WHAT HAPPENS NEXT: HOW TO REVERSE THE RISING TIDE OF AD FRAUD

2017

WHAT HAPPENS NEXT: HOW TO REVERSE THE RISING TIDE OF AD FRAUD

The&Partnership and m/SIX have long taken seriously the growing issue of advertising fraud: a problem which has for several years represented a threat not just to the brands and media owners we work with – but also to the future of the advertising industry itself.

As the youngest of the "M"s at GroupM, and the only "M" born in the age of addressable media, m/SIX 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 and cost of ad fraud has until now been significantly under-reported:**

- 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)**
- To put it in context, this means **nearly 20% of total digital adspend in 2016 ($66bn) was wasted on fraudulent advertising placements**

FUTURE OUTLOOK:

- If ad fraud continues to evolve at this rate, **the money we stand to lose to ad fraud in 2017 could be as high as $16.4bn** (This is as digital spend grows to hit $80bn, as forecast by eMarketer, and the programmatic / direct split shifts to a 50:50 balance)

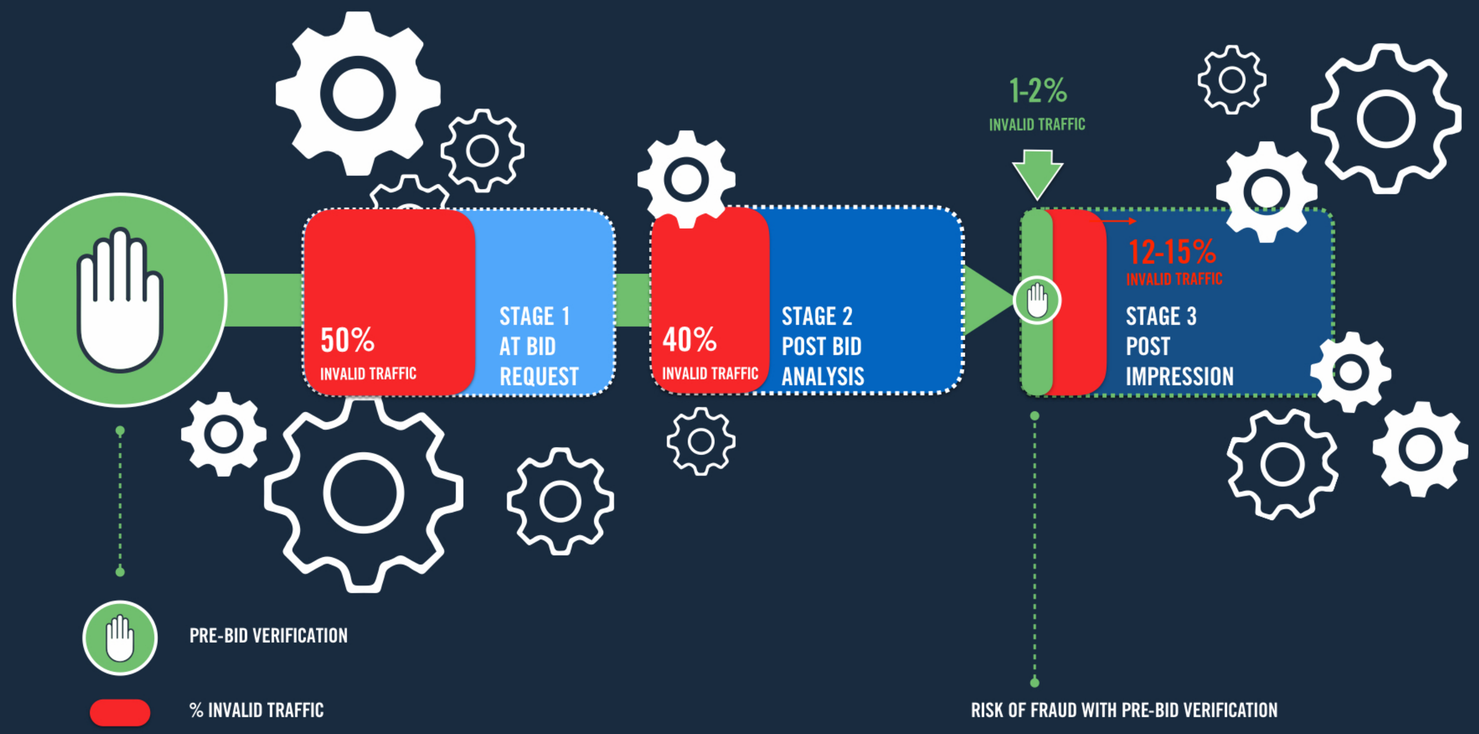
OF THE TWO MAIN TYPES OF DIGITAL ADVERTISING SPEND:

