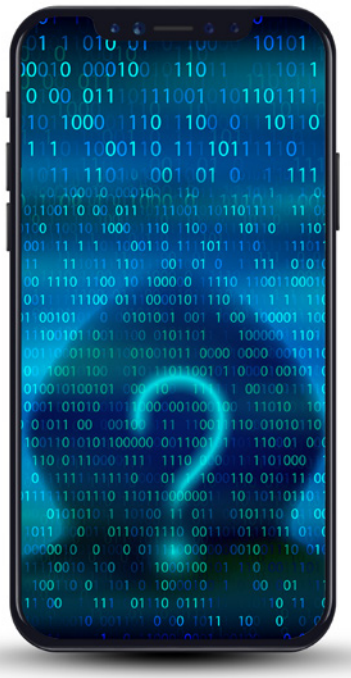
ORACLE
Data Cloud

THE ESSENTIAL GUIDE TO PROTECTING YOUR AD SPEND FROM INVALID TRAFFIC



Introduction

Invalid traffic (IVT) is endemic in online advertising and inflates an advertiser's budget with ad clicks or impressions that were never seen by a valid user.

While growth and sophistication of fraud is significant, not all IVT is fraud. Much is simply a side effect of the digital ecosystem, and the shift to programmatic is only increasing the challenges. However, whether a direct media buy or a programmatic campaign, marketers should not pay for impressions that are considered invalid.

In this white paper, we will break down the state of invalid traffic, explain what the industry is doing to solve for it, and show how you can educate yourself to keep your budget safe.

What is invalid traffic?

A big myth is that all IVT is only fraud, when in fact it is most commonly clicks or impressions that artificially inflate an advertiser's budget or a publisher's earnings. When it's malicious, like in the case of domain/app spoofing, both advertisers and publishers can be victims. While fraudulent tactics and ad fraud make headlines, it's important not to lose sight of the common and even unintentional forms of IVT.

In an effort to help advertisers guard against IVT, the Media Rating Council (MRC) launched the IVT accreditation in 2015 to help prove the effectiveness of measurement providers on IVT for desktop, mobile web, video, and in-app mobile. There are two mutually exclusive categories:

1. **General Invalid Traffic (GIVT)**
   Identified through routine means of filtration executed through application of lists or with other standardized parameter checks.
2. **Sophisticated Invalid Traffic (SIVT)**
   Difficult-to-detect situations that require advanced analytics, multi-point corroboration/coordination, significant human intervention, etc., to analyze and identify.

While the MRC accredits organizations for SIVT and filtration methodology overall, it's important to understand the differences between the two:

GIVT

- Known data center traffic
- Bots, spiders, and other crawlers
- Activity-based filtration
- Non-browser user-agent headers or unknown browsers
- Pre-fetch or browser pre-rendered traffic (unless never counted as a gross impression)

SIVT

- Bots and crawlers pretending to be legitimate users
- Hijacked devices and user sessions
- Invalid proxy traffic
- Adware and malware
- Incentivized manipulation of measurements
- Falsely represented sites and ads
- Cookie stuffing
- Manipulation or falsification of location data

While GIVT is a thorn in the side of advertisers, SIVT is the larger threat—harder to detect, and strong data and methodology is needed to measure against it.

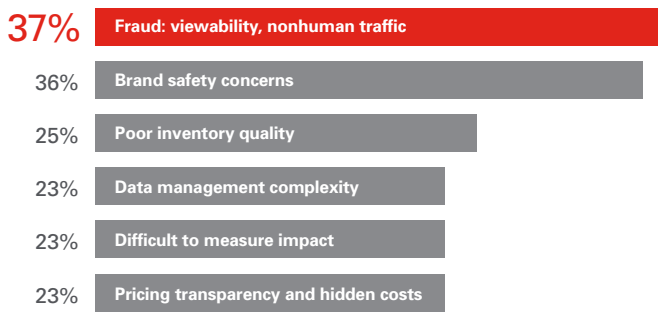
Why advertisers care about IVT

Digital campaigns have evolved since the inception of the internet, and more so since the launch of programmatic. Adding mobile web and apps to the equation creates an unlimited number of loopholes for bots and fraudsters to attack. Given these factors alone, it's not hard to see why advertisers have lost trust in the old ways of measuring their campaigns. Changing attitudes toward the quality of softer metrics like clicks, as well as the overall losses to advertisers for fraud—reported as $19 billion in 2018— illustrates the inherent challenges in digital that advertisers and publishers need to be educated about so they can understand the solutions.

