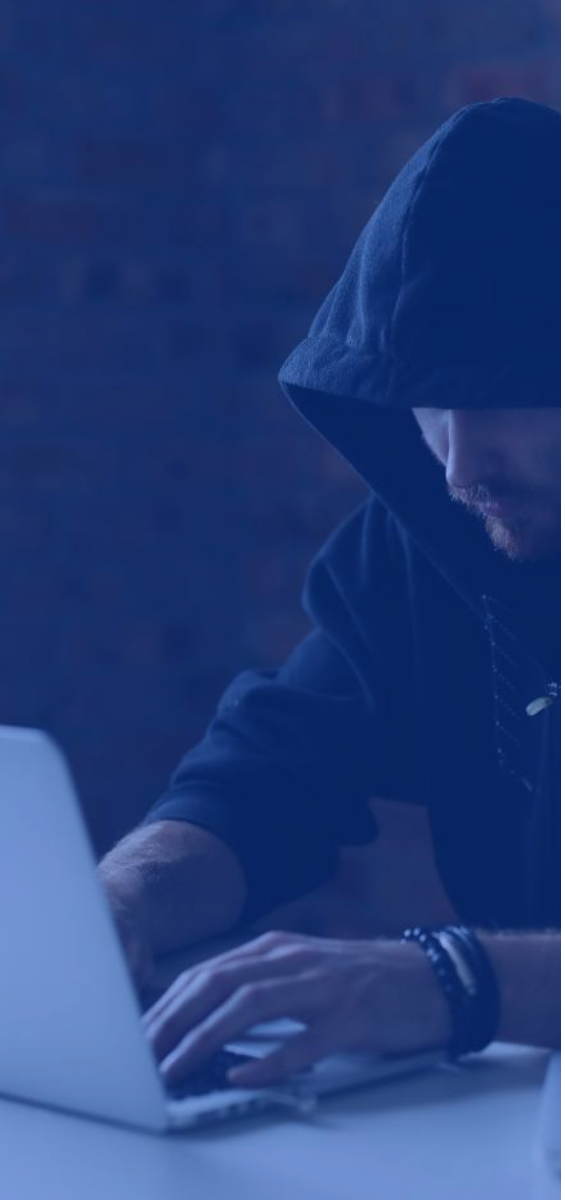


Ad Fraud in Mobile Marketing

How can Brands Detect And Prevent **Ad Fraud**

INTRODUCTION

Billions of dollars are wasted yearly in marketing budgets due to Ad Fraud in Mobile Marketing. It has become a primary concern for major mobile marketers as they fear losing business and even have to give up on their businesses as they accept the fact that fraud detection is too hard and that fraudulent clicks and app installs are unavoidable at the best.

There are times when detection and prevention of ad fraud would seem impossible in mobile advertising campaigns. But that doesn't mean it's not doable.

In fact, even we at Trackier have witnessed certain mobile ad networks with 80% fraud or even higher.

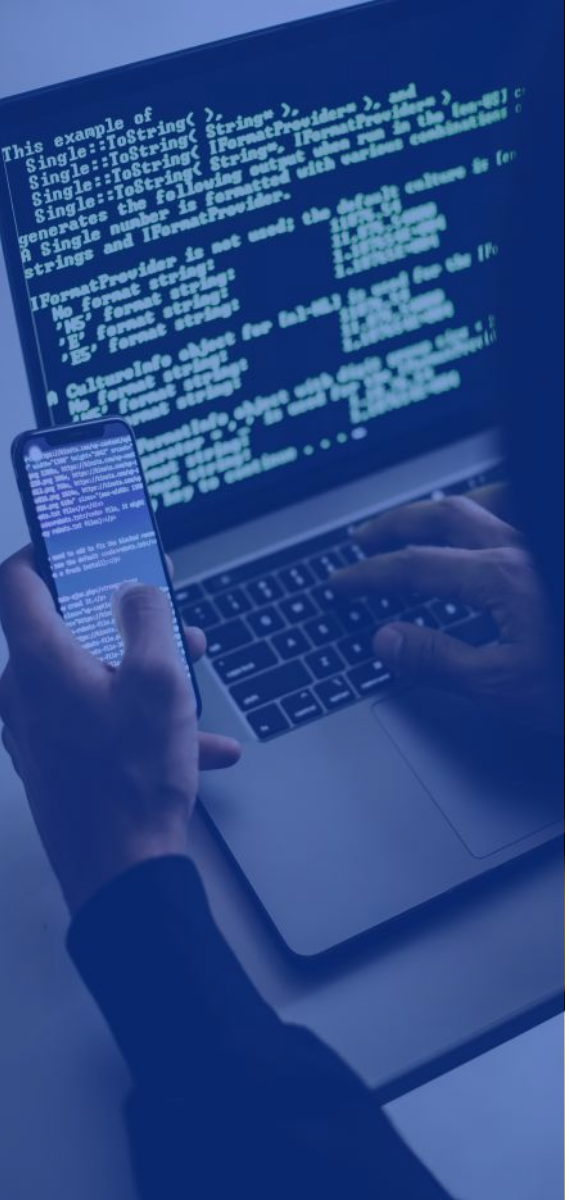
Also, keep in mind that there is plenty of bot traffic and fake click-in mobile ads out there that even specialized fraud detection companies fail to detect.

