Compendium of ad fraud knowledge for media investors

Co-authored by WFA &
THE ADVERTISING FRAUD COUNCIL

Mikko Kotila
Principal, botlab.io
mailme@mikkokotila.com

Ruben Cuevas Rumin
Assistant Professor, UC3M
rcuevas@it.uc3m.es

Shailin Dhar
Independent Ad Fraud Consultant
adtechexpert@gmail.com

WFA WORLD FEDERATION OF ADVERTISERS

Compendium of ad fraud knowledge for media investors

CONTENTS

ABOUT THIS DOCUMENT

The intention of this compendium is to raise awareness of ad fraud among brand owners and to provide the knowledge and best practices to effectively counter it. This document seeks to encourage brand owners to adopt these best practices and to work with industry partners to make the changes necessary to reduce fraud substantially.

This document was championed by members of the WFA Global Transparency Group and approved by member of WFA's **MEDIA**FORUM and **CDO**FORUM.

The WFA have been supported in the creation, data and research behind this guide by Botlab.io, a research foundation focused on researching ad fraud, user rights violations and other malicious practices in the online advertising supply-chain.

This document is intended as advice only and not a definitive guide. It aims to provide general, high level guidance to assist WFA members when taking unilateral decisions concerning their internal and external operations with digital media.

Published 2016

EXECUTIVE SUMMARY

- Ad fraud is likely to represent in excess of **$50 billion by 2025, even on a conservative basis**. Without sufficient counter measures, it's easy to produce scenarios where ad fraud revenues equate to $150 billion per annum in the same timeframe.
- Virtually **any programmatic buy can be exposed to ad fraud**. 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.**
- Ad fraud is being perpetrated by multiple protagonists. Despite this, **the unintended main benefactor of ad fraud is the marketing industry.**
- **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.
- A silver bullet solution to the problem does not exist on the market, in fact, **a single-digit percentile of exposure to ad fraud will very likely prevail against any counter measure**.
- Until the industry can prove that it has the capability to effectively deal with ad fraud, **advertisers should use caution in relation to increasing their digital media investment**, to limit their exposure to fraud.
- **Much can be achieved by advertisers to improve the situation**, including setting new standards, making contractual changes, demanding increased transparency and putting in place internal resource dedicated to countering ad fraud.
- **Behavior change is required across the industry**, which can only be achieved with appropriate understanding, motivations and a common shared approach.

"Ad Fraud is one of the most important issues that we face today. We're committed to continuing the dialog so that we can heighten awareness and build solutions. We hope this guidance can lead the industry along the road to identifying the opportunities and solutions for advertisers, media owners and tech companies alike".

Benjamin Jankowski,
Group Head, Global Media
MasterCard
& WFA MEDIAFORUM Chair

WHAT IS AD FRAUD?

By definition, ad fraud is associated with an activity where impressions, clicks, actions or data events are falsely reported to criminally earn revenue, or for other purposes of deception or malice. Ad fraud activities aimed towards generating revenue are more common, but noise creation and other non-revenue generating activities are also present in the internet advertising ecosystem today.

In summary, there are four types of ad fraud scheme:

1. impression fraud
2. click fraud
3. conversion fraud
4. data fraud

In each of these cases, reporting validates a visitor to be authentic, but it is actually fraudulent. These fraudulent visitors can be entirely mechanical, human or a mix of both.

HOW BIG IS THE AD FRAUD PROBLEM?

With researchers reporting ad fraud exposure between as low as 2% [1] and as high as 90%, it seems clear that there are no widely available ways of assessing the absolute exposure rate. The challenge of establishing such a figure is underlined by recent WFA research findings which demonstrate that 36% [2] of respondents say they don't know to what extent they are exposed to ad fraud.

One of the highest profile research initiatives into ad fraud was the recent "Bot Baseline" [3] led by the Association of National Advertisers (ANA) in the US. 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 are outlined below), suggest that the scale of the problem may in fact be much more substantial:

- 88% of digital ad clicks deemed fraudulent [4]
- digital publishers lead all industries in bad bot traffic at 32% [5]
- bots inflate monetized audience by 5% to 50% [6]
- bot traffic is up to 61.5% of all website traffic [7]
- just one form of in-app fraud accounts for 13% of all in-app inventory [8]
- 22% year-on-year growth for fraudulent bot traffic [9]
- 40% of mobile ad clicks are essentially worthless [10]
- bot traffic rises for the first time to over 50% of total [11]
- more than 18% of impressions/clicks come from bots [12]

The focus for this paper is not to conduct additional empirical research to quantify the value that ad fraud represents today. To affect change in our industry however, it is helpful to propose what the likely scale of the problem is now, and what it may reasonably become in the future, according to different scenarios.

Two scenarios have been used throughout this document: a relatively conservative global exposure rate of 10% and a higher figure of 30%. Based on studies already conducted by third-parties and primary research by Botlab.io and its partners, it is clear that the true figure may well be higher than 30%.

It is worth underlining that ad fraud is not only manifested in the form of bot traffic, but also other forms of invalid activity (briefly outlined in this paper), so the total global ad fraud exposure rate will be higher than the share that bot traffic represents among all other traffic.

The real cost of ad fraud is far greater than the revenue it creates. An ongoing global study by Deloitte and the WFA, and similar work by the Advertising Association in the UK[13], shows that for every dollar lost due to advertising inefficiency, up to 6 times more is lost in terms of business. The kinds of damages caused by ad fraud can be summarised as:

1. cost to marketing effectiveness;
2. cost to the business (and the category of the business);
3. cost to the national economy (and the tax payer).

This means that as a result of attacking the advertising effectiveness of a given advertiser, the national economy in which the advertiser is a contributor to will also suffer. In this way ad fraud poses a new kind of security risk, providing a way to attack a given nation's economy.

