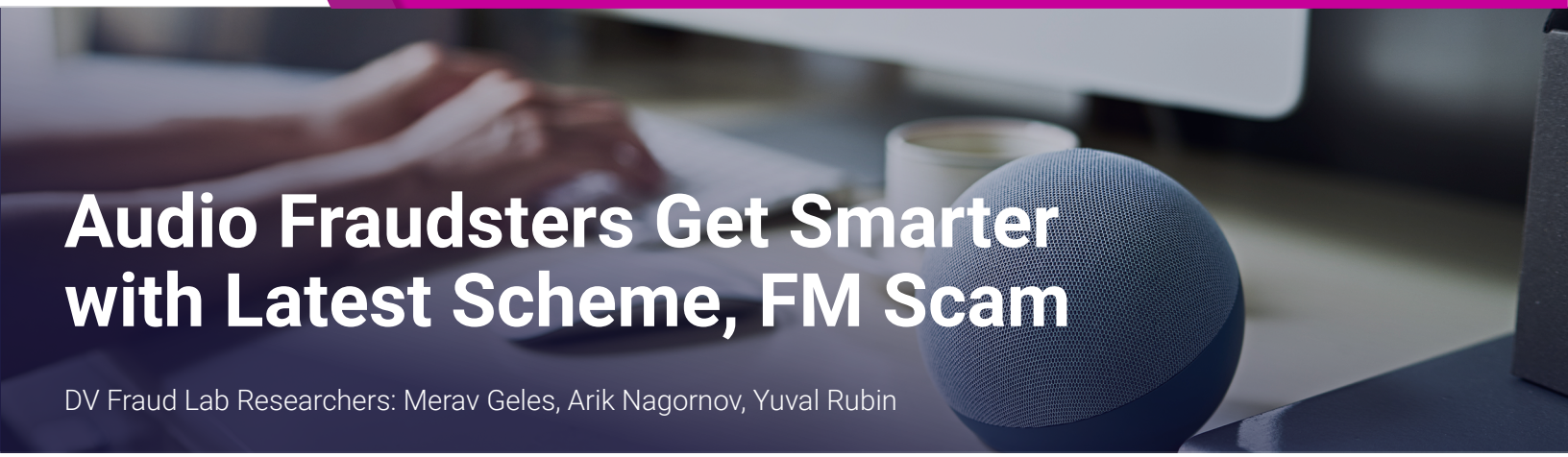


Audio Fraudsters Get Smarter with Latest Scheme, FM Scam

DV Fraud Lab Researchers: Merav Geles, Arik Nagornov, Yuval Rubin

Second Large-Scale Ad-Impression Scheme Targeting Audio Begins Spoofing Smart Speakers and Mimicking Listener Sessions

Audio, as an emerging media channel, is quickly becoming a lucrative target for fraudsters looking to avoid detection. The latest scheme to exploit this new frontier is FM Scam, which The DV Fraud Lab has successfully identified and mitigated using a proprietary combination of AI-powered technology and human review.

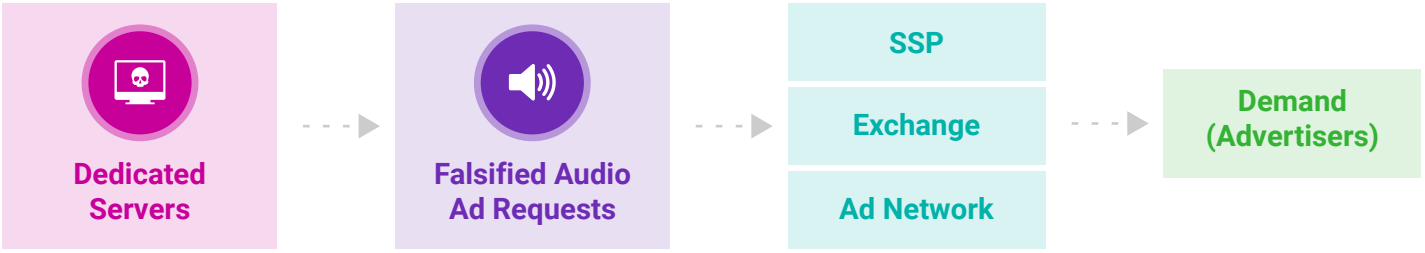
FM Scam is the second major global scheme to target audio spending. It emerged shortly after The DV Fraud Lab eliminated the first significant scheme, BeatSting. At their peak, these schemes were draining over $1 million every month from unprotected advertisers.

How FM Scam Operates

FM Scam operates by falsifying audio traffic through dedicated servers. The fraudsters behind this scheme then spoof different types of devices and players associated with playing audio content. Through these spoofed devices and players, they attempt to make their invalid traffic blend in with legitimate traffic and remain undetected by more closely mimicking human behavior. Fraudsters auction this invalid traffic through supply-side platforms (SSPs), exchanges and ad networks. FM Scam is generating an alarming 100 million ad requests per month, according to DV's estimates. This underscores the adaptability of fraudsters and the growing challenges in the audio space.

