Interceptd

How Fraudsters Take Advantage of Programmatic Mobile Advertising

How a prominent food delivery app used Interceptd and caught a well-known app to be fraudulently sending impressions and clicks to other famous e-commerce and betting apps over programmatic.

The ever-growing number of mobile devices around the world are making mobile advertising the top choice for promotions. Automated advertising methods, like programmatic ads on mobile, are becoming favored solutions due to the vast reach and variety of targeting options that they provide. However, with its increasing popularity, programmatic mobile advertising has also become a desired target for fraudsters, who are looking to take advantage of this trend. **By entrusting their budgets to programmatic buying, advertisers may think that they are safe due to the transparency provided, yet that is not always the case in reality.**

Motivated by bringing advertisers' attention to the intricacies of programmatic advertising, this case study is built to reveal how this advertising trend can also be subjected to fraudulent activity. The client in this particular case is a food delivery app, looking to increase their volume and reach new target markets.

No industry is safe from mobile fraud, but due to the rising popularity of food delivery apps, we are seeing this field become more sensitive to fraudulent activity, which includes generating fake traffic to apps and stealing organic installs. We have observed the activity of the DSP on which the campaign was running and proved that, even without showing an ad, publishers are sending clicks to hundreds of ads, resulting in 20% of fraud in the overall traffic.

Short Introduction of the Client and the Campaign

- Food Delivery App

- Advertising Region

  Latin America

- Description

  After researching different possibilities, they have decided to try programmatic advertising.

What makes programmatic mobile advertising an attractive solution for mobile app developers?

Programmatic advertising or programmatic buying is described as the automated process of media buying. It allows advertisers to generate data about the users and to utilize it to make ads more personalized and targeted. Programmatic buying is suitable for both desktop and mobile advertising as it provides access to a high volume of users. The latter, however, is gaining more and more popularity, due to the fact that nowadays everyone is on their mobile devices and everything that is developed is mobile-first.

Studies show that people spend 3-5 hours on their mobile devices daily, and 90% of this time is occupied by browsing different mobile apps.

In light of these facts, our client, a prominent food delivery app, was also quite interested in programmatic advertising.

As a food delivery app, users need to be targeted at a very specific time of day - morning - for breakfast; noon - lunch; and in the evening - dinner. Since programmatic advertising relies on data generated from the users, this makes it the best solution for customized approaches when targeting and identifying the most suitable customers. However, this does not mean that the app will be targeting one or two users at the same time. As customized as it is, the target audience for a programmatic campaign in a capital city, for example, can reach millions of users without a problem and in only just a few seconds. And in addition, the advertiser and the app developers can enjoy the **transparency** of the traffic that they receive from the programmatic publishers. Full access to publisher data allows for a deeper understanding of quality and potentially optimizing the return on advertising spend by targeting only the most profitable placements.

What should you be aware of when advertising on programmatic?

