JICWEBS

Joint Industry Committee for Web Standards

JICWEBS

Good Practice Principles for Reducing Risk to Exposure to Ad Fraud

Version 1 Issued May 2016

CONTENTS

1. Introduction 3

2. Good Practice Principles 4

3. Examples of Good Practice & Independent Verification 4

1. Introduction

JICWEBS has one clear aim - to promote trusted digital ad trading.

The independent verification of businesses processes to a recognised, industry-agreed set of Good Practice Principles, aimed at reducing the risk of traffic fraud, is an important move forward. The Good Practice Principles and examples of good practice set out in this document form the basis of the independent verification process.

The JICWEBS Cross-Industry Anti-Fraud Working Groups were established in December 2014 with the purpose of creating cross-industry guidelines and principles to educate the wider market to reduce the risk of exposure to ad fraud, creating a safer, more transparent supply chain.

JICWEBS' steps to "anti-fraud" in digital advertising are:

1. Industry guidance on risk reduction (issued June 2015)

2. Taxonomy of types of traffic (issued October 2015)

3. **Good Practice Principles for risk reduction (this document)**

4. Independent review (and resultant "seal") for organisations demonstrating application of these Good Practice Principles

The six Good Practice Principles were first published in the industry guidance on risk reduction ('Traffic Fraud: Best Practices for Reducing Risk to Exposure' – issued by JICWEBS in June 2015) under section 3.5 'What You Can Do'.

This document confirms the principles and includes examples that demonstrate how the Principles can be applied to minimise the risk of exposure to traffic fraud, for buyers, publishers or intermediaries.

The verification process will require a Verification Provider appointed by JICWEBS to form an independent opinion, and provide a report, on the policies, processes and technical solutions, with a recommendation (or not) that a JICWEBS 'Seal of Compliance' be issued. JICWEBS' review of such reports will, if accepted, result in the JICWEBS seal being awarded.

2. Good Practice Principles

1. Educate yourself about traffic fraud and the risks that it poses to your business.

2. Adopt policies and strategies to identify fraud and mitigate its impact.

3. 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.

4. Practice safe sourcing and trust only business partners who have earned trust.

5. Implement technology to detect and prevent fraud.

6. Filter traffic through vendors who prioritize fraud detection.

3. Examples of Good Practice & Independent Verification

Below is a table that shows, for each of the JICWEBS Good Practice Principles as stated in Section 2, examples of good practice, for any business involved in the trading of digital advertising (for example publisher, buyer or intermediary).

Businesses seeking independent verification must appoint a JICWEBS approved Verification Provider (VP) and be able to provide:

1) A ‘Statement of Compliance’ that references their policies, procedures and technical solutions, that address each of the Principles, and makes reference to some or all of the good practice examples (as relevant);

   And,

2) Evidence to the VP of the policies, procedures and technical solutions in place, so that the VP can form an independent opinion that the ‘Statement of Compliance’ is appropriate.

Principle	Examples of Good Practices (as applicable)
1. Educate yourself about traffic fraud and the risks that it poses to your business	Provide training for staff on: 1) How traffic bots infect legitimate systems 2) How traffic bots generate false traffic 3) How traffic fraudsters make money 4) Why you […] care. 5) What you can do And for publishers, provide training for staff on: 1) How buying traffic increases the risk profile 2) How non-human traffic can be present on your media properties 3) The benefits and risks of purchasing traffic And when purchasing traffic, to mitigate risk consider: 1) Paying the higher price can help to buy quality 2) Seek a natural affinity between […] purchased audience[s] 3) Use technology to detect non-human traffic (on all the traffic you buy) 4) Don't lower your standards when performance slips below your goals 5) Know your consultants and where they are sourcing traffic
2. Adopt policies and strategies to identify fraud and mitigate its impact	For publishers 'Questions to ask inventory sources' & for buyers 'Questions to ask Publishers': Does the publisher have a policy and technical methodology to determine which traffic is generated by humans (and how they determine suspect fraudulent traffic, flag, investigate and remove it)? For intermediaries 'Take Notice': Look for tell-tale characteristics of bad actors. Do you take account of the following general red flags? 1) Publisher has no prior history of substantial traffic 2) High audience overlap between disparate websites 3) Browser stats that are inconsistent with known industry usage stats 4) Publisher seeks out representation 5) More than four [ad) tags on a page And the following red flags in RTB environments: 1) No bid" reason flag and other automated indicators 2) Negatively target traffic fraud For intermediaries 'Make a stand': Building collaborative relationships in the industry builds a wall of resistance that turns bad actors away. Do you have/use: 1) Partnerships for rapid and free information sharing? 2) Vendors that offer fraud and malware detection? For intermediaries 'Address the bad actors': Taking steps to identify and defend against bad actors goes a long way to improving the value of a network. Do you have ways to combat the bad actors once identified: 1) Sales disincentive 2) Block suspicious ads 3) Block payment fraud

