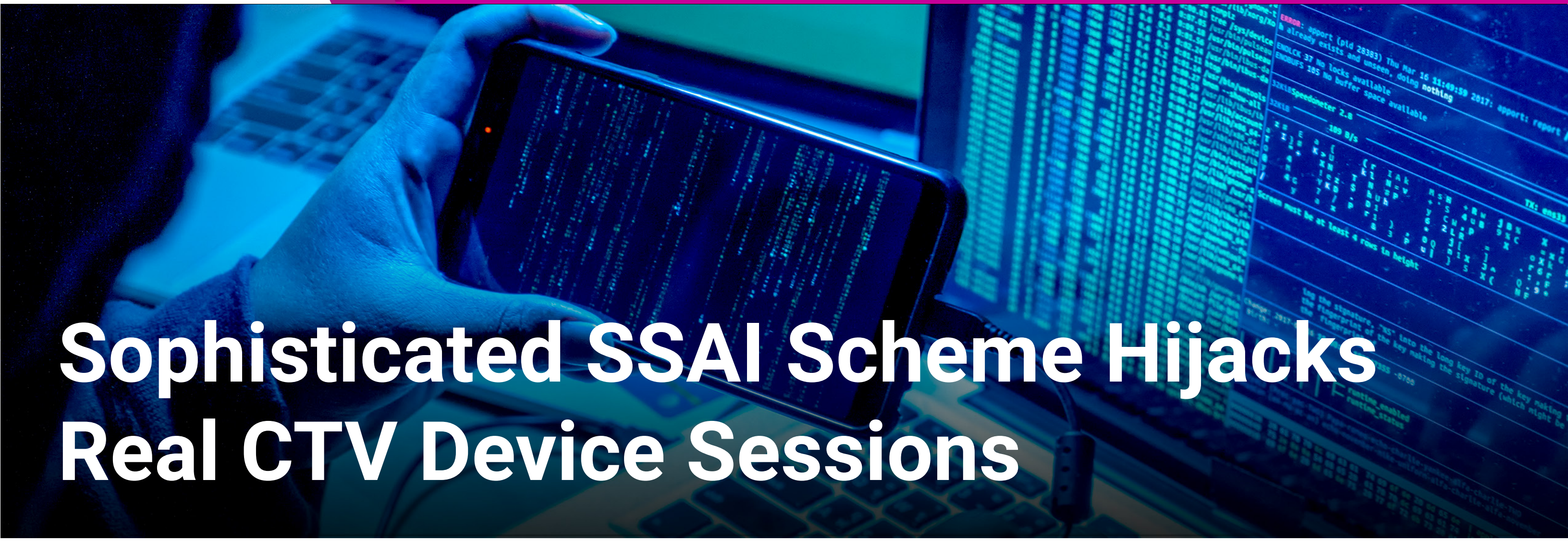
DoubleVerify

FRAUDLAB
FLASH REPORT



Sophisticated SSAI Scheme Hijacks Real CTV Device Sessions

DV's Fraud Lab has identified the first-ever server-side ad insertion (SSAI) scheme known to hijack real CTV device sessions. The scheme, SneakyTerra, operates by obtaining impression trackers from multiple ads through spoofed SSAI calls. The fraudsters then insert these impression trackers into one ad. With this ad, they bid on an impression opportunity that gets served to a real CTV device during a real user's viewing session. Although only one ad is seen, impressions for multiple ads are generated.

