Whitepaper

CYBAGE
Delivering Value. Scientifically.

Proactive Campaign Monitoring Against Ad Frauds and Performance Anomalies

Table of Contents

Media agencies and advertisers are always engaged in safeguarding the brand reputation and media spend on Search, Display, and Video advertising. This white paper explains how proactive monitoring of media campaigns to detect fraudulent activity or performance anomaly can save both brand reputation and media spend. On the other side of the programmatic advertising spectrum, the reputation of entities such as demand side platforms (DSPs) and supply side platforms (SSPs) involved in trading of ads inventory can also be safeguarded through a proactive monitoring approach.

The key takeaways:

- Ad frauds and their impact on media quality
- Performance anomaly and its impact on media quality
- Proactive campaign monitoring to safeguard media spend
- Prevention of ad frauds and performance anomaly by proactive campaign monitoring

Intended audience:

- Brand owners and advertisers
- Media agencies and media planners

Executive Summary

"Half the money I spend on advertising is wasted; the trouble is, I don't know which half."

— John Wanamaker, considered the father of the U.S. department store.

Said more than a century ago, this statement still remains relevant today for many marketers. With the advent of programmatic advertising, marketers must contend with multiple stakeholders and work in a large gray zone of complexity and technological challenges, making programmatic advertising more prone to ad frauds and performance anomalies, resulting in low ROI.

This paper discusses the need to proactively monitor media campaigns against ad frauds and performance anomalies in digital advertising. It explains how proactive monitoring of campaigns helps various stakeholders (brands, supply side platforms, demand side platforms and publishers) to enable greater efficiencies, effectively deal with issues such as brands reputation, and safeguard the media spend.

INTRODUCTION

When a digital advertising campaign is about to take off, certain defined goals and metrics (Key Performance Indicators or KPIs) that indicate the success of the campaign are put in place. The campaign success depends on two factors:

- Meeting the defined KPIs
- Preventing ad frauds

In recent years, a significant number of digital media buying transactions have moved to programmatic buying platforms. The absence of inventory transparency in programmatic buying and selling of inventory through real-time bidding makes brand safety a daunting task.

The brand's reputation will take a nosedive if the brand's advertisement appears alongside inappropriate content. For example, a consumer brand's ad displayed in the form of a violent video or its appearance next to a racially-charged hate speech can malign the brand's reputation. A single ad displayed alongside inappropriate content can have the following consequences:

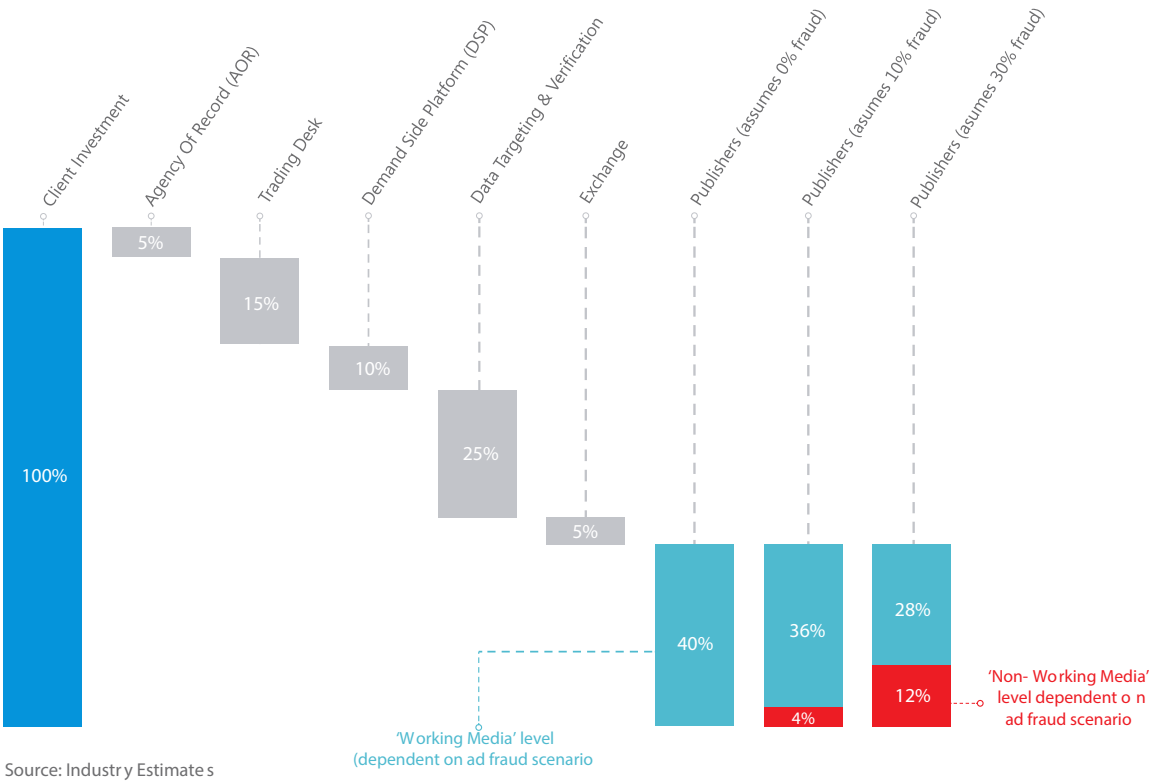
- Waste of ad spend because such an ad will not drive impact
- Damage to the brand's reputation
- Mistrust and reputation damage
- Public relations nightmare for the brand

