

UK Good Practice Principles certificate

<p>ANTI AD FRAUD</p>	<p>JICWEBS</p>	<p>VALID TO:</p>
		<p>AUGUST 2019</p>



Company: Encore Digital Media Ltd
 73 Bermondsey Street
 London, SE1 3XF
 UK
<http://encoredigitalmedia.net/>

Business/Brands verified:	Encore Digital Media Ltd
Service provided:	Trading Desk
Month of verification:	July 2018

Findings

Good Practice Principles	Description of compliance with the Principles
<p>1 Educate yourself about traffic fraud and the risks that it poses to your business</p>	<p>Encore Digital Media delivery team members receive training on digital ad fraud, including:</p> <p>Internal ad fraud training: Is provided to new employees and thereafter on a quarterly basis. Training is lead by Encore Digital Media’s Head of Delivery using internal data and delivery results, materials from their third-party verification vendors, and industry resources.</p> <p>Weekly delivery meetings: Using the weekly delivery reports, data from third-party verification vendors, and industry news from the week, the team reviews the internal and industry-wide ad fraud issues and insights.</p> <p>Monthly Town hall meetings: This is a company-wide meeting where each department presents and discusses insights from the industry, including the latest developments in ad fraud identification and prevention. Often outside speakers and industry leaders are brought in to present.</p> <p>Encore Digital Media staff continuously monitors industry fraud trends and update processes accordingly.</p>
<p>2 Adopt policies and strategies to identify fraud and mitigate its impact</p>	<p>Encore Digital Media only places advertisements on sites that have been vigorously vetted. Vetted and approved sites are added to the Encore Digital Media whitelist. Encore Digital Media only run campaigns using the approved whitelist.</p> <p>Encore Digital Media works directly with JICWEBS ad fraud certified vendors, IAS and Doubleverify, to identify and filter</p>



Good Practice Principles	Description of compliance with the Principles
	<p>fraudulent activity. Campaigns are run with pre-bid targeting to remove any non-human traffic. Encore Digital Media also uses DSP filters to minimize any fraud.</p> <p>Ads.txt: has been implemented to identify authorized sellers.</p> <p>Publisher/Partnership contracts: are reviewed to ensure publishers/partners have, and adhere to, ad fraud policies.</p> <p>All Encore Digital Media campaigns require the following controls to be applied to them:</p> <ul style="list-style-type: none"> • Viewability – The strongest filter for viewability from either IAS (Integral) or DoubleVerify depending on which monitoring has been applied to the ad tags. • Suspicious Activity - The strongest filter for viewability from either IAS (Integral) or DoubleVerify depending on which monitoring has been applied to the ad tags. • Fraud – DV/IAS segments of ‘Bot Sites’ (Non-human traffic must be ANTI-targeted). • Traffic Filter – Must be set to maximum strength. • Transparent URL Sites – The ‘only serve on sites with transparent URLs’ checkbox must be ticked. • Unknown Technology – All ‘unknown’ Browsers and ISPs must be ANTI-targeted. <p>In addition, each campaign requires a completed Encore Digital Media Brand Safety and Anti fraud checklist, indicating all the above steps have been applied or completed.</p> <p>Lastly, campaign results are reviewed daily and outlier activities are investigated. Sources of fraudulent activity are blacklisted.</p>
<p>3 Set clear objectives for your media campaigns that focus on the measurement of real ROI, which is difficult for fraudsters to falsify.</p>	<p>Media campaign objectives are created by the advertisers/agency. Campaign objectives are agreed to prior to campaign set up. These objectives are discussed and guidance is provided to avoid outcomes that could result in a high level of fraudulent inventory. Primary campaign objectives include metrics that are based on human activity such as Cost Per Acquisition, Cost Per Registration, Cost Per Download as well as impressions where Encore Digital Media uses internal benchmarks to assist.</p>



Good Practice Principles	Description of compliance with the Principles
<p>4 Practice safe sourcing and trust only business partners who have earned trust</p>	<p>Encore Digital Media has a robust site review and vetting process for adding sites to the Encore Digital Media whitelist. Review and vetting includes:</p> <p>Genuine Publications The URLs of the site must be checked to make sure that it does not redirect. The site must have genuine editorial content rather than being a portal purely for adverts.</p> <p>Content Specific For general whitelist use, a site must fall into one of the categories of News, Business, or Technology. For campaign/advertiser specific whitelist use, a site must be related to the specific content/industry/subject which is the subject of the campaign/advertiser.</p> <p>Brand Safe The URLs of the site are checked to the Encore Digital Media Brand Safety standards. Non-compliant sites have an elevated risk of fraud.</p> <p>Not be exclusively User-Generated Content Sites with purely user-generated content are prohibited.</p> <p>Have predominantly content flanked ad placements For whitelist use, a site must have ad placements which are commensurate on the page with the content of the page. The pages of the site are checked from top to bottom.</p>
<p>5 Implement technology to detect and prevent fraud</p>	<p>Encore Digital Media works directly with JICWEBS ad fraud certified vendors, IAS and Doubleverify, to identify and filter fraudulent activity.</p>
<p>6 Filter traffic through vendors who prioritise fraud detection</p>	<p>Encore Digital Media works directly with JICWEBS ad fraud certified vendors, IAS and Doubleverify, to identify and filter fraudulent activity.</p>

Verified by

Company: BPA Worldwide
 20 Jerusalem Passage
 London
 EC1V 4JP
 www.bpaww.com





Statement of verification provider:

We have reviewed Encore Digital 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, Encore Digital 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.