PUSHSPRING
Audience data for a mobile world

Eliminating Ad Fraud in Mobile Apps

June, 2015

Overview

The global mobile advertising opportunity is massive, estimated at $69 billion in 2015 and projected to surpass $100B in 2016[1]. As a result, mobile app publishers are increasingly expanding the volume and availability of mobile ad inventory. In fact, in 2014, 70% of app publishers relied on advertising revenue to support their apps, and 69% of these publishers made portions of their inventory available programmatically through mobile exchanges[2]. With over 200B monthly in-app impressions available in the US alone on open RTB exchanges[3], advertisers need methods for identifying and preventing fraudulent impressions and clicks to avoid paying for non-human traffic.

Prevalence of Advertising Fraud

Advertising fraud is well-documented in the digital space. Estimates vary depending on the type of fraud, the environment, ad format, and other factors, ranging from 11% to as much as 23% of available display and video ad traffic[4,5]. In mobile advertising specifically, however, fraud rates can be much higher. Fraudsters are moving into mobile as fast as the advertiser budgets are, and they are finding ways to exploit the nuances of the mobile environment to proliferate ad fraud in programmatic exchanges.

In a recent campaign analysis, PushSpring found fraudulent or invalid devices on 41% of impressions available on mobile app exchange inventory. By applying basic optimization techniques such as blocking inventory from apps with high fraud percentages, overall fraudulent in-app campaign traffic was reduced to less than 15%. However, with the application of PushSpring Fraud-Free Targeting™ data to the same campaigns, invalid devices were eliminated completely, reducing unattributable impression traffic to less than 3%.

Types of Mobile Ad Fraud

In mobile advertising, fraud exists in three main forms: impression fraud, click fraud, and install fraud.

Impression Fraud: Non-human traffic generated by bots to register impressions within ad units. Impression fraud in mobile is generated the following ways:

- ***Invalid devices*** – Jail-broken or otherwise altered devices are used to machine-generate impression traffic that is sent to exchanges. These impressions are bid upon and served an ad that is never seen, but inflates cost to the advertiser. Often Invalid devices are used to generate traffic in combination with invalid apps, or valid apps that are supplementing legitimate traffic with fraudulent traffic to drive revenue.

- ***Invalid apps / traffic sources*** - Apps that produce fraudulent impressions, often redirected through multiple networks, exchanges, or via other domain masking processes to monetize traffic. More sophisticated fraudsters blend fraudulent traffic with human

traffic across legitimate apps and invalid apps to produce aggregated inventory that doesn't appear to be blatantly fraudulent.

Click Fraud: Clicks initiated by non-human activity. Click fraud in mobile is generated the following ways:

- ***Invalid devices*** – Similar to the above, jail-broken or otherwise altered devices are used to machine-generate impression traffic and ultimately clicks. Often Invalid devices are used to generate traffic in combination with invalid apps, or valid apps that are supplementing legitimate traffic with fraudulent traffic to drive revenue.

- ***Server-side fraud*** – code within an ad unit placement served by the app publisher's server automatically triggers an ad to click, usually after a certain duration, or combination of scrolling activities within the app.

Install Fraud: App installs generated from both human and non-human traffic, but representing fake users that have no intention of using or even opening the app. Typically fake installs are uninstalled within 1-2 days.

- ***Invalid devices*** – Jail-broken or otherwise altered devices programmed to serve machine-generate impressions, clicks, and ultimately install apps known to pay high bounties via CPI (cost per install) campaigns.

- ***App Farms*** – Multi-device labs pairing a single human operator across hundreds of devices, repeating sequences of app activity patterns to receive install-promoting ads, and perform fake installs.

PushSpring Fraud-Free Targeting™

PushSpring offers mobile app audience data, tools, and intelligence products for publishers and advertisers. . We process over 100 billion device signals every month to validate devices, apps, and behaviors to create accurate and unique targeting segments. We also monitor approximately hundreds of millions of programmatically available impressions across hundreds of app publishers and networks to qualify inventory sources and devices. Specific techniques we use to validate devices, IDs, and apps for successful fraud detection and elimination are:

- *Device interrogation* – Interrogation of basic device settings and attributes to eliminate invalid devices.

- *ID-level activity pattern recognition* – Monitoring device advertising IDs for known activity patterns associated with fraudulent impressions and clicks.

- *Traffic source quality scoring* – Monitoring programmatic traffic sources for indicators of fraudulent impression and click activity, including presence of identified fraudulent devices and IDs.

The resulting pool of PushSpring validated devices is targetable by advertising ID (IDFA and Android Advertising ID) and made available to advertisers in aggregate as PushSpring Fraud-Free Targeting™ IDs, as well as via PushSpring Personas and custom segments. For an example of the kind of data available through PushSpring, visit http://www.pushspring.com/personas.html

Performance Impact

Advertisers utilizing PushSpring Fraud-Free Targeting™ will realize immediate performance impacts to their mobile ad campaigns. Depending on the type of fraud typically prevalent in existing campaigns, the impact on performance metrics will vary as follows:

- *Impression fraud elimination* – Eliminating impression fraud removes wasted ad spend, lifts CTR, and lowers cost of acquisition and engagement.

- *Click fraud elimination* – Many advertisers will see a decline in CTR upon successful removal of fraudulent click-producing devices and IDs from their campaigns, but click to conversion rates will rise dramatically.

- *Install fraud elimination*– Install fraud is a primary reason CPI rates are lower for app advertisers. Successful removal of install fraud will raise CPI rates significantly, but app marketers will see a noticeable increase in app open and engagement rates, lowering their overall cost per engaged user.

Contact us

To learn more about PushSpring targeting and fraud elimination solutions, visit www.pushspring.com, or contact us at: hello@pushspring.com

References

1 http://www.emarketer.com/Article/Mobile-Ad-Spend-Top-100-Billion-Worldwide-2016-51-of-Digital-Market/1012299
2 STATE OF THE APPS - 2015 INDUSTRY SNAPSHOT; Millennial Media
3 Internal PushSpring estimates
4 IAS Ad Fraud Product Brief
5 The Bot Baseline: Fraud in Digital Advertising White Ops, Inc. Association of National Advertisers