On the other side of the digital advertising spectrum, DSPs and SSPs, ad-tech providers, and media aggregators are also concerned about safeguarding their reputation and revenue by deliberately not trading fraudulent impressions and inappropriate content. It is also challenging for them to ensure that advertisers purchasing media from their platforms are not presenting illegal, fraudulent, or inappropriate products and services. Therefore, pro-actively monitoring of campaign KPIs and safeguarding of campaigns against ad frauds is the need of the hour.

Proactive monitoring of campaigns can help detect anomalies and frauds at an early stage of the campaign before further damage is done and revenue is lost.

Typical Client Media Spend

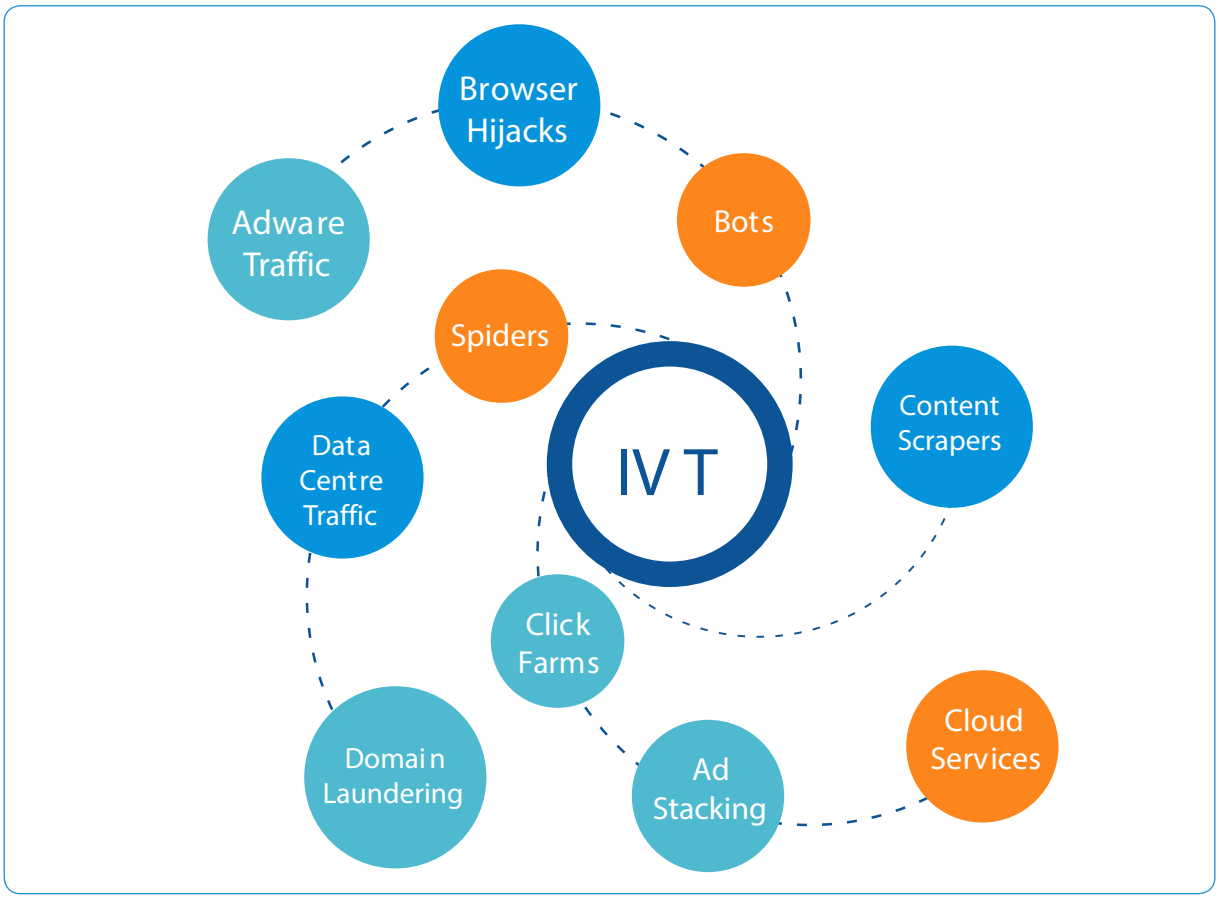
The media spend of the client is distributed in the following way.