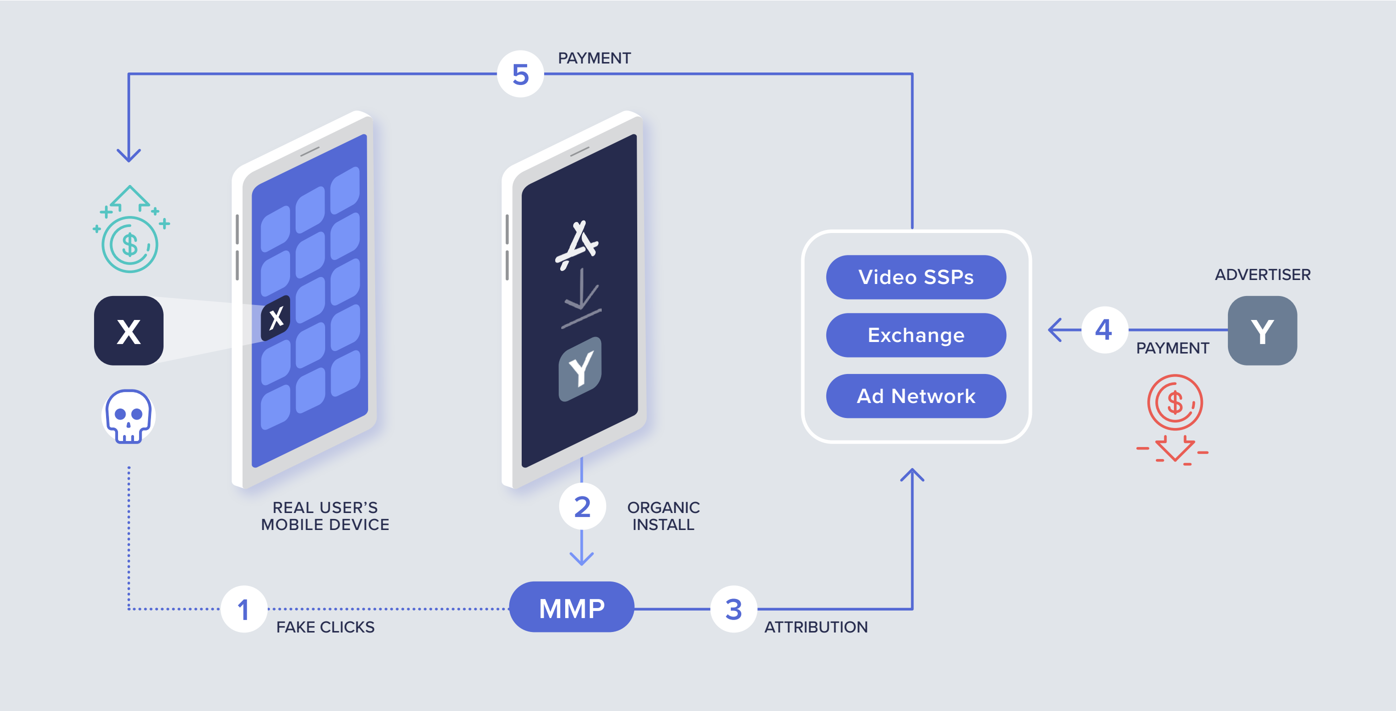
The growing potential of programmatic mobile advertising is making it a lucrative target for fraudsters, whose deceptive practices are costing mobile advertisers and developers billions)

Mobile fraud can take many shapes and forms, some of the most common are: hidden ads, click spamming, fake app installs, and click injection. In some cases these types of fraud are easily detected, in others, the fraudsters are using advanced techniques and the advertisers and app developers need help identifying the malicious activity. Mobile app developers nowadays learn to rely on MMPs (Mobile Measurement Partners) in order to attribute the activity that they receive from different sources (like programmatic advertising), but they also use the MMPs ad fraud prevention tools. In some cases, like the case that is described below, the MMPs are not sophisticated enough to detect all of the more advanced fraud patterns.

In the case of our client - the food delivery app - they have decided to run on programmatic campaigns, because of the aforementioned precise targeting, speed, and transparency. However, our in-depth investigation of the programmatic traffic provided by the selected DSP to the campaign, as transparent and efficient as it may be, was **not fraud free.**

What did we find?

Through the course of the promotion, the majority of the traffic came to the Android campaign from a well-known DSP. It is a known fact that campaigns on Android devices are more exposed to fraudulent activity in comparison to



iOS devices (Android devices have a 1.7x higher mobile fraud rate. What was odd in this particular case is that many of the installs came from a popular entertainment app, which claims to be safe and secured and has over 300 million downloads. By examining the app we were able to understand what it was actually doing - **this app was mimicking real users' behavior by sending hundreds of clicks to our client, but also to other apps - well-known e-commerce apps and sports betting apps - and some ad networks.**

Apps that generate clicks this way in many of the cases do not need real users to see the actual ads. They are running impressions and clicks in the background, without the user's knowledge and the only thing they need is the app to be installed on the phone.

