Anti-Fraud Principles
March, 2015

Supply sources (SSPs/exchanges, ad networks, and publishers) are challenged by a lack of consistent and independently measurable principles on how they each should identify and expunge fraudulent traffic.

If the majority of large supply sources come forward and adhere to the principles below, then the amount of poor quality traffic will quickly be pushed out of the system. Broad adoption of these principles will allow principled actors to differentiate themselves from sources that generate or trade in poor quality or fraudulent traffic.

The Principles

1: Fraud Detection

There exists a set of ad-related actions generated by infrastructure designed not to deliver the right ad at the right time to the right user, but rather to extract the maximum amount of money from the digital advertising ecosystem, regardless of the presence of an audience. There also exists a set of actions generated in the normal course of internet maintenance by non-human actors – search engine spiders, brand safety bots, competitive intelligence gathering tools.

These and other actions, whether they be page views, ad clicks, mouse movement, shopping cart actions, or other seemingly human activities, must be expelled from the supply chain.

Bots:

Identify hijacked devices, crawlers masquerading as legitimate user, data-center traffic, and other non-human activity so that malicious ad fraud can be mitigated.

Illegitimate Human Activity:

Identify AdWare traffic and other traffic that comes from humans coopted into interacting with ads.

Action:

Supplier is required to implement technological and business practices to effectively identify illegitimate and fraudulent traffic. Such traffic is prohibited from being sold.

2: Source Identification

Illegitimate traffic is often generated through blind sources, and the inability for buyers to accurately determine the URL location or placement of their advertisements or marketing messages undermines trust in the digital supply chain.

Action:

Supplier to clearly signal the specific placement URL to potential buyers. Publishers or their Exchanges may choose to explicitly mask the URL, provided sufficient trust is provided to the buyers.

3: Process Transparency

Each source of supply (publishers, SSP/exchanges, ad Networks) will describe in sufficient detail the business and technical processes they have employed to address each of the above principles.

- What business processes are in place currently?
- Are partners, customers, and vendors appropriately filtered for threats to genuine business practices?
- What, if any, tools or technologies are used?
- How often are the methodologies employed updated?
- Are methodologies and detection methods used on statistical traffic samples, time intervals across the entire network, or on an impression by impression basis?
- Is there a rating or some other scale applied to the traffic in question, and is this made available to buyers?
- If there is a rating scale, is that scale and score made available to potential buyers of the traffic?
- Are traffic acquisition and marketing techniques monitored and shared?
- How is efficacy measured?
- If a rating scale is used for traffic quality, what is done with traffic detected to be lower quality and/or fraudulent?

4. Building Accountability

The intent of the process transparency is not to disclose publicly any specific tactics or technological details used in detection or filtering, but rather to detail the methodologies used to identify fraudulent traffic and to facilitate industry compliance and the creation of an effective accountability program to monitor such compliance.

For each of the three principles a set of best practices will be developed to provide clear guidance for companies to achieve compliance. These best practices will be developed for an accountability program that will operationalize the principles and monitor for compliance