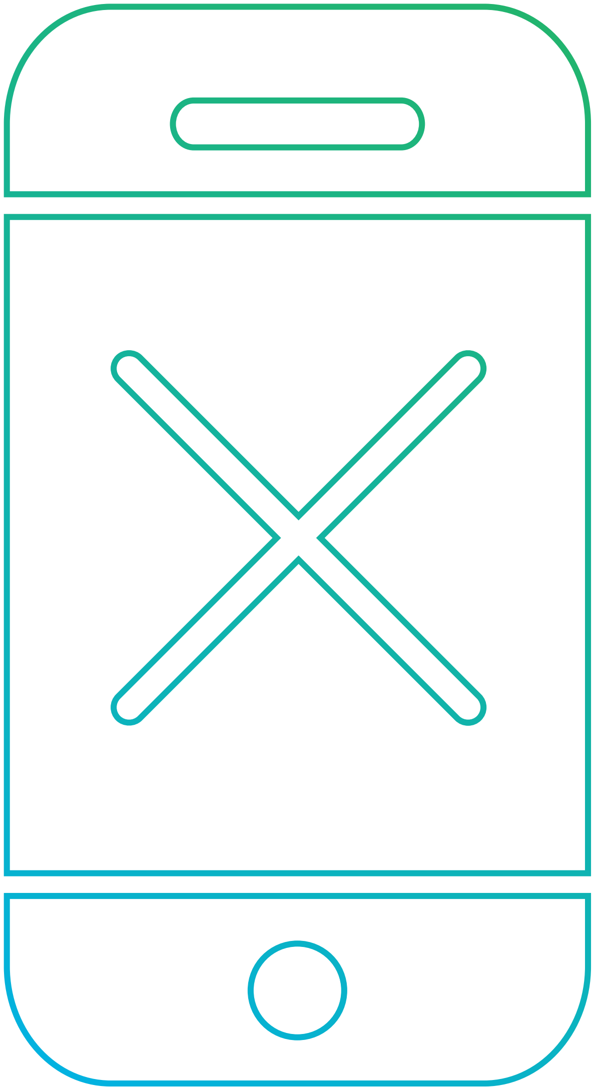
WTF IS MOBILE AD FRAUD?

DIGIDAY | OpenX

Contents



Introduction

In the spring of 2017, *The Economist* declared data to be a commodity "more valuable than oil" in our digital economy. If that's true, then ad fraud is a significant threat to our industry's chief export.

Ad fraud thickens our data with impurities that render it useless or, best case, in need of costly refining. Fraud distorts data, warping marketers' ability to understand their audience and costing them measurability and effectiveness, the great promises of the digital era.

Just like web before it, mobile app advertising is vulnerable to fraud. Bad actors using a blend of old and new techniques are estimated to have bilked the digital advertising industry to the tune of $7.2 billion in 2016. That figure is believed to have doubled in 2017, along with corresponding spikes in the cost of labor needed to rein it in.

"Consumer time and advertiser money continue to flow into mobile apps and games. It's natural that fraud is going to follow," according to eMarketer senior analyst Lauren Fisher. Mobile ad fraud presents a serious challenge for mobile marketers, but how does it work and what can we do to stop it? Keep reading to find out:

WTF is mobile ad fraud?

Defining mobile ad fraud

Mobile ad fraud is as varied as the mobile ecosystems across which it is committed. While fraudsters may import some classic tactics from web fraud, it's often not possible to identify mobile app fraud using conventional techniques. The mobile environment lacks the standardization and maturity of web-based verification solutions. According to Maggie Mesa, vp of business development at OpenX, the best way to define mobile ad fraud is by looking for outliers in user behavior— high download rates coupled with low engagement rates, for example—which may suggest fraudulent traffic.

Bot fraud

Install fraud

Targeting fraud

Bot fraud

Bots are the most pervasive source of fraudulent traffic, whether on web or app. Fraudsters can use botnets — huge networks of compromised devices that are controlled by a central authority — to generate false impressions or clicks. Alternatively, they might use racks of devices sitting in someone's basement to mimic real users. Unscrupulous app developers might even serve ads invisibly in the background while a real user interacts with an app. Either way, the effect is the same in each case: These tactics artificially inflate impressions without actually delivering any reach, boosting the cost for marketers without offering any value. Bots, as it turns out, don't have a lot of disposable income.

Install fraud

In install fraud, scammers create fake installations to inflate the value of their app's audience. Using bots or paid networks of human accomplices, they are able to create the appearance of a larger user base in order to extract a higher CPM from marketers or game Cost-Per-Install campaigns.

