# AD FRAUD AMERICA: THE REAL SCALE OF THE PROBLEM AND HOW TO FIX IT

2017

THE & PARTNERSHIP

adloox

# AD FRAUD AMERICA: THE REAL SCALE OF THE PROBLEM AND HOW TO FIX IT

The&Partnership have long taken seriously the growing issue of advertising fraud: a problem which has for several years represented a threat to the brands and media owners we work with.

As an agency, The&Partnership has taken a specialist interest in advertising fraud – digging deep into the best practices, policies and available technologies in order to pioneer a new approach to brand protection in the programmatic era.

Last year, we partnered with ad verification specialists Adloox to conduct an in-depth piece of research into the real scale and cost of ad fraud, suspecting the problem to be significantly larger than previously reported.

The study, conducted across a robust 200bn daily bid requests, 4bn ad calls and 10bn ad impressions a month, for a period of 12 months, showed that the real scale of ad fraud has until now been significantly under-reported.

## 2016 COST OF AD FRAUD:

- Previously believed to cost advertisers $7.2bn globally each year (according to the ANA's '2014 Bot Baseline Report'), **the actual cost of advertising fraud is $12.48bn (nearly twice as high)**
- In the US alone in 2016, of the $32.17bn spent on digital video and display advertising, a full $7.52bn (23%) may have been wasted on fraudulent advertising
- To put it in context, this is approximately the same figure that the ANA two years ago predicted would be lost globally to ad fraud in 2016

## FUTURE OUTLOOK:

- If ad fraud continues to evolve at this rate, **the money we stand to lose to ad fraud in the US in 2017 could be as high as $9bn** (This is as Display and Video spend is forecast to grow to around $37bn*, and the programmatic / direct split shifts to a weighting of over 70%* programmatic)

## OF THE TWO MAIN TYPES OF DISPLAY ADVERTISING SPEND:

- $21.6bn* in the US was spent in programmatic, accounting for 67%* of all display spend, of which 29% was invalid traffic – costing $6.25bn.
  – Main drivers of in-valid traffic: adware and botnet fraud (accounting for ¾ or $4.7bn)
- $10.6bn* was spent in non-programmatic display or publisher-direct media, accounting for 33%* of all display spend, of which 12% was invalid traffic, costing $1.3bn.
  – Main drivers of invalid traffic: adware and botnet fraud (accounting for ½ or $0.6bn)

*Source: eMarketer, Magna Global 2016

## METHODOLOGY

The study is based on a combination of 3 key data points:

- Listening to the bid requests (before impressions). Highest point in the bid food chain
- The post-bid analysis. Mid-point in the bid food chain
- And the post-impression filtration. After the bid>impression>delivery>payment

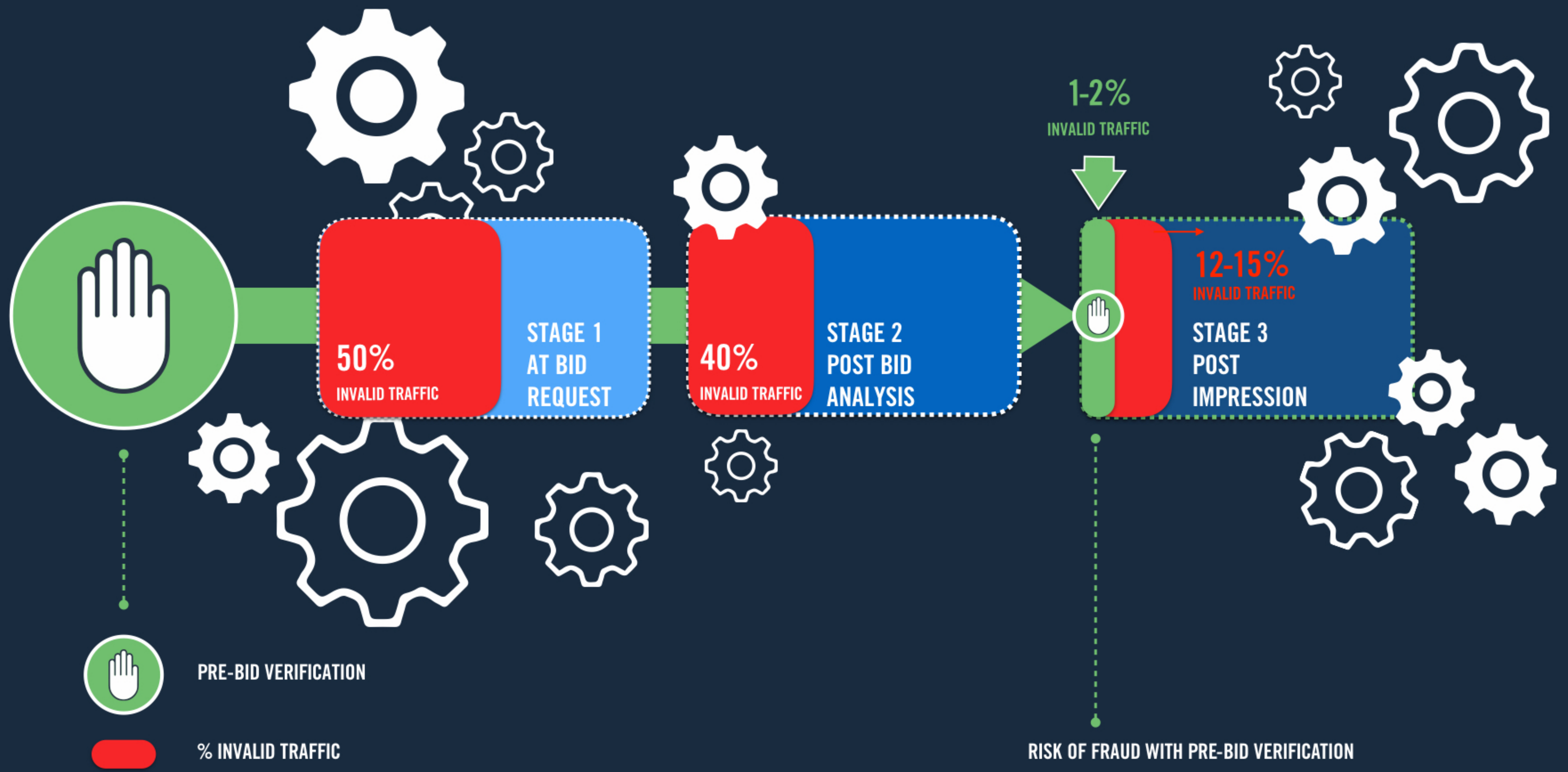
The bid request analysis was based on a sample of over 200 billion daily bid requests, which the servers globally receive and filtrate across 6 different data centers and across 3 continents. The conclusion was that approx. 50% (49.9%) of bid requests are either made by users flagged as Botnet or users flagged as hijacked device, originating from supplier sources of mainly fraudulent inventory, and users coming from "fake domains”.

