AD FRAUD AND BRAND SAFETY

THE CHALLENGE

In 2019, online display and video advertising spend hit $3.5 billion in Australia. We know that on average 2-3% of this category of advertising spend is lost to ad fraud, suggesting that in excess of approximately $100m per year is forfeited - a significant figure in anyone's eyes.

While ad fraud has the greatest direct financial impact on advertisers, brand safety has a significant impact as the perception and value of a brand can be eroded by the placement of ads beside content that is deemed unsuitable and, in extreme cases, harmful.

Ad fraud and brand safety are separate and significantly important issues posing a major challenge to advertisers as they consider where to invest their advertising budgets. However, the practices and tools employed to address them are often the same.

WHY ARE AD FRAUD AND BRAND SAFETY IMPORTANT?

Ad fraud is the practice of fraudulently representing online impressions, clicks, conversions or data in order to generate revenue. The impressions that result from intentionally deceptive practices, designed to manipulate legitimate ad serving or measurement processes or to create fictitious activity lead to inflated impression numbers which can skew media results and waste marketing dollars. Publishers are also impacted as they ultimately lose revenue.

There are three key descriptors of ad fraud:

- Invalid Traffic (IVT): Any traffic to a website that is generated, either intentionally or unintentionally, that is invalid. This comes in two distinct forms:
  - General Invalid Traffic (GIVT): Traffic that comes from known non-human sources on publicly available IP lists such as crawlers, proxy traffic, data centre traffic, bots and spiders. These are benevolent (whilst still being non-human) and do not engage with ads. Most ad serving and tracking systems are sophisticated enough to ignore these by default.
  - Sophisticated Invalid Traffic (SIVT): Non-human traffic that is more difficult to detect, is the result of criminal efforts and requires advanced analytics or human intervention to analyse and identify. Examples include malware installed on a computer, hijacked devices, cookie stuffing (the practice of dropping multiple cookies after someone views a page or clicks on a single link) and incentivised browsing.

It may sound complicated but at its most simplistic level, ad fraud involves the gaming of digital advertising, mostly through the use of technology.

Some real-world examples of ad fraud include:

- The delivery of pre-roll video placements in display banner slots.
- Falsifying user characteristics such as location and browser type.
- Hiding ads behind or inside other page elements so they cannot be viewed.
- Selling inventory automatically generated by bots or background mobile-app services.
- Serving ads on a site other than the one provided in a real-time-bidding request, a practice known as domain spoofing.
- Hindering a user's opportunity to engage by frequently refreshing the ad unit on a page.

The real challenge is that there is no way to remove all risk of ad fraud, but it can be minimised.

Brand safety refers to exposure to an environment and/or context that will be damaging or harmful to the brand.

This could be an ad published next to, before, or within an unsafe environment that promotes religious extremism, child endangerment, pornography, drugs or extreme violence.

AD FRAUD AND BRAND SAFETY

It is important to distinguish between websites that feature content promoting these topics from websites that report on them via public interest journalism.

It is an advertiser's responsibility to define what it views as acceptable levels of risk regarding brand safety, where risk is defined as strategic, operational, financial or regulatory.

Additionally, brand suitability must be considered, which refers to a brand appearing in a safe environment adjacent to, before or within content or a domain that is deemed by the brand to be unsuitable. An example of this could be a brand's ad appearing alongside news content that is negative for the particular industry or brand.

Brand safety is important because having an impression in the wrong context may be wasteful, but a potentially harmful impression can also contribute to poor brand perception, diminished brand equity or even lead consumers to boycott the brand and its products.

AD FRAUD AND BRAND SAFETY CHECKLIST

1. Determine your risk areas

Brand safety and suitability are broad topics that cover many different parts of a brand's business. There are a range of factors to consider, including whether advertising falls under certain legislation and regulation.