Targeting fraud

Rather than an elaborate technical cheat, targeting fraud is nothing more than lying. Bad actors serve ads to the wrong audience to generate impressions or clicks that don't serve the marketer's goals but inflate the campaign's apparent success. This can be done by serving ads in irrelevant contexts or geographic regions and masking location data. Some fraudsters also bundle and sell ads to third parties, extending the campaign to their partner's audience without disclosing it to marketers.

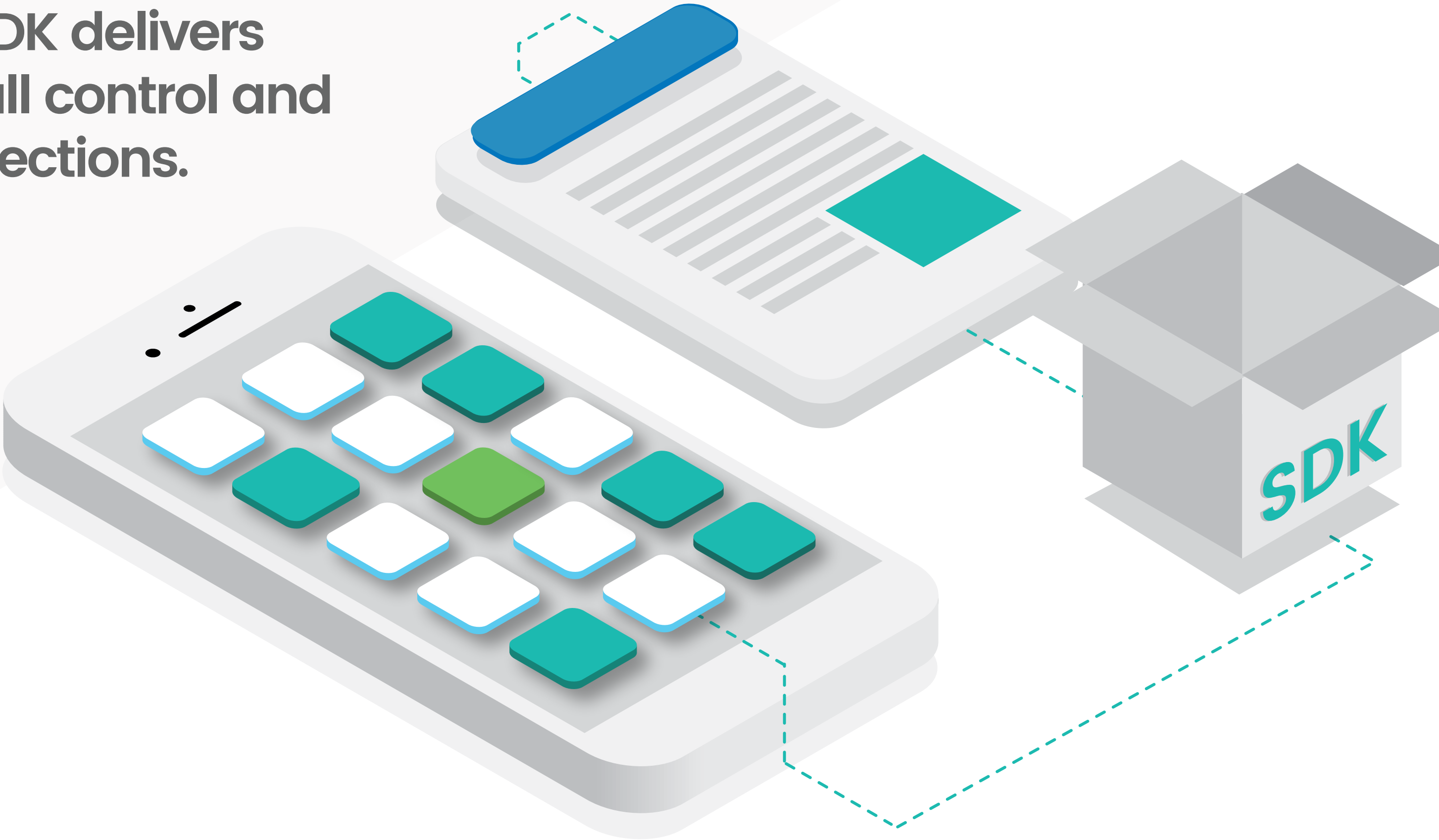
OpenX Mobile SDK

MORE FORMATS WITH MORE QUALITY CONTROL

The OpenX Mobile SDK delivers premium formats, full control and superior quality protections.

Empowering app publishers to attract more advertising spend without impacting the stability and quality of the app environment.

Learn More



Challenges

Transparency

Fraud thrives in low-quality, opaque marketplaces. The cure for these problematic transacting environments is transparency, said John Murphy, vp of marketplace quality at OpenX. Marketers want certainty about which audiences they're paying for. The Wild West nature of the mobile ecosystem disadvantages buyers, who don't enjoy confidence in the audiences, as well as mobile developers and publishers, who lose potential revenue to that lack of confidence.