> *"As advertisers, we have a responsibility to tackle ad fraud head on, both for the benefit of the consumers we serve and the communications industry overall.*
>
> *It's important that we work together with our peers and industry partners to address the challenges we face, and collaborate to change the way the current ecosystem operates."*

Luis Di Como,
Senior Vice-President, Global Media. Unilever & WFA Global Transparency Group & Executive Committee member

1 *Digital Content Next & White Ops > https://digitalcontentnext.org/wp-content/uploads/2015/09/DCN-Bot-Benchmark-Report-2015-.pdf*
2 *Members only survey Nov. 2015 > http://www.wfanet.org/en/knowledge/global-knowledge-base#/item/314*
3 *ANA & WhiteOps. The Bot Baseline 2015 > http://www.ana.net/content/show/id/botfraud-2016*
4 *Oxford BioChronometrics > https://oxford-biochron.com/over-88-of-digital-ad-clicks-deemed-fraudulent-new-study-by-oxford-biochronometrics-suggests/*
5 *Distil Networks 2015 > http://resources.distilnetworks.com/h/i/155404518-distil-networks-releases-new-data-on-the-state-of-digital-advertising-fraud*
6 *ANA & White Ops 2014 'The Bot Baseline' > http://www.whiteops.com/botfraud*
7 *Incapsula Bot Traffic Report 2013 > https://www.incapsula.com/blog/bot-traffic-report-2013.html*
8 *Incapsula, Mobile app fraud study 2015 > http://www.prnewswire.com/news-releases/forensiq-projects-in-app-ad-fraud-will-surpass-1-billion-in-2015-300117453.html*
9 *Solve Media 2014 > http://www.businessinsider.in/Botnets-Will-Cause-11-6-Billion-In-Wasted-Ad-Spending-This-Year/articleshow/29508619.cms*
10 *Trademob 2012 > https://gigaom.com/2012/08/31/report-40-percent-of-mobile-clicks-are-fraud-or-accidents/*
11 *Solve Media 2013 > http://www.adweek.com/news/advertising-branding/bot-problem-keeps-getting-worse-154585*
12 *Bin Liu, University of Southern Calfornia 2014 > https://www.usenix.org/node/179764*
13 *Deloitte & Advertising Association (UK) 2011 > http://www.adassoc.org.uk/publications/advertising-pays/*

WHAT DOES THE FUTURE HOLD?

Digitisation, cybercrime and counter ad fraud trends are the main drivers behind how ad fraud will grow over the next 10 years. Unless the ability to counter ad fraud increases in parallel with money invested in digital, ad fraud exposure rates will increase significantly in absolute terms.

There are just a few cases where ad fraud has led to prosecution[14] and conviction[14], meaning that the 'risk' level is low, relative to other digital crime. A recent report from Hewlett Packard classifies ad fraud as having a higher 'potential payout' than any other form of digital crime[15]. The combination of these factors is predicted to attract 'spammers', organised crime organisations, and other criminals who may have previously focused on alternative areas.

Source: Hewlett Packard Enterprises, 'The Business of Hacking', May 2016

The longer the growth of ad fraud is allowed to go on, the more difficult countering it becomes.

By 2025 the total global investment on digital media is projected to be within a range of $400 billion to $500 billion[16]. If just 10% of the upper limit within this range is exposed to ad fraud, this will be second only to cocaine and opiate markets as a form of organised crime[17].

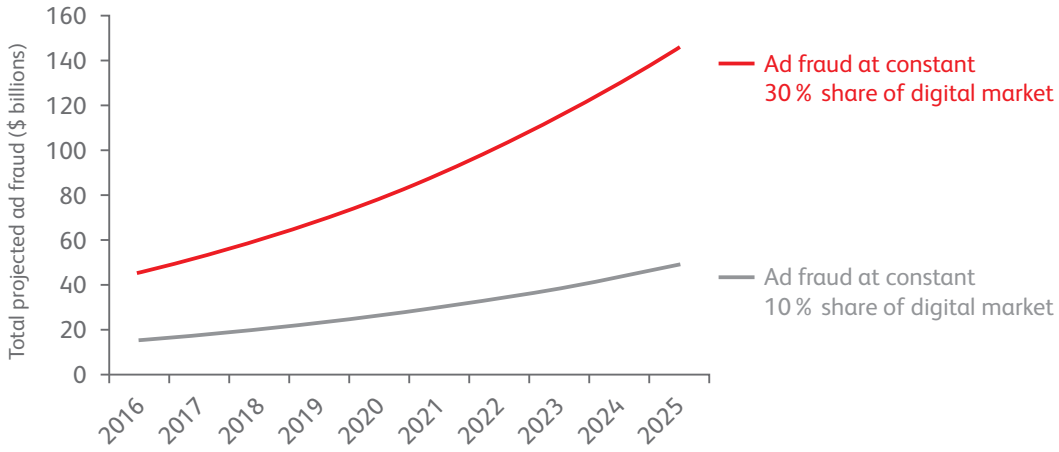
As illustrated earlier, however, existing research identifies that ad fraud represents far more than 10% of the digital market. In fact, this may already constitute well in excess of 30% - the more severe ad fraud scenario we refer to throughout this document.

Simple mathematics show that 30% of the $150 billion market in 2016 would equate to $45 billion. Assuming that this would remain constant over the next 9 years, so growth comes only through the enlargement of the digital advertising market, ad fraud would represent $140 billion by 2025.

[14] *Notably, the FBI's expose of fraud conducted by affiliate marketers (http://uk.businessinsider.com/ebay-the-fbi-shawn-hogan-and-brian-dunning-2013-4?r=US&IR=T) and the sentencing in the US of an individual for click fraud (http://www.reuters.com/article/us-usa-cybersecurity-malware-idUSKCN0XN2WX)*
[15] *Hewlett Packard Enterprises, 'The Business of Hacking', May 2016*
[16] *Based on historical trends from GroupM and ZenithOptimedia, plus WFA projections based on future market forces.*
[17] *https://www.unodc.org/toc/en/crimes/organized-crime.html*

Of course it is highly unlikely that ad fraud will not grow beyond its current base, but will in fact grow rapidly, as the perpetrators increase in sophistication. While it could be debated as to whether 10%, 30% or a higher exposure rate is correct, it would be hard to dispute that there is a strong element of conservatism built in to the below projections.

Unless dramatic changes take place in the advertising technology ecosystem, and in the way money is being invested into media by advertisers and their industry partners, the lower figure of c. $50 billion by 2025 illustrated in the chart below may soon appear like an impossibly low figure, rather than a conservative estimate.