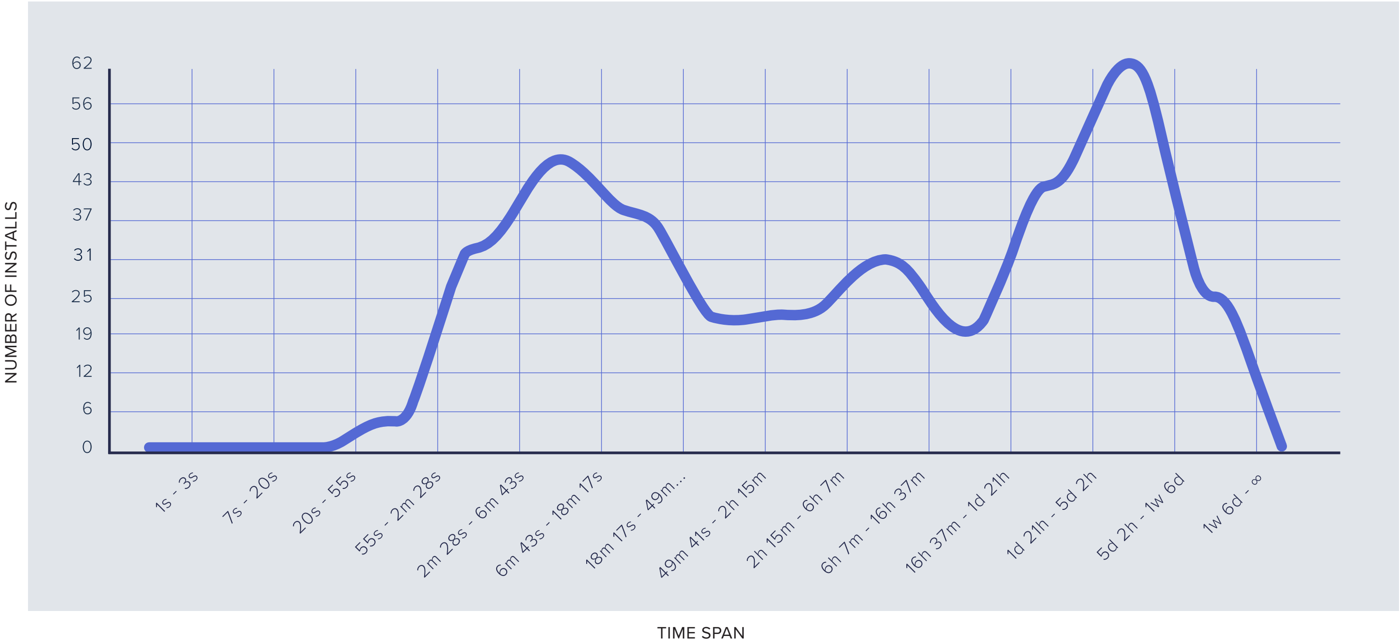
This kind of behavior is very difficult to detect - however there are some patterns that can help the advertisers to recognize this fraudulent activity.

Nowadays advertisers rely on the reports that they receive from their attribution partners. The MMPs employ a technique called "last-click attribution" meaning the very last click on the ad gets all the credit for the install transaction. In our case study, various fraud tactics and techniques were employed by "fraudsters" in order to manipulate the MMP and diminish its capability of detecting the misattribution and invalid traffic. Only in some of the cases was the MMP able to recognize that the clicks brought by the app were not real, and as a result, the majority of the traffic received in this campaign was deemed legit (and only 3% of the install of these clicks were rejected by the MMP). In fact, over 65% of the overall number of installs was fraudulent and needed to be rejected by the MMP and not post-backed to the advertiser and ad network.

Interceptd was able to flag this fraudulent activity and give the advertiser a chance to get a refund. We detected Click Spamming and Click Injection - both suggesting the stealing of the organic users from the advertiser.

- Click spamming: Sending large numbers of fraudulent clicks in the hope of delivering the last click prior to an organic install and hence getting the credit for the transaction.
- Click injection: When a new app install takes place, the app/code sends a series of clicks to the MMP before the install is completed in order to get credit for the install.