- **$27bn** was spent on programmatic (of which **29%** was invalid traffic) – costing **$7.8bn**
  - Main drivers of invalid traffic: adware and botnet fraud **(accounting for ¾ or $5.15bn)**
- **$39bn** was spent on non-programmatic or publisher-direct media **(of which 12% was invalid traffic) – costing $4.65bn**
  - Main drivers of invalid traffic: adware and botnet fraud **(accounting for ½ or $2.325bn)**

ACROSS OUR SAMPLE OF 200BN DAILY BID REQUESTS, 50% WERE DETECTED AS EITHER:

- Non-human traffic (a bot, or hijacked device)
- A fraudulent traffic source from the supplier and/or a fake domain

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 m/SIX 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

These figures serve as a stark reminder that much still remains to be done in order to protect and nurture the future vitality of the digital economy.

We have a duty to come together as an industry – from media agencies and industry bodies, to big-platform players like Google and Facebook; bringing in government help if we need it – in order to protect our own future and those of our clients.

Good work is already being done by many, including the ANA, IAB, ISBA and the IPA, as well as the recent combined efforts of TAG in the US and the Joint Industry Committee for Web Standards (JICWEB) in the UK – but these new figures show that we need to move further, much faster. And there are concrete steps we should all be taking to make that happen.

As a first step, media agencies must invest time, energy and talent into providing the best possible strategies and policies to protect their clients.

Secondly, they need to pass the learnings on, and urge advertisers likewise to invest in real, robust brand protection.

m/SIX has since it was founded taken a specialist interest in advertising fraud and has a policy requiring all its clients to invest in third-party, pre-bid ad verification from specialist providers such as Adloox – reducing the risk of fraudulent placements from 12-15% to 1-2%.

Together with Adloox, we have reduced the average ad fraud score for clients including Vitality, JUST EAT, TalkTalk, Virgin Money and News UK down to just 0.4% – so it can be done.

Many other reputable agencies have taken the same stance – refusing to buy media for their clients unless they have robust pre-bid ad verification policies in place. But the responsibility doesn't stop with agencies.

Clients likewise need to be willing to invest in proper, robust brand protection. Many of the major advertisers do have some form of protection in place – but for all the diligent clients out there, there are plenty of others who are well aware of the dangers of advertising fraud, but still opt not to pay for pre-bid technology – which costs all of 3 pence per 1000 impressions, accounting for approximately 2% of clients' overall media spend.

Advertisers and agencies alike need to rethink this "cost-saving" mentality. What might look like thrift on the budget sheet is in fact a false economy, as advertisers – often wilfully – turn a blind eye to the money they are allowing to leak out of their budgets and into cybercriminals' pockets.

Thirdly – and this is critical if we want the internet to become a fairer, safer environment for our brands to thrive in – the big-platform players in the media industry like Google and Facebook need to step up to the plate, fully engage with the likes of TAG and JICWEB, and take far more seriously the responsibility for what they do and don't allow to happen online.

Beyond the wider debate about whether they should allow compromising content to be published on their platforms in the first place, as a very minimum they ought to have proper measures in place to ensure that this type of content isn't – and cannot be – ad-enabled.

Appearing in the ad space next to grossly offensive content is hugely damaging for any brand and, by standing by and allowing it to happen, big-platform media owners are neglecting their responsibility to do the right thing by the valuable customers who buy ad space with them.

Finally, the time has come for the Googles and Facebooks to stop marking their own homework, and allow specialist, third-party auditors inside their walled gardens – to verify the viewability, non-human traffic and brand safety scores they send back to clients. Only then will we truly break the back of the ad fraud problem.