Detecting fraud can certainly be challenging with the advent of real-time bidding, programmatic ad campaigns, and modern fast-paced digital marketing.

We know it can be a hard bargain, but again let us reassure you that, ***Fraud detection and prevention are possible.***

It wouldn't be a wise decision for app publishers to give up when they come across ad fraud and surrender their marketing budgets to fraudsters and ruin their attribution reporting.

There are strong Anti-fraud, Fraud Prevention, and click fraud detection methods and tools out there that can help avoid such fraudsters and reduce your losses massively.



Trackier MMP helps App Owners from Mobile Ad fraud

Ad Fraud is a booming and lucrative business for these fraudsters. It is estimated that digital ad fraud losses are anywhere between $20 billion to $42 billion dollars roughly per year. And the numbers are going up as newer methods of fraud are haunting businesses every single day.

The need of the hour is a solution that adapts just like these fraud adapt. A permanent fix and prevention of such problems is required.

For what it's worth, one has to spend a good amount of time and research for the best fraud protection tool in the advertising industry and save their ad spending limited to legitimate and necessary activities.

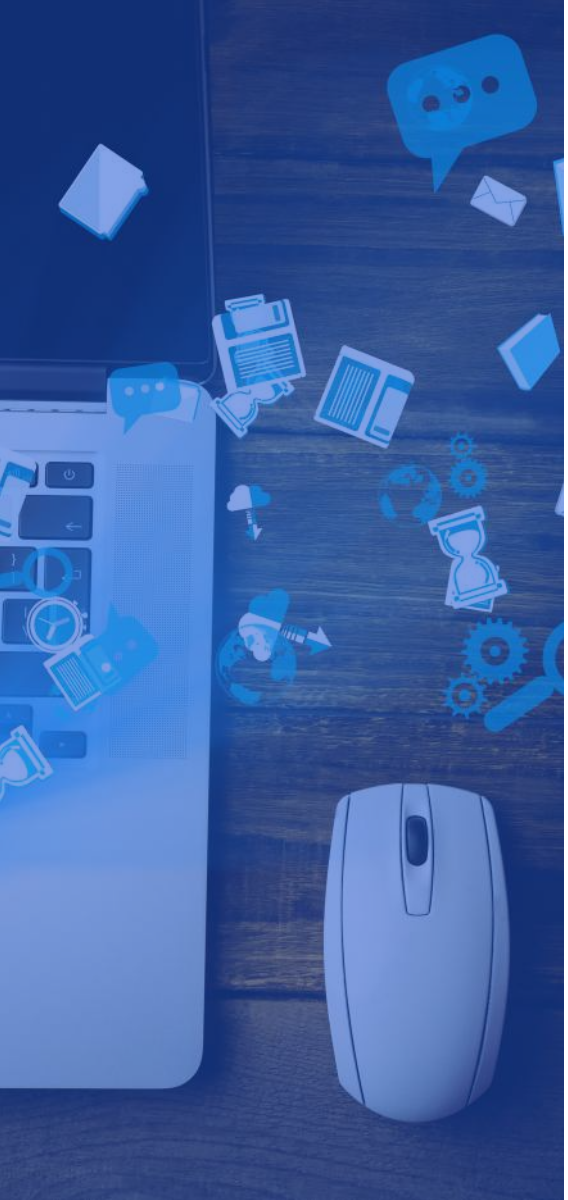
Trackier's each and every platform has an Anti-Fraud tool, especially on our Mobile Marketing Platforms

We specialize in focusing on all types of ad frauds, including click frauds, fake ad impressions, and majorly mobile app frauds.

