Anti-Fraud Principles and Proposed Taxonomy

September 2014

Anti-Fraud Principles

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 a principled actor 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 incentivized browsing, AdWare traffic, and other traffic that comes from humans coopted into interacting with ads through means other than the ad itself.

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 these methodologies 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 made available to buyers?
- 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.

Proposed Taxonomy

Note: the taxonomy is not necessarily mutually exclusive.

Illegitimate and Non-Human Traffic Sources:

- **Hijacked device** – any user's device (browser, phone, app or other system) that has been modified to call html or make ad requests that is not under the control of a user and made without the user's consent. These include:

    - **Hijacked device with a fully automated browser** – a hijacked device where the device is a browser and the modification is that the browser is hidden from user view and engaged in making html or ad calls.
    - **Hijacked device with session hijacking** – a hijacked device where a user is present and additional html or ad calls are made independently of the content being requested by the user. Ads and redirections are inserted into the user experience by the program running on the device.

- **Crawler masquerading as a legitimate user** – a browser, server or app that makes page load calls automatically without declaring themselves as a robot, instead declaring a valid regular browser or app user agent where there is no real human user.
    - **Advanced** – declares a user agent string normally associated with human activity, and also renders the page.
    - **Basic** – only declares a user agent string normally associated with human activity, does not render the page.

- **Data-center traffic** – traffic originating from servers in data-centers, rather than residential or corporate networks, where the ad is not rendered in a user's device (there is no real human user).

Non-traditional/other traffic:

- **AdWare traffic** – a device where a user is present and additional html or ad calls are made by the AdWare independently of the content being requested by the user.

- **Proxy traffic** – traffic that is routed through an intermediary proxy device or network where the ad is rendered in a user's device where there is a real human user. This includes:
    - **Proxy traffic that is anonymized** – Proxy traffic where the request is anonymized. (e.g., Tor)
    - **Proxy traffic that is not anonymized** – Proxy traffic where the request is not anonymized.

- **Non-browser User-Agent header** – a device that declares a User-Agent header not normally associated with human activity.
    - **Non-browser User-Agent header App traffic** – a device that declares a non-browser User-Agent header that is sold as app traffic.
    - **Non-browser User-Agent header Non-app traffic** – a device that declares a non-browser User-Agent header that is not sold as app traffic.

- **Browser pre-rendering** – a device that makes html or ad requests ahead of specific human-initiated navigation to the requested resources.
    - **Browser pre-rendering, un-rendered** – Browser pre-rendering calls where the page never exits the pre-rendering state. For example, the process by which the Safari browser creates thumbnails for its new tab page.
    - **Browser pre-rendering, rendered** – Browser pre-rendering calls where the page does exit the pre-rendering state. For example, pages requested by the Chrome and Firefox browsers in certain conditions.

Hijacked Tags:

- **Ad Tag Hijacking** - Taking ad tags from a publisher's site and putting them onto another site without the publisher knowledge.
- **Creative Hijacking** - Copying the creative tags from a legitimately served ad so they can be rendered at a later time, without the consent of the advertiser or their contracted service provider.

Site or Impression Attributes:

- **Auto-refresh** – a page or ad unit that calls for a new rendered asset more than once.
    - **Declared minimum interval** – Auto-refresh where the minimum time interval between calls is declared explicitly
    - **Declared minimum interval with user interaction** – Auto-refresh where the minimum time interval between calls is declared explicitly and user interaction with the page is detected at the time of refresh.
    - **Undeclared** – Auto-refresh without any declaration of time or user interaction.
- **Incentivized browsing** – a human user that is offered payment or benefits to view or interact with ads.
- **Ad density** – the number of ads or percentage of the page / app covered by ads
    - **Number of ads** – the ad density where the number of ads is declared
    - **Percentage of page** – the ad density where the percentage of the page / app covered by ads is declared
    - **Undeclared** – the number of ads or percentage of the page / app covered by ads is not declared
- **Hidden Ads** – ads placed in such a manner that they can not ever be viewable e.g., stacked ads, ads clipped by iframes, zero opacity ads.
- **Viewability** – declaration of viewability per the MRC standard.
- **Misappropriated Content** –
    - **links** – site contains links to copyrighted content but does not have the content itself

    - **content** – site contains copyrighted content (from another, unaffiliated entity) without the rights to monetize such content
- **Falsely represented** – html or ad calls that attempt to represent another site or device or other attribute, other than the actual placement e.g., referrer spoofing
- **Non-brand safe** – as defined per the Quality Assurance Guidelines.
- **Contains malware** – malware is found on the site or the app contains malware.

Ad creative/other:

- **Cookie-stuffing** – The process by which a client is provided with cookies from other domains as if the user had visited those other domains.