Whitepaper

CYBAGE
Delivering Value. Scientifically.

FIGHTING **AD FRAUD**

Table of Contents

Introduction 03

Impact of Ad Fraud 03

What is Ad Fraud? 05

How to Detect Ad Fraud? 07

How to Fight Back Against Ad Fraud? 09

Introduction

The year 2017 promised a good landscape for the ad tech industry, as the Association of National Advertisers (ANA) presumed that ad fraud would drop from **$7.2 billion** in 2016 to **$6.5 billion** in 2017, but the presumption was short lived when new facts started pouring in and defined a different tale altogether.

Adobe monitored traffic across thousands of its client sites and found that 28% of the traffic showed “non-human signals” indicating that it was fraudulent.

Bob Hoffman of The Ad Contrarian predicted that advertisement (ad) fraud may reach **$66 billion** in 2018, which is whopping 10 times more than the **$6.5 billion** thought about in 2017 by the ANA.

This white paper discusses the various areas Ad fraud has impacted in the digital landscape and the techniques, which the industry is using or can use to fight the same.

Impact of Ad Fraud

- Ad fraud has been significantly marring the online ad tech industry, be it digital, mobile, or video ads.
- Digital ad fraud remains rampant – an estimated $19 billion was lost on display ads alone in 2018, a figure that will rise to $44 billion by 2022, according to a research conducted by Juniper.
- Video ad fraud is roughly twice as common when compared to display. As per reports from a leading third-party media verification company DoubleVerify, approximately 10% of the video impressions scanned in North America were found to be fraudulent (on the contrary only 5% of display impressions were marked as fraud).
- Video ads are currently the most profitable module in the advertising game, while being the most vulnerable to bot fraud.

- With an incredible increase in the number of mobile users, mobile ad fraud is rising equally, as is the ad spend in that segment. 2018 saw a rise in mobile ad fraud and the financial exposure to ad fraud hit $800 million. Ad spend in mobile has already exceeded the ad spend on desktop, with 60% of global digital advertising budgets being attributed to mobile advertising in 2018.

- The sheer increase in the spend ratio for mobile advertising has created a conducive environment for fraudsters.

- **Pixalate** (a fraud protection provider) collected global programmatic advertising data between May – Aug 2018 to measure Invalid Traffic (IVT) rates across devices and channels. Their data revealed that the mobile in-app video on both smartphones and tablets was the riskiest environment for the advertisers.

Estimated Global Ad Fraud Rates by Format and Transaction Type

when it comes to programmatic, mobile display inventory presents the highest risk of fraud.

Detected Rate of Ad Fraud

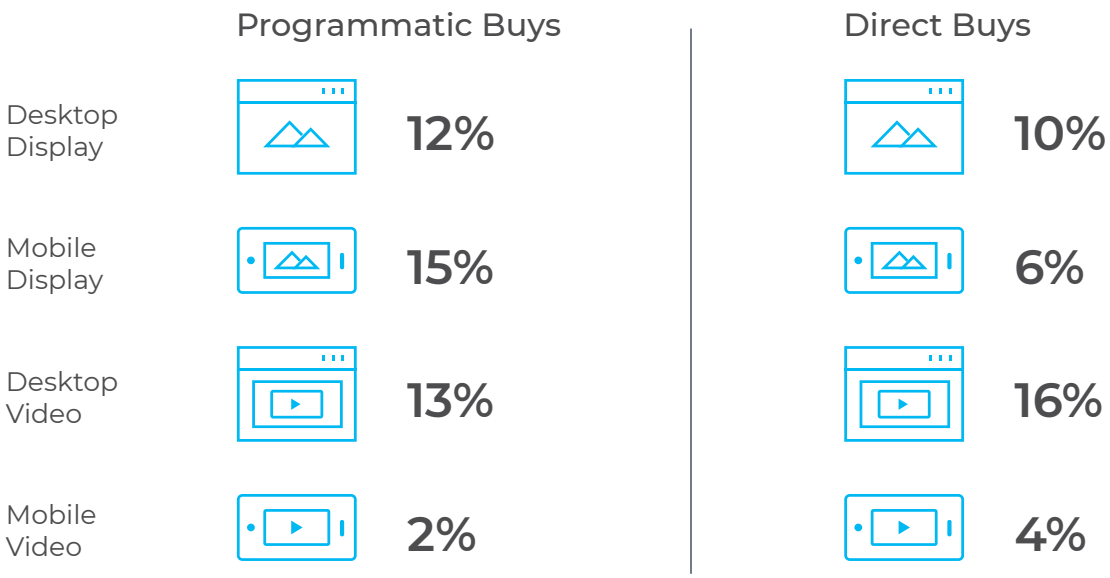
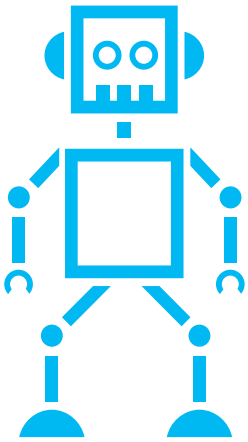