Source: Industry projections based on growth of digital media market and possible scenarios for ad fraud growth

Findings from WFA research identify that 9 in 10 (92%) of advertiser respondents agree that ad fraud is perpetuated by the structure and systems in the digital media ecosystem. It is incumbent upon the ecosystem, including publishers and others on the sell-side, plus programmatic companies, agencies and others on the demand-side, to prove that the capability to effectively deal with ad fraud is in place. **Until this time, advertisers should use caution in relation to their overall digital media investment, to limit the growth of ad fraud and their exposure to it.**

"Increased investment in digital has offered many opportunities as well as challenges, but few are as pressing as this. We need to put the appropriate measures in place to protect our brands and our customers. There is plenty to learn from the financial sector who continue to fight a similar battle with online fraud"

Mark Butterfield,
Head of Global Media,
Boehringer Ingelheim Ltd
& WFA Global Transparency
Group member

WHAT FORMS DOES AD FRAUD TAKE?

There are three primary forms of ad fraud:

1. Website. Can be further split in to websites that are directly under the control of the perpetrator[19], and those that the perpetrator is acting as an affiliate for, as is typically the case in conversion fraud schemes.

2. Platform. Can be anything from a social networking site to a video hosting site. Where brands are more familiar with platforms, inevitably there is greater trust and less suspicion of fraud. There is evidence that major platforms have significant issues with ad fraud[20].

3. Data. This refers to any circumstance where adversaries are able to monetize user data through data marketplaces. There are various ways in which this is practically executed, but one example is by sending a botnet to visit publisher sites, making these bots become part of what the publisher would consider to be first party data. Many publishers use cookies to target audiences and sell ads on sites other than their own, using audience extension techniques, thereby propagating false impressions across the web. Additional steps include sending bots to visit advertiser owned sites, qualifying cookies as an advertisers' first party data and leaving brand data poisoned[21].

Virtually any programmatic buy can be exposed to ad fraud; even direct programmatic TV buys are vulnerable. Any claims to the contrary should be treated with caution.

In the case of website fraud, the oldest and most commonly used form of ad fraud, there are three key aspects to consider.

1. Spam-sites. These are a phenomena (covered in some detail below) uniquely associated with ad fraud. While extensive resources are available for analysing and blacklisting IP addresses associated with fraudulent traffic, no similar resources are available for ad fraud related spam-sites. Out of the top 5,000 sites based on traffic available for media buyers through ad exchanges, almost 30% use privacy solutions making it hard, or virtually impossible, to connect the website to any individual or company.

   Such sites typically send 10 to 100 times more traffic to advertising exchanges than sites such as Alexa[22] suggest to be possible. It is not uncommon for such a site to send a hundred million impressions (or more) to be sold in ad exchanges in a single day.

2. Traffic. It is important to understand that there are two kinds of traffic; one with potential for advertising effectiveness, and the other with no potential for advertising effectiveness. Examples of the kind of traffic that fall in to the latter category include:

   - auto-refresh traffic - when the user's browser keeps refreshing the page (or ads on the page)
   - clickjacking traffic - where a user is "forced" to click something else than what they think they are clicking[23]
   - cloudbot traffic - traffic coming from hosting company cloud IP addresses[24]
   - common botnet traffic - traffic coming from compromised user devices
   - cookie stuffing traffic - redirection of a user to a website for the purpose of dropping an affiliate cookie on the browser[25]
   - farm traffic - user actions (usually conversions), repeated by a large number of people[26]
   - hidden ads - ads 'stacked' on top of each other, or otherwise hidden from user view
   - social spam traffic - misleading links posted on social media result in worthless visits

3. Spambots. A typical social bot may post content from multiple sites thousands of times per day. These social spambots are used to create the impression of a popular site, by showing high levels of sharing associated with the content on the site.

Ultimately it is irrelevant if the illegitimate traffic is composed of botnet traffic, one of the other forms of traffic mentioned above or other means. What matters is the absence of potential for advertising effectiveness.

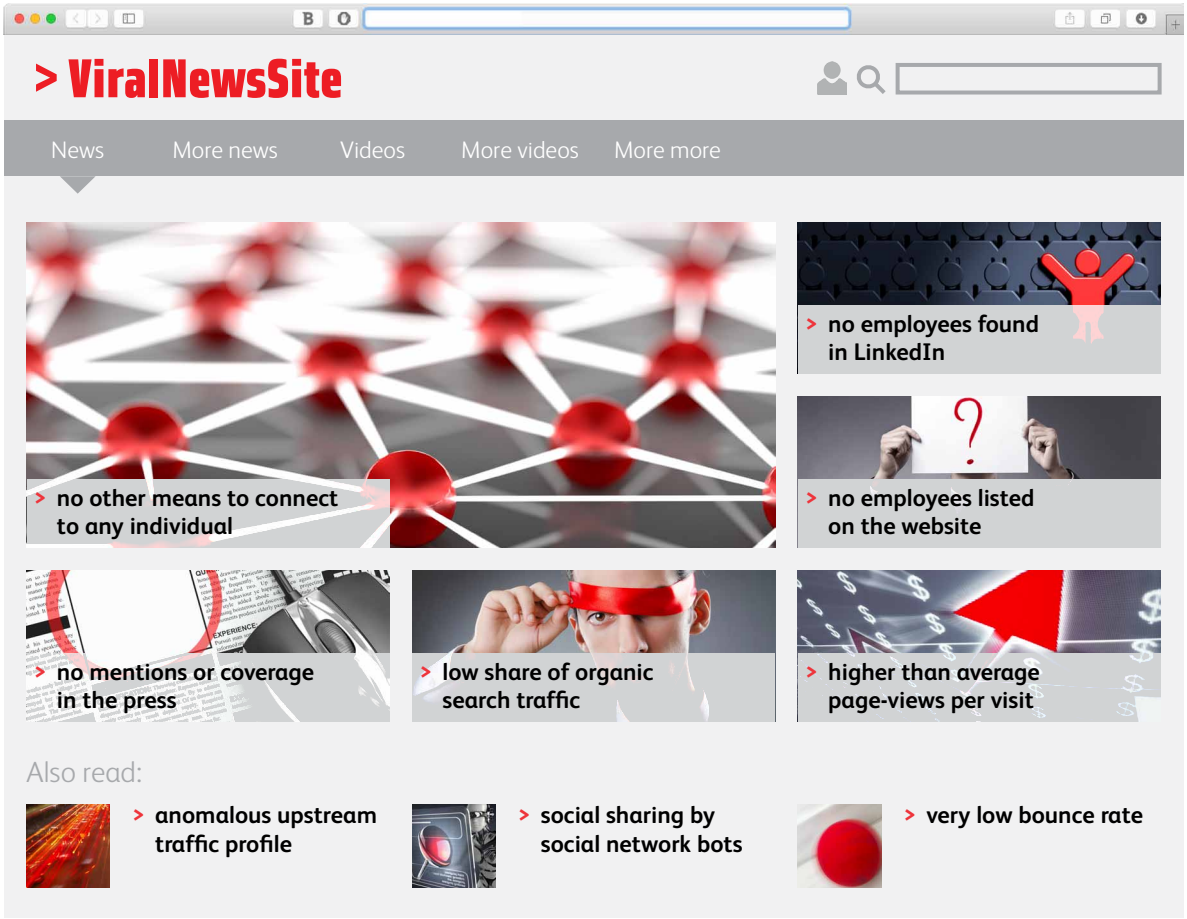
The industry's focus should be concentrated on the two areas where the ad fraud money is being made; spam-sites and sourced traffic.

