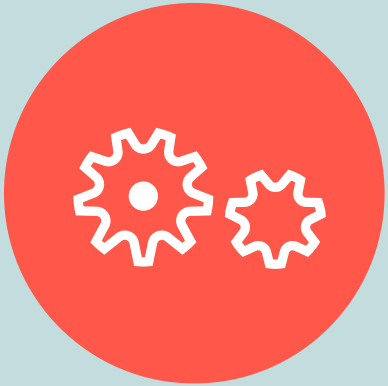
Ad fraud

A short guide

IAS Integral Ad Science

Everyone knows there is a problem, but it's not always clear:

What exactly is fraud



How it works

How to eliminate it from the digital ecosystem

We're here to make this complex topic easy to understand and address.

So, what *exactly* is ad fraud?

Selling inventory automatically generated by bots or background mobile-app services

Serving ads on a site other than the one provided in an RTB request—this is known as domain spoofing

Delivering pre-roll video placements in display banner slots

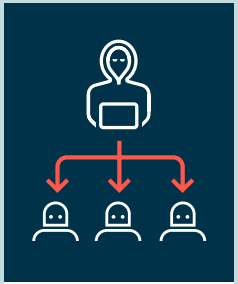
Falsifying user characteristics like location and browser type

Hiding ads behind or inside other page elements so that they can't be viewed

Hindering a user's opportunity to engage by frequently refreshing the ad unit or page

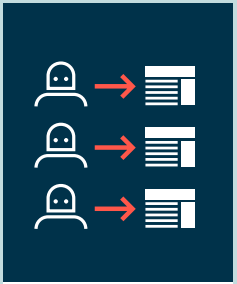
Why does ad fraud occur?

How does fraudulent traffic occur?

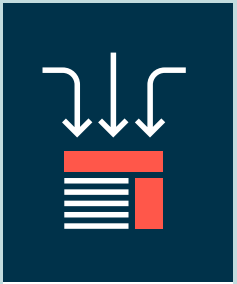


Hackers use code to create bots able to take orders from botnet center

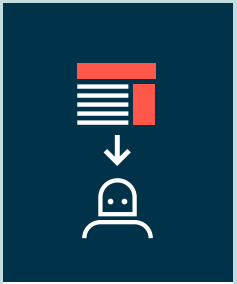
Users unknowingly download and install bot engines on their computers



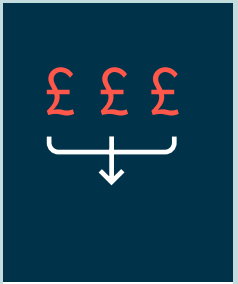
Bots are instructed to visit premium sites, picking up desirable cookies, and then visit fraudulent sites



Highly trafficked fraudulent sites use exchanges and networks to attract advertisers



Ads are continuously served to bots



Botnet operator gets paid

Types of fraud

Ad fraud disrupts the aim of advertising: delivering the right message, to the right person, in the right place. Fraudsters compromise all three areas of advertising through various techniques like pixel stuffing, ad stacking, nonhuman traffic, domain spoofing, user-agent spoofing, and more.

The most prevalent forms of fraud are nonhuman traffic and domain spoofing.

Pixel stuffing
Serving one or more ads in a single 1x1 pixel frame, so that the ads are invisible to the naked eye.

Cookie stuffing
Cookie stuffing can happen in different ways. One method of cookie stuffing is to place multiple cookies on a user or bot so that they get targeted at higher CPM.

Ad stacking
Placing multiple ads on top of each other in a single placement, with only the top ad being viewable.

User-agent spoofing
The header information is modified to lie about the browser that's being used, which can interfere with some kinds of user targeting.

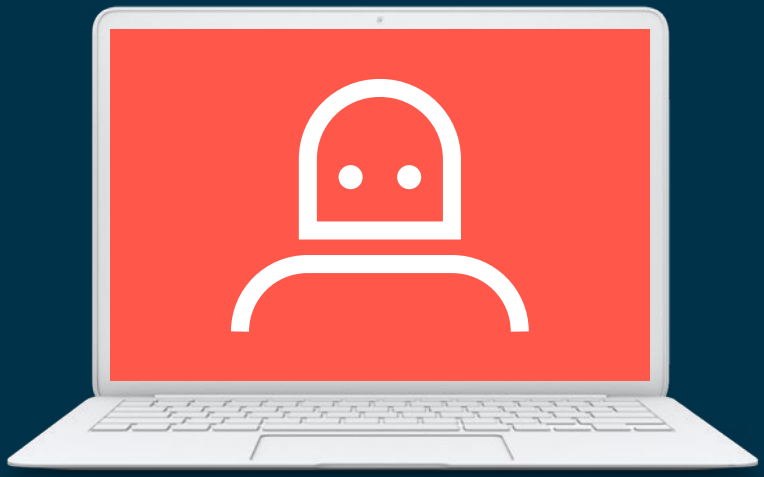
Location fraud
An advertiser pays for inventory to be served in a particular country or region, but the traffic is actually served elsewhere.