Detection and Prevention of such Ad frauds remain to be our primary goal, and we have been making it customizable for all sorts of businesses, so that for every parameter attributed, we have a check for fraud.

We don't want their false positives to ruin your ROI measurement analytics.

Hence, it becomes very much in our interest to spend our time focusing to create an Anti Fraud tool that can be used on any of our attribution platforms.



How Ad Fraud is committed in Mobile Advertising?

- As we know, Ad Fraud sucks billions out of the advertising ecosystem every year. But to fix this, we need to understand how ad fraud works and how your hard-earned advertising budget is converted into dishonest money
- Advertising fraudsters start their lucrative money-making business by setting up an ad exchange as a Publisher.
- It is generally an anonymous copycat mobile application or some utility app like a flashlight or calculator.
- Keep in mind, that this can also be a big publisher's app, as there are apps kicked out of the Google play store for committing Mobile ad fraud.
- There have been cases where fraudsters buy existing apps that publishers have given up on and use them to display and engage with ads.
- As soon as fraudsters get a place to display their ads, they start to create "human" interest, and engagement as that's what mobile marketing is all about. And even though it is done by fraud in disguise of a publisher, the ad works resulting in an app install and payout to the fraud.

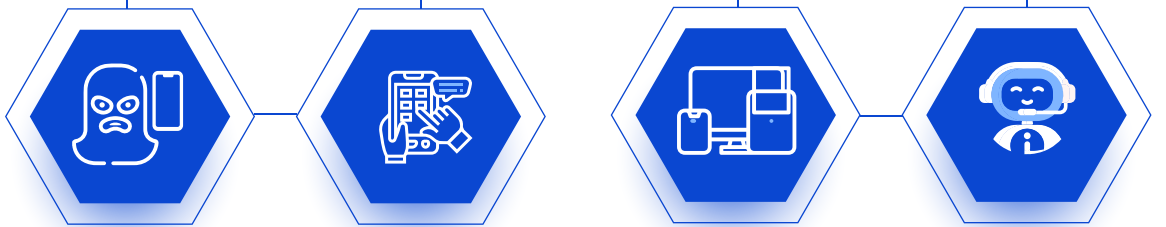
Now, there can be different types of Fraud. We will discuss the two major types of fraud that can occur. The first one is creating Fake installs and the other is Attribution Hijacking.

ATTRIBUTION HIJACKING

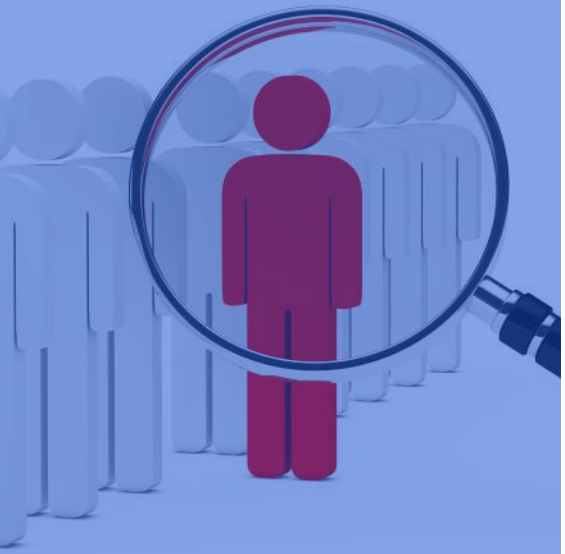
Fraudsters trying to steal credits for real installs by manipulating attribution.

FAKE INSTALLS

Fraudsters report in-app events such as clicks or installs which have never occurred.