Image Source: https://www.appnexus.com/sites/default/files/whitepapers/guide-2018stats_2.pdf

What is Fraud?

An 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 a specific, defined audience. Any deliberate activity to prevent the delivery of this message is referred to as an ad fraud.



- The ad fraud landscape is not constant, it keeps changing very often. While it may concentrate on one site for this week, it may do so on another site, the next week. Bot attacks can hit even the premium publishers.

- Some of the most common forms of ad fraud prevailing across various online ad platforms are as follows:

Bot Attacks: Selling inventory generated automatically by background mobile-app services or bots.

Delivering pre-roll video placements in display banner slots.

Hidden ad impressions: Hiding ads behind or inside other page elements, so that they can't be viewed by the user viewing the web page.

Domain spoofing: Serving ads on a site other than the one provided in a real-time bidding (RTB) request.

Falsifying user characteristics such as location and browser type.

Hindering user engagement by frequently refreshing the ad unit or page.

Invalid Traffic (IVT): Nonhuman Traffic (NHT) or Suspicious Activity Detection (SAD), is online traffic generated from machines or other bot activity that interacts with digital ads. General Invalid Traffic (GIVT) and Sophisticated Invalid Traffic (SIVT) are subtypes of IVT.

Fake Installs: Mimicking real mobile devices using emulators and then installing apps.

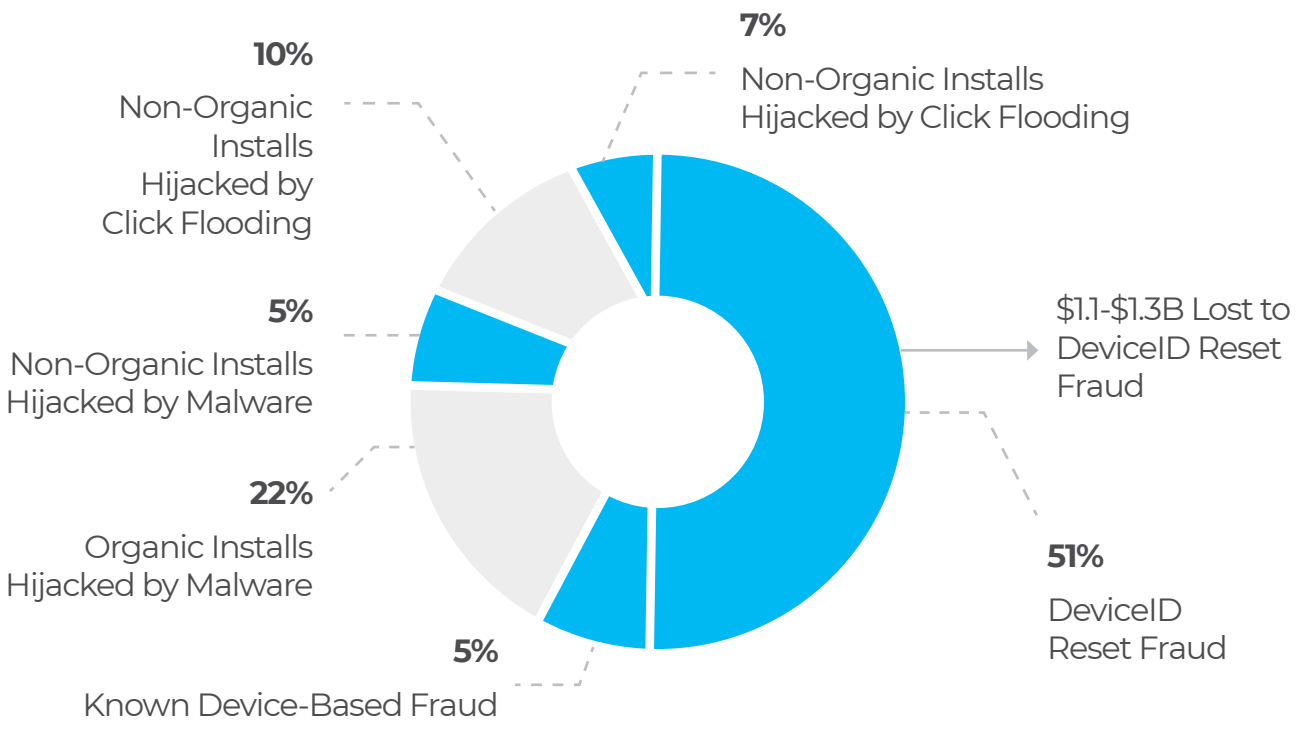
Attribution manipulation: Sending clicks, app installs, in-app events, hijacking mobile IDs, and generating a fake click.