The post bid analysis is analysing the ad requests just before the impressions are bought. This study was based on a randomly selected sample of 4 billion ad calls a month (across 2016) made by SSP’s. The conclusions here were that: Fraud levels are consistent throughout the year. Up to 40% were detected as IVT (invalid traffic). The study cited the emergence (or classification) in Q1-Q2'16 of Domain Spoofing as a main category of Ad Fraud, with DS accounting for more than half of the IVT reported in these first two quarters.

The post impression filtration analysis is based on a sample of 60 clients and 10B impressions /month. The levels of invalid traffic (IVT) with clients using pre-bid filtration is down to 1-2%. Monitoring only (before pre-bid was activated), the IVT levels detected were between 10-12%. The main fraudulent categories reported were Botnet +Adware and Fake Domains. New categories of IVT detected (forced traffic) were forced autorefresh, external traffic or traffic generated via site under/pop up. This surfaces as a real issue in Q3/4 of 2016 and is a growing menace in 2017. As a comparison to the 10-12% Fraud IVT in Programmatic, overall IVT levels in direct buying was 4-5%. This IVT is mainly caused by bots generating cookie stuffing and legitimate bots not yet declared to/by the IAB.

*Source: eMarketer, Magna Global 2016

# THE SOLUTION: PRE-BID AD VERIFICATION



In spite of the implementation of pre-bid blocking, new categories of advanced fraud continue to emerge, such as pop-unders and auto-page-refresh – meaning a combination of constant human vigilance and continuous updates to ad verification technology policies is required to continue to protect brands.

This is why The&Partnership has a policy of requiring all its clients to invest in third-party, pre-bid ad verification from specialist providers such as auditing firm Adloox – which recently became the first European tech company to be accredited by the Media Ratings Council (MRC) for all general (GIVT) and advanced (SIVT) display categories of invalid traffic.

## WITHIN THIS, THERE ARE THREE MAIN POINTS IN TIME WHERE AD FRAUD IS DETECTABLE:

1) Before a bid request is made (the highest point in the chain, before any blocking occurs – when 50% of traffic is fraudulent).

2) Post-bid analysis (mid-point in the chain, where the call is made to serve an impression. 40% of traffic is invalid at this stage, of which almost half was attributed to domain spoofing in the first half of 2016. Spoofing is defined as a bot posing as a verified publisher on the programmatic exchange by mimicking that publisher's domain.

3) Post-impression (after the impression has been served). Pre-bid verification or blocking helps reduce this invalid traffic from 12-15% to just 1-2% if accurately removed pre-emptively.

# WHAT HAPPENS NEXT?

## POINT OF VIEW FROM JOHNNY HORNBY, FOUNDER, THE & PARTNERSHIP

“Having highlighted the problem, it’s important to also highlight the solution. The proper use of ad verification software can reduce the 23% of advertising spend that may be being wasted on fraudulent – often reputation-threatening – advertising placements in the US down to 1 or 2%, if not better.

The issue, however, is that the big-platform players – and most critically YouTube, as part of the Google family – are still refusing to allow access of our ad-verification software to their platforms. Meanwhile, other platforms such as Facebook are also failing to allow us full access to their walled gardens – giving advertisers the visibility and transparency they deserve.

Without this, not only are these platforms denying our clients the clean, brand-safe environments they quite rightly demand – but advertisers also lack full transparency and visibility in terms of the money they are losing to fraudulent advertising and advertising that never gets seen.

If Google wants to see advertisers returning to YouTube in significant numbers, it is going to have to move quickly on the following two things:

Firstly, Google needs to stop grading its own homework (as Keith Weed, Unilever Global CMO, recently observed) – fully opening up its walled gardens to independent, specialist ad verification software, to give brands the visibility and transparency they deserve.

Secondly, Google will need to start looking at brand safety from completely the other end of the telescope. Instead of allowing huge volumes of content to become ad-enabled every minute, and then endeavouring to convince advertisers that the dangerous and offensive content among it will be found and weeded out, it should be presenting advertisers only with advertising opportunities that have already been pre-vetted and found to be 100% safe.

Only then will we see the advertiser exodus from Google reversed – and brands begin to trust and invest in YouTube once again.”