CTIT Distribution



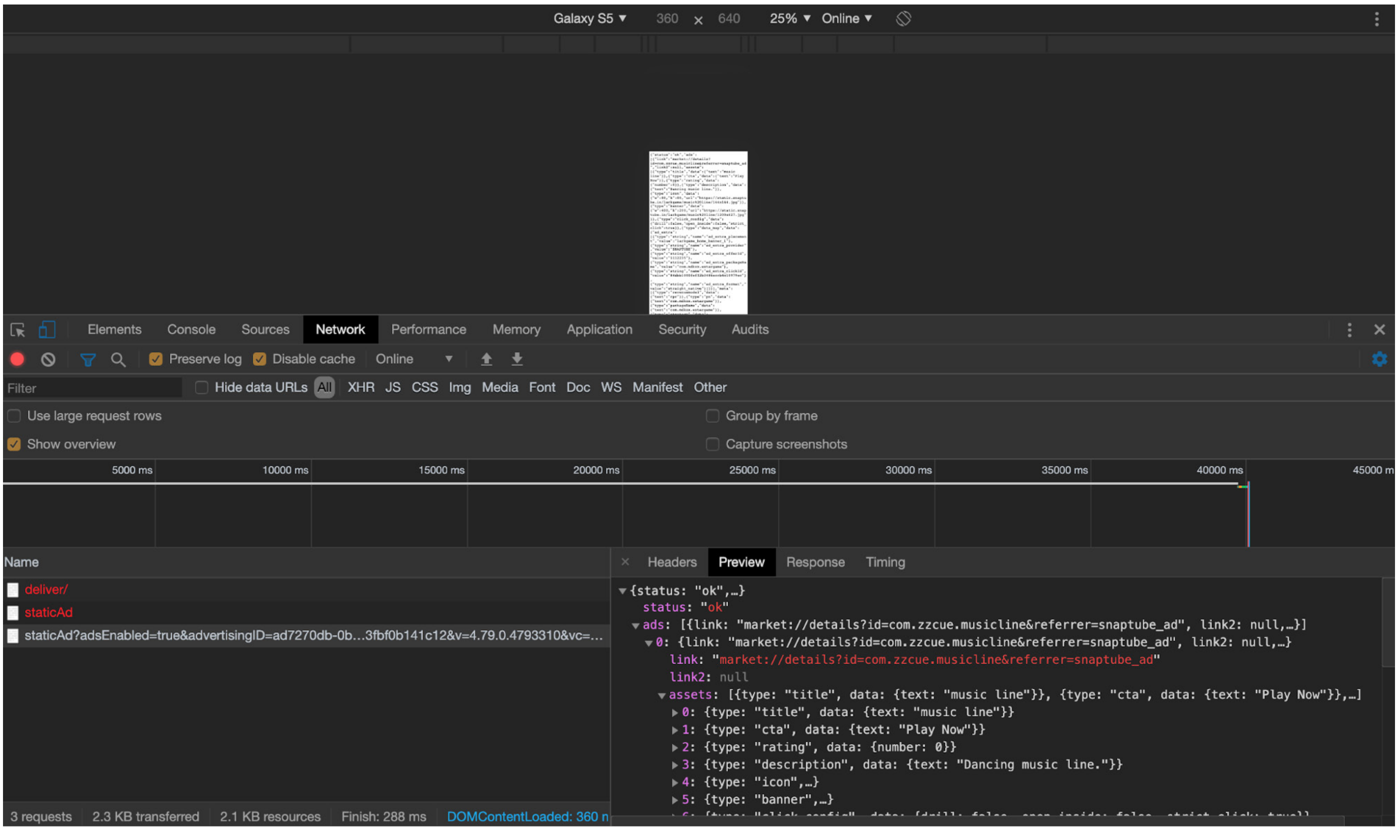
How does the fraud behind the app work?

On a fraudulent publisher app, there are fixed ads displayed to the users which belong to their own campaigns/apps or their partners' apps. Once a user starts using the app, they fire clicks on the background to many profitable ad campaigns, often of popular applications that are likely to be downloaded organically and hence in reality, whose ads are never even shown to the user. This gives them the opportunity to run ads for many different brands and deplete the advertisers' budget without delivering the expected results. Many fraudsters are also sophisticated enough to trigger clicks on these ads. The clicks are not real though, they are generated to maintain their "high performance" state as their CTR would be high, and generated by the malware. Since devices are real, it is hard for many tools to differentiate this from genuine ad clicks.

Similar behavior was observed by our Research Team when they examined an app that was available in the inventory of a reputable DSP. We detected click spamming activity and raised a click spamming alarm. We also suggested one of our advertisers to block a specific publisher. Since the publisher was a high performer, the advertiser requested a deep dive into that case.