[19] *Digiday/Mike Nolet > http://digiday.com/platforms/one-fraud-site-netted-161-million-impressions-one-week/*
[20] *http://www.ft.com/cms/s/0/53ac3fd0-604e-11e5-a28b-50226830d644.html#axzz49fKzb39V*
[21] *https://medium.com/ad-fraud/direct-buy-poisoning-how-data-fraud-leaves-transactions-vulnerable-to-fraud-a5cc25f11319*
[22] *http://alexa.com*
[23] *https://en.wikipedia.org/wiki/Clickjacking*
[24] *http://www.darkreading.com/cloudbot-a-free-malwareless-alternative-to-traditional-botnets/d/d-id/1297878*
[25] *https://en.wikipedia.org/wiki/Cookie_stuffing*
[26] *https://en.wikipedia.org/wiki/Click_farm*

VIRAL SPAM-SITES AND SOURCED TRAFFIC

The great majority of the Top 5,000 sites (by inventory) available in ad exchanges, are some form of viral-news site[27]. These sites, and countless others like them, are taking a substantial share of the total investment on programmatic media, while their traffic quality suggests that there is very little room for any advertising effectiveness from the investment made.

Typical attributes for such a site include:



Because these sites compete directly with premium publishers for their share of global media investment budgets, premium publishers are pressured to buy sourced traffic. Some researchers consider sourced traffic buying to be a widespread practice among even the most well-known publishers.

Sourced traffic has become to internet publishing what performance enhancing drugs became to sports; if you want to compete at the highest levels of the game, the surest way to do that is by resorting to "doping". Similar to doping in sports, sourced traffic gives the publisher an unfair advantage over those that are clean.

The issue is that once doping begins, it becomes almost impossible to stop without negatively impacting performance.

"While conclusively establishing a credible overall exposure rate to ad fraud globally or even locally is still hard at this point, during our regular campaign monitoring on behalf of our major advertiser clients, we have seen many individual publishers with 100% non-human activity, and some major (premium) publishers with +70% of non-human traffic. Although some publishers might directly engage in purchasing traffic via botnets, nonhuman traffic on premium publishers is mostly because of low quality sourced traffic, web crawlers and scrapers."

Ehsan Mokhtari,
President & Founder of Sentrant Security & Advertising Fraud Council member

Traffic can be acquired specifically to meet the requirements of leading verification vendors, at well below $0.01 per click, including audience measurement companies and counter ad fraud companies. It may also be manipulated to have the appearance of higher viewability rates than legitimate traffic. Whereas legitimate publishers can only offer what they actually have, perpetrators of ad fraud can adjust their inventory to appear more desirable to buying algorithms, establishing an advantage over legitimate sellers in winning buyer bids for inventory.

Recommendations for advertisers to better manage, and limit, their exposure to sourced traffic are documented in the Association of National Advertisers' (ANA, US) recent report: 'Sourced Traffic: Buyer Beware'. Recommendations include requesting transparency, requesting reporting from agencies, setting reasonable campaign goals and paying attention to mid and long-tail publishers.

This report also refers to Publisher Sourcing Disclosure Requirements (PSDR), a set of guidelines being developed by the Trustworthy Accountability Group (see more on pg. 18 below), whereby publishers are required to disclose the share that sourced traffic represents among their broader audience count.

Algorithms may also prioritise certain viral spam-sites over other sites due to being perceived as offering more 'desirable' inventory. This is linked to the widespread use of run-of-exchange targeting by trading desks and demand side platforms, a fact easily verified by investigating a given DSP's advertiser specific trading logs. One of the desirability factors is the ability for such a publisher to meet any volume of demand. Because of the pressure trading desks are under to meet budget goals, often set by clients over any other demand criteria, buying platform algorithms can be influenced towards buying poor quality sites[28].

Until run-of-exchange buys are replaced with a smarter way to achieve the same goal, spam-sites will continue to capture a large share of the programmatic ad market, now representing over 200 billion events per day.

[27] *Botlab.io Media 5k > http://botlab.io/media5k/*
[28] *http://www.minonline.com/news/The-Bots-Have-It-Ad-Fraud-and-Premium-Pubs_26247.html#.VzRM3hUrK7p*

WHO IS PERPETRATING AD FRAUD?

The main perpetrators of ad fraud are so-called 'black hat' marketers - highly skilled marketing technologists. Other adversaries include illegitimate ad networks and cybercriminals.

Involvement in this area from organised crime is limited at this point in time, but this is likely to change as criminals that have traditionally been involved in spamming and other forms of cybercrime increase their involvement in ad fraud. To slow down such progress, legal precedent for comparable sentences with other forms of cybercrime across major jurisdictions is needed. This is one of the key factors in preventing what could otherwise lead to dramatic ad fraud growth.

Ad fraud is typically perpetrated by the following adversaries that fall under three distinct groups, each with varying degrees of skill level and commitment to the practice.

