TAG Invalid Traffic Taxonomy

Providing accurate and consistent terminology to describe types of invalid traffic in order to foster transparency and collaboration in the fight against ad fraud.

Version 2.0
Release January 2019
DRAFT

About the TAG Certified Against Fraud Program

The mission of the TAG Certified Against Fraud Program is to combat fraudulent, invalid traffic in the digital advertising supply chain.

In order to guide companies in fighting fraud effectively, the TAG Anti-Fraud Working Group developed and maintains the Certified Against Fraud Guidelines, as well as a suite of anti-fraud tools to aid in compliance with those guidelines.

Companies that are shown to abide by the Certified Against Fraud Guidelines can achieve the Certified Against Fraud Seal and use the seal to publicly communicate their commitment to combatting invalid traffic in the digital advertising supply chain.

About the Trustworthy Accountability Group

The Trustworthy Accountability Group (TAG) is the leading global certification program fighting criminal activity and increasing trust in the digital advertising industry. Created by the industry's top trade organizations, TAG's mission is to:

- Eliminate fraudulent traffic,
- Combat malware,
- Prevent Internet piracy, and
- Promote greater transparency in digital advertising.

TAG advances those initiatives by bringing companies across the digital advertising supply chain together to set the highest standards.

TAG is the first and only registered Information Sharing and Analysis Organization (ISAO) for the digital advertising industry.

To learn more about the Trustworthy Accountability Group, please visit www.tagtoday.net.

Table of Contents

Executive Summary

The digital advertising industry continues to build momentum in the fight against invalid traffic, as demonstrated by initiatives such as TAG's Certified Against Fraud program.

As the industry continues to foster awareness and drive initiatives to fight invalid traffic, there is an increasing need to ensure that discussions and information exchange about invalid traffic (including ad fraud) are consistent and specific. The TAG Fraud Taxonomy, originally released by the IAB's Traffic of Good Intent Task Force in 2015, was created to address this need.

Since the initial release of The TAG Fraud Taxonomy, the digital ad industry and its fight against invalid traffic have evolved significantly. While industry efforts, including widespread adoption of the TAG Certified Against Fraud Program, have made it possible to reduce fraud rates significantly, misinterpretation of fraud-related terminology continues to result in miscommunication between partners sharing the same goal of fighting invalid traffic. Further, the 2015 version TAG Fraud Taxonomy no longer accurately reflects for the terminology in use today.

Version 2.0 of the TAG Invalid Traffic (IVT) Taxonomy was designed with several goals in mind, including to:

- Provide accurate and consistent terminology for all types of "invalid traffic," of which ad fraud is a subset.
- Decouple the original terminology from related, but extraneous, categories such as "non-brand-safe" and "viewability" classifications.
- Provide a resource that fosters consistency, avoids ambiguity, and minimizes confusion around discussions about invalid traffic.
- Increase adoption of the taxonomy across the digital advertising industry.

In releasing an updated and better tailored TAG Invalid Traffic Taxonomy, TAG strives to improve analysis and resolution of invalid traffic reporting discrepancies and provide a consistent framework to structure specific reporting and initiatives around combatting invalid traffic.

Principles

The TAG Invalid Traffic Taxonomy was created with following principles in mind:

- Build trust throughout the digital advertising ecosystem.
- Provide sufficient granularity in terminology to help partners in the digital advertising supply chain resolve confusion and troubleshoot implementation issues for the purposes of reducing invalid traffic.
- Improve the process of resolving invalid traffic reporting discrepancies between different parties in the digital advertising supply chain.

IVT Traffic Taxonomy and Examples

Definitions

Invalid Traffic[1] **-** Traffic that does not meet certain ad serving quality or completeness criteria, or otherwise does not represent legitimate ad traffic that should be included in measurement counts. Among the reasons why ad traffic may be deemed invalid is it is a result of non-human traffic (spiders, bots, etc.), or activity designed to produce fraudulent traffic.

General Invalid Traffic (GIVT)[2] - Traffic identified through routine means of filtration executed through application of lists or with other standardized parameter checks. Key examples are: known data-center traffic (determined to be a consistent source of non-human traffic; not including routing artifacts of legitimate users or virtual machine legitimate browsing), bots and spiders or other crawlers (except those as noted below in the "Sophisticated Invalid Traffic" category), activity-based filtration using campaign or application data and transaction parameters from campaign or application data, non-browser user-agent headers or other forms of unknown browsers and pre-fetch or browser pre-rendered traffic (where associated ads were not subsequently accessed by a valid user; pre-fetch clicks associated with accessed ads should not be counted until acted-upon by a valid user).