What is Ad Fraud?

An advertisement (Ad) is the delivery of a message (promotional or awareness) to the right people at the right time and at the right place with a specific communication task to be accomplished among specific defined audience. For example, displaying an ad of latest mobile phone to a user planning to buy a one. Any deliberate activity to prevent the delivery of this message is referred to as ad fraud.

Most often, fraud refers to a certain traffic type that is not of publishers or ad tech partners, but forms a part of the supply chain. There are publishers with high proportions of fraudulent traffic and others with very low proportions. The following figure shows the various types of invalid traffic.



The ad fraud landscape is not constant: it keeps changing very often, for this week, it may concentrate on one site and on another site next week. Bot attacks can hit even premium publishers . Every traffic source requires constant re-evaluation, with some of the most common ad frauds as mentioned below:

1. Selling inventory automatically generated by bots or background mobile-app services
2. Delivering pre-roll video placements in display banner slots
3. Hiding ads behind or inside other page elements so that they can't be viewed by the user viewing the web page
4. Serving ads on a site other than the one provided in a real time bidding (RTB) request—this is known as domain spoofing
5. Falsifying user characteristics such as location and browser type
6. Hindering user engagement by frequently refreshing the ad unit or page

Ad Fraud Impacts

According to a study from the Interactive Advertising Bureau (IAB), 8.2 billion USD are lost in the US-market due to ad-fraud. About half of it is attributable to non-human-traffic; that is simulated ad impressions being paid for by advertisers, although no human being will ever see them. On top of that, 169

million USD are annually spent for the battle against ad fraud. Also researchers reporting ad fraud exposure between as low as 2% and as high as 90%, it seems clear that there are no widely available ways of assessing the absolute exposure rate.

One of the high-profile research initiatives into ad fraud was the recent 'Bot Baseline' led by the Association of National Advertisers (ANA) in USA. The cost of ad fraud is estimated at $7.2 billion in this report, or approximately 5% of the total global digital media market.

Although this is undoubtedly a hugely significant sum, primary research conducted by Botlab.io together with its academic partners and other third parties (a sample of which is outlined below), suggests that the scale of the problem may in fact be much more substantial:

- Eighty-eight percent of digital ad clicks deemed fraudulent
- Digital publishers lead all industries in bad bot traffic at 32%
- Bots inflate monetized audience by 5% to 50%
- Bot traffic is up to 61.5% of all website traffic
- Just one form of in-app fraud accounts for 13% of all in-app inventory
- 22% year-on-year growth for fraudulent bot traffic
- 40% of mobile ad clicks are essentially worthless
- Bot traffic rises for the first time to over 50% of total invalid traffic
- More than 18% of impressions/clicks come from bots

Source: https://www.wfanet.org

What is Performance Anomaly?

KPIs are measurable values used by marketing teams to demonstrate the effectiveness of campaigns across all marketing channels. From social media to email marketing to lead generation, the digital marketing strategy includes a number of activities. With such a wide variety of channels being used, it's important for marketing teams to actively track progress and performance in real time with accurate marketing metrics and KPIs. Anomaly occurs when any or all of the KPIs are not met. A few monitoring points for a display campaign are as mentioned below:

- Preflight campaign checks
- Page load monitoringBroken links monitoring
- Advertiser site availability
- Click Through Rate

In case of search engine marketing, monitoring points will be different. For example, consider an ongoing PPC campaign. Several internal and external factors will determine the success of this campaign. Some of the factors are as follows:

- Advertiser site availability
- Domain
- Approved ad copy
- Priority keywords
- Disapproved keywords
- No impressions on priority keywords

For the wellbeing of any media campaign and to get the maximum ROI, the data points have to be monitored periodically to check for anomaly.