	SKILL	COMMITMENT	THREAT
Marketing adversaries			
Black hat marketers	EXPERT	VERY HIGH	MODERATE
Certain illegitimate ad networks	MODERATE	LOW	MODERATE
Criminal adversaries			
Common cybercriminals	MODERATE	LOW	LOW
Organised criminals	MODERATE	HIGH	HIGH

Source: categories and descriptors based on the research and experience of the Advertising Fraud Council. Threat refers to the level of threat the class of adversary creates to society.

Black hat marketers. Many black hat marketers come from a webmaster, affiliate marketing or advanced SEO background. Even as lone operators, black hat marketers are able to operate at very large scale and are typically highly skilled marketing technologists with a deep understanding of persuasion and counter operative psychology.

Certain illegitimate ad networks. There are ad networks or ad platforms that knowingly participate in ad fraud activity, often by acting as an intermediary between black hat marketers and advertising exchanges. Performance (CPA) models are common among these ad networks. Some such ad networks appear totally legitimate under superficial inspection and often have access to premium advertising dollars directly from brands, or their agency partners.

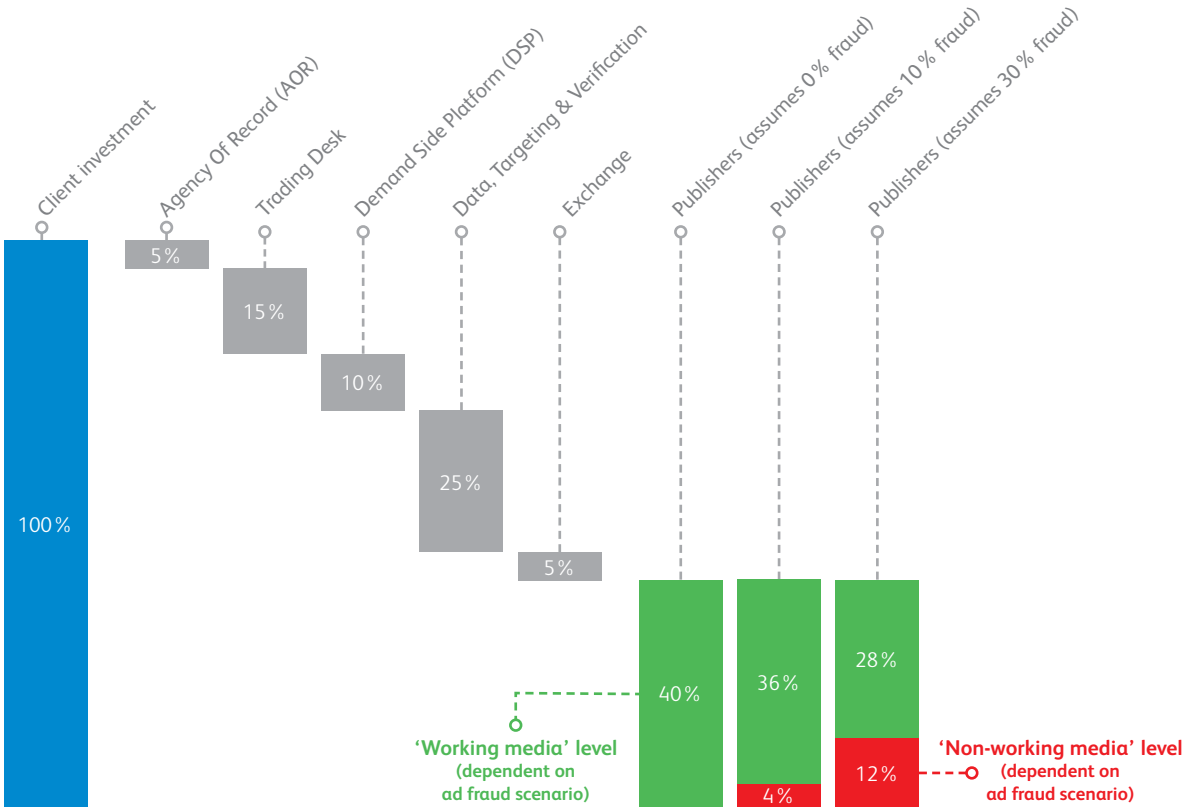
Common cybercriminals. With a background in cybercrime, spam and phishing, for example, cybercriminals may have been attracted to ad fraud due to the greater potential rewards available.

Organised crime. It's likely that there will be significant involvement from the kinds of criminals that had not previously been involved in cybercrime. The growth model introduced in this paper predicts that ad fraud will, on the current trajectory, be second in revenue only to cocaine and opiates by 2025 as a form of crime.

THE AD FRAUD MONEY-FLOW: COUNTING THE COST THROUGH THE CHAIN

There are various ways in which advertisers can buy digital media, but programmatic is by far the fastest growing means of doing this. There are many reasons for this, not least that many advertisers have identified a number of performance improvements from buying programmatically. However the complex infrastructure has served to exacerbate the vulnerabilities of the ecosystem, as outlined in the WFA's guide to Programmatic Media Management[29].

Given programmatic is widely anticipated to become the universal approach to buying all media, a typical programmatic buy has been taken as the basis for the following analysis. This shows where ad fraud enters the ecosystem and illustrates the impact it has on an advertiser's investment throughout the process.



Source: Industry estimates

Various intermediaries are involved in the typical programmatic buy, including trading desks, Demand Side Platforms (DSP), verification vendors and so on, each requiring a share of advertiser investment.

Approximately 40% of spend is received by the publishers with access to users at the end of the chain. So called 'working media'. But the reality is that a share of the traffic is fraudulent and has no potential for advertising effectiveness.

After introducing the ad fraud exposure scenarios established earlier in this document, working media levels are inevitably diluted further: to 36% when applying the 10% exposure level and just 28% working media under the 30% ad fraud scenario.

[29] *WFA Guide to Programmatic Media 2014 > www.wfanet.org/programmatic*

Before the ad fraud perpetrator enters the chain, the 'formal' industry has already been involved and paid for their part in the process. This, of course, is the case irrespective of the ad fraud exposure level and irrespective of whether the ad network or publisher is legitimate or operating an ad fraud scheme.

In both exposure scenarios considered in this analysis, **the main benefactor of ad fraud (albeit unintended), is the marketing industry. While 12% of revenues earned from ad fraud are received by the perpetrators in the 30% scenario, the remaining 18% is absorbed by the legitimate ecosystem.**

It should not be assumed that by going direct to publishers (programmatic direct) all risk of fraud exposure is removed. Spam-sites appearing as premium are prevalent among exchanges and even legitimate premium publishers present some ad fraud risks, due to the use of sourced traffic (covered earlier in this document), together with other factors.

