Best Practices to Eliminate Non-Human Inventory Sources

Introduction

Reducing the ability for bot suppliers to profit from their actions will help reduce non-human traffic in the ecosystem.

Three common entry points for fraudulent inventory in the marketplace include:

1. As a buyer, purchasing impressions from ad exchanges and other platforms without trusting and verifying the identity of the organization with whom you are buying from – bad actors can present themselves by (a) constantly changing identities, leading to blacklisting and a game of constant whack-a-mole (explained in more depth later in this document), and (b) through impersonating the identities of legitimate publishers, breaking whitelists and leaving you vulnerable to bots.

2. As a publisher, buying "traffic" from 3rd party companies to increase your audience and impression volume – more often than not this traffic is bot ridden.

3. As a publisher, buying impressions from ad exchanges and other platforms for the purposes of audience extension, mixing external impressions with your own, and then selling those impressions to buyers. The same risks in #2 apply here, but the problem is amplified, as buyers who trust your brand may risk exposure indirectly to these activities.

Identify which area your company would fall under within this document and be sure to have conversations about this subject within your company as well as with clients.

Buyers

Advertisers should feel confident that the right tools exist to limit exposure to questionable inventory.

In any marketplace, there are always going to be people looking to game the system, that's as true for digital advertising as for any other. But, as we've seen across our industry, if you invest in preventing fraud, it will make a huge impact. The digital advertising space is already leaps and bounds ahead of where it was a few years ago and only getting better.

Identify the tools that will best fit your campaign's needs. Do not compromise on prioritizing this within your organization by skipping this vital step.

Find the right balance between performance and environment.

Performance benchmarks need to take into consideration the scope of inventory and adjust accordingly. While a closed marketplace will almost certainly deliver higher quality impressions, many standard performance benchmarks will deliver a less favourable result. It is important that marketers are conditioned to expect the right results relative to the environment they're buying.

The open market provides a higher risk threshold for fraud versus a closed marketplace.

Move beyond the click, focus on ALL the metrics.

Impressions, views, time spent, clicks, conversions and revenue are all very important metrics, so pay equal attention to each of them. Bots love to click on ads, so only focusing on clicks and click through rate can lead your campaign towards the inventory you most want to avoid. Almost every metric can be subject to fraud, but moving towards a hard conversion metric (any metric that demonstrates clear ROI lift or user activity) will be much more difficult to game. Focus on all the metrics holistically, and the hard (revenue generating) conversions will follow.

Measures which are easy for bots to fake:

- Ad views
- Clicks
- Video completes
- Cookie attribution
- Viewability scores

The following measures likely indicate human interaction:

- Purchases
- Subscriptions
- Validated panels
- Other verifiable engagements

Target trusted exchange environments that can deliver enough volume for your campaign goals.

Be mindful of the inventory sources you're running on; not all ad exchanges and platforms operate under the same business rules. Audit ad exchanges and other platforms frequently to understand which are part of your media efforts, and what they have in place for policies to limit the existence of questionable inventory. Also understand what policies they have in place to determine how new entrants to the exchange are classified; proactive versus reactive reviews of new inventory. And finally, understand what recourse you as a buyer have in the event the ad exchange or platform harbours fraud which you inadvertently purchase.

If you must buy unmeasurable inventory (iframe jailed), subject those vendors to a higher level of

scrutiny and contractual compliance. Request multiple sample URLs where you can observe the ads being delivered into the page.

Don't just set it and forget it. Trust the technology, understand the human component.

Know where you're buying and look at the results regularly. Develop trust in the ad exchanges, platforms and inventory sources that deliver real results and are validated as fraud free. There are standard reports that will give you the data you need to quickly identify bad traffic sources. Work with your programmatic team to understand the strategies to eliminate questionable inventory by monitoring the right reports and having a strategy to remove questionable sources.

- Request site lists up front from any new inventory source
- Verify delivery against those site lists, and monitor closely for violations
- Assess all metrics available, and not just CTR, look at viewability, fraud rates, engagement rates, etc.

Avoid anonymous inventory until the exchange/platform and source have been proven as trustworthy.

Anonymous inventory may include high quality publishers who prefer to be unlisted so they can protect their higher margin sales channels. That inventory is valuable and important. However, anonymous inventory can also include low quality sites that have fraudulent traffic. Without named site reporting, they are grouped together and it can be impossible to separate the high and low quality inventory. Only invest in supply sources which have a proven track record of quality. You can easily obtain that data by working with your programmatic team to run the required reports.

Set up private deals.

Once you have sites and sellers that you have seen consistent results from, you can secure large quantities of premium inventory at a negotiated price in a preferred deal or private auction environment.

De-prioritize manual blacklisting & whitelisting.

Blocking bad sites and giving the green-light to good sites can improve results; however it's much more efficient to focus on the previous tactics mentioned in this best practices document. Blacklisting sites on the open exchanges can be a bit like playing an endless game of whack-a-mole. It's a full time job and won't have a very good effort-to-results ratio. Whitelisting will not result in priority access or potentially fixed price rates that private deals have, either. Whitelisting domains alone will not work. Domains can be spoofed, so be very careful about over reliance of whitelists.