For a couple of days, our Research Team analyzed the app and listened to the signals that it was sending to other ads and ad networks. The findings were troubling. The app sent thousands of clicks to advertising URLs other than the one promoted by the advertiser. Those clicks were being generated to multiple ad networks running campaigns in several regions and for several advertisers.

Where are all the requests going?



☐ Use large request rows
☑ Show overview

Name

```
deliver/
staticAd
staticAd?adsEnabled=true&advertisingID=ad7270db-0b...3fbf0b141c12&v=4.79.0.4793310&vc=...
```

3 requests | 2.3 KB transferred | 2.1 KB resources | Finish: 288 ms | DOMContentLoaded: 360 n

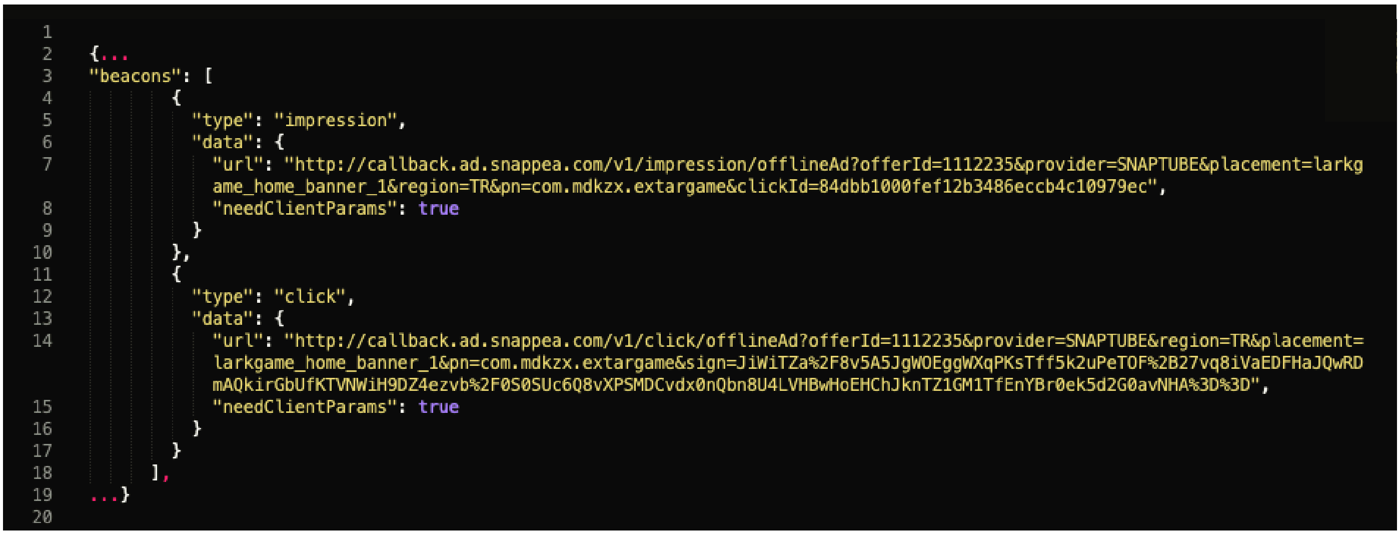
```
▾{status: "ok",…}
   status: "ok"
  ▾ads: [{link: "market://details?id=com.zzcue.musicline&referrer=snaptube_ad", link2: null,…}]
    ▾0: {link: "market://details?id=com.zzcue.musicline&referrer=snaptube_ad", link2: null,…}
       link: "market://details?id=com.zzcue.musicline&referrer=snaptube_ad"
       link2: null
      ▾assets: [{type: "title", data: {text: "music line"}}, {type: "cta", data: {text: "Play Now"}},…]
        ▸0: {type: "title", data: {text: "music line"}}
        ▸1: {type: "cta", data: {text: "Play Now"}}
        ▸2: {type: "rating", data: {number: 0}}
        ▸3: {type: "description", data: {text: "Dancing music line."}}
        ▸4: {type: "icon",…}
        ▸5: {type: "banner",…}
        ▸6: {type: "click_config", data: {drill: false, open_inside: false, strict_click: true}}
```

The cycle contains mainly two parts.

