Fraud taxonomy
March, 2015

The terms defined in the taxonomy below are not necessarily mutually exclusive of one another. Ad impressions can have different but sometimes overlapping definitions.

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 call is anonymized. (e.g., Tor)
    - **Proxy traffic that is not anonymized** – Proxy traffic where the call 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-standard or invalid User-Agent header that is sold as app traffic.
    - **Non-browser User-Agent header Non-app traffic** – a device that declares a non-standard or invalid User-Agent header that is not sold as app traffic.

- **Browser pre-rendering** – a device that makes html or ad calls prior to the rendering of the resulting assets or web-page to an end user.
    - **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's 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.
- **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** – sites or impressions represented as one thing that are another, including:
    - **Context** – 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.