App laundering: Delivering ad content to laundered (illegitimate or low valued) in-app or potentially just a dark screen.

Fake in-app purchases: Making an in-app purchase without making any real payment. Such fake in-app purchases disguise the app by making the purchase appear as a valid one where in reality it isn't. Fake in-app spends skew user quality analysis and ROI analysis metrics.

Device Farms: Locations full of actual mobile devices programmed to click on real ads, download real apps hiding behind fresh IP addresses and resetting device IDs to prevent detection. As shown in the figure below, over 50% of all the mobile install frauds have been a result of device ID reset.

Distribution of Mobile App Install Fraud by Type

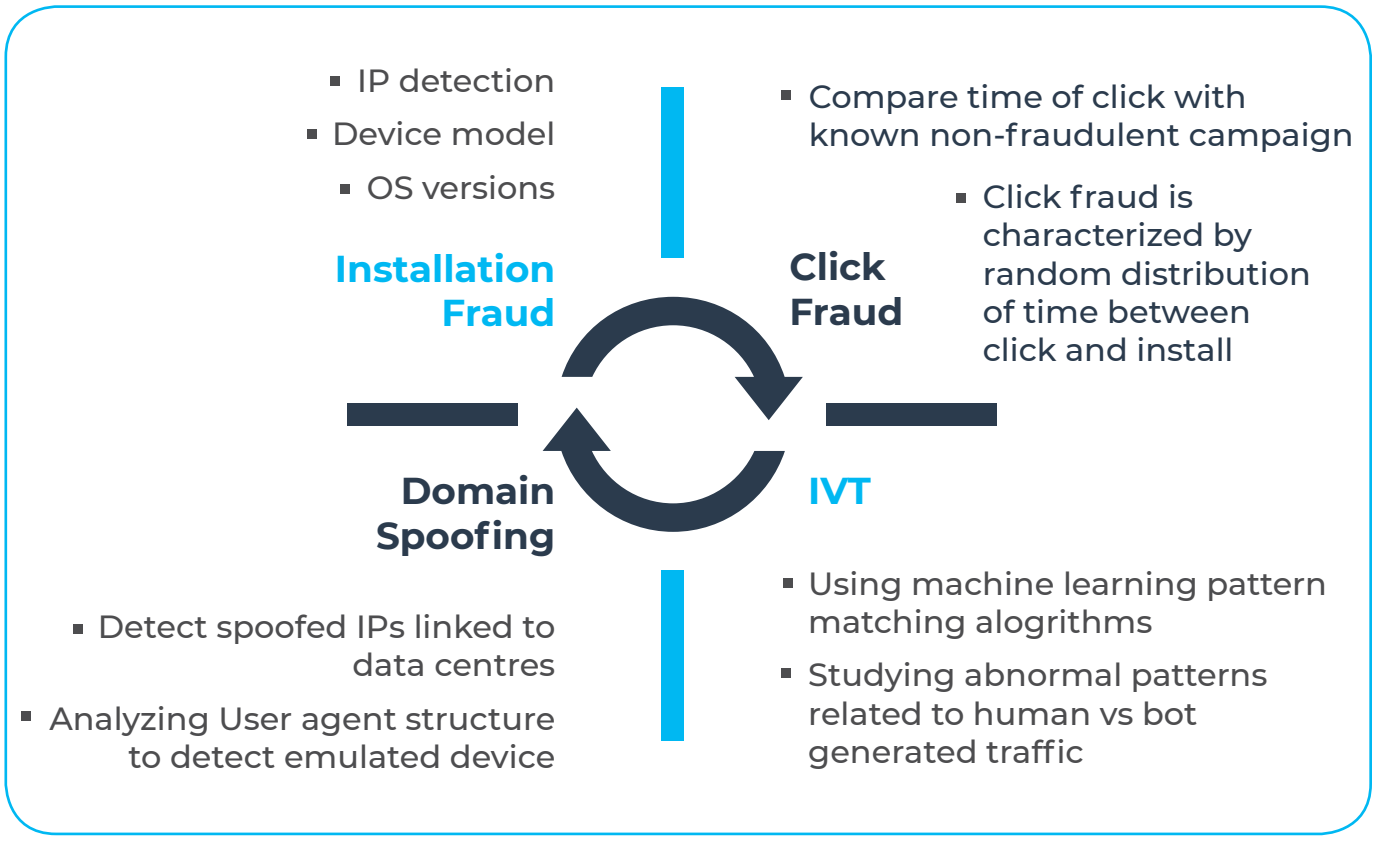


Img Sourcce: https://www.appsflyer.com/resources/deviceid-reset-fraud-data-study/

How to Detect Ad Fraud?

Any behavior that is abnormally clustered around a specific variable can be an indicator of fraud. Technology plays a vital role in detecting ad fraud. More and more data is being collected to aid analysis and recognition of fraud patterns and it is proving to be the most effective method of identifying and fighting fraud