Domain spoofing
Domain spoofing is commonly used to mask unsafe sites. Fraudsters can spoof the domains of sites like video piracy sites, etc., in order to conceal their real identity and monetise the traffic.

Bots

When most people think of ad fraud, they think of bots. While other forms of fraud provide small boosts to CPMs, bot traffic can create revenue streams where there were none before. Bot traffic also makes it harder for the industry to identify who's behind it.

While only 43% of the industry said they understand how fraud is detected, there is increasing demand for transparency when it comes to fraud reporting, especially for bot traffic. Advertisers and media partners need more informative conversations about fraud in order to mitigate the risk within campaigns, which requires more information in general.



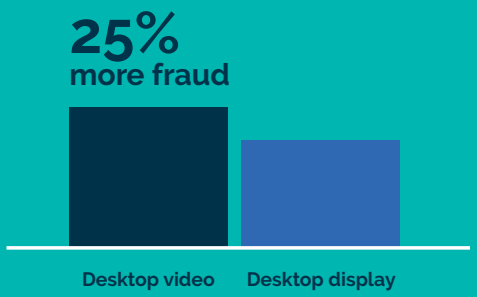
Fraud and video

According to the IAB, in the first half of 2016, brands spent over £400m on digital video in the UK—a 69% increase since the start of 2015.

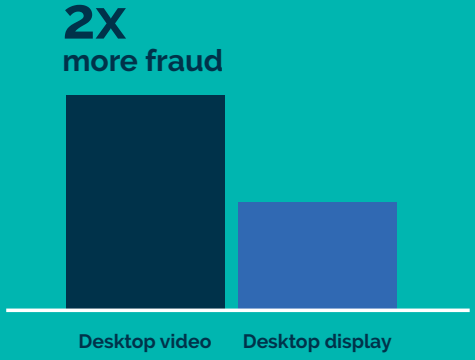
Nothing is more powerful than connecting with consumers through sight, sound, and motion.

But video inventory is particularly susceptible to fraud—across premium and programmatic video—because the medium has the highest CPM and the greatest expected impact.

PROGRAMMATIC BUYS



DIRECT BUYS



Fraud and mobile

Mobile ad spend is projected to top £1.72 billion in the UK in 2016, according to the IAB.

That's 51% of the entire digital market.

As mobile continues to grow in consumer usage—and as advertising follows—it's expected that fraud techniques will become more tailored, and more pervasive.

Malicious apps
Apps can generate fraudulent impressions without the user knowing. This can be thought of as a kind of mobile malware.

Hidden ads
Common in desktop fraud, hidden ads are generated in-app in a way that is not visible to the user.

Background services
Services running in the background are able to render ads even when the app is closed—or not even started!

Cloud hosting
In-app impressions are generated by hosting mobile-operating-system emulators or devices in the cloud and running apps that display ads.

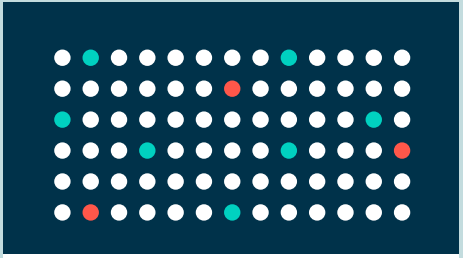
App-name spoofing
Similar to domain spoofing in display, app scan submit a false ad-unit identifier or app identifier to the bidding platform.

How to identify and fight fraud

As fraud becomes more sophisticated, the digital industry needs more sophisticated fraud detection to evaluate the legitimacy of impressions and to prevent the buying and selling of fraudulent inventory.

Watch Scott Knoll, our C.E.O. and president, discuss the global fight against fraud with *The Drum*.

There are really three pillars in dealing with ad fraud:



Behavioural and network analysis

Using data science to understand users

Browser and device analysis

Using web technologies to understand implementation

Targeted reconnaissance

Using malware analysis, software disassembly, and the infiltration of hacker communities (also known as black-hat monitoring) to guide detection development and identify emerging threats

These techniques are all required for a well-rounded, sophisticated, program of detection and prevention.

In order to effectively combat fraud, it's critical to develop techniques leveraging data science and advanced web development, both guided by intensive intelligence gathering. Techniques relying on specially designed data collection within the ad display environment are sometimes referred to as session-based signals or side-channel analysis.

With these three pillars as a foundation, today's technology applies advanced learning about fraud to real-time signals to make a decision about the existence of fraud on a given web page.

