TRAFFIC FRAUD

Best Practices for Reducing Risk to Exposure

iab australia

August, 2014

Published by IAB Australia's Brand Safety Council based on the IAB US' Traffic of Good Intent Taskforce's document of the same title, published in January, 2014

The IAB Best Practices on Traffic Fraud was developed by a task force of council members from 22 IAB member companies

The IAB Australia Brand Safety Council Members are as follows:

Timothy Whitfield	Xaxis
Anya Collingwood	Match Media
Ben Maudsley	Exponential
Chris Levings	Adconian
Christopher Blok	SpotXchange
Dan Robins	OMD
Dylan McBride	PubMatic
Gus Soewono	Sizmek
Jason Tonelli	Starcom
Jonathan Airey	Bohemia
Jon Moffat	Fairfax
Kathy Damatopoulos	ANZ
Kenny Griffiths	Volt Media
Matthew Hunt	Adconian
Mitch Waters	Adap.TV
Peter Ostik	TVN
Rhys Williams	Google
Ross McNab	Kinected
Sam Smith	TubeMogul
Sebastian Henrici	Google
Stephen Dolan	Integral Ads
Sarah Wyse	Videology

This document was developed by the IAB US Traffic of Good Intent Task Force, and adapted for Australia by the IAB Brand Safety Council.

About the IAB Brand Safety Council

The council's mission is to identify, understand and raise awareness of the issue of non-intentional traffic and to offer insight and recommended solutions to the digital advertising industry.

TABLE OF CONTENTS

Executive Summary

Advertisers expect that all online content is delivered to human audiences. But an alarming portion of digital advertising is being diverted by nefarious entities that exploit the ecosystem to deliver fraudulent traffic.

The potential for fraud exists anywhere that media spending is significant and performance metrics are ambiguous or easily gamed. Online advertising is particularly vulnerable. Disreputable groups have found ways to profit from infiltrating legitimate systems and generating false ad views, ad clicks and site visits using robotic programs.

Robotic traffic — known popularly as "bots" — is driven by code and not humans. These bots are often smart enough to mimic human behavior, and they can be difficult to detect. While more sophisticated bots can simulate conversions such as clicking through to sites, they don't generate real conversions by buying goods and services, and they certainly don't engage with brands. Activity generated by these bots waters down engagement metrics driven by human traffic, which dilutes the value of legitimate publisher inventory. Advertisers end up spending campaign dollars on specious ad impressions never seen by humans.

Traffic fraud takes an organised effort to generate "results" that fool both buyers and sellers. The fraudsters are not just gaming the system; they often are engaging in other organised criminal activity. Ignoring traffic fraud enriches those engaged in such activities. Identifying traffic fraud and destroying the economics that drive this nefarious activity is imperative to restoring trust in the industry.

This document outlines steps that can be taken by individual businesses in the digital advertising marketplace to address traffic fraud within their organisations. Both the buy-side and sell-side need to play a role in defending against traffic fraud and improving the digital ecosystem.

Overview

Traffic fraud is not always easy to detect. Knowing how the bad actors operate can help reduce your risk of being victimised by them.

How traffic bots infect legitimate systems

Fraudsters often operate undetected in legitimate systems by masquerading as ordinary content and tools typically implemented by unwitting consumers.

Some of the ways they infiltrate systems:

- Getting consumers to install toolbars in their browsers.
- Simulating applications such as games or video players in an alternate browser.
- Bundling hidden applications with consumer downloads.
- Inserting code snippets, undetected, on publisher sites.
- Using malicious code to exploit operating systems and browser security vulnerabilities to surreptitiously install fraudulent traffic-generating code.
- Using real web pages as fronts for fake businesses so they can join networks and exchanges.

How traffic bots generate false traffic

After infiltrating legitimate systems, fraudsters can use bot code in different ways to generate false traffic. They often operate just under the surface or when human users aren't present to detect foul play.

Some of the ways bot code generates false traffic:

- Generating ad views while consumers browse unaware.
- Hijacking user controls to generate fake clicks when the computer is dormant.
- Running invisible processes behind the scenes to simulate consumer activity.
- Compromising cookie data to simulate high-value consumers.