Per eMarketer, 37 percent of marketers and agencies identified viewability and non-human traffic as the worst aspect of programmatic in a 2018 Advertiser Perceptions survey, narrowly beating out brand safety concerns.

What are the worst aspects of programmatic ad buying for US agency and marketing professionals?

% of respondants, July 2018[1]

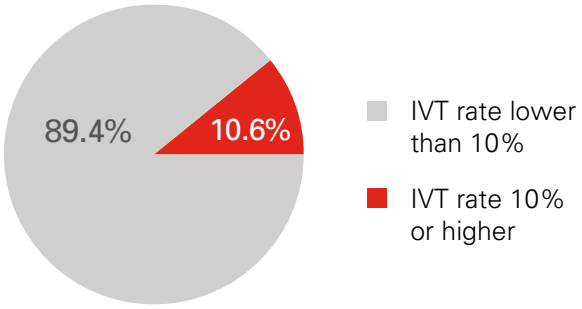


[1] Advertiser Perceptions, "DSP Report Q3 2018," Nov 5, 2018.

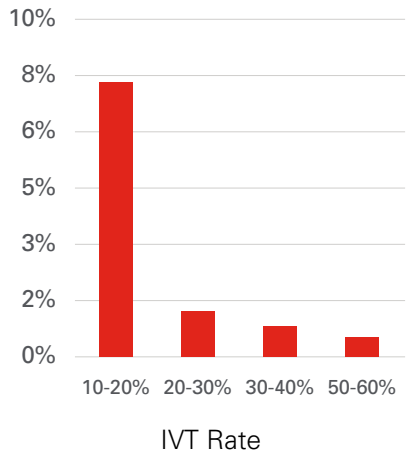
Setting the stage for combating IVT

Brands and agencies need to adjust the way they plan and measure their campaigns. No matter if the objective is brand awareness or sales lift, the first step is making sure you're reaching real users. Whether malicious or not, undetected IVT can devalue performance metrics, or worse, deplete budgets for which marketing organizations often fight so hard.

All measured channels



Channels with 10%+ IVT



Based on Oracle Data Cloud's Moat Analytics benchmarks, more than 89 percent of channels have less than a 10 percent IVT rate. However, more than 30 percent of the rest have more than a 20 percent IVT rate.

There are a host of suitors in waiting, vying for your business to help you identify valid impressions. Measuring IVT is not a one-size-fits-all solution. However, transparency is paramount in your search for a good partner. Brands, agencies, and publishers alike are challenging their partners to expose what's behind the curtain—that is, to go beyond the surface-level differentiators.

Methodology and transparency matter

Oracle Data Cloud's Moat Analytics deploys a unique methodology for SIVT detection and filtration that has been granted accreditation from the MRC for desktop, mobile web and, most recently, mobile in-app.

The methodology comprises nine client-facing categories, including:

GIVT

- Data Center Rate
- Spider Rate
- Excessive Activity Rate

SIVT

- Automated Browser Rate
- Incongruous Browser Rate
- Invalid Proxy Rate
- Invalid Source Rate
- Hidden Ad Rate
- Session Hijacked Rate

For each of the categories listed above, there are several methodologies used for Moat Analytics to determine whether it applies to an impression. These categories are thought of as padlocks to a valid ad impression. In other words, fraudsters—whether on desktop, mobile web, video, or in-app mobile—need to be able to unlock all the detection methodologies within each of these IVT categories before they can claim a valid impression. New methods are regularly added to continually improve each type of IVT detection.

At a high level, here's how Moat Analytics detects:

Data Center Rate: Whenever impressions come from IPs that we know belong to data centers, we can safely label them as invalid.

Spider Rate: The industry-standard IAB/ABC International Spiders and Bots List is used on each impression to identify invalid traffic that announces itself as such.

Excessive Activity Rate: When a user is generating too many impressions too quickly or has browsing activity that's too uniform to originate from a human, those impressions are flagged as invalid for as long as the suspicious behavior persists. Dynamic thresholds that update regularly are used to define what counts as invalid, using a methodology based on extensive research into the traffic characteristics of the billions of impressions measured each day.

Automated Browser Rate: Browser environments are inspected to identify impressions served to browsers that are driven by automation software, such as Selenium WebDriver; or "headless" browsers that are always automated, like PhantomJS.

Incongruous Browser Rate: Hundreds of browser properties are inspected, and those signals are compared with the user agent received from the user. We consider an impression invalid when we identify a mismatch in browser properties (i.e., a spoofed user agent). Our machine learning automatically identifies comprehensive sets of signals that enable robust incongruous browser detection as new browser updates are released.