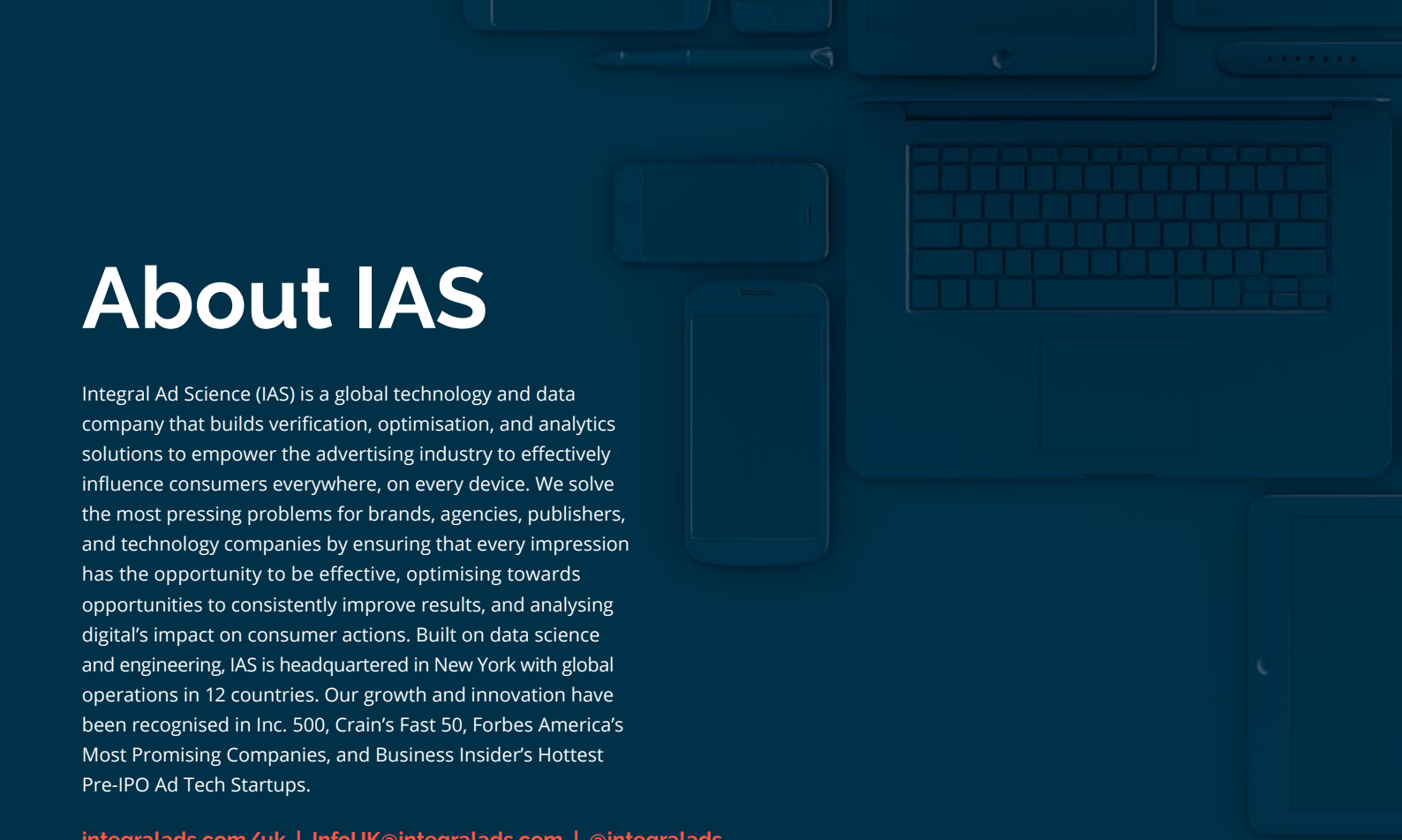
Identify fraud

- Measure fraud across all campaigns to understand aggregate performance against fraud.
- Use fraud solutions that have been accredited by the MRC for both general *and* sophisticated IVT.
- Follow the MRC guidelines for IVT detection and filtration.
- Ask your ad server, fraud solution, or other vendor how it measures for bots and other forms of IVT.
- Offer and request more transparency into inventory and traffic, including sourced traffic and audience extension
- Use verification and fraud services that can confirm ads were delivered on plan (to the sites, devices, geographies, and audiences desired); whether the environment had ad clutter and other placement concerns; whether it was brand-safe.

Prevent fraud

- **Block fraudulent impressions before they hit the creative ad server.**
- **Anti-target infected machines that have been tagged in order to prevent future ad targeting.**
- **Anti-target pages that have historical levels of fraud, which can be tracked through page-level scoring.**
- **Use blacklisting and/or whitelisting.**
- **Use pre-bid screening.**

The biggest factor here is awareness and participation. It's critical that all members of the digital ecosystem are a part of the process and solution.



About IAS

Integral Ad Science (IAS) is a global technology and data company that builds verification, optimisation, and analytics solutions to empower the advertising industry to effectively influence consumers everywhere, on every device. We solve the most pressing problems for brands, agencies, publishers, and technology companies by ensuring that every impression has the opportunity to be effective, optimising towards opportunities to consistently improve results, and analysing digital's impact on consumer actions. Built on data science and engineering, IAS is headquartered in New York with global operations in 12 countries. Our growth and innovation have been recognised in Inc. 500, Crain's Fast 50, Forbes America's Most Promising Companies, and Business Insider's Hottest Pre-IPO Ad Tech Startups.

integralads.com/uk | InfoUK@integralads.com | @integralads


IAS
Integral
Ad Science
Digital made smarter