DoubleVerify Identifies BeatSting, the First Large-Scale Ad Impression Fraud Scheme to Hit Audio

Digital audio spend is steadily increasing, and fraudsters are paying attention. Early in the second quarter of 2022, the DV Fraud Lab detected a dramatic increase in fraudulent activity targeting audio channels, after initially noticing smaller instances of an attack in 2021. The scheme spiked a second time in January 2023, and The DV Fraud Lab again quickly mitigated the attack. This is the first time a fraud scheme, now known as BeatSting, has generated fake audio traffic at scale through large audio platforms.

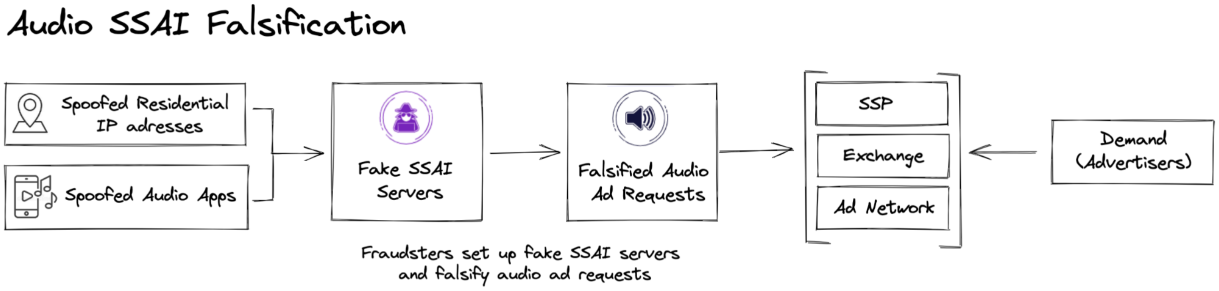
BeatSting is part of a larger family of server-side ad insertion (SSAI) fraud schemes that has been targeting CTV inventory since 2019. In SSAI schemes, fraudsters set up counterfeit SSAI servers and then manufacture inventory across an unlimited number of apps, IPs and devices. These fraudsters can spoof and rotate between millions of devices each day as they try to evade detection.

In total, this family of fraud schemes has siphoned over $20 million from advertisers since The DV Fraud Lab first identified it in 2019. And BeatSting alone is responsible for costing unprotected advertisers up to $1 million per month this summer.

How SSAI Falsification Works Across Audio

Audio SSAI falsification works similarly to SSAI fraud on CTV. Fraudsters begin by spoofing residential IP addresses and audio apps, all while setting up fake SSAI servers to falsify audio ad requests. This makes it seem like the apps have users and inventory on which advertisers would want to bid. These requests then go out to supply side platforms (SSPs), ad exchanges and ad networks (see *Figure 1*). If an advertiser wins a bid on this inventory through any of these platforms, their ad dollars are wasted on a fraudulent opportunity. By creating fraudulent inventory, fraudsters effectively siphon money away from legitimate audio channels.

Figure 1

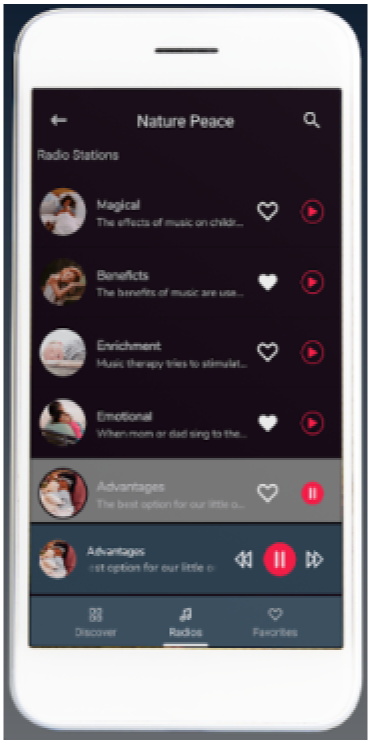

Audio SSAI Falsification
Spoofed Residential IP adresses
Spoofed Audio Apps
Fake SSAI Servers
Falsified Audio Ad Requests
SSP
Exchange
Ad Network
Demand (Advertisers)
Fraudsters set up fake SSAI servers and falsify audio ad requests