Sellers

Understand the value of your sites, why people visit and what they consume. Monitor your audience for anomalies.

If you invest in content and publish exclusive, engaging material, your human traffic patterns will have a rhythm. Through monitoring your analytics, you may see anomalies to this behaviour. If it looks too good to be true (e.g. 1 million contest entries in a day but they are all from Eastern Europe), it is.

Know where bots are concentrated and direct your resources to avoid them.

Bots are more prevalent in older browsers, for example, so choosing to support newer browser releases to older ones may reduce a publisher's exposure to ongoing bot traffic.

Be strict and diligent with trackers (beacons, pixels and tags) that are permitted on your sites.

Bot suppliers monitor the prevalence of third-party trackers, such as tags, pixels, and beacons on sites. Sites with a high concentration of bots allow up to four times as many trackers as legitimate, popular sites. Know that acceptance of trackers can increase your exposure to bots infecting your audience. Aim to know what each tracker is doing, why it is there and consider a direct contractual relationship with each tracking supplier to protect your interests as a publisher.

Protect yourself from content theft and ad injection.

Use a domain detection or bot detection service to monitor for content-scraping (presenting another site's content in a separate website and monetizing the scraped content with ads) and evidence of ad injection (when ads are forced into a website, unsanctioned by the publisher, often displacing the publisher's content or legitimate ads).

Approach any 'bought/sourced traffic' with extreme caution, or avoid it all together.

Sourced traffic, when a publisher 'buys' audience, should be monitored with the same scrutiny that an advertiser evaluates you. If you are investing in your content, what is the opportunity cost of infecting your sites with fraudulent audience and the risk of ad injection? If the industry moves to a cost per human metric, what is your value as a publisher?

Know where your inventory is traded, and look for it where it shouldn't be traded.

Police your brand's identity. In the programmatic space, domain spoofing is a common problem. Domain spoofing is a practice where an ad placement poses as a placement on a legitimate site by replacing the name of the domain where the ad appears (e.g. JoesGolfBlog.com posing as Sportsnet.ca). As a publisher, seeking out your inventory on exchanges and other platforms where you know you are not trading inventory can allow you to track down domain spoofing of your assets. Demand those exchanges/platforms blacklist the inventory and improve their policies for accepting inventory supply.

Glossary

Arbitrage – media bought at one price and sold at a higher price without any value add.

Bots – programs that move through the internet gathering and generating data from page visits. There are good bots that are filtered from media reporting and bad bots that aim to present themselves as the common consumer.

Cookie stuffing – Made for Programmatic inventory can be made even more valuable to fraudsters when the traffic appearing on the site(s) is identified as belonging to specific advertiser audience segments. To make this true, the controller of the fraudulent site(s) will often visit advertiser sites, cut and paste the pixels that set retargeting cookies, and install these pixel calls into their fraudulent sites.

Fraudulent clicks – Generating HTTP requests to advertisement click URLs, usually after an ad is served.

Fraudulent conversions – Similar to click fraud but requires certain requests for file downloads, or follows a specific order of page visits to generate a conversion. This only works if the action does not require spending money directly, like purchasing an item from the website.

Fraudulent traffic / botnets / impression fraud – Involves fake visits to publisher pages or ad servers directly, to artificially inflate traffic targets on campaigns. Botnets are the most difficult type of fraud to detect, and it is the most common source of fraudulent internet ad traffic. Botnets are unique in that the software required to perpetrate fraud is located on many benign users' machines. The malicious software usually comes in one of two types: those that run behind the scenes and act as normal click bots, and those that attempt to coerce the user of the machine to perform some of the ad fraud actions.

Made for Programmatic inventory – Web sites are created using pirated content (i.e. taken from other sites like YouTube or news sites). The ad inventory available on the fraudulent sites is made available to programmatic buying through exchanges. Robotic traffic and fraudulent clicks on ads appearing on this inventory result in the site appearing to perform well, thus

human buyers and algorithms will increase spend on the inventory, creating a positive feedback loop.

Media metric vs. currency – a metric is something that has been measured, while currency is the metric upon which trade is conducted. In any transaction there can be multiple metrics but only one currency.

Non-human traffic – online traffic activity that is created by bots.

Online ad fraud – selling online ad impressions and/or clicks that are not created by the common consumer.

Transparency – data symmetry on the terms and conditions of a transaction between buyer and seller.

Viewable/Viewability – "viewable" is a metric that allows for the industry to measure "opportunity to see". Instead of the impression being defined as "served" it is being changed to "rendered on a screen". Collaborating with the Interactive Advertising Bureau in the US, the Media Ratings Council (MRC) released guidelines defining what "viewable" means. For an ad to be considered viewable, 50% of the pixels must show up in the viewable portion of a browser window for at least 1 second. The term "viewability" refers to measuring the percentage of delivered impressions that were viewable vs. non-viewable.

Appendix

An existing relevant supporting document was previously produced by IAB US:

- Traffic Fraud: Best Practices for Reducing Risk to Exposure (PDF)