FRAUD FOLLOWS THE MONEY: **DV IS ROOTING OUT FRAUD ON CTV APPS**

Connected TV (CTV) ad spend in the U.S. is projected to grow by over 50% this year, reaching $20.1 billion, Tru Optik estimates.

Unfortunately, the adage holds true – fraud follows the money. This is especially the case within emerging channels, where standards have yet to be established, independent measurement isn't broadly adopted and demand outstrips supply.

DV identifies over 500,000 fraudulent CTV devices per day and has identified over 1,300 fraudulent CTV apps in the past 18 months. More than half of these apps have been flagged in 2020 alone, illustrating just how quickly fraudsters are turning to CTV. We've also identified that app stores on premium platforms are often unwitting enablers of CTV app fraud, as a result of the legitimacy these platforms confer.

500K+

FRAUDULENT CTV DEVICES IDENTIFIED BY DV PER DAY

Why Have CTV Apps Become a Source for Fraud?

Online video has seen massive audience gains since the near-global lockdown, according to reporting from eMarketer. Greater demand, coupled with the near halt in TV production, is driving the need for more content. Yet it is incredibly expensive to produce new broadcast-quality content.

Enter public domain content. Such content already exists and is not protected by copyright law or other restrictions. Silent films, old westerns and vintage cartoons, for example, are often in the public domain because their copyrights have expired.

Since public domain content can be copied, shared, altered and republished at no cost, it can easily and freely be repurposed in a CTV app by anyone – including fraudsters.

How Is App Fraud Committed Using Public Domain Content?

After identifying public domain content that can be copied and repackaged, fraud takes place in three stages:

1. App Creation

To create their apps, fraudsters can find developers on freelance marketplaces that will repackage long-form content for a few bucks. Or they can also do the work themselves, by exploiting CTV platform tools designed to help publishers easily upload their content.

2. Legitimacy Cloaking

After creating an app, fraudsters submit the app to stores on premium platforms such as Amazon Fire or Apple TV to tap into the platform's credibility and association with legitimate advertisers.

Now, they can leverage the halo effect of being accepted by premium platforms to lower the barrier to entry required to create a selling account on direct and indirect monetization platforms.

3. Fake Usage

Because of the way most CTV ad inventory is delivered (via SSAI), information about the placement is often self-declared. Advertising systems rely on the data sent by the seller to decide how to target and serve ads. This means once the fraudulent apps are part of the ecosystem, they can send ad requests that claim to be from apps running on real CTV devices in people's homes – when in fact very few real humans ever installed or used the apps.

There are two main paths to generating fake traffic:

- Set up fake SSAI servers, or use existing ones, to completely falsify all the information about an impression opportunity (e.g. app/IP/device/etc.) and generate fake traffic.
- Use schemes to create fraudulent inventory. This can be done through tactics such as reselling display impressions as video impressions or by manipulating information about the environment (e.g. app/IP/device/etc.) to make real desktop and mobile video impression opportunities look like they're originating from CTV devices.

Simply put, fraudsters use public domain content to create apps, and they generate fake impressions and fake impression data. Then they monetize this fake traffic through selling accounts associated with their apps that have been accepted by a legitimate CTV platform.

What Is DV Doing to Root Out CTV App Fraud?

By identifying the patterns in how app fraud is perpetrated on CTV, we are able to apply our solutions throughout the buying process – from pre-bid avoidance to post-bid measurement.

For example, we combat fraud on CTV by:

- Identifying IPs that are used for SSAI-served ads.
- Distinguishing between valid SSAI IPs and fraudulent, non-human data-center traffic (where the client IP is not provided).
- Pinpointing cases of fraudsters manipulating an IP address to make it appear valid.

But to truly clean up the ecosystem, we need third-party, client-side verification across CTV platforms and app ecosystems.

In the absence of measurement on direct buys, it is impossible for DV to validate that the fraudulent impressions we see are monetized solely through programmatic/indirect sales channels. Further, it is not possible for DV to identify and prevent the association of any brand with these fraudulent apps when we are unable to monitor the ad program.

What Can Advertisers Do?

You can take the following steps to protect your brand:

☑ 1. Make sure the platforms you're buying from – whether programmatic or direct – allow independent, third-party ad verification.

☑ 2. Advocate for standards and work with partners to adopt the IAB Tech Lab's OTT/CTV App Identification Guidelines and VAST macros for consistency and enhanced transparency into your buys.

☑ 3. Work with platforms certified by DV for CTV fraud detection.

Together, we can eradicate fraud within the CTV advertising ecosystem – contact Sales@DoubleVerify.com today to learn more about our CTV solutions.

Let's Build a Better Industry®!