Invalid Proxy Rate: Impressions that originate from IPs known to be used as proxies are invalid. Some proxies are exceptions to this, such as proxies owned by universities and corporations.

Invalid Source Rate: These are domains and apps that are known to generate only invalid traffic on an ongoing basis. This includes conditions proving that a legitimate-looking traffic source is being spoofed.

Hidden Ad Rate: These are conditions implying that certain ads could never have been seen by a user, such as those that are set to be invisible for their entire lifetimes. They are often caused by honest mistakes made by web developers rather than malicious activity.

Session Hijacked Rate: This covers cases where a real user's session is being manipulated to generate invalid traffic, such as impressions that occur inside pop-under browser windows, or impressions served on mobile devices where sensor data indicates that users have long stopped interacting with their phones.

Eliminate waste and stop serving ads to bots!

It's important to note that Moat Analytics's world-class IVT detection is part of a full suite of ad verification solutions that help advertisers plan, optimize, and measure campaign effectiveness, to help advertisers:

Protect ad spend before a bid is placed to ensure the campaign is set up for success from the start

Monitor IVT rates and the metrics that matter to the objectives, including automatic alerts when unacceptable IVT levels are reached

Ensure ads only appear in brand-suitable environments and targeted geographic locations with real-time, post-bid blocking

Differentiating powerful data signals

Oracle Threat Intelligence

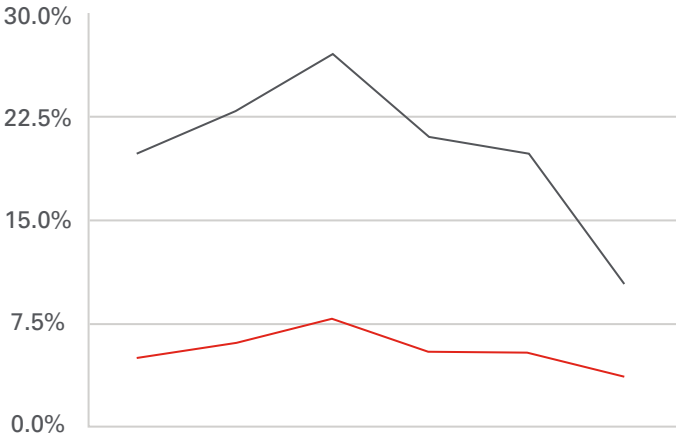
Moat Analytics offers the unique ability to detect the most advanced forms of automated bot and fraudulent activity through exclusive access to Oracle's global web security intelligence and experts that specialize in DDoS, DNS analytics, malicious Bot traffic, targeted web attacks, and newly emerged threats. This powerful threat intelligence and experience provides customers with vastly expanded detection of inappropriate malicious and non-malicious traffic that can affect website statistics and performance.

For example, Oracle's threat intelligence team can flag to Moat Analytics DDoS activity that is creating invalid traffic. With this information, Moat Analytics flags fraudulent apps, URLs, IPs, and traffic paths and patterns that promote fraud, as well as internet degradation that can affect ad load times and effectiveness.

Unique ability to avoid inaccurate IVT detection

Moat Analytics stands out with the ability to avoid false positives by leveraging the Oracle ID Graph. In one instance, we were 3.75x more accurate in avoiding false positives for a client, as the graph can flag a legitimate (or not) IP address with incredible accuracy.

False positives are detrimental to an advertiser's campaign, as they unnecessarily reduce reach by claiming that an impression is invalid.



Ad Age top 100 brand found a competitive IVT provider over-classifying domains leading to false positives.

Oracle was found to be

3.75x

More accurate

What now?

It's critical to protect campaigns from invalid traffic, whether it's a known spider providing a useful service or a nefarious ad fraud criminal network impacting publishers, advertisers, and consumers. Thwarting criminal enterprises that benefit from the anonymity of the web and the complexity of our digital ad ecosystem is an imperative. Along with partnering with the right measurement provider, here are some steps you can take to help in the fight:

1. Measure multiple metrics and connect them to outcomes.
2. Employ IVT avoidance technology where possible.
3. Set up your datasets to promote actions by helping identify and address questionable ad supply.
4. Work with your publishers to better understand the causes of IVT on their sites, and encourage them to manage it with tools like Yield Intelligence.
5. Test, learn, optimize, and repeat.

Contact your Oracle Data Cloud representative today to learn about our IVT detection solutions, or click here to request a Moat Analytics demo.