Why is Pro-Active Monitoring of Campaigns Required?

- Ad fraud tops the list of concerns that have a direct negative impact on marketing campaigns.
- Ad fraud is likely to exceed $50 billion by 2025, even as a conservative estimate. Without sufficient countermeasures, it is easy to create scenarios in which ad fraud revenues reach $150 billion per annum in the same time frame.
- Virtually any programmatic ad buy transaction can be exposed to ad fraud. However, claims to the contrary should be treated with caution.
- Viral spam sites, providing little to no opportunity for advertising effectiveness, are endemic across the Internet. But ad fraud is also found among premium publishers; for example, in the form of sourced traffic. Low quality sourced traffic has become common place among publishers, often as a means to deliver campaign targets to advertisers.
- Advertisers lose out entirely from ad fraud, and unless effective action is taken, the issues related to this threat will continue to grow in magnitude and complexity. To protect advertisers from low quality inventory that will not be converted to customer.
- Media campaigns not monitored and updated periodically for KPI metrics will result in performance anomalies.
- Protect client's media spend from poor performing campaigns by taking timely corrective action.
- Provide visibility on campaign progress to all stakeholders on all the data points being monitored.

Challenges:

- Ad fraud is a complicated phenomenon that involves hackers, different software black markets, traffic brokers, and publishers with varying degrees of awareness. Not all aspects are explicitly illegal, and those that are, typically occur in countries with indifferent or ineffective cybercrime law enforcement.
- The main challenge in ad fraud is detection of the fraud as more intelligent bots exists that can mimic human behavior, click videos, submit forms and trigger conversion.
- The recent research findings of the World Federation of Advertisers have revealed, '36% of respondents say they don't know to what extent they are exposed to ad fraud'.
- With automation of processes in programmatic media buying led to emergence of a blackbox that consist of Agency Trading Desks, Demand Side Platforms and Ad-exchange Platforms. There is no transparency in transactions that happen within blackbox .
- A situation can arise wherein a publisher wants an ad from a particular ad network, but that specific ad network is not available in the ad mediation.
- End users might be subjected to repetitive ads.

CYBAGE'S PERSPECTIVE

There is no dispute that digital ad fraud exists. The digital advertising ecosystem is under evolving threat from bots. Also, no one disputes the existence of non-viewable ad impressions, many ads appear in the areas of sites that cannot be seen in part or whole by the intended audience. This issue is of extreme importance for all the stakeholders involved.

Many times, campaigns have to be monitored continuously and corrective changes done to live campaigns, depending on the campaigns' performance.

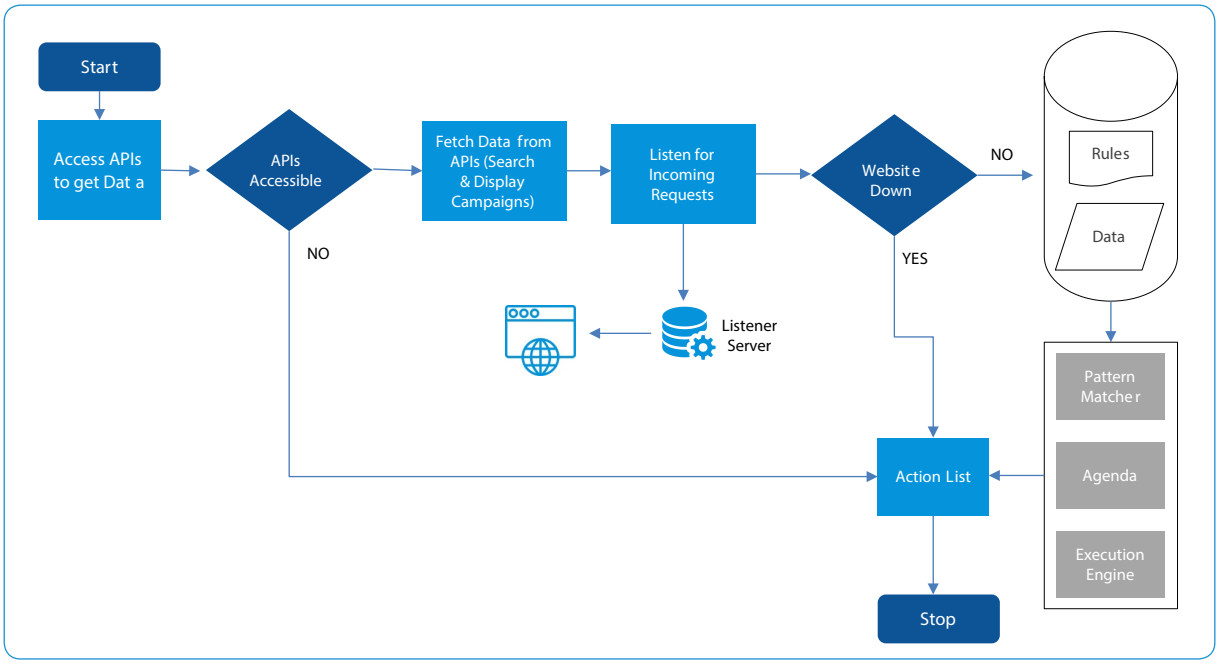
We believe that it is necessary to provide a validation mechanism to protect the media spend and reputation of the advertisers. It is necessary for the advertisers and agencies to invest in tools to protect themselves from ad frauds and performance anomalies.