Related to their earnings from the digital media ecosystem, most advertising technology companies and ad platforms lack the motivation to take the urgent actions that are needed in order create a safe and transparent internet advertising ecosystem. **As a result, the costs of ad fraud are borne exclusively by advertisers and tax payers.** Advertisers have no scope for effectiveness from their investment, and in some circumstances consumer computers' may be infected by malware in order to perpetrate fraudulent actions, seemingly on the part of the user.

THE AD FRAUD MONEY-FLOW: HOW THE TRANSACTIONS TAKE PLACE

Perpetuation of the ad fraud problem is largely connected with the policies and practices the other stakeholders have in respect to paying their publisher partners. In many cases a major ad network or exchange has just an email address for contacting a publisher partner they are paying tens or hundreds of thousands of dollars per month in publisher payouts. They might have never met any individual associated with the publisher. Yet over time millions of dollars may be transacted between the two parties in this way. The larger the ad network is, the harder diligence in this respect becomes.

Ad fraud transactions - where programmatic buys are placed through a trading desk

1. Advertiser pays the agency
2. Agency pays the demand side platform
3. Demand side platform pays the exchange
4. Exchange pays the publisher (or a conduit ad network who then pays the publisher)

All the transactions take place through the formal banking system according to the accounting practices of often very large companies. **This way the publisher, who may in fact be a large scale cybercriminal, can operate as a part of the formal economy.**

Shell companies are not uncommon as a way to further disconnect the adversary from the ad fraud activity they are engaged in. Such companies can be set up quickly and at scale. Ad networks and ad platforms do not typically conduct sufficient background checks on their partners, who they often never actually meet, so it is just as simple to operate under a fabricated identity, for example one acquired on the identity black market.

In summary, the larger the legitimate ad network or ad platform is, the larger their share of the total ad fraud economy. Even without any direct involvement in such activity or without having any intent for earning from ad fraud.

AN ADVERTISER'S GUIDE TO COUNTERING AD FRAUD

Ad fraud, and the various aspects related to, and causing it, are complex, but much can be achieved in terms of short-term results at the level of an individual advertiser. **But unless there is action from major advertisers, coupled with a common shared approach to tackling the problem, even individual short-term gains will quickly diminish as the underlying structural issues in the advertising industry continue to grow in both magnitude and complexity.**

This guide will not outline various counter ad fraud research and data analytics methods, detection methods or information that is widely available in the context of ad fraud directly. In the rapidly moving ad fraud market, such methods used in isolation from the guidance provided below, will lead to individual short-term gains at best, and to further sophistication of the adversaries at worst.

The only way for things to change is through successful behaviour change. In this case, understanding, managing and effectively countering ad fraud. **Behaviour** change is the result of **triggers** that act as a reminder as to why a given behavior is important to change; **motivations** that emphasise the seriousness of the needed change, and **abilities** that allow the needed change to take place.

1. PEOPLE & TECHNOLOGY

Develop in-house resources.

As all third-party solutions are provided by either small startups or companies that have previously been doing something different, **it is essential to develop in-house expertise to support vendor selection and other decision making - even if this is just one dedicated person.** Over reliance on third-party verification vendors at this point in time is not advised. Neither is reliance on your agency to lead counter ad fraud activities, as they are not yet incentivised or equipped to do so.

Encourage third-party vendors to leverage open solutions.

One of the keys to success with both Intrusion Detection Systems and Email Spam Filtering, (two major fields in countering cybercrime activity similar to ad fraud), is that even the largest and most respected vendors today tend to use the same open solutions as a basis for their propriety offering. The success achieved with network security (Intrusion Detection) and email spam detection, based on common and open technologies, illustrates the need for the same approach with ad fraud, as opposed to tactical propriety solutions. **Pure propriety solutions are easily reduced to a game of whac-a-mole against the perpetrator at best, and an improved ability for the perpetrator at worst.** Where propriety third party counter ad fraud solutions are deployed, it's recommended that regular spot tests are conducted side-by-side with other solutions, to monitor the fidelity of the technology.

Work closely with cybersecurity partners.

Most major advertisers will already have substantial relationships with cybersecurity companies. These companies have an established track record in systematically reducing exposure to problems similar to ad fraud and will also have less bias towards a particular approach to countering ad fraud. Working together with partners in the field of cybersecurity outside of adtech is a simple way to improve understanding of the common threats related to internet advertising, and to receive unbiased evaluation of advertising technology vendors and solutions.

Demand full transparency for your investment.

Much of media investment is currently to some extent opaque at the exchange level. **Discussions around transparency must start with the provision of full and accurate disclosure of referrers (websites), pertaining to investments above a certain level of inventory.** The other common reason for advertisers not having full disclosure to how their money is being spent, is linked to the way media agencies report investment. Insisting on transparency at this level throughout the ecosystem is one of the surest and fastest ways to create grounds for a safer marketplace.

2. EDUCATION & COMMUNICATION

Set clear expectations.

Revision of partner incentives and contracts has to start with a clear articulation of expectations. For example, it is not a reasonable expectation to say that there can be no fraud at all, as this will force the partner to find ways for reporting something that simply cannot currently be possible. **It is very important to understand that a single-digit percentile of exposure to ad fraud will very likely prevail against any counter measure.** Vendor claims to the contrary should be treated with caution.

Set appropriate metrics.

Partners have not been sufficiently incentivised to avoid fraud - an issue at the heart of the epidemic. It is important to understand that **moving from CPM to CPC or CPA is not a solution to reduce ad fraud - it will often make the condition worse and harder to tackle.** The only exception is those cases where payments for CPA deals are based on the actual business outcome, such as a new customer for a bank or goods sold that are no longer refundable. As an example, a bank does not get any business value from a credit card application resulting from a CPA deal, but from a customer actually making a deposit to an opened account or using a card of the bank in question. Performance metrics need, where possible, to relate back to an advertiser's business outcomes.

Open information sharing.