Audio Falsification Using Fake Servers That Send Ad Requests Containing Spoofed Device Details

FM Scam evolved in key ways to surpass its predecessor, BeatSting, in sophistication.



Fraudsters operate dedicated servers and falsify audio ad requests

Comparing BeatSting to FM Scam: Key Advances in Audio Fraud

	BeatSting (Active 2021-2023)	**FM Scam** (Active 2022-Present)
Level of sophistication	**Medium**	**High**
Spoofed devices	Spoofing mobile devices	Spoofing a wide range of devices and audio players, including CTV devices and smart speakers
Evasion techniques	Basic evasion techniques, such as rotating quickly between spoofed devices, which makes the invalid traffic easier to detect	Enhanced evasion techniques, such as spoofing continuous sessions that mirror the activity of real users and allow an attack to blend more effectively with legitimate audio traffic

Shutting Down FM Scam

When FM Scam emerged, The DV Fraud Lab quickly tied IP addresses used by the attack to a CTV scheme first detected in 2019. A portion of the IPs were further associated with a variety of malicious activities across many verticals including the spread of malware. The DV Fraud Lab immediately mitigated FM Scam's attacks and has been continuously shutting down new variants of this scheme through a strong combination of AI-powered technology and human review.

The Evolution of Audio Fraud

In March 2024 alone, FM Scam spoofed over 500,000 devices. Part of the scheme's sophistication involves spoofing a wide range of popular devices used for audio streaming including different types of audio players and smart speakers, mobile phones and tablets, CTV devices and even smartwatches. Notably, this is the first instance where The DV Fraud Lab observed fraudsters spoofing popular smart speakers. Spoofing a wide range of audio streaming devices allows the fraudsters to mimic typical usage patterns and better conceal their behavior.

The Evolution Of Audio Fraud: Spoofing Multiple Devices, Including Popular Audio Players, To Blend In With Legitimate Traffic

BeatSting
2021-2023

Type of devices spoofed

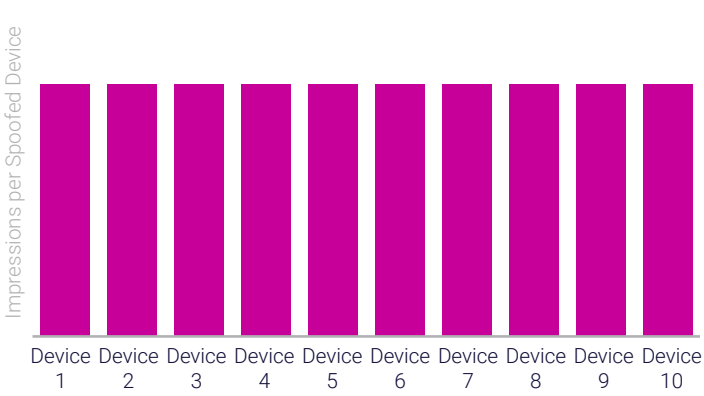
FM Scam
2022-2024

Type of devices spoofed

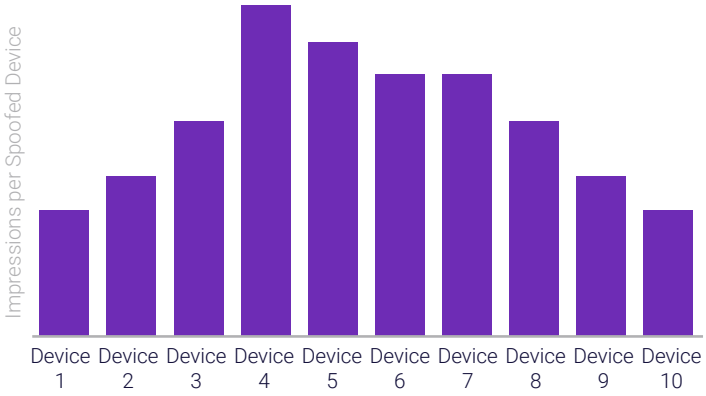
FM Scam further blends in with legitimate traffic by mimicking the behavior of a typical continuous ad session. Unlike BeatSting, which switches between devices after generating a certain number of impressions, FM Scam creates longer, uninterrupted sessions. This randomizes the traffic pattern to appear more human-like, as opposed to delivering a consistent, fixed amount of impressions across devices.

Traffic Patterns in BeatSting vs. FM Scam

BeatSting



FM Scam



Protecting Clients Against Fraud in Emerging and Established Formats

DV has been protecting its clients from fraud in emerging media since 2018. The DV Fraud Lab identifies and flags fraudulent impressions in real time, which helps quickly neutralize the monetary impact on DV advertisers and platform partners.

Leading the Charge Against Audio Fraud with Innovative Solutions

The usage patterns in the audio environment differ significantly from other media types, with a broader range of players and devices (e.g. smart speakers) that are sometimes exclusive to audio. As audio continues to grow, it becomes an increasingly attractive target for fraudsters. They frequently target emerging media that attracts advertising spend but lacks comprehensive measurement standards.