Cybage has helped digital advertising businesses to build ground-up campaign monitoring applications to pro-actively monitor their media campaigns detect anomalies and frauds at an early stage of the campaign before further damage is done ..

A typical campaign monitoring tool or application consists of a rule engine with a predefined set of rules. This engine can be configured to data points. The rules are invoked based on the scheduled time interval and checks are carried out to ensure the preset condition is met; in case the preset condition is not met, the alerting mechanism sends alerts to the concerned user. Once the user is notified, corrective action is and further damage is controlled.

Proactive Campaign Monitoring Tool Functional Workflow:

Proactive campaign monitoring tool can be used by two types of users, namely, media planners and advertisers. At the heart of the campaign monitoring tool is the rule engine with a predefined set of rules and integrations with third-party applications to capture data points. A simple rule for a search campaign can be to monitor keywords not generating impressions and alert the user by email or SMS.



The chronology of the activities in monitoring campaigns is as follows:

1. Rules are defined based on performance metrics and suspicious activity.
2. The system is configured to retrieve performance data and fraud intelligence data through APIs.
3. The system is configured to retrieve campaign data from the campaign management platform.

4. Predefined rules are mapped to campaigns against performance anomaly and ad fraud.
5. Rules are scheduled for periodic intervals, depending on the campaign type and rule type.
6. Rules are invoked on the time mentioned in the schedule, data is retrieved from the third party, and the rule engine looks for preset value match in case of performance anomaly and suspicious data in case of ad fraud.
7. In case the data pattern matches, action is taken as defined in the action list.
8. Here, an alert message is sent to the concerned user group and changes can be made to the campaign to prevent further damage. These changes can be done from the tool itself or the user can log on to the required application and make the changes. Also, corrective action can be taken to control damage.
9. A dashboard gives complete visibility into campaigns progress, rules executed alerts or actions triggered.

Business-level Benefits:

- Increased ROI on media spend.
- Improved overall customer ad experience.
- Protection of the advertiser's reputation and media spend.
- Performance is monitored and alerts are sent through email and/or text messages when the performance is not in line with the KPI expectations.
- Visibility for clients into all the data points being constantly monitored on their behalf.
- Availability at one place of all critical information required to manage campaigns, and stop important information from reaching users through different, disparate systems.
- Ads are not displayed alongside or with inappropriate content.

CONCLUSION

Preventive steps to protect media campaigns against ad frauds and performance anomalies reduce the efforts needed to deal with the consequences of not doing so. The consequences include poor performing campaigns and waste of media budget.

A tool or application to monitor media campaigns can help brands and media agencies to protect the media spend and safeguard brand reputation. With continuous monitoring of data points and timely information updates (alerts) on the performance of a campaign, media planners can act proactively and steer the campaign to success and maximize the ROI by making the required changes. Also, with information alerts on suspicious traffic, brand reputation can be protected and wasteful spend of media budget avoided.

CYBAGE
Delivering Value. Scientifically.

Cybage Software Pvt. Ltd.
[ISO 27001 Company]
India | USA | Canada | UK | The Netherlands | Germany | Japan | Australia | Singapore

www.cybage.com