Findings related to ad fraud should be shared with all possible counterparts internally and externally to the fullest extent that is legally possible. Ad fraud is easy to move around but very hard to reduce, so sharing information openly together is a key to success for all parties involved. **Working together and sharing openly is one of the areas where the formal industry can be better than the perpetrators, who often operate in total isolation of each other, or exhibit hostility to one another.**

3. STANDARDS

Lists that replace run-of-exchange buys.

Run-of-exchange (ROE) buys should be avoided. These buys, where ads are bought blindly across millions of sites, are one of the surest ways of allocating money to ad fraud. ROE buys benefit the advertising technology vendors, and have no other unique benefit. A common vendor-side counter argument to this is that it's the only way that an ad platform can meet budget goals in terms of total spend per campaign or over a given time period. An argument that in itself clearly indicates the deep structural issues of the industry. **In the short-term, advertisers have to accept that in some cases digital investment 'targets' will not be achievable without exposing buys to high levels of fraud.**

"Advertising inventory that is completely ad fraud free might be impossible to achieve. We should be relentless, however. By working together. Sharing and learning internally and externally. And through setting targets we will progress, bit by bit. We're using the same approach with viewability - and it's working."

Gerhard Louw,
International Media,
Deutsche Telekom AG
& WFA Global Transparency
Group member

A database of common websites.

A database of websites maintained by an independent party, where quality metrics and other key transparency factors are available in an open and free manner for the entire ecosystem to readily access. If an investment to a website exceeds a certain amount in a given period, such a website should be required to register additional information about their business in the common website database.

A database of common adtech vendors.

With the exception of well-known ad platforms, it can be very hard to find out which company is behind a given ad tag. Tags handling a very high volume of requests are often hosted on domains that are only weeks or months old, and are using an obscure domain name combined with complete privacy protection. Even if a researcher wanted to create a picture of the ad traffic flow, and the money-flow based on this, it would be possible only at a relatively superficial level. To effectively counter this, a common vendor database is needed. This is an example of where initiatives such as the US' Trustworthy Accountability Group (TAG*) could play a role.

**TAG is a cross-industry accountability program. A joint marketing-media industry program, TAG was created with a focus on four core areas: fraudulent digital advertising traffic, combating malware, ad-supported Internet piracy and promoting brand safety. TAG was created by the Association of National Advertisers (ANA), American Association of Advertising Agencies (4A's), and Interactive Advertising Bureau (IAB) and works with companies throughout the digital ad supply chain. http://www.tagtoday.net/*

4. GOVERNANCE

Contractual changes.

Contracts with agency and vendor partners should be revised to the extent where contractual liability becomes the key driver for partner behaviour change. The focus should be on penalties for misallocating spend to ad fraud related inventory, where preventing it could be reasonably achieved.

Working with the authorities.

Advertisers can help by sharing findings and data, and by reporting significant issues in the ecosystem with the relevant authorities. The UK's Incorporated Society of British Advertisers (ISBA) has embarked on one such initiative* with the City of London police relating to brand safety.

**ISBA has worked closely with the City of London's Police Intellectual Property Crime Unit, as part of a unique partnership between the police and the UK digital advertising industry to fight illegal activity related to online advertising. The goal is to protect advertisers by ensuring that their ads don't appear on illegal, IP infringing websites, thereby starving these sites of revenue advertisers unwittingly provide.*

Pushing for legal consequences equal to those from similar crimes.

Because there is no legal precedent for sentences, law enforcement agencies are not appropriately resourced to seriously investigate ad fraud crimes, regardless of the size of the operation or other factors.

Seeking retrospective remedy from partners.

The commissions/fees made by ad networks, ad platforms or agencies where campaigns were subject to ad fraud should be returned to the respective advertisers. Seeking remedy is important because it will signal to the vendor ecosystem that it is no longer possible to earn commissions from passive inaction.

"This guidance is not about apportioning blame. It's about starting along the road to finding workable solutions for advertisers. Behaviour change is needed from all players in this ecosystem. Not only brand owners, but from all of those to whom we entrust our investment, not least our agency partners."

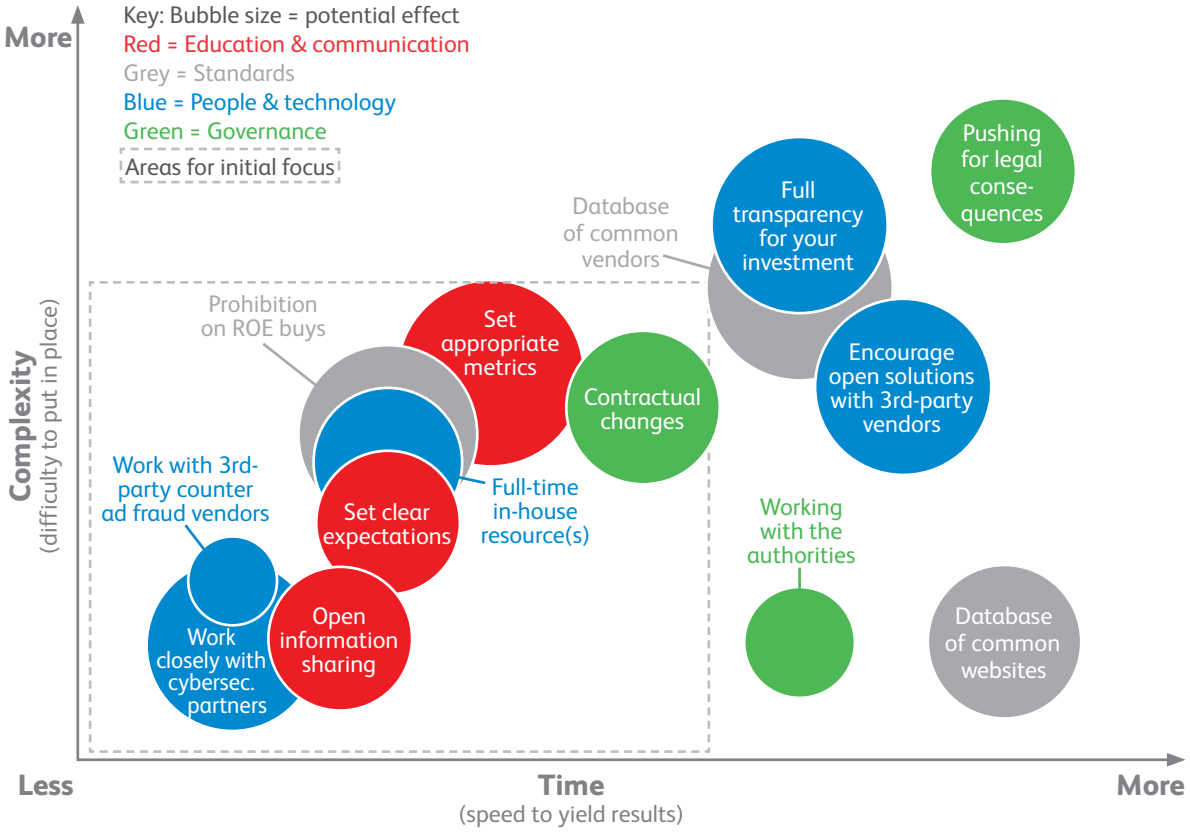
Sital Banerjee,
Global head of Media, Philips & WFA Global Transparency Group member

