home Security

About

Contact

Press

News

Deals

Home Security

Family Safety

Senior Safety

Internet Security

Home Safety

Smart Home

Car Safety

Pet Safety

Personal Safety

Emergency Prep

Stay Safe!

Subscribe to SafeWise for updates on safety news, product releases, and deals!

By signing up, you agree to our Terms and Conditions and Privacy Policy | Cookies Settings

Terms of Service | Privacy Policy | How We Rank and Review |  Your Privacy Choices

*SafeWise has conducted impartial research to recommend products. This is not a guarantee. Each individual's unique needs should be considered when deciding on chosen products.

© 2026 SafeWise. All rights reserved.