UK Good Practice Principles certificate

JICWEBS ANTI AD FRAUD VALID TO: abc SEPTEMBER 2019

INSKIN

Company: Inskin Media Ltd
233 High Holborn
London
WC1V 7DN
http://www.inskinmedia.com

Business/Brands verified:	Inskin Media
Service provided:	Technology
Month of verification:	June 2018

Findings

	Good Practice Principles	Description of compliance with the Principles
1	Educate yourself about traffic fraud and the risks that it poses to your business	Inskin Media use multiple channels to keep the organisation informed about issues / advancements regarding ad fraud detection. Staff members attend industry events such as IAB events and JICWEBS Town Hall meetings, and subscribe to newsletters from JICWEBS and ad verification providers. Inskin Media also actively participates in JICWEBS Technical and Commercial Group meetings. Weekly commercial meetings are held during which the latest industry, trade and research news are presented to staff. All staff training is internal. New staff receive an induction including a dedicated training package which covers ad fraud and uses available JICWEBS materials. Examples of training content include: how ad fraud affects the ecosystem, best practices on how to reduce ad fraud, and direct measures that Inskin Media takes to identify invalid traffic. Inskin Media also have an internal "Knowledgebase" system where articles and documents are held which give information on ad fraud. This is accessible to all staff.

Good Practice Principles	Description of compliance with the Principles
2 Adopt policies and strategies to identify fraud and mitigate its impact	Inskin Media's policy and strategy to identify and mitigate ad fraud is detailed in their Anti Ad Fraud process document, held on their internal "Knowledgebase" system. The document also includes links to further documents such as Moat Invalid Traffic (IVT) Metrics (defines metric definitions), and Network Monitoring Tool Usage Guide (outlines use of proprietary tool that monitors every site for metrics such as high CTR and viewability). Inskin Media use a multi-layered approach to detect and filter Invalid Traffic (IVT): 1. Monitoring (3rd-Party): Every impression served by Inskin Media carries the Moat tag, which enables them to deploy Moat's IVT tracking technology across their network. Both General IVT (Spiders, Excessive Activity, Data Centre Traffic) and Sophisticated IVT (Invalid Proxy, Automated Browser, and Incongruous Browser) are detected by Moat on a network, campaign and site level. 2. Filtration (3rd-Party): Using IP intelligence provider Digital Element, Inskin Media have introduced a process that allows them to invalidate ad requests that are associated with data centre traffic, a common form of General IVT. 3. Filtration (proprietary): Inskin Media have introduced a proprietary tool for suspicious traffic filtration. Providing an additional verification layer, this tool registers IP addresses from impressions where there have been multiple clicks within a second or a high number of clicks on a single impression. The tool logs the IP to a database which Inskin Media's Integrations team use to identify repeat offenders. Upon identification of repeat offenders, these IPs get added to the firewall. Inskin Media's Brand Safety Policy also details some anti ad fraud processes such as vetting, blacklists and whitelists and is located publicly on their website at http://www.inskinmedia.com/brand-safety.html Inskin Media also support the ads.txt protocol and have been awarded the IAB Gold Standard Seal. *All tools referred to above and in the sections below are non JICWEBS certified for ad fraud and have not been tested by ABC.*
3 Set clear objectives for your media campaigns that focus on the measurement of real ROI, which is difficult for fraudsters to falsify.	Campaign objectives are agreed via Insertion Orders (IO's). All campaigns are run on Inskin Media's whitelist of approved sites. Monitoring of campaign objectives is achieved via reporting from Moat, network monitoring, Digital Element filtration, and proprietary filtration.

Good Practice Principles	Description of compliance with the Principles
	These reports identify levels of Invalid Traffic (IVT) at campaign and site level, so that any high instances can be investigated, and appropriate action taken such as blocking IP addresses. End of campaign reports are also sent to Inskin Media's clients. These detail statistics for the campaign such as impressions served, performance indicators, industry benchmarks etc.
4 Practice safe sourcing and trust only business partners who have earned trust	Inskin Media's Publisher Services team vet all publishers against a set of criteria which include anti ad fraud principles, prior to adding them to the whitelist. In order for a publisher to be added to the Inskin Media network, sites are vetted on a range of factors, including: high quality of editorial content, compliance to Inskin Media's brand safety policy, minimum page impression volumes and guarantee of no syndication of Inskin Media placements to 3rd-Party sites or outside the permitted publisher site list. Publishers must be individually selected and vetted by Inskin Media's Publisher Services Team only. Additionally, all newly onboarded publishers must demonstrate steps taken to combat ad fraud. For all new integrations, the publisher integrations team will check the publishers Ads.txt and supply the Inskin Media code to the publisher. Integrations will check on sign off if the publisher has implemented the Inskin Media reseller ID into their ads.txt. This is a requirement for signing a site off. When a new site is added to the whitelist, the whitelist itself is checked to ensure sites are still considered to be appropriate.
5 Implement technology to detect and prevent fraud	Moat, network monitoring, Digital Element filtration, and proprietary filtration are all used as described in the three step process in GPP2. If a client requests the use of another 3rd party verification tool such as Integral Ad Science (IAS), Inskin Media will enable its use.
6 Filter traffic through vendors who prioritise fraud detection	Inskin Media vet all publishers prior to be being added to their network, (see GPP4) and use third party tools from MOAT and Digital Element along with their own internal tool on all campaigns (see GPP2 / GPP5).

Verified by

Company:	ABC Ltd Saxon House, 211 High Street, Berkhamsted, Hertfordshire. HP4 1AD

Statement of verification provider:	We have reviewed Inskin Media's policies and procedures for reducing risk to exposure to ad fraud in accordance with the JICWEBS Good Practice Principles. Our enquiries were designed to independently confirm that the anti-fraud policies stated have been implemented and clearly documented where required. Our review did not extend to testing the effectiveness of any processes, procedures or controls for ad fraud. In our opinion, at the time of our review, Inskin Media had established policies to minimise the risk of ad fraud as described in the JICWEBS Good Practice Principles.

About JICWEBS

JICWEBS (The Joint Industry Committee for Web Standards in the UK and Ireland) was created by the UK and Ireland media industry to ensure independent development of standards for measuring performance online and benchmarking best practice for online ad trading.

About the JICWEBS Anti-Ad Fraud Commercial Group

The Anti-Ad Fraud Commercial Group is an industry body made up of representatives from across the digital display advertising ecosystem, including the buy- and sell-side. It comprises representatives from advertisers, agencies, agency trading desks, demand side platforms, advertising exchanges, sales houses, advertising networks, supply side platforms and publishers.