HOW CAN ADVERTISERS TAKE ACTION TODAY?

The actions outlined above can be further broken down by time (how quickly it yields results), effect (how great the result is), and complexity (how difficult it is to do).

Many of the solutions covered in this document fall within the bottom, left-hand quadrant of the chart. As they're relatively less complex and take less time to implement they are recommended as 'areas for initial focus.' Working with cyber security partners and open information sharing are clear areas to concentrate on in terms of their relative ease to put in place, while setting appropriate metrics may have the greatest effect overall.

At the other end of the spectrum, pushing for legal consequences should not be discounted due to the relative complexity and time required to implement the process. There can be few signals to the market as strong as this which convey the intent of the advertiser community.



"The problem we face is complex and may appear intimidating. But ignoring it by looking the other way, is not an option. For many brands who have spent the past decade or more advocating for greater investment in digital media, this will not come as welcome news.

The answer is not to abandon digital nor stifle innovation. However, we do need to apply far more caution and greatly enhance our capabilities in this fight. WFA will be focusing our efforts on further developing solutions for our members to protect their brands and their investments.

It is also incumbent on the broader industry to accept the need for change; to put aside vested interests and embrace the potential for open solutions similar to those which have proven to be effective in other instances of cybercrime.

This will not be an easy fix. But we're convinced that, collectively, our industry can address the challenge to the benefit of the digital ecosystem and society at large."

Stephan Loerke,
Chief Executieve Officer, WFA
& WFA Global Transparency
Group member

GLOSSARY

Ad stacking > a fraud technique where multiple ads are served to a single ad-slot on a page, effectively on top of each other, meaning that ads beneath the top layer are not visible.

Audience extension > a practice used by publishers in situations where they cannot meet demand for their advertising inventory. A publisher may use their first-party audience data to buy the same audience on other websites, and sell inventory as their own. This technique risks a significant drop in inventory quality versus the publisher's own inventory, while advertisers may be under the impression that their ads are being served only on the publisher's site.

Botnet > a 'bot' is a type of malware used to control an infected computer or mobile device. A group or network of machines that have been co-opted this way and are under the control of the same attacker is known a 'botnet'.

Click fraud > where fraudulent clicks are reported as legitimate ones.

Conversion fraud > where fraudulent user actions, such as sign-ups to receive more information about a product, are reported as legitimate.

Cookie stuffing > a technique where an affiliate cookie, from a third-party website, is delivered to a user's device without the user visiting the third-party website in question.

Data fraud > where data (first or third party), is poisoned in a manner where cookies, or other identifiers, connect to bots and not users. In other cases identifiers may be correctly associated with users, but as a result of fraudulent activity the actions may be misreported.

First party data > YOUR data. This is data collected from your own customers/audiences and can include: behaviours, actions or interests demonstrated across your website(s); personal data you have in your CRM database; subscription data; owned social data.

Fraud farms > a human-powered approach, where fraud (typically conversion fraud), is executed at low cost by using cheap labour, more often found in developing countries.

Impression fraud > where fraudulent impressions are reported as legitimate ones.

Intrusion Detection Systems (IDS) - an IDS is a device or software application that monitors network or system activities for malicious activities or policy violations..

Run Of Exchange/s (ROE) > a commonly used targeting option where inventory is purchased from any site available from the exchanges, accessible through a given ad buying platform.

Social Spambots > bots that share links from social platforms.

Sourced traffic > fake traffic that is bought from the sourced traffic market. Typically the traffic originates from toolbars (injections) or other adware, cloudbots or conventional botnets, or other fraudulent sources.

Spam-sites > websites that are typically focused on arbitraging sourced traffic in the legitimate online advertising ecosystem, or are engaged in other forms of fraudulent activity.

Third party data > is data generated on other platforms and often aggregated from other websites. It can be used for standalone marketing purposes or to augment and enhance first party data.

Web crawler > an Internet bot which systematically browses the World Wide Web, typically for the purpose of Web indexing.

Web scraper > computer software technique of extracting information from websites.

Botlab.io is a research foundation focused on researching ad fraud, user rights violations and other malicious practices in the advertising technology supply-chain. It is the only internet user focused public advocacy group started by ex adtech industry insiders and led by researchers. Mikko Kotila is Principal for Botlab.io, an internet advertising veteran and a respected advertising technology industry influencer and innovator. Mikko has researched ad fraud and related topics actively since 2005, has more than 20 years of experience as an internet researcher and works with Botlab.io as a full-time volunteer. Mikko co-authored this guidance with the WFA.

Advertising Fraud Council is a collaborative research and advocacy initiative curated by Botlab.io that focus on advanced research on the topic of advertising fraud. The council members consist of a major adtech company counter fraud lead, CEO of a counter ad fraud startup, independent security researcher, academic professor, independent ad fraud consultant and one non-profit leader. The council members work closely together by sharing resources and data, and by joint research and development.

WFA is the voice of marketers worldwide, representing 90 % of global marketing communications spend – roughly US$700 billion per annum – through a unique, global network of the world's biggest marketers and biggest markets. WFA's champions responsible and effective marketing communications worldwide. More information at www.wfanet.org

WFA - World Federation of Advertisers
Avenue Louise 166
B-1050 Brussels – Belgium
+32 2 502 57 40
info@wfanet.org wfanet.org @WFAmarketers