Measurement

Fraud in desktop and mobile web has largely been checked through the rigorous application of comprehensive measurement tools. The mobile app measurement ecosystem is not as robust. Because ads are served directly to apps, buyers often don't have the opportunity to run additional scripts that could measure and evaluate non-human traffic.

Third-party verification does exist, but it hasn't yet been scaled and standardized the way web solutions have. These external verification services only work if the developer of the app in question has elected to use the same verification SDK as the verifier, leaving buyers few options other than to take figures provided by app operators and perform their own analysis after the fact.

Marketer solutions

Marketers may feel outmatched by fraudsters' myriad tactics, but the industry has developed tools to help them fight back. By enforcing standards for mobile campaigns and instituting a program of rigorous quality assurance, marketers can push back against fraud and reclaim budgets, data, and accuracy.

- Measurement standards
- Viewability standards
- Quality assurance

Measurement standards

"One reason that ad fraud can be so effective is that mobile marketers are only measuring the success of their campaigns on clicks and impressions," said Jason Kint, head of digital media advocacy group Digital Content Next. Kint and trade groups like the IAB agree that a more robust suite of marketer KPIs that includes engagement, video watch-time, and people-based audience metrics can help to curb fraud. He also suggests that marketers push app developers to adopt open source verification solutions offered by industry bodies like the IAB.

Viewability standards

Viewability has proven a difficult nut for marketers to crack. Most mobile ads are only viewable 50 percent of the time. On the one hand, demanding high levels of viewability seems like a no-brainer. On the other hand, experts argue that too much focus on highly viewable inventory can limit campaign reach and cut marketers off from legitimate audiences that frequent low-viewability sites. Still, boosting viewability standards and demanding accountability from app developers and other mobile media partners is an easy way to minimize loss due to lack of viewability.

Quality assurance

Although it can be labor intensive, a rigorous quality assurance program administered either in-house or by a third party contractor will help marketers to eliminate some of the more esoteric forms of fraud. Whitelists can help here, said Mike Zaneis, CEO of the Trustworthy Accountability Group, an industry organization dedicated to fighting ad fraud in all environments. TAG's database of legitimate publishers has grown to include a significant number of mobile-first and mobile-only publishers, including app publishers. "It's a good first step to know who you're doing business with," he said.

Publisher solutions

Publishers and app developers also have a part to play in combating ad fraud. While ad fraud costs marketers' money, time, and data, it costs the sell side something even more precious: credibility. A fraud-free mobile ecosystem benefits publishers and app creators looking to engage in high-trust relationships with advertisers and maximize the value of their inventory.

- Check your code
- Standardize verification
- Avoid low-quality exchanges
- Establish private marketplaces
- Detect & block non-human traffic

Check your code

For publishers, preventing fraud starts with the build. "If you're putting code into your app, you should know who it is coming from," said Zaneis. Rogue code in sketchy SDKs can be a portal for malware, a primary method for fraudsters trading in non-human traffic. Any code that auto-redirects should be scrutinized, Zaneis said, because malicious code can run up false impressions on fraudulent sites. "That's a big chunk of how fraud is operating."

Standardize verification

Third-party verification of mobile ads is only possible when the app developer and the verifying platform employ the same verification SDK. To combat this fragmentation of the verification market, the IAB has created and endorsed its own verification SDK, encouraging developers to adopt a single standard verification solution. Wide adoption of the IAB standard could create a more trusting environment for marketers and compliant app publishers to do business in.

Avoid low-quality exchanges

Ad exchanges provide a ready-made way for app developers and publishers to make money from their mobile content. However, many of these exchanges have a dubious—and well-earned—reputation for aiding and abetting fraud. "There's a reason these exchanges are less trustworthy," said Zaneis. "For publishers it's also a data security issue, because your user base is having malware installed."

Establish private marketplaces

For app publishers with in-demand content, it may be wise to establish a private marketplace. "It's still early days" for mobile app PMPs, said Zaneis. However, as in desktop, mobile PMPs provide assurance to advertisers that the impressions they buy will be delivered fraud-free. PMPs with multiple premium partners provide the benefit of a mutual quality endorsement. One participant vouches for another, creating a trusted community in which to transact business on a level playing field.