Identifying the First Large-Scale Audio Ad Impression Fraud Scheme

DoubleVerify has identified and measured fraud across digital audio ad traffic and display companion banners since 2016. And, today, The DV Fraud Lab identifies many types of sophisticated fraud schemes – including non-human devices, device farms and other illegitimate tactics that apply to audio inventory. But this is the first time fraudsters have used SSAI tactics to orchestrate large-scale impression fraud by falsifying audio traffic.

The fraudsters behind BeatSting typically spoof or falsify obscure mobile apps, such as generic streaming apps that have minimal downloads. Several of the apps associated with this scheme include com.digigrad.jazzmusic, com.digitalsquadra.rockmusic, video.games.radio and com.snkdigital.bakaradio. In total, the DV Fraud Lab identified over 60 apps tied to the scheme associated with three main publishers.

Figure 2: Screenshot of App Involved/Used As Part of the Attack


Nature Peace
Radio Stations
Magical
The effects of music on childr...
Benefits
The benefits of music are usa...
Enrichment
Music therapy tries to stimulat...
Emotional
When mom or dad sing to the...
Advantages
The best option for our little o...
Advantages
...st option for our little o
Discover
Radios
Favorites

Audio Fraud, the Next Frontier

The DV Fraud Lab experts use advanced machine learning and algorithms to quickly identify and flag spoofed traffic generated via rogue SSAI servers. In this case, the DV Fraud Lab observed an abnormally high volume of traffic with anomalous patterns across the spoofed apps. In other cases, apps that had not been updated for a long time and did not have relevant audio content were generating a suspicious volume of audio traffic.

In the early days of mobile and CTV schemes, fraudsters similarly used low-traffic apps as a facade for fraud. Two primary drivers behind the shift into SSAI audio fraud are likely:

1. Financial Opportunity

Fraud always follows the money – especially in emerging channels of digital advertising, where standards are developing and may not always be transparent to advertisers and networks. Fraudsters are often early adopters of new technology for this reason: non-standard integrations often provide an excellent way to circumvent fraud detection.

Ad volume and the opportunity for ad fraud in audio have grown in tandem with user adoption. Not only is digital ad spend increasing consistently, it is the fastest growing digital segment, according to the latest IAB Internet Advertising Report. In fact, it increased by 57.9 percent to $4.9 billion in 2021. Although this is a fraction of the total advertising spend, fraudsters will likely increase their activity across this channel as audio traffic continues to grow. This makes transparency and partnership between verification providers and platforms critical to protect ad dollars.

2. Ongoing Attempts to Evade Detection

Fraud schemes change tactics in attempts to remain undetected. Moreover, when schemes operate under the umbrella of a fraud family, different variants may take on different tactics. One of the most notable fraud families is OctoBot, a scheme that first became active in November 2019.

BeatSting also originated as a single CTV scheme in 2019. Since this family has not always targeted audio, it is possible the attack will again shift focus away from audio apps and potentially migrate fully back to CTV.

To date this year, the DV Fraud Lab detected and stopped an additional seven new SSAI variants aimed at falsifying CTV traffic. BeatSting's family of fraud schemes, in particular, has shown unusual mutations beyond the move into audio. Another scheme in the BeatSting family, LeoTerra, began attempting to hide its behavior by targeting Internet-of-Things (IoT) devices during H1 2022. The evolutions identified here show the lengths to which fraudsters will go in adapting their strategies to avoid detection.