Sophisticated Invalid Traffic (SIVT)[3] – Situations that require advanced analytics, multi-point corroboration/coordination, significant human intervention, etc., to analyze and identify. Key examples are: bots and spiders or other crawlers masquerading as legitimate users; hijacked devices; hijacked sessions within hijacked devices; hijacked ad tags; hijacked creative; hidden/stacked/covered or otherwise intentionally obfuscated ad serving; invalid proxy traffic

[1] http://mediaratingcouncil.org/101515_IVT%20Addendum%20FINAL%20(Version%201.0).pdf, Section 1, pg. 3.
[2] http://mediaratingcouncil.org/101515_IVT%20Addendum%20FINAL%20(Version%201.0).pdf, Section 1.1.2, pg. 6.
[3] http://mediaratingcouncil.org/101515_IVT%20Addendum%20FINAL%20(Version%201.0).pdf, Section 1.1.2, pgs. 6-7.

(originating from an intermediary proxy device that exists to manipulate traffic counts or create/pass-on non-human or invalid traffic or otherwise failing to meet protocol validation); adware; malware; incentivized manipulation of measurements (fraudulent incentivized promotion of an entity, without its knowledge or permission – excludes cases where the entity paying for the incentive is the entity being promoted**); misappropriated content (where used to purposefully falsify traffic at a material level); falsified viewable impression decisions; falsely represented sites (sites masquerading as other entities for illegitimate purposes) or impressions; cookie stuffing, recycling or harvesting (inserting, deleting or misattributing cookies thereby manipulating or falsifying prior activity of users); manipulation or falsification of location data or related attributes; and differentiating human and IVT traffic when originating from the same or similar source in certain closely intermingled circumstances.

Examples

These charts explain the different types of invalid traffic with corresponding examples. These examples are meant to be illustrative to help represent the differences between categories and represent only a subset of possible invalid behaviors & tactics. Note that an impression may be classified into one or more categories listed below; these categories are not exclusive of each other.

General Invalid Traffic (GIVT)		
CATEGORY	**DEFINITION**	**EXAMPLE(S)**
Data Center	Ad traffic originating from servers in data centers whose IPs are linked to invalid activity (typically non-human traffic). These are usually known data center IPs, which may be included in an industry list, such as the TAG Data Center IP list.	TAG Data Center IP List
Known Crawler	A program or automated script that requests content and declares itself as non-human through a variety of identification mechanisms. These are crawlers that may be included in an industry list, such as the IAB Tech Lab International Spiders and Bots List[4].	IAB Tech Lab International Spiders & Bots Blacklist
Irregular Pattern	Ad traffic that includes one or more attributes (e.g., user cookie) associated with known irregular patterns, such as non-disclosed auto-refresh traffic or duplicate clicks.	Repeat Transactions, Throttlers, Duplicate or Expired Clicks

[4] https://iabtechlab.com/software/iababc-international-spiders-and-bots-list/

Sophisticated Invalid Traffic (SIVT)		
CATEGORY	**DEFINITION**	**EXAMPLE(S)**
Automated Browsing	A program or automated script that requests web content (including digital ads) without user involvement and without declaring itself as a crawler, such as and primarily referring to botnets.	Botnets
False Representation	An ad request for inventory that is different from the actual inventory being supplied, including ad requests where the actual ad is rendered to a different website or application, device, or other target (such as geography)	Spoofed measurements, Domain Spoofing, Emulators Masquerading as Real User Devices, Parameter Mismatch (Inconsistencies in Transaction and Browser/Agent Parameters)
Misleading User Interface	A web page, application, or other visual element modified to falsely include one or more ads. This includes rendering ads that are not visible to the User, injecting ads without a publisher's consent, or tricking users to click on an ad.	Stacked Ads, Ad Hiding, Clickjacking, Pop-unders
Manipulated Behavior	A browser, application, or other program that triggers an ad interaction without a user's consent, such as an unintended click, an unexpected conversion, or false attribution.	Attribution Manipulation, Accidental Traffic, Forced New Window, Forced Installation of a Mobile Application
Undisclosed Classification	Invalid traffic that cannot be classified using any of the other categories in the taxonomy, or sensitive invalid traffic that cannot be disclosed.	Invalid traffic identified by machine learning models not able to classify traffic into a specific category, Sensitive invalid traffic whose classification cannot be disclosed
Undisclosed Use of Incentives	The invalid and undisclosed use of any financial or other incentive to cause users to interact with one or more ads for the sole purpose of receiving said incentive. This does not include content where the incentive is known or properly disclosed to the other party in the transaction.	Click farms, Pay to Click

Conclusion

While industry efforts, including widespread adoption of the TAG Certified Against Fraud Program, have made it possible to reduce fraud rates significantly, misinterpretation of fraud-related terminology continues to result in miscommunication between partners sharing the same goal of fighting invalid traffic. In releasing an updated and better tailored TAG Invalid Traffic Taxonomy, TAG strives to improve analysis and resolution of invalid traffic reporting discrepancies and provide a consistent framework to structure specific reporting and initiatives around combatting invalid traffic.