Innovation is the key to combating IVT in emerging media types. By leveraging a combination of AI-powered models and human review, DV has developed cutting-edge tools and algorithms to protect clients against fraud in audio.

Three Key DV Differentiators

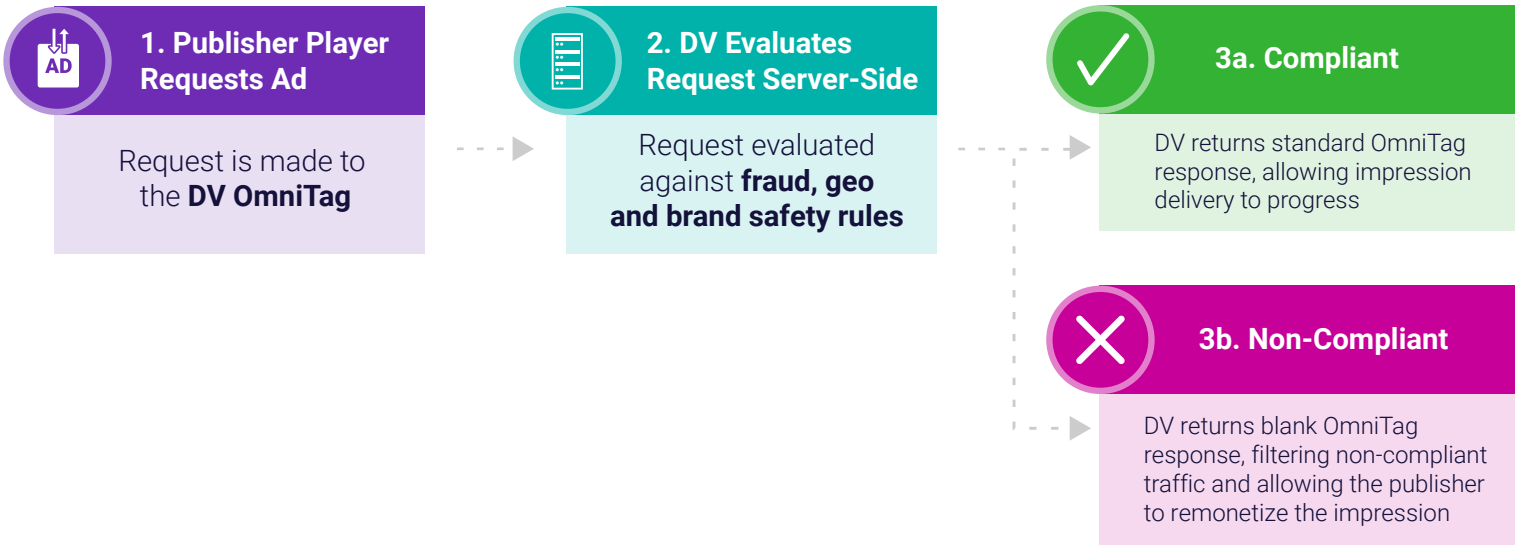
Advertisers working with DV are protected from fraud schemes and their variants. DV offers support for fraud on audio campaigns throughout the transaction, from pre-bid to filtering to post-bid blocking across formats and devices.

DV's key differentiators include:

1. DV Filtering

DV Filtering is an MRC-accredited, industry-first solution that works even in environments where VPAID blocking is not supported — such as CTV and mobile in-app. It evaluates data from ad requests and filters out unsuitable impressions to prevent advertisers from wasting their media investment, while still enabling publishers to monetize the placement with another, brand-suitable ad.

DV Filtering adds an additional layer of protection to video and audio campaigns by providing information that helps identify fraud schemes and how they morph. In this case, DV Filtering analyzed data provided by the server and client device that showed whether it was safe to serve the ad.



2. Sophisticated Tools and Algorithms

DV uses sophisticated tools and algorithms to accurately identify individual impressions that are the product of fraud schemes. Once identified, DV provides maximum brand protection throughout the media transaction — pre- and post-bid, across all media channels and device types. DV updates its internal fraud database globally within 8 minutes and its partner platforms over 100 times per day. Customers can see fraud impressions reflected in DV performance reporting as bot fraud activity.

3. The DV Fraud Lab

The DV Fraud Lab employs a rigorous process to evaluate and pinpoint ad fraud across all devices and environments. At any given time, The DV Fraud Lab monitors hundreds of data points on every impression, analyzing traffic patterns and leveraging numerous human-tuned algorithms to identify anomalies across billions of events.

Making the Internet **Stronger, Safer and More Secure**

The DV Fraud Lab is powered by a dedicated team of data scientists, researchers and analysts from the cyber fraud prevention community. The DV Fraud Lab detects and prevents new forms of fraud by using everything from AI and machine learning to manual review. Through continuous analysis, scenario management and research, The DV Fraud Lab pinpoints the sites, apps and devices responsible for fraudulent activity — and then updates protection for advertisers in real time.

To learn more about our fraud solutions and how we help advertisers protect their brands and publishers protect their inventory, reach out to **sales@doubleverify.com.**

LET'S CONNECT | Contact **Sales@DoubleVerify.com** or Visit Us at **DoubleVerify.com**