How traffic fraudsters get paid

Fraudster business models vary, but a common theme tends to be their high profit margins. Even though fraudulent traffic accounts for only a small percentage of real human traffic, that small percentage generates disproportionate ad inventory and a significant diversion of digital marketing budgets. Premium publishers are often themselves buyers of traffic. If they buy from traffic vendors that are bot-riddled, the bots end up on the premium sites, inflating their impression volume.

Some of the ways fraudsters get paid:

- Selling cheap traffic to publishers wishing to extend their inventory.
- Selling their own robotic inventory to buyers through an exchange that is unaware of the traffic source.
- Becoming part of a legitimate network that pools inventory for buyers. The legitimate network is often unaware of any foul play.
- Creating a network by infecting legitimate sites with bot code, known as a "botnet," that generates traffic for which they can bill.
- Making ad calls that serve ads one behind another (stacked) or into 1x1 pixel frames, creating hidden ad inventory that generates false impressions from both human and non-human traffic.

Fraudsters contaminate legitimate businesses. For example, purchasing traffic is a generally acceptable way for publishers to extend audience and increase inventory. When legitimate businesses unknowingly purchase traffic from fraudulent businesses, they pollute their available inventory and undermine their relationship of trust with advertisers.

Why you should care

Allowing the bad actors in our industry to profit from traffic fraud affects the entire online community. In addition to diluting inventory value and diverting funds from legitimate businesses, traffic fraud undermines the integrity of digital media.

Some of the negative impacts of traffic fraud:

- Brands waste money on ad campaigns that are served to invisible inventory.
- Digital media is degraded, and brands look elsewhere for their marketing solutions.
- Ad performance and website visit data are contaminated, undermining analysis.
- Artificial fraudulent inventory floods the market and decreases the value of legitimate (real human) inventory.
- Illegal activity is enabled.
- The industry may be subjected to government oversight, negative press and potentially business-dampening enforcement.

What You Can Do

The solutions to traffic fraud are not always intuitive. For example, the outright blocking of fraudulent traffic gives information to the fraudsters that helps them better cloah their activities and become more difficult to identify.

In addition to the following general guidelines, steps specific to buyers, publishers and networks are outlined in subsequent sections.

The following general guidelines can help any online business get started:

- Educate yourself about traffic fraud and the risks that it poses to your business.
- Adopt policies and strategies to identify fraud and mitigate its impact.
- If you are an advertiser, set clear objectives for your media campaigns that focus on the measurement of real ROI, which is difficult for fraudsters to falsify. Measures such as click-through rate, completion rate, and last-touch attribution are easy to game.
- Practice safe sourcing and trust only business partners who have earned trust.
- Implement technology to detect and prevent fraud.
- Filter traffic through vendors who prioritise fraud detection.

Best Practices for Buyers

Buyers in online media have much to lose when it comes to traffic fraud. Taking steps to inspect the quality of your buys can go a long way toward preventing fraud in the digital marketplace. The following recommendations should help you achieve quality media buys by identifying and eliminating traffic fraud.

Set goals

Setting goals before buying media is generally a good practice. Some specific recommendations for buying digital media:

- List specific objectives for your media campaign. Don't leave objectives broad and open to interpretation. Examine whether your goals accommodate fraud.
- Be willing to pay the real price for the media you want. For example, pre-roll video targeted to a specific real-human audience with good attention will cost more than linear video ads placed at random simply to increase views.
- Document your goals clearly and get the seller to sign off on those goals. Agree to pay only for results that align with what's documented as your goals.
- Don't optimise for cost alone. Results that seem too good to be true probably are.

Manage the relationship

Trustworthy sellers shouldn't have any trouble backing up their claims for quality media. Keep in mind the following points to help you manage the relationship with your sellers:

- Filter media sellers before you buy. Even after the campaign is running, ensure that your sellers are following through.
- Despite the best efforts of sellers, all fraud cannot be eliminated. Determine the risk you are willing to accept and use that model to discount your media.

Measure results

Since bots can't engage the way humans can, consider measuring campaign results using more sophisticated metrics that ensure humans are interacting with your ads.