Protecting Clients Against SSAI Fraud in Emerging and Established Formats

DoubleVerify has been protecting its clients from SSAI fraud since 2018 and SSAI fraud in CTV since 2019[1]. The DV Fraud Lab identifies and flags fraudulent impressions in real time, which helps quickly neutralize the monetary impact on DV advertiser and platform partners. And the BeatSting findings demonstrate that DV solutions also are protecting DV clients against SSAI fraud in audio.

Three Key DV Differentiators

Advertisers working with DV are protected from SSAI 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.

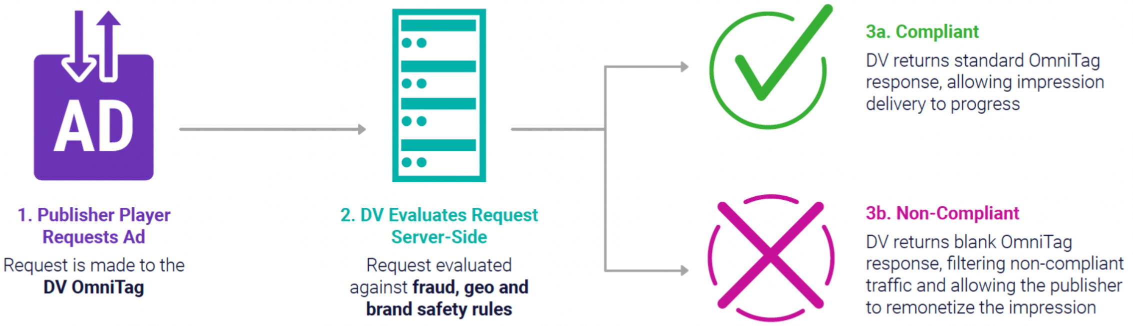
DV's key differentiators include:

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.

   Figure 3 shows how DV Filtering quickly determines whether or not an ad is compliant.

   Figure 3: How DV Filtering Works


AD
1. Publisher Player Requests Ad
Request is made to the DV OmniTag
2. DV Evaluates Request Server-Side
Request evaluated against fraud, geo and brand safety rules
3a. Compliant
DV returns standard OmniTag response, allowing impression delivery to progress
3b. Non-Compliant
DV returns blank OmniTag response, filtering non-compliant traffic and allowing the publisher to remonetize the impression

   DV Filtering adds an additional layer of protection to video and audio campaigns by providing information that helps identify SSAI schemes and how they morph. In this case,

[1] For a timeline of DV's history in SSAI fraud, see the appendix.

DV Filtering analyzed data provided by the SSAI 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 SSAI fraud. 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 SSAI fraud reflected in DoubleV performance reporting as bot fraud activity.

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

Making the Internet Stronger, Safer and More Secure

Neutralizing emerging fraud schemes reinforces our mission to make the Internet stronger, safer and more secure, thereby preserving the fair value exchange between buyers and sellers of digital media.

Should you have questions about this fraud scheme, please reach out to your DV account manager or Sales@DoubleVerify.com.

Appendix

DV's History of Identifying and Blocking SSAI Fraud

DV has a long history of identifying and blocking SSAI fraud. The timeline below highlights some of the most nefarious SSAI schemes.

2018: DV identifies and blocks Colorius, the first SSAI scheme.

2019: DV identifies and blocks the first three CTV and/or SSAI bot fraud schemes.

2020: SSAI bot fraud schemes become more prevalent and more sophisticated. During the second half of 2020, **LeoTerra**, a CTV scheme that evolved from the earlier, less-sophisticated CTV schemes, becomes predominant and exhibits many distinct phases and permutations.

2021: DV identifies two additional variations in LeoTerra, followed by a new scheme, **ParrotTerra**, which spoofs three times more devices and IPs than any previous SSAI scheme.

H1 2022: DV identifies **ViperBot**, an SSAI scheme that redirects verification tags to siphon CTV and mobile video ad spend. The Fraud Lab also discovers further variations in LeoTerra that begin spoofing IoT devices.