Eliminating Invalid Traffic ("IVT") from MoPub Marketplace

Invalid impressions and clicks are prohibited on MoPub's ad exchange. Our publisher policies require that impressions and clicks on ads must be the result of legitimate human user activity. In order to help us ensure that participants comply with this policy, we have invested in a comprehensive, multi-step solution for preserving traffic quality across our exchange.

Publisher vetting

Twitter's global Policy Operations team vets the IVT risk of every prospective publisher who wishes to participate in MoPub's ad exchange by leveraging Pixalate's *Media Ratings Terminal*, in addition to manual checks of app store listings and user reviews.

Pre-bid IVT blocking

MoPub's ad server is integrated with Pixalate's *Threat Intelligence* data feeds to automatically scan every ad call to our exchange and block Media Ratings Council-defined types of general and sophisticated IVT.

Post-bid IVT detection

DoubleVerify and Pixalate directly monitor post-bid impression samples across regions and ad formats to detect any potential supply-side threat signals, such as malicious IP addresses or user agents, spoofed bundle IDs, etc.

Investigation & policy enforcement

Analytics dashboards flag potential IVT to Twitter's Policy Operations team for further investigation. Publishers found to be in violation of MoPub's policies are subject to enforcement actions in accordance with MoPub's policies, which may include suspension from the exchange.

MRC-accredited partners

Accredited by Media Rating Council®

pixalate

DoubleVerify

Directly-integrated data & technology

Dedicated global resources

www.mopub.com | mopubDSPsuccess@twitter.com

Examples of in-app IVT

Data center	The user's IP address matches that of a known data center.
Duplicate impressions	High volumes of duplicate impressions, which may indicate an integration issue
Idiobots	Bots (or users) that change their User Agent string (spoofing), while keeping the same cookie
Click farm	An impression originating from a user who has been flagged as being associated with human click farm activity
Bundle ID spoofing	The app on which the ad content is delivered is misinterpreted via a fake or illegitimate app identifier (Bundle ID)
Device ID stuffing	Activity from a device that has connected to the internet via a statistically significant inflated number of different IP addresses
IP obfuscation	An IP that has been spoofed such that the impression is rendered to a different IP from the one originally offered
Location obfuscation	Activity originating from an IP where multiple impressions deviate significantly from the geographic location that is reported in the advertising transaction
Masked IP	The IP of a user does not match the IP and the associated ISP reported in the advertising transaction
Proxy	The impression is from an intermediary proxy device that exists to manipulate traffic counts, pass non-human or invalid traffic or which fails to comply with protocol.
Video impression fraud	Video ad impressions that are generated from the same browser or device at a statistically significant inflated rate

Helpful documents

Media Rating Council, Inc.

Business partner qualifications ..... MRC IVT Guidelines 3.4

Definitions of SIVT & GIVT ..... MRC IVT Guidelines 1.1.2

iab.

Types of fraud ..... IAB Anti-Fraud Principles and Proposed Taxonomy

Enhancing in-app tracking ..... Mobile Application Advertising Measurement Guidelines 5.0

Recommended and required attributes ..... OpenRTB API Specification

mopub

www.mopub.com | mopubDSPsuccess@twitter.com