The following measures indicate human interaction:

- Purchases
- Subscriptions
- Verifiable brand survey results
- Validated panels

Other verifiable engagements Measures that are easy for bots to fake:

- Ad views
- Clicks
- Click-through rate
- Video completes
- Cookie attribution

Address traffic fraud

Your internal operations can only go so in attempting to filter out traffic fraud. Look to vendors who specialise in detecting and reducing the more sophisticated cases of traffic fraud.

• License technology specifically developed to discern traffic sources. Brand safety, viewability and placement quality are all fine measures of inventory quality, but they cannot detect the presence of non-human traffic.

Questions to ask publishers

As you filter for publishers that offer quality traffic, asking questions about how they manage quality control can help you find a good fit for your campaign. The following questions and preferred responses can help you get started finding quality sellers:

Do you have your audience measured by verifiable third-party systems?

The publisher should have their audience measured by independent vendors so that you can measure the traffic generated for your ads against an independent benchmark, making anomalies easier to spot. Note, however, that some audience measurement vendors' techniques can be easily fooled by fraudulent traffic. Review vendor methodologies when shopping for a vendor you can trust.

Do you have a clean record with third-party brand-safety reports?

Bad site quality is not necessarily correlated with traffic fraud, and high quality sites are not immune to traffic fraud. So screening sites for brand safety is an extra measure that helps ensure sites are involved in efforts to reduce fraud. Along with first-party data, sites should be screened against third-party reports to remove fraudulent and inappropriate environments. There are many different types of brand safety detection and prevention. Investigating third-party methodologies can help you make an informed decision.

How do you determine which impressions are exposed to real humans?

Advertisers want to engage with viewers who are engaged with content, not with users who may have left a web page open accidentally. Each site should have a policy and technical methodology to determine which traffic is generated by real humans. The site methodology should cover how they determine suspect fraudulent traffic and then flag, investigate and remove it.

How do you assure that ads are served as reported, and that URLs are visible to the advertiser?

Ad opportunities on publisher sites should correspond with the site URL that is reported by first- and/or third-party campaign performance analytics.

Do you provide protection from malware?

Websites should provide a safe environment for advertisers and consumers by actively screening for malware. Each publisher should be able to provide information on established approaches.

Are impressions generated by malware redirecting to a site?

Unusually large volumes of traffic and poorly performing placements should be investigated for malicious virus activity. Sites should monitor traffic patterns in real time to recognize anomalies resulting from malware.

Best Practices for Publishers

Buying traffic increases the risk profile for a premium publisher. If you want to minimize your risk, don't buy traffic from non-organic sources. Even without buying traffic from non-organic sources, you may have some non-human traffic on your media properties, sent there without your control. For example, consumers who install browser tools or applications may inadvertently open the gate to robotic traffic. In addition, bots may be programmed to browse legitimate sites to build up their targeting cookie pool while avoiding detection.

Despite your best efforts, you may find the need to extend your audience and increase your inventory. For example, if you've committed to delivering more ad impressions than are currently available on your media properties, your choice is to either under-deliver for your advertiser or supplement your inventory with purchased traffic.

If you must increase inventory, the following guidelines can help mitigate your risk:

- As a premium publisher purchasing traffic, pay the higher price to buy quality.
- Look for a natural affinity between your content and the purchased audience.
- Use technology to detect non-human traffic on all of the traffic you are buying.
- Don't lower your standards when performance slips below your goals.
- Know your consultants, and where they are sourcing traffic.

Questions to ask inventory sources

When you purchase traffic, you put yourself in the buyers' shoes. The following questions are nearly identical to the questions that buyers should ask of publishers. Use the following questions to filter traffic sources that promise to help you increase inventory:

Do you have your audience measured by verifiable third-party systems?
The publisher should have their audience measured by independent vendors so that you can measure the traffic generated for your ads against an independent benchmark, making anomalies easier to spot. Note, however, that some audience measurement vendors' techniques can be easily fooled by fraudulent traffic. Review vendor methodologies when shopping for a vendor you can trust.

How do you determine which impressions are exposed to real humans?
Advertisers want to engage with viewers who are engaged with content, not with users who may have left a web page open accidentally. Each site should have a policy and technical methodology to determine which traffic is generated by real humans. The site methodology should cover how they determine suspect fraudulent traffic, and then flag, investigate and remove it.