1. Getting Ads

This well-known entertainment app sends ad requests to its SSP, which has two publishers authorized in their “ads.txt.” When a publisher makes a request for an ad, it sends a response with certain ad payload to the party who is requesting the ad. It’s the normal chain that is currently done in programmatic ad tech.

The callbacks are as follows:



```

{...
"beacons": [
        {
          "type": "impression",
          "data": {
            "url": "http://callback.ad.snappea.com/v1/impression/offlineAd?offerId=1112235&provider=SNAPTUBE&placement=larkg
            ame_home_banner_1&region=TR&pn=com.mdkzx.extargame&clickId=84dbb1000fef12b3486eccb4c10979ec",
            "needClientParams": true
          }
        },
        {
          "type": "click",
          "data": {
            "url": "http://callback.ad.snappea.com/v1/click/offlineAd?offerId=1112235&provider=SNAPTUBE&region=TR&placement=
            larkgame_home_banner_1&pn=com.mdkzx.extargame&sign=JiWiTZa%2F8v5A5JgWOEggWXqPKsTff5k2uPeTOF%2B27vq8iVaEDFHaJQwRD
            mAQkirGbUfKTVNWiH9DZ4ezvb%2F0S0SUc6Q8vXPSMDCvdx0nQbn8U4LVHBwHoEHChJknTZ1GM1TfEnYBr0ek5d2G0avNHA%3D%3D",
            "needClientParams": true
          }
        }
      ],
...}

```

2. Phantom Clicks - Request for Ad

The app requests for ads like the following example to its SSP.

```
// http://api.ad.snappea.com/v1/deliver/staticAd?local_timezone=3&networkType=WIFI&ad_type=1&ppi=320&androidID=73586c-
%206c63df11b9&longitude=32.8108&reqid=5d060d40-2501-462b-aec5-
f2a95fecca27&offset=0&placement=youtube_details_%20banner_adx&ratio=320*180&count=1&advertisingID=ad7270db-0b34-4730-b4ab-
a08fe7bac215&ad_h=50&avr=6.0.1&lo-%20cation=Turkey%7CAnkara%7C%7CAnkara%7C&imei=358003075317232&brand=samsung&ad_w=320&directDown-
%20load=true&latitude=39.915&local_time=16%3A26&recentIAds=video.like%2Cvideo.like%2Cvideo.like%2Cvideo.%20like%2Cvideo.like%2Ccom.w
eieyu.yalla%2Cvideo.like&cache_flag=all&imsi=&model=SM-J500F&u=d2e-
%20c5507015abf5019343fbf0b141c12&v=4.79.0.4793310&ch=tube_uptd_as&networkCountryIso=TR&region=TR&lo-
%20cale=tr_TR&lang=tr&pn=com.snaptube.premium&f=phoenix2&net=WIFI&random_id=10&os=23&vc=479331
```

Some Tracks

Phase 0: AdMobo click

Phase 1: AppsFlyer touch

Phase 0: Click fired to tracking.lenzmx.com

Phase 1: Redirect (302)

Phase 2: AI Ad target (202) -> Response js scrip

Phase 3: Cloudfront index *(Final touch)*

Phase 0: Ad Request

Phase 1: 1st touch

Phase 2: 2nd touch

Phase 3: 3rd touch

Some Tracks

All the evidence suggested that intentional fraudulent behavior was performed by this entertainment app, deliberately stealing the organic traffic of the advertiser's app.

The moral of this case study is that despite the trust that we have in programmatic advertising and the transparency that is provided by the DSP, fraudsters still find a way to cheat the system and steal budgets that are dedicated to acquiring new and REAL users.

What are the key findings in this case study?

- Some of the biggest challenges that advertisers face on programmatic buying is fake transparency, which makes it difficult to verify the quality of the data that has been received, and lack of knowledge and understanding of the overcomplicated programmatic ecosystem.

- Programmatic mobile advertising is an innovative and an interactive way of advertising, but it is clearly not fraud free.

- Having an MMP as a fraud prevention tool would not be enough, as MMPs are not capable of automatically excluding/blacklisting such kind of publishers from the ad campaign and their protection is not enough as proposed in the study.

- Being vigilant about where your campaigns are running is very important, but so is finding a good partner that will keep a watchful eye over the quality and performance of these campaigns.