Principle	Examples of Good Practices (as applicable)
	And as required of buyers: ‘Set goals’: 1) List specific objectives for your media campaign, don’t leave objectives broad and open to interpretation. Examine whether your goals accommodate fraud 2) Be willing to pay the real price for the media you want 3) Document goals clearly and get agreement from the seller 4) Agree to pay only for results that align with what’s documented 5) Don’t optimize for cost alone For buyers ‘Manage the relationship’: Trustworthy sellers shouldn’t have any trouble backing up their claims for quality media. Consider: 1) Filter media sellers before you buy 2) Ensure sellers are following through (as the campaign is running) 3) Determine the risk you are willing to accept and use that model to discount your media For buyers ‘Questions to ask Publishers’: 1) Does the publisher have their audience verified by independent 3rd party systems/vendors? 2) Have you reviewed vendor methodologies to ascertain which you can trust? 3) Does the publisher have a clean record with 3rd party brand safety reports? 4) What protection does the Publisher provide from Malware?
3. Set clear objectives for your media campaigns that focus on the measurement of real ROI, which is difficult for fraudsters to falsify.	For buyers ‘Set goals’: 1) List specific objectives for your media campaign, don’t leave objectives broad and open to interpretation. Examine whether your goals accommodate fraud 2) Be willing to pay the real price for the media you want 3) Document goals clearly and get agreement from the seller 4) Agree to pay only for results that align with what’s documented 5) Don’t optimize for cost alone For buyers ‘Measure results’: Measure campaign results using more sophisticated metrics that indicate human behaviour such as: 1) Purchases 2) Subscriptions 3) Verifiable brand survey results 4) Validated panels 5) Other verifiable engagements Rather than: 1) Ad views 2) Clicks 3) Click-through rate 4) Video completes 5) Cookie attribution Which are easy for bots to fake.
4. Practice safe sourcing and trust only business	For publishers: 1) Actively decide whether to under deliver or increase inventory with purchased traffic with associated risks

Principle	Examples of Good Practices (as applicable)
partners who have earned trust	For publishers: ''Questions to ask inventory sources' 1) Does the publisher have their audience verified by independent 3rd party systems/vendors? 2) Have you reviewed vendor methodologies to ascertain which you can trust? 3) Does the publisher have a clean record with 3rd Party brand safety reports? 4) What protection does the Publisher provide from Malware? For buyers 'Manage the relationship': Trustworthy sellers shouldn't have any trouble backing up their claims for quality media. Consider: 1) Filter media sellers before you buy 2) Ensure sellers are following through (as the campaign is running) 3) Determine the risk you are willing to accept and use that model to discount your media For buyers 'Questions to ask Publishers': 1) Does the publisher have their audience verified by independent 3rd party systems/vendors? 2) Have you reviewed vendor methodologies to ascertain which you can trust? 3) Does the publisher have a clean record with 3rd Party brand safety reports? 4) What protection does the Publisher provide from Malware?
5. Implement technology to detect and prevent fraud	For buyers 'Questions to ask publishers' & for publishers 'Questions to ask inventory sources': 1) How does the Publisher provide assurance that ads are served as reported i.e. does publisher reporting (by URL) match to first- and/or 3rd Party campaign performance analytics? 2) How does the Publisher determine whether ads are auto-initiated or user-initiated? 3) Does the Publisher match the ad interactions requested with the ad interaction fulfilled, and report anomalies? In addition, when buying traffic (as required of buyers) 'Measure results': 1) Measure campaign results using more sophisticated metrics that indicate human behaviour
6. Filter traffic through vendors who prioritise fraud detection	When buying traffic (as required of buyers) 'Address traffic fraud': 1) Use vendors who specialise in detecting and reducing traffic fraud 2) License technology specifically developed to discern traffic sources (over and above tools that address brand safety, viewability and placement quality)

Further Enquiries

Please contact your representative trade body or JICWEBS directly at info@jicwebs.org

Joint Industry Committee for Web Standards

Contact us via info@jicwebs.org