keynes

Brand Safety & Marketplace Quality

Marketplace Quality

We offer total brand safety through our marketplace quality solutions via our DSP partner. Our DSP partner identifies non-human traffic patterns and institutes immediate platform-wide exclusions on suspicious traffic through proprietary algorithmic fraud detection and exclusion models. These models are implemented pre-bid, eliminating suspicious traffic before it reaches the bid stream. Their dedicated Marketplace Quality team continuously refreshes their proprietary algorithms with updated data.

Internal Solutions

Marketplace Quality Team

This team applies learning and data from past activity to decision-making algorithms to prevent fraud and malicious activity in future transactions. Combined with our DSP partner's algorithmic solutions, the Marketplace Quality team also analyzes campaigns for fraud in real-time.

- Click clusters are sifted through by both algorithms and a team of individuals to determine if they are fraud or instances of classrooms, businesses, or other IP groupings.
- Known proxies, the ability to set cookies, and IP addresses are evaluated.

Exchange-Level Decisions

Our DSP partner works directly with inventory suppliers to prevent fraud at the source.

- Entire networks, intermediaries, and publishers are turned off at the exchange level in cases of egregious violations or systemic quality concerns associated with the entity.
- When applicable, non-human audited inventory is excluded.

System-Wide Exclusion List

Inventory that goes against our DSP partner's SSP guidelines is automatically added to this list, including but not limited to categories like adult content, copyrighted material, non-COPPA compliant inventory, hate speech, and inventory with predominantly fraudulent traffic. As part of this process, all sites are reviewed for suspicious activity and unusually high click rates, known bot traffic is scrubbed, and previously detected invalid IPs, sites, and user IDs are excluded.

Site-Level Protection

Bids are based on domain or have an ID specified within the bid request. Unfortunately, elements outside of any individual ad server's control may result in the ad being served on an alternate domain rather than the domain delivered with the bid. To meet this industry issue head-on, our DSP partner continuously improves projections and takes the required actions to address the problem at the source with supply vendors.

Our DSP partner activates internal tools to ensure the best quality and control possible. Site fraud prevention activities include:

- Active exclusion of suspicious domains and traffic.
- Accepting only human-audited inventory from SSPs, when offered.
- Turning off and globally excluding suspicious publishers or other partners suspected of fraudulent activity.
- Continuous monitoring of changes in inventory volume.
- Internal click scrubbing and monitoring processes.

We also work with various pre-bid partners including IAS, Grapeshot, Peer39, and DV for additional measures or more customized category blocks, if desired. Categories include, but aren't limited to Adult content, Alcohol, Drugs, Hate/Profanity, Racist, Gambling, Illegal Downloads, Offensive Language, Violent Content and Weapons, Terrorism, Tobacco, Negative News/Content, Disaster, Military, Gossip, Alternative, Occult, Sex Education, Fraud/Spyware/Malware, Unsafe Content for Kids, Kids Content.

Advanced Processes

Advanced fraud detection processes are required to evaluate the legitimacy of impressions. Our DSP partner maintains the following procedures to combat existing (and prevent future) impression fraud:

- Identifies and prevents a single bid request from winning multiple impressions.
- Identifies and excludes suspicious sites based on exceeding a pre-determined threshold for percent of site traffic versus bids/impressions.
- Monitors IP addresses.
- Identifies and prevents too many impressions stemming from a single user ID.

Domain Classes

Certain categories of non-standard or controversial inventory are restricted to prevent them from being purchased accidentally. They can be intentionally targeted on an opt-in basis through site inclusion lists, seller inclusion lists, or single-publisher 1:1 deals. These categories include ad arbitrage, controversial political, rewarded traffic, provocative content, and desktop apps.

Industry Initiatives

Our DSP partner provides multilayered fraud detection and prevention via HUMAN, which screens all inventory, regardless of device type, and excludes fraud in real-time at no additional cost. HUMAN is MRC accredited for both their pre-bid and post-bid products, including for CTV fraud. HUMAN's bot-prevention product, MediaGuard, blocks fraudulent traffic pre-bid, using post-bid identifiers like bots and domain spoofing, and then blocks the traffic where needed. Details of HUMAN protection on CTV include:

- Dedicated threat intelligence capabilities on CTV, with specialties in threat hunting, malware reverse engineering, and threat modeling
- Global visibility and scale— Our DSP partner observes over 225B+ CTV requests per month across their global footprint.
- Security researchers and data scientists analyze devices and platforms to create CTV-specific algorithms utilizing at-network, OS, and business-level signals.

HUMAN's methodology involves fraud prevention at both the detection and prevention stages:

- Detects human traffic and IVT across CTV
- Detection across 20+ platforms including SmartTVs, Gaming Consoles, and CTV devices (i.e. AppleTV, Chromecast).
- Detection of SIVT types including device impersonation, app spoofing, hidden ads, incentivized ads, device farms, and SSAI spoofing
- Prevents IVT in real-time, before an impression is served
- Combines global detection cloud with closed-loop machine learning to deliver accurate predictions in milliseconds

Our DSP partner is a Trustworthy Accountability Group (TAG) member, a first-of-its-kind cross-industry program dedicated to eliminating fraudulent digital advertising traffic, combating malware, and promoting brand safety through greater transparency. They hold Certified Against Fraud, Certified Against Malware, and Cert*ified for Brand Safety seals. They are also proud supporters of the IAB UK Gold Standard.*

To continuously clean up the supply chain, our DSP partner promotes ads.txt, which is approved by the Interactive Advertising Bureau and filters out unauthorized digital sellers and resellers. Ads.txt allows you to purchase inventory only from sellers who have documented authorization and allows our team to identify sellers on the platform who may be attempting to spoof inventory. Unauthorized inventory is automatically excluded on the open market and all deals.

Our DSP partner has also adopted sellers.json and the OpenRTB SupplyChain object. Together, these specifications help identify and stop bad actors from selling fraudulent or low-quality inventory, driving spend instead to legitimate inventory and promoting quality content to protect our clients. They use the data from sellers.json and Supply Chain to understand a given publisher or intermediary's breadth of inventory across all exchanges. This results in greater control for clients and provides them with seller traffic information for learning and decision-making.