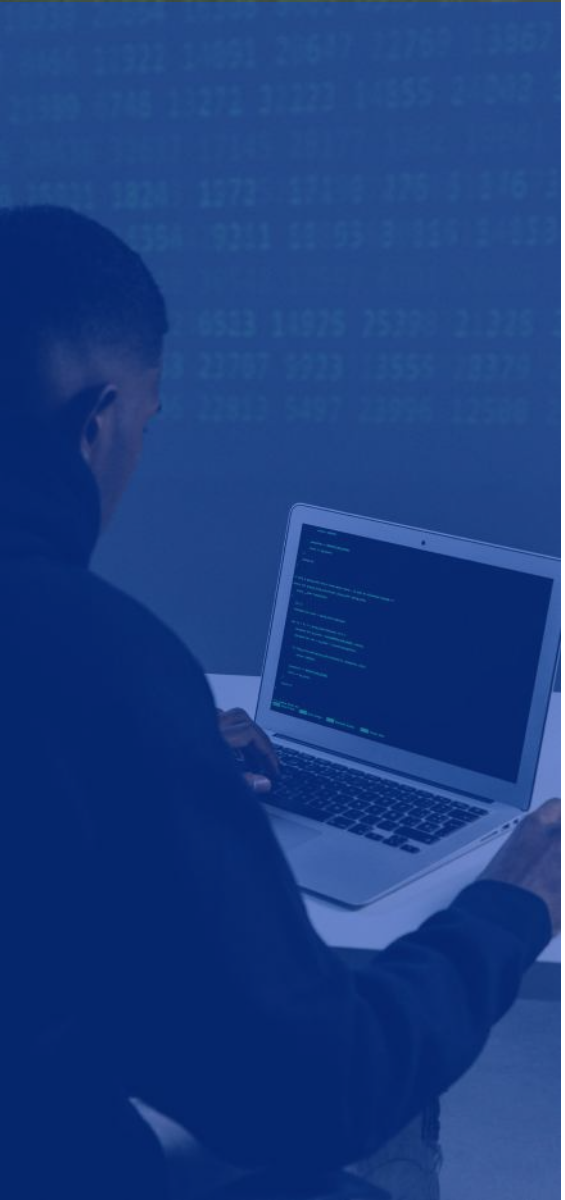


- Install Hijacking
- Click Flooding
- Device Farms
- Bots



Attribution Hijacking

- Attribution hacking methods use fake click reports of real users to manipulate conversion attributions.
- Fraudsters inject clicks at different points across the user journey in order to steal credit for installs and user leads collected and provided by other media sources.
- Mobile App Attribution is dominated by last-click attribution model, where Fraudsters send fabricated clicks (click injection) to attribution partners and hope to get credit for an app install.
- Unlike Fake installs where the entire user journey is fake, in attribution hijacking, users are real. But Impressions, clicks, installs and in-app events remain to be fake.
- It is obvious to say that advertisers lose value on their advertising activities and resources with both types of fraud, but unlike fake installs where the entire user acquisition data worthless, attribution hijacking methods still use real users who can pose some value to advertisers.



SDK Hacking

- Another popular method of ad fraud is SDK hacking or SDK spoofing, which is a bot-based fraud hat is executed by malware hidden on a different app within the user's device. This allows fraudsters to bypass install fraud detection as they feed false information into the advertising servers using real user devices.

- SDK spoofing creates a flood of new "organic" users along with users from paid marketing campaigns. Well, both types of users are fake, since the fraudsters keep changing their publisher IDs making it impossible to track.

- As these fraud spoof and make quick money, some of them even start their own ad networks, or register themselves into a programmatic exchange. Now, they can play around with market demand and expand their fraud by providing ad supply, all the while looking completely transparent.

- But the reality is that, there is no transparency, as no real brand exists and information on user devices encountering ads in an organic way are completely fabricated.

Fake Installs

In Fake Installs, users are completely fake and any interaction made within the app is pre-programmed to drain even more CPA rates from the advertiser and cause more damage.

The advertiser's data will often be worthless as these fake users mix with real ones, making retargeting efforts pointless.

There are two types of Fake Install fraud.

Device farms

- Device farms are basically physical locations filled with actual mobile devices used to click on real ads and download real apps while hiding behind false IP addresses and fresh device IDs.
- Operated either by low-paid employees or emulators, working around the clock on constant app engagement and device resetting. They endlessly tap around, install apps, and reset phones to get a new advertising ID such as GAID or AAID on Android.
- The more efficient the operation is at creating engagement and resetting its device identities, the more revenue it can generate.
- It is a relatively simple method and combined with lower mobile device prices, and economic difficulties introduced a second wave of device farms in common western households as a means of creating additional income.
- Even though these fake apps don't have any real users or much engagement, the fraudsters fake good metrics.