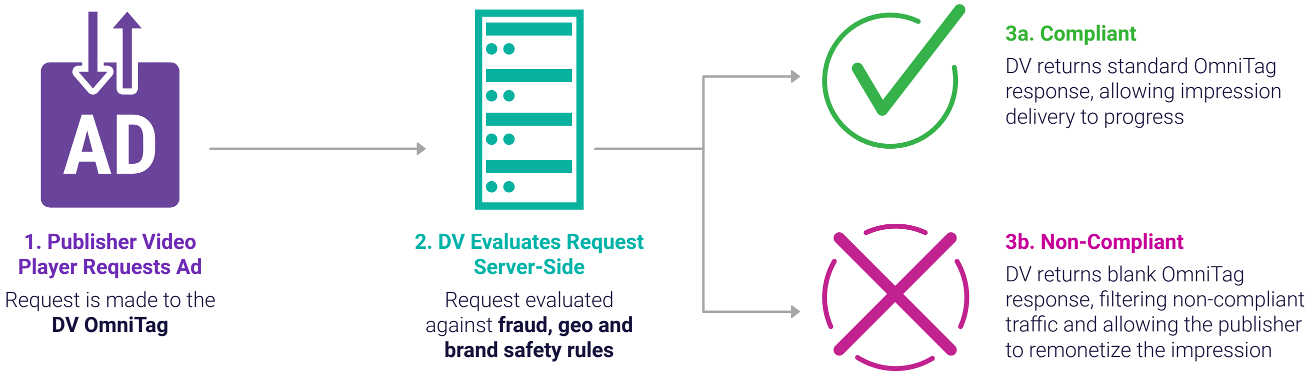
Catching SneakyTerra

SneakyTerra marks an important evolution in CTV fraud; because the ad calls associated with the scheme all serve on real devices, SneakyTerra is more difficult to detect than previous SSAI schemes. Despite the scheme's sophisticated tactics, however, the DV Fraud Lab caught SneakyTerra in October 2020 and has continued monitoring it throughout the first quarter of 2021.

DV Differentiator: DV Video Filtering

DV Video Filtering played a critical role in helping the Fraud Lab catch SneakyTerra. With DV Video Filtering, the Fraud Lab could see SneakyTerra's spoofed SSAI transactions before the fraudsters went to execute their impression on a real CTV device.

DV Video Filtering is an industry-first solution that provides a last-line of defense for advertisers in video environments, such as CTV, where blocking fraudulent, non-brand safe or non-brand suitable and out-of-geo impressions requires a technology standard called VPAID, which is not supported in CTV.



1. Publisher Video 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

Contact Sales@DoubleVerify.com or Visit us at DoubleVerify.com to learn more.

How SneakyTerra Goes Beyond Anything Seen Before

SneakyTerra's ability to hijack real sessions on real CTV devices was meant to mask fraudulent behavior and make detection more difficult. To understand what makes SneakyTerra such a pivotal fraud scheme, it's helpful to ask why SSAI fraud is evolving and how, specifically, did SneakyTerra evolve.