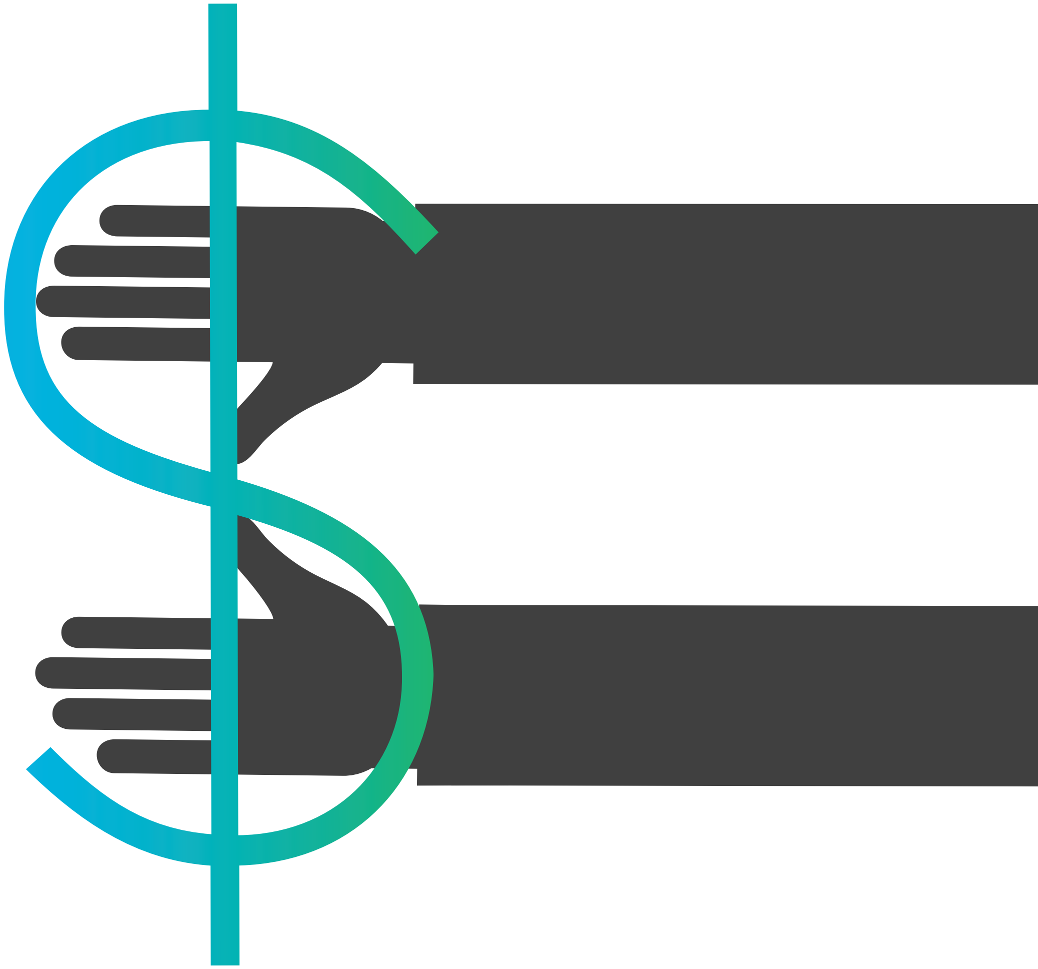
Detect and block non-human traffic

Sometimes even honest publishers can find themselves on the receiving end of non-human traffic. Bot-networks sometimes target reputable publishers, either as part of an attack or in an attempt to boost specific content, artificially driving up their clicks and impressions. While a spike in KPIs can appeal to publishers' egos, this kind of fraud impedes their ability to collect legitimate audience data. It's incumbent on publishers to actively detect and block abnormal spikes in traffic. Analytics platforms provide tools to monitor unusual traffic spikes and to block regions and domains in order to mitigate their effect.

Conclusion

The mobile app advertising ecosystem can seem like a wild frontier where marketers and publishers alike are subject to occasional banditry. Fortunately, it does appear that order is taking root in this previously lawless province. As in any frontier town, what's required is for all the residents to come together and agree on a set of guidelines for how to live. Industry bodies like the IAB have begun this work by putting forward open source solutions and encouraging app developers and mobile publishers to standardize their approach to measurement.

All that remains is for honest actors to adopt these solutions. The end of mobile ad fraud as a serious threat is likely to come not from some sweeping action, but rather from the gradual squeezing out of bad actors unwilling to participate in a more civilized mobile economy. As premium publishers realize the value of participating in a standardized form of third-party verification, smaller publishers will follow suit, eager to cash in on the ad dollars following toward trusted inventory. Those who choose not to participate will increasingly face a cold shoulder from an advertising industry that's less desperate for unverified mobile inventory. While challenges remain, the future of mobile advertising is looking more and more transparent, and the fate of mobile fraudsters, more and more grim.



PRODUCED BY CUSTOM FOR DIGIDAY MEDIA

Custom is a creative content agency that translates tech-speak into human-speak. Our journalists, strategists and artists help companies in disrupted industries stand out.

Want to work with us?

Contact Digiday SVP Drew Schutte, **drew@digiday.com**