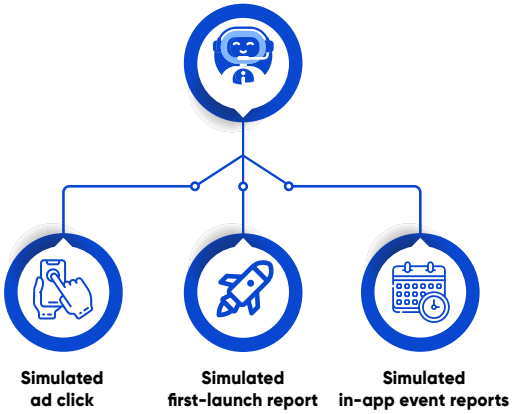
Some even emulate mobile devices in cloud-based servers which are much more profitable as they can automate the repetitive tasks of faking engagement, watching advertising videos, clicking on ads, and “installing” apps.

The web equivalent of this is buying traffic from bots that look human but aren’t. They are easily available via multiple botnets active on the dark web.

Bots

Bots are server-based malicious codes that are used to run a set program or action. In this case, bots aim to send clicks, installs, and in-app events for installs and register in-app events that never really occur.

Bots can be trained to automate any action within the app itself and even replicate different fraud methods. They can be used to mimic real user behavior based on biometric data gathered by malware planted on user devices.This makes these trained bots look real and make it harder for marketers to detect and block.



What’s even worrying is that Fraudsters adapt to advanced detection and train bots accordingly to run through in-app engagement attribution points as real users. This makes fraudsters look like valuable quality publishers and gain CPA revenue from in-app events undetected.

Different Ad Fraud Require Different Type of Detection and Prevention

Now that you've seen a few different forms of mobile ad fraud, it shouldn't be surprising to you that each requires unique methods of ad fraud prevention.

- One is what we just discussed: fake install fraud. The device might be real but the users certainly fake, and the install is certainly false.
- Another is attribution Hijacking where everything, from the device to the actual app installation is real, but the click reports and data are stolen from some genuine ad networks who have done all the hard work of targeting a user, placing an ad, and driving an app install.
- And there are other fraudsters who exploit by SDK spoofing or click fraud, ad stacking, mobile click fraud or countless ways of stealing advertisers' hard earned money.

These are some of the primary reasons why Trackier offers different forms of ad fraud prevention features. These are the certain KPI's that we include in Trackier SDK to identify Fraudulent attributions:

- **SKAdNetwork post-install events**
- **Device ID validation**
- **Click hijacking**
- **SDK spoofing**
- **Android Install Validation**
- **Click to Install Time Validation**
- **Outdated SDK Version**
- **Outdated App Version**
- **Non-Play Store Installs**
- **Click/Install Origin Country**
- **Blacklisted Publishers**
- **Blacklisted IP Addresses**

Real-Time Ad Fraud Prevention and Detection

At Trackier, we take one thing very notably, i.e, Ad fraud prevention needs to operate in real-time and be a form of proactive prevention. Proactive fraud prevention solutions block ad fraud before an attribution decision is made.

We believe that making a decision about fraud detection and prevention post the launch of your app install can be fatal, as fraudsters are much more likely to get away before our initial measurement as advertisers might have already paid them.

Mobile marketing is a fast-paced industry and every aspect of your app's performance is really important. It will all seem good as you skim through your high click rates, conversion installs from various campaigns, and other metrics. But you'll realize that your user acquisition and user retention would remain low. And by the time you realize this, fraudsters are already gone.

What worsens, even more, is the fact that whatever data has been collected is bad and false. You cannot make future decisions based on such data which is extremely dangerous for your business.

That is why Trackier recommends to its customers that an early decision on a proactive approach in fighting ad fraud can help marketers avoid dealing with fraudulent ad networks, instead of paying them heftily.

This also allows our clients to make sound strategic decisions quickly, optimize their user acquisition data and attract the right audience to their app while avoiding a massive mobile marketing disaster called an Ad Fraud.

Learn more about how Trackier can help

Trackier Anti Fraud Tool is comprehensive, curbs every kind of ad frauds and delivers the widest selection of transparent fraud alarms based on deterministic and probabilistic data analysis.

You can set & customize block rules for each campaign to verify traffic sources and be assured that the settings you need are enabled.

Our tool is a constant work in progress and adaptive. We constantly work on updating our tool for new forms of ad frauds and attacks.

Trackier's Anti Fraud tool will help you understand just how much you're compromising on your advertisement spending,identify where it is being allocated and help you boost your ROI by identifying good ad networks by eliminating the fraudulent ones.

Check out our **Anti-Fraud tool** and Get a **free demo** now.