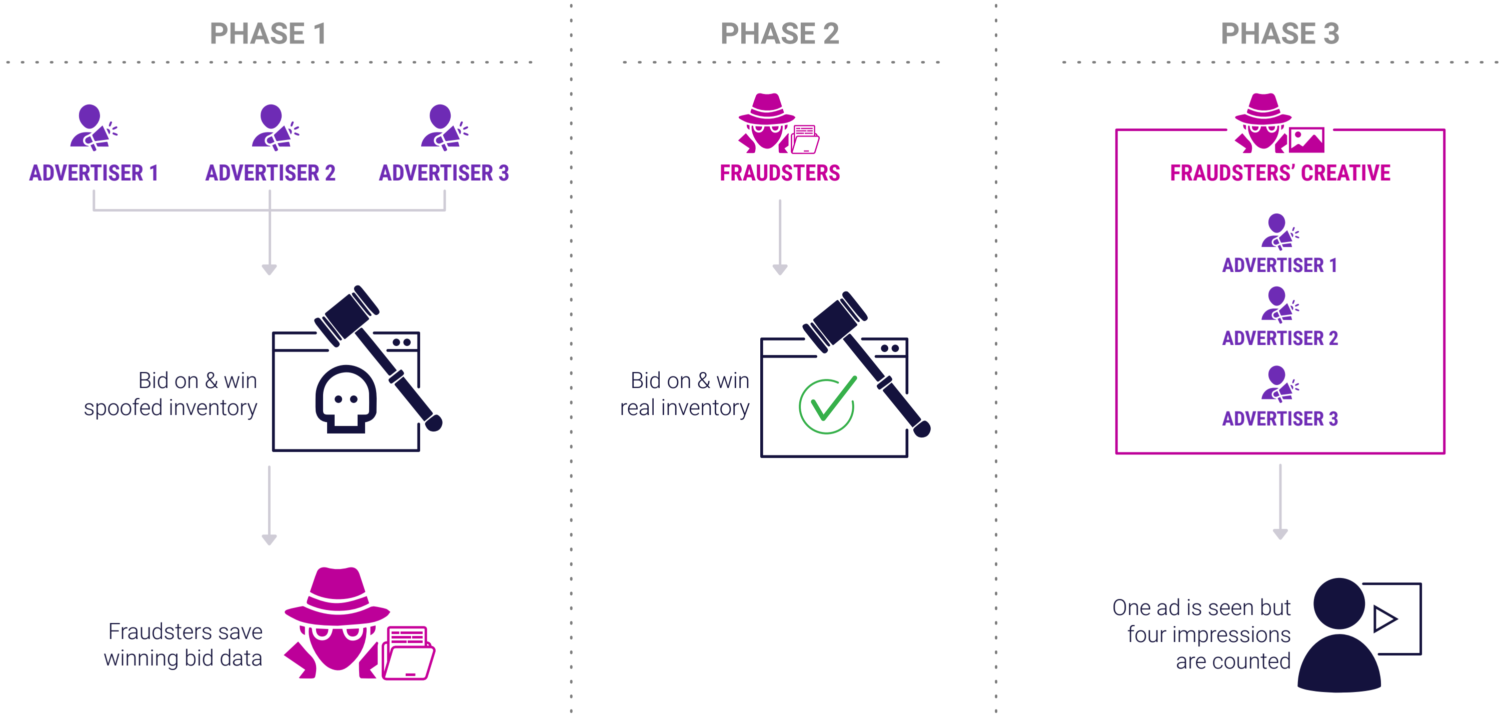
Understanding Why SSAI Fraud Is Evolving

DV's experts in the Fraud Lab use advanced machine learning to quickly identify and flag spoofed traffic that is generated via rogue SSAI servers. Even when fraudsters have previously attempted to evade our detection by mutating or changing their initial approach — as we've seen with other large schemes such as **LeoTerra and ParrotTerra** — the Fraud Lab quickly identifies the schemes. Over the past year, the Fraud Lab has caught and stopped 12 SSAI schemes. This means fraudsters have had to adapt their strategy in order to avoid detection.

SneakyTerra's New Tactics

SneakyTerra exhibits multiple advanced components, all meant to increase the fraudsters' earnings and make detection more difficult.

Imagine the following scenario that takes place in three phases:


PHASE 1
ADVERTISER 1
ADVERTISER 2
ADVERTISER 3
Bid on & win spoofed inventory
Fraudsters save winning bid data
PHASE 2
FRAUDSTERS
Bid on & win real inventory
PHASE 3
FRAUDSTERS' CREATIVE
ADVERTISER 1
ADVERTISER 2
ADVERTISER 3
One ad is seen but four impressions are counted

Phase One: Executing SSAI Fraud

- Three advertisers, Advertiser 1, Advertiser 2 and Advertiser 3, all bid on what they think is a real impression opportunity and then win their respective bids. In this case, however, the impression data has been spoofed by fraudsters — meaning the opportunity isn't real.

Phase Two: Storing Winning Bids

- After perpetrating SSAI fraud, the fraudsters behind SneakyTerra store the winning bids and the associated ads for future use.

Phase Three: Carrying Out Fraud on a Real Device, During a Real User-Session

- Posing as middle men, the fraudsters behind SneakyTerra buy a legitimate impression over an exchange for their own ad.
- Then, the fraudsters incorporate the stored impression signals from Advertiser 1, Advertiser 2 and Advertiser 3 into their creative.
- When the fraudsters' creative is served to a real user during a CTV session, the impression trackers for Advertiser 1, Advertiser 2 and Advertiser 3 fire along with the fraudsters' ad. Only the fraudsters' ad is seen, but instead of counting one impression, four impressions are counted.