How do you assure that ads are served as reported, and that URLs are visible to the advertiser?
Ad opportunities on traffic-sourced sites should correspond with the site URL that is reported by first- and/or third-party campaign performance analytics.

Do you provide protection from malware?
Websites should provide a safe environment for advertisers and consumers by actively screening for malware.

Each traffic source should be able to provide information on their approach.

Are impressions generated by malware redirecting to a site?
Unusually large volumes of traffic and poorly performing placements should be investigated for malicious virus activity. Sites should monitor traffic patterns in real time to recognise anomalies resulting from malware.

Best Practices for Networks

Networks can engage in some key efforts to combat non-human traffic. Differentiate yourself in the marketplace by embracing the practices listed here.

Take notice

Botnet operators work hard to function under the radar. Malicious players shy away from the light. Your best defense is to look for the telltale characteristics of bad actors.

General red flags:

1. Publisher has no prior history of substantial traffic
When a publisher comes to you with traffic built overnight, you can be confident it didn't come from hard work and legitimate content.

2. High audience overlap between disparate websites
A handful of common visitors to sports sites and sites on the joys of growing flowers is certainly plausible. However, when a large proportion of the audience for either of these sites visits the other site, this most certainly a cause for alarm and something to be scrutinised and likely acted upon.

3. Browser stats that are inconsistent with known industry usage stats
Any publisher touting a billion unique visitors probably does not have the attention of one-seventh of the world's population.

4. Publisher seeks out representation
Publishers who have earned their traffic get noticed and don't need to ask for representation.

5. More than four tags on a page
The more ad tags on a page, the lower the quality of the page. While low quality may mean more traffic fraud, keep in mind that more sophisticated fraudsters will flock to higher quality pages to remain undetected.

Red flags in RTB environments:

1. No Bid reason flag and other automated indicators
The no bid reason flag in OpenRTB 2.2 is an optional flag a bidder can use to tell the exchange that they are not bidding on the inventory because they believe it to be non- intentional. Both exchanges and bidders are encouraged to create and implement non- intentional traffic detection algorithms.

2. Negatively target traffic fraud
Consider using anti-fraud tools in RTB to exclude any bid requests with a high probability for fraud.

Make a stand

Bad actors will take the road of least resistance. Building collaborative relationships in the industry builds

a wall of resistance that turns bad actors away.

1. Partnerships for rapid and free information sharing
Collaborative relationships with other supply chain partners, such as exchanges and DSPs, will enable an open channel of communication about bad traffic. Sharing information openly and quickly builds a defense against bad actors.

2. Vendors that offer fraud and malware detection
Your internal efforts to fight unintentional traffic are the right start. But the more successful you are, the more you'll need help to address sophisticated botnet operators. Certain companies have made fighting fraud and malware the core of their business. Integration with one of these companies sets up a security gate through which you can run all new traffic before selling it.

Address the bad actors

Taking steps to identify and defend against bad actors goes a long way to improving the value of your network. However, their persistence and changing tactics are designed to poke holes in your efforts. Some ways to combat the bad actors once identified are:

1.Sales disincentive
Your sales teams have the best intentions, but they can unwittingly bring in bad traffic sources. Build in a sales disincentive when that happens, so that sales can focus on finding the higher-grade human traffic.

2.Block suspicious ads
All known traffic fraud should be blocked as soon as it's detected. Suspicious traffic should be monitored, and blocked as soon as it is confirmed to be from a fraudulent source. Many advertisers insist that fraudulent traffic be blocked and refuse to pay for any known traffic fraud.

3. Block payment for fraud
Blocking known traffic fraud subsequently blocks payment to bad actors. When suspicious traffic isn't immediately blocked, fraudsters may demand payment for the impressions that were served. Resist their demands, as fraudsters most likely will back down if asked to prove that their traffic is valid.

Closing

For all the well-intentioned industry members who read this guide and adopt its practices, there are fraudsters out there who are also reading this document to discover ways to work around your efforts to thwart them. We have purposely avoided describing detailed strategies here that would help the perpetrators achieve their nefarious ends.

Whatever practices you adopt, you must remain diligent and continue to seek out the expertise to defeat the bad actors that are intent on hijacking the system and robbing legitimate businesses.