Bots, which can mimic human behavior, tend to generate suspicious patterns at some point of time and it is here that Big Data technologies and Machine Learning (ML) are being extensively leveraged to recognize fraud patterns of such bots.



By contrasting the data from campaigns with expected user behavior, abnormal patterns related to IP distribution, reported user devices or time from click to install distribution become apparent.

Robust algorithms can be designed to identify fraudulent behavior by analyzing the variance obtained by comparing campaign generated data with its expected behavior. For example, a pattern observed in campaign data where in cost-per-click (CPC) is extremely high but relative campaign performance is zero (e.g. 1000 clicks but no conversions), by analyzing and modelling such behavior to detect ad-fraud, one can identify and blacklist fraudulent URLs and IP addresses.

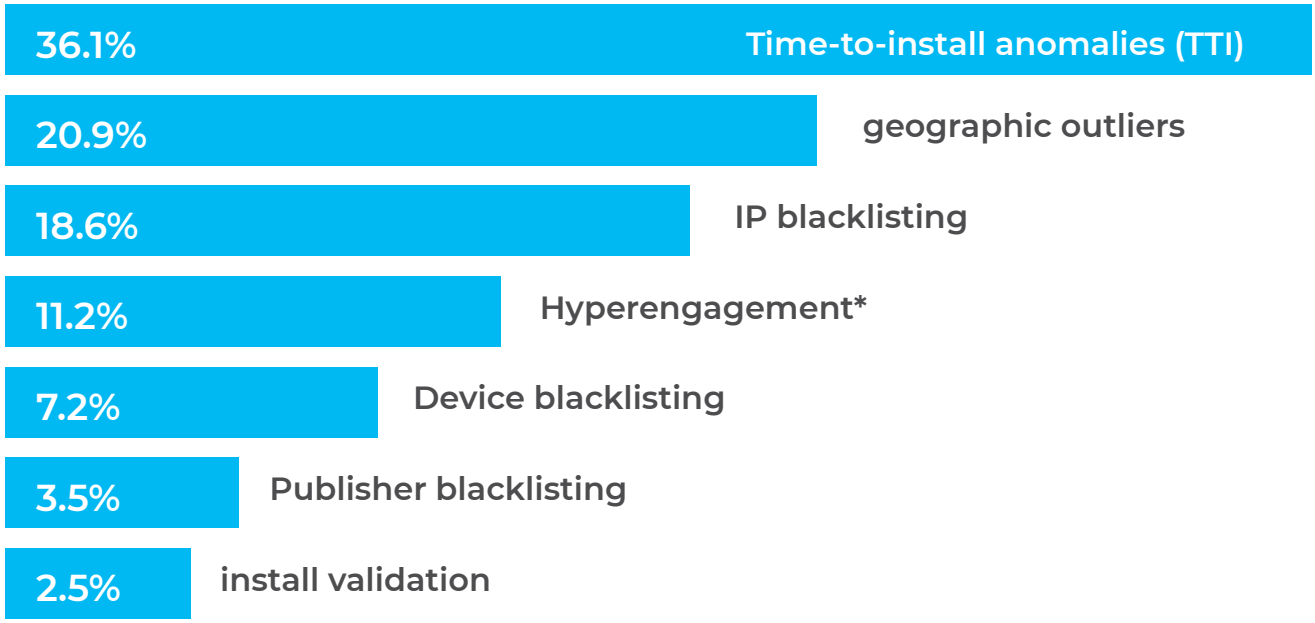
Another option is integrating with fraud detection platforms like **Fraudlogix**, **White Ops** **DoubleVerify**, which help in detecting and blocking fraudulent activity during Real Time Bidding (RTB).