It is therefore critical to implement a risk assessment, control and action plan for ongoing review which considers the following:

- Define the business's risk tolerance: How much of a problem would it be to have a brand safety incident? What are all the themes which are deemed high or low risk to the brand and what do you consider to be issues? Are there any legal requirements when advertising that you need to adhere to? For example, the exclusion of advertising for gaming and alcohol products or restrictions around advertising to children.
- Complete a risk matrix: Consider the different types of inventory you will be using then assess the technologies available to manage these risks. Identify which stakeholders are required to sign off on the risk matrix.
- Ensure stakeholders understand there is no way to remove all risk: It can only be minimised, controlled and adjusted. Explain the types of risks you may face to various stakeholders — marketing, media, internal communications, legal, chief technical officers and external agencies.

The more risk averse a brand is, the more the opportunity of inventory is reduced. This can limit reach, increase cost for campaigns and also restrict the effectiveness of data being used to target an audience.

2. Determine and document suitable and unsuitable advertising environments

Depending on the risk assessment, control and action plan outcome, some brands may wish to avoid specific environments all together. For example, user-generated environments, native content, app networks and video networks have no way of preventing ads appearing against inappropriate content.

It is advisable to develop a brand suitability playbook which clearly sets out all parameters for new starters and agencies to use.

AD FRAUD AND BRAND SAFETY

3. Measure and monitor

Once a risk assessment has been performed, measuring and monitoring is key to ensuring compliance. All stakeholders, from internal through to media and creative agencies, must be aligned on the assessment and understand what is being tracked and measured; and what the acceptable metrics and standards are.

If all parties are clear on measurement and acceptable metrics, risk is reduced and, if a brand safety incident arises, management of the issue can be expedited.

4. Create an exclusion list to protect your brand's image

An exclusion list, sometimes previously known as a blacklist, is a list of websites and mobile applications which a brand does not wish to advertise on. Typically, an exclusion includes sites and apps that contain inappropriate content, excessive ad placement, deliver poor performance and have high levels of ad fraud.

When developing an exclusion list, advertisers should consider the balance between the cost to brand image from appearing on an inappropriate site versus the impact of reduced reach and the incremental cost of monitoring these sites.

5. Create an inclusion list

Rather than develop an exclusion list, some brands prefer to develop an inclusion list, sometimes previously known as a whitelist, which includes the sites and apps where ad placements can run. An inclusion list gives advertisers the most control and typically includes sites and apps that contain appropriate content, have quality ad placements, have low levels of fraud, a good historical performance and will help protect the brand's image.

Building an inclusion list of long-tailed sites would be resource intense so generally speaking, sites and apps with high audience volumes are recommended for this approach.

This approach is also not recommended for brands looking to target niche content, as it would likely limit the direct response performance of campaigns by limiting reach.

6. Create a negative keyword list

A negative keyword list of explicit terms or 100% unsafe words, should be created to exclude unsafe or unsuitable environments. It should be used in conjunction with an inclusion/exclusion list approach to exclude ads from being triggered by toxic content or placed on sites that hold toxic content categories.

An example of this would be if content on the site refreshes or changes at a regular occurrence, such as a news site. You might choose to avoid negative news such as a terrorist attack or a natural disaster. Ensure you are aware of how often the technology being used scans (also known as 'spiders') the site for content and if the technology is reliant on the site correctly tagging and using metadata for analysis.

It's advisable to manage your keywords in conjunction with semantic contextual tools if possible, so as to fully understand the editorial context, and any associated risk, instead of relying on simple lists of blocked keywords (e.g. 'coronavirus' or 'crash').

7. Create a negative environment list

In addition to keywords, publishers have other filters available to specify the right level of brand suitability for your brand. These can include broader inventory modes, content labels similar to those used in the film industry, as well as more specific topics and categories to be avoided. You are encouraged to consider developing a list which specify specific environments that should be excluded

AD FRAUD AND BRAND SAFETY

in campaigns. An example of a common practice is to exclude mature content, unless the brand specifically wants ads to show alongside more risky content.

