The ripples effects of ad fraud

By **Media Samosa** - June 4, 2020

Shubham Jha, Sales Manager India, Adjust simplifies Ad Fraud in mobile advertising, while explaining how to stay safe on this front.

Mobile ad spend is on the rise in India, with projections putting spending at $1.73 billion USD in 2021, up from $460 million in 2017. But ad fraud remains a major challenge in the sector — even among social apps. In fact, in 2019, Adjust found that around 11% of all social installs were fraudulent.

Despite all its challenges, 2020 is undeniably proving to be a year of growth, but that can easily be undermined by ad fraud. Fast-growing regions like Southeast Asia can be especially attractive to fraudsters, as fraud prevention tools aren't as commonplace. The losses aren't just monetary — fraud also skews the accuracy of datasets, drives bad user acquisition decisions, and hides the best-performing channels. To make the most of 2020's opportunities, fraud prevention needs to remain a key priority for growth marketers.

So how do we prevent fraud? First, we have to understand it.

Ad fraud, simplified

Mobile ad fraud describes the actions that fraudsters take to siphon off advertisers' budgets by exploiting mobile advertising technology. Fraudsters use four main methods to commit their crimes: Click Injection, SDK Spoofing, Click Spam, and Fake Users. Ultimately, you can distinguish between two types of fraud — those that spoof ad engagements (like views or clicks) and those that spoof app activities (like installs, sessions, and events). The former is known as Spoofed Attribution. The latter is called Spoofed Users.

Fraudsters are also incredibly resourceful, and once they realize fraud filters are blocking a certain type of fraud, they will try and find a workaround or move on to those that are not protected.

But the ripple effects of fraud, the ones which aren't talked about, are how marketers are affected by fraud-filled datasets which influence their marketing decisions.

What fraud means for your metrics

Ad fraud doesn't just steal from advertising budgets — it also interferes with user acquisition decisions.

For instance, a partner might look like it's bringing tons of new installs, but there's a chance these attributions are fraudulent. If marketers can't tell the difference between fake and real users, they're likely to spend more money with the networks that appear to be yielding more or better users — effectively opening themselves up to further fraud. Marketers get caught in a feedback loop, directing money away from those sources that bring them real, high-quality users.

We also haven't considered the domino effect fake users have on in-app activity and purchase data. Some marketers may not be too concerned about fake installs: in some instances, they may even view it as a good thing as their user acquisition numbers look great on paper. But other valuable metrics, such as retention and lifetime value, won't match up, and that'll become a serious problem down the line.

Dishonest industry players could also attempt to poach organics by using Click Spam and Click Injection methods. The table below shows an example of the extent to which these methods of fraud could be affecting your metrics — just take a look at the difference in returns and ROI.

While most ad networks are reputable and have their clients' best interests in mind, sources further down the chain may be taking advantage of advertisers without the network's knowledge. In an ideal, fraud-free world, a marketer could be working with a network that brings them 500 installs at a CPI of $5, the total profit of which could stand at $1,000. Alongside this, they may also gain 1,000 organic installs, from which they profit $10,000. That's a pretty considerable ROI.

Also read: Podcast Marketing 101: Leveraging the medium during lockdown

But let's say the network now brings 800 installs at a CPI of $5. That's a big increase, which looks great at first glance. At the same time, the number of organic installs drops to 700. While it's not impossible, it's more likely that this particular source of traffic is using Click Spam or Click Injection to poach organic users and users from other networks in order to pass them off as their own. Marketers waste their budgets on paying for them, and their ROI drops significantly.

What's the solution to ad fraud?

While the industry may never be able to get rid of ad fraud completely, there are many approaches marketers can take to protect themselves. The most important step is understanding the problem, and then taking fraud seriously. Set up a clear process and internal point person to handle the issue. Growth marketers are in the perfect position to look at the numbers, see where they don't add up, and then escalate the issue.

It's also important to work with your partners towards transparency so that you know where exactly your ads are displayed. Fraudsters thrive off black-box models, so mobile marketers need to evaluate who they partner with and ask them how they're fighting ad fraud.

Ad fraud evolves fast, so stay educated. By joining summits and workshops, keeping up to date with the news, and opening up the conversation with networks and MMPs, UA managers can gain a better understanding of potential new threats and solutions. After all, bringing better education and awareness of the issue can help flush out fraudsters and keep your mobile marketing activities on track.

This article piece is authored by Shubham Jha, Sales Manager India, Adjust

Related posts:

Decade Samosa: Evolution of PR industry in the last 10 years...

Beti Ko Finance Padhao...

Disruption of a Trillion Dollar Industry: How can events industry rebuild

Comments

0 comments