How to Fight Back Against Ad Fraud?

On one hand, ad-fraud detection tools are increasing rapidly, while on the other, the invention and innovation to exploit the system is raising its bar. New sophisticated and smart bots are being designed to escape detection.

It is rightly said that prevention is better than cure. The ad tech industry today is focusing more on prevention rather than curbing the fraud happening at real time. Some of the most widely used prevention techniques in the mobile world are displayed in the following chart.

Methods Used to Prevent Mobile Ad Fraud Among Mobile Apps Worldwide, Sep 14-Oct 14, 2017 (% of total)



Img Source: https://www.emarketer.com/Chart/Methods-Used-Prevent-Mobile-Ad-Fraud-Among-Mobile-Apps-Worldwide-Sep-14-Oct-14-2017-of-total/213881

At Cybage we recommend following approach against fighting this global issue:

- **Maintain a database of IPs** that meet the criteria of IVT, blacklist them, and then block the traffic coming from them.
- **Update software development kits** (SDKs) regularly for security updates and patches, keep a check on data anomalies, and perform regular audits for preventing mobile app frauds.
- **Using Ads.txt and App-ads.txt:**
  - According to MarTech, till January 2018, 705 of top publishers had implemented ads.txt.

- The **IAB's ads.txt** Initiative that has helped ad buyers to verify the inventory and control domain spoofing which in turn has helped maximizing revenue and CPMs for legitimate publishers.

- The recent launch of **IAB's app-ads.txt** is being seen as great milestone towards addressing the ad fraud plaguing the mobile industry.

- The way ads.txt works is

  - Prevents a publisher's inventory from being fraudulently sold to an unrelated third party that has an intention to spoof up the publisher's domain.

  - Provides a list of identified partners who are reselling publisher's inventory through an existing exchange.

- **Use Big Data and Machine Learning:** Large data sets in the form of logs and reports when analyzed properly by experts can help understand the pattern of an ad fraud and the volume of fraud traffic. Thereby, help determine proper model and policies to be applied to the ad campaign and minimize the invalid traffic or clicks.