As with keywords it's important to document these exclusions to ensure they are used consistently and to keep these lists updated over time.

8. Maintain all your exclusion and inclusion lists

To be effective, exclusion and inclusion lists must be dynamic, being updated regularly to reflect the constant evolution of risks, sites and platforms. Document and implement a process for the upkeep of the lists which might include:

- Setting up a system of review at regular intervals.
- Establishing if URLs that are flagged as fraudulent or not brand-safe will be automatically added to the exclusions list, or if this will need to be done manually. If it will be done manually ensure someone is assigned this responsibility.
- Understanding how exclusion and inclusion lists are applied and verified by agency partners.

9. Set clear guidelines on transparency and accountability

Clear guidelines around accountability and transparency need to be set for every vendor and partner that is involved transacting or ad-serving ad placements for your campaigns. These guidelines should be considered when establishing or reviewing vendor agreements and the onus is on the advertiser to:

- Agree how impressions lists are supplied and when.
- Check whether anonymous/masked URLs are to be blocked.
- Check whether site lists have domain-level transparency and if aggregated exchanges or networks are blocked? Do they need to be?
- Establish a declaration of any guaranteed inventory sources in an aggregated buy.
- Ensure there is the opportunity for any sites to be removed mid-campaign within 24 hours of request.

10. Determine your technology

There are numerous considerations around which technology should be used to combat ad fraud and brand safety issues. These include:

- Agree which ad verification technology vendor to use: Understand each vendor's pros and cons and the cost implications of using their technology.
- Accreditation: Ensure that the vendors you are considering are accredited and meet MRC industry measurement standards for the filtration and disclosure of invalid traffic.
- Is URL analysis needed?: If you want to analyse a site's URL and the page URLs this will be required. For example, a news website may be 95% brand safe but there may be certain articles on the site that are not safe for the brand. URL analysis will help to determine these.
- Will the technology analyse inbound and outbound links?: Inbound and outbound links are sites that link to the page or sites the page links to. For example, a page full of adult images may have no keywords to analyse in the verification process, but the page may contain links to other adult sites that can provide an indication of the content.
- Will the technology conduct metadata (code) analysis?: Metadata does not appear on the page itself but it includes keywords and other indicators in the site code that are important.
- Ads.txt : An IAB-approved text file that aims to prevent unauthorised inventory sales, the ads.txt file lists all of the companies that are authorised to sell a publishers' inventory. Programmatic platforms also integrate ads.txt files to confirm which publishers' inventory they are authorised to sell. The use of ads.txt allows buyers to check the validity of the inventory purchased, however not all publishers have adopted ads.txt so it may reduce campaign reach if only ads.txt authorised sites are used.
- Investigate using pre-bid solutions: As the name suggests, a pre-bid service can assess the brand safety risk ahead of the time of the bid. This can provide additional safety; however, the costs are often much higher and may restrict the reach and performance of the campaign.

AD FRAUD AND BRAND SAFETY

11. Determine your reporting requirements

Ensure reporting requirements are discussed and agreed. This should include a site list for all impressions delivered and you should consider manual URL spot checks pre, during and post campaign delivery.

12. Establish a breach process

Agree on a process to be implemented if a brand safety or ad fraud breach occurs. This needs to cover risk scenarios, stakeholder responsibilities and actions both internally and externally.

13. Sense check ad fraud and brand safety standards with your campaign goals

Optimising for ad fraud and brand safety can impact campaign cost, coverage and reach, so it's important to weight up the benefits of all elements. This includes supply and demand to cost, as well as understanding the percentage of activity that is being run through private marketplace and the open exchange. Buying from open exchanges is cheaper and can be effective, but there is more possibility of ad fraud or brand safety issues.

14. Define the billing process

If booking through an agency, the billing process will depend if an advertiser has a "guarantee outcome based model" or "itemised model" (sometimes referred to as undisclosed and disclosed models) arrangement with their agency. See page 5 in the Digital Value Chain module for more details on this.