The use of purchased impressions — stuffed with multiple fake ads that will never be seen by a real person — makes SneakyTerra more difficult to detect. Ad servers and measurement vendors get real data on where the ad served, rather than spoofed SSAI data, because SneakyTerra's stuffed impressions serve on real devices

Potential Impact

After first identifying SneakyTerra in October 2020, the Fraud Lab continued to track the scheme closely. In January 2021, SneakyTerra expanded as the fraudulent actors gained the ability to spoof additional CTV inventory in multiple environments.

In attempts to evade detection, SneakyTerra used numerous parameters that were carefully spoofed to mimic the hijacked real-device sessions. It expanded its reach into spoofing more operating systems than any previous scheme. At its peak, SneakyTerra was spoofing over 2 million devices each day and may have cost unprotected advertisers more than $5M per month, based on an average **$20 CPM** across CTV.

Importantly, DV clients remained protected during SneakyTerra's expansion, but this expansion meant the fraudsters behind SneakyTerra were able to trick more unprotected advertisers into placing bids on spoofed inventory in step one of their scheme.

2M

Devices Spoofed Each Day by SneakyTerra

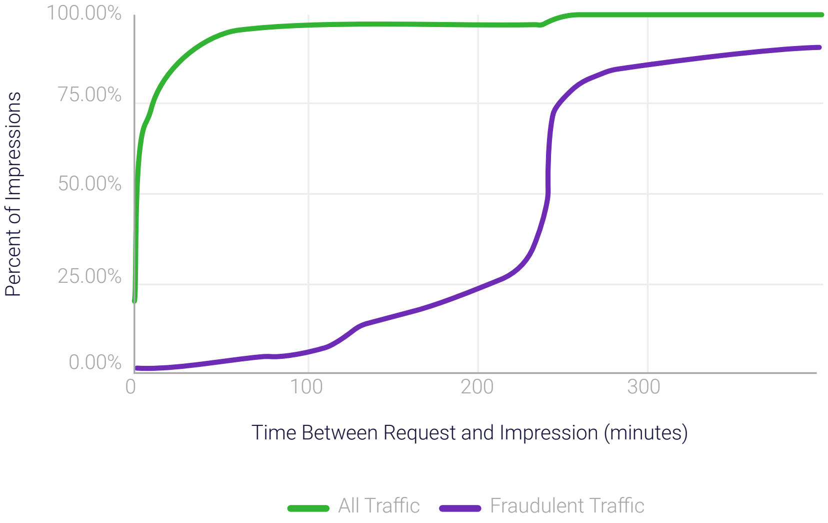
How DV Is Protecting Clients Against SneakyTerra

Despite SneakyTerra's unprecedented level of sophistication in spoofing and evasion techniques, DV's Fraud Lab
is able to identify and flag fraudulent traffic.

Identifying and Blocking Counterfeit Servers

The Fraud Lab is adept at blocking counterfeit SSAI servers and quickly developed an algorithm that identifies SneakyTerra's requests.

The graph on the right juxtaposes **SneakyTerra's requests** against legitimate traffic. When a legitimate buyer purchases an impression, in most cases, the ad pixel fires almost instantly after the request. SneakyTerra's fraudulent requests, however, show a delay of about 240 minutes. The Fraud Lab believes the sources of this delay are all attributed to the fraudsters' attempts to evade detection and increase their operational efficacy.



Real-Time Updates

The Fraud Lab shares device signatures in real-time with our partners, which effectively blocks the scheme from affecting any DV client using our avoidance, monitoring, blocking and filtering solutions.

DV Video Filtering

As explained above, DV Video Filtering is uniquely suited to detect and block this scheme. Video Filtering adds an additional layer of protection to video buys. In this case, Video Filtering helped catch SneakyTerra by analyzing data provided by the SSAI server or client device to determine if it is safe to serve the ad.

Let's Build a **Better Industry**®

Neutralizing emerging fraud schemes demonstrates our commitment to power the new standard of marketing performance across devices, formats and ad delivery platforms by offering advertisers clarity and confidence in their digital investment.

Should you have questions about this fraud scheme, please reach out to your DV account manager.