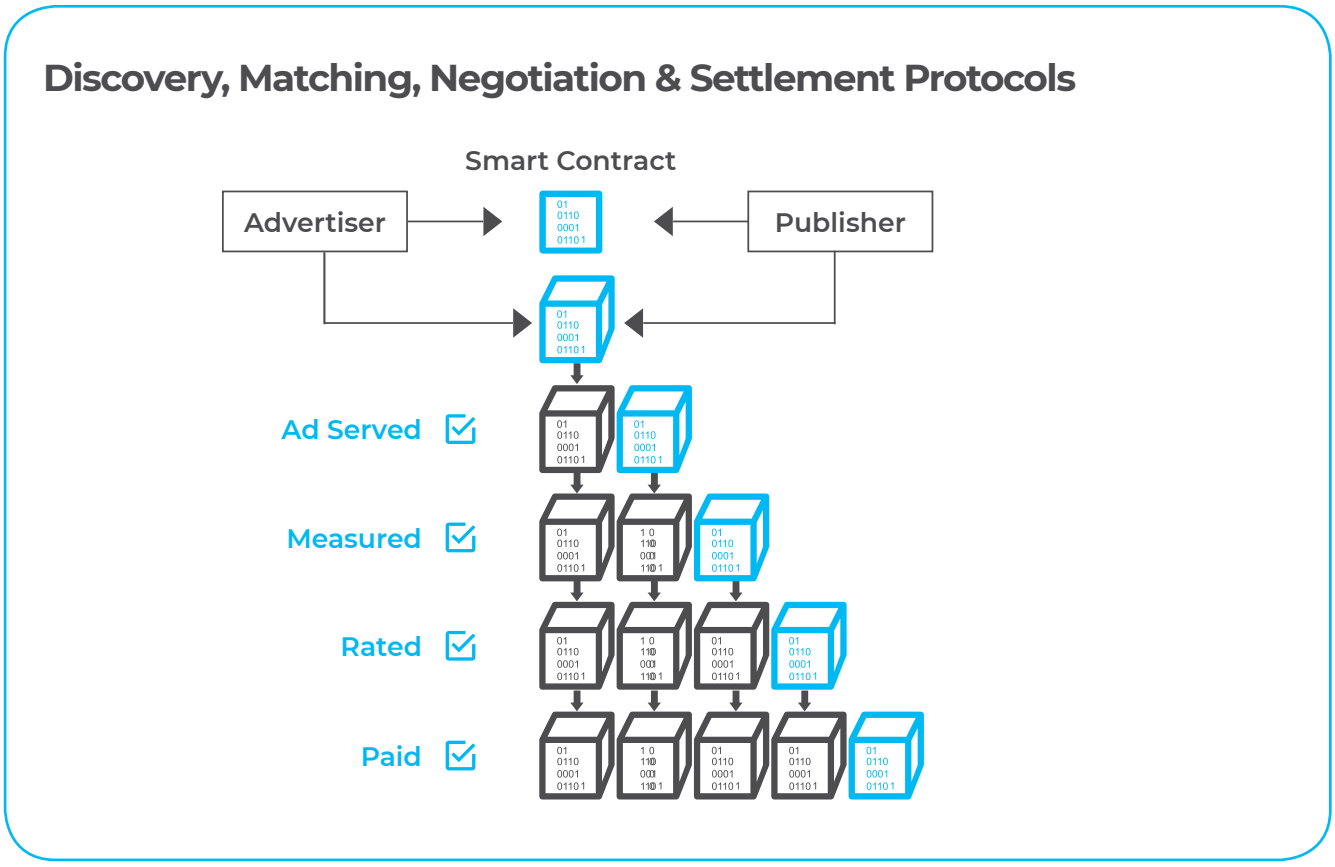
- **Use Blockchain:**

  - According to **MediaPost**, Blockchain is forecasted to create $122B in business value for advertising, media by 2030.

  - Blockchain has the potential to overturn the digital advertising industry by removing the middlemen. By implanting transparency in the entire value chain, it will eliminate the current inefficient model of transaction in the advertising world and help publishers and advertisers cash in on their investments with utmost security and authenticity.

  - The entire ecosystem can be realized in form of nodes starting from Publisher to Advertiser as shown in the following image.

  - Each transaction that occurs at any node is maintained in the ledger that is visible to each connected member of the eco system.



- Cybage, with its strong consulting-led approach, can help design a solution and develop a solution based on the IAB standards.

References:

- http://www.snpa.org/stories/fraud,4145207
- https://www.nativo.com/non-human-traffic-monitoring
- https://www.digilant.com/es/digilant_university/programmatic-buying-101-what-do-digital-marketers-need-to-know-about-ad-fraud/
- http://blog.pixalate.com/mobile-app-video-ad-fraud-programmatic
- https://digiday.com/marketing/wtf-ads-txt/
- https://www.mediapost.com/publications/article/323040/blockchain-forecast-to-create-122b-in-business-va.html

CYBAGE
Delivering Value. Scientifically.

Cybage Software Pvt. Ltd.

[ISO 27001 Company]

India | USA | Canada | UK | The Netherlands | Germany | Japan | Australia | Singapore

www.cybage.com