COMBATING
MOBILE ADVERTISING FRAUD
THE NEXT
BATTLEGROUND

AppLift

TABLE OF CONTENTS

Foreword

Ad fraud is ubiquitous and continues to attract attention and discussions within the industry, with mixed estimates on the depth of financial losses due to ad fraud. One study puts the amount of global digital ad spend wasted on fraudulent traffic as high as $16.4 billion in 2017, twice than the previous projections (Business Insider). Another recent research projects $6.5 billion in financial losses due to ad fraud, down 10% from the estimated $7.2 billion in 2016 (White Ops).

Despite the numbers, one thing is certain: the scale and sophistication of ad fraud has grown since mobile advertising picked up in 2012. Ad fraud is pervasive at various levels, with fraudsters finding new ways to trick the system.

Until now the industry had a rather myopic view on ad fraud, viewing it as mainly an issue for the advertisers. But it affects more than just app developers and advertisers — ad fraud breaches the trust between networks, publishers and advertisers, damaging the reputation of the entire industry.

As an active player in the ad tech space, we have been focusing our efforts on detecting and preventing ad fraud. Our first comprehensive study on the extent of mobile programmatic fraud in the industry was published in 2015. With that study we took a deep look at the fraud statistics and patterns within mobile programmatic to understand the fraud trends we saw at that point.

Today, the industry is exposed to new challenges and the issue of ad fraud has become more important than before, as simple bots have made way for sophisticated techniques that are harder to detect without a sound understanding of pattern detection and heuristics and requires a combined efforts of humans and technology to win the war against ad fraud.

With this study, we make an attempt to explain the challenges we are confronting on an ongoing basis. This eBook is an attempt to provide an update on the fraud patterns, illustrate key heuristics for fraud detection and prevention.

We also provide concrete guidance for designing and executing fraud fighting measures as a basis for all stakeholders to come together and fight it.

Stefan
Managing Director
AppLift

Executive Summary

The mobile industry is constantly evolving, and we have seen huge progress together ever since advertising on mobile first began. But even so, we are presented with constant challenges. Ad fraud is one of the most pressing and complex issues today.

Having evolved from simple Bots and Auto Redirects, fraudsters have developed more sophisticated techniques such as click spamming, ad stacking and click injection — what can be called the hot bed of the ad fraud battleground. Fraud distribution across the globe exposes the vulnerabilities we face today — relatively newer markets such as India and Indonesia have a higher percentage of fraud as compared to the more developed markets of the West.

We categorize fraud into the dimensions of Compliance Fraud and Technical Fraud, with most modern-day fraud occurring along the segment of Technical Fraud (i.e., fraud committed through the use of technology to "game" the ad tech system). We segment fraud at each stage of the funnel and take a look at some of the common ad fraud types of Attribution Fraud and Install/Post-Install Fraud, which present dangers to the advertisers today.

These technical fraud types are hard to detect on a surface level and require sophisticated pattern-detection technologies along with human effort. There are six main patterns to detect such fraud types:

IP Filtering and Blocking:

Detecting fraud at early stages by mapping the installs received by IPs/Subnets for fraud-free versus suspect traffic can be a first filter to see if particular IPs/Subnets are delivering unusually high installs.

Analysis of Devices:

Information about the device also helps to detect fraudulent activity by implementing algorithms to monitor traffic coming from different sources to identify cases of any strange activity.

Intraday Distribution of Installs:

Taking a look at abnormal spikes in a 24-hour period helps to identify suspicious traffic, as a mapping will show a curve that will have stable installs through the 24-hour period, versus flat or abnormal spikes in case of fraudulent traffic. This metric, however, should be carefully applied to take into account the traffic from various timezones.

Click-To-Install-Time (CTIT) Distribution:

Distribution modeling of the time between clicks and installs is a significant metric to detect any suspicious patterns. Typically CTIT follows a pattern with a lot of installs coming within a short period of time after the click and less installs afterwards. There's also usually a lag between the time when a user installs an app and uses it. Factors such as size and the type of app will also affect this.

In-App Activity Related:

User's behavior within the app can be a good metric to identify if the install is of fraudulent nature. Typically, if it is seen that users coming from a given source have no or significantly low post-install in-app activity, that particular source can be flagged as fraudulent.

Conversion Rate:

Similar to in-app activity behavior, unusually high or very low conversion rates can also be used as indicators for any suspicious traffic.

Introduction

“FOLLOW THE MONEY” is a popular catchphrase from the 1976 drama “All the President’s Men”, referring to the money trail and corruption within high political offices.

In mobile advertising, fraudsters exactly know this — mobile apps and websites have become an attractive target for fraudsters as the advertising spends have increased. In the last two years, as an industry we have made good progress in detecting, preventing and fighting fraud at various levels of the funnel. But as is the nature of any fraud, fraudsters try and find new ways to identify vulnerable spots, evolving and changing shapes as the industry evolves.

To understand how ad fraud has evolved in the industry, we need to take a look at the history of ad fraud to make sense of the trends we see now.

History of Fraud and Current Challenges

Fraudsters are like chameleons: they blend in to run unnoticed. Their techniques, since the early days of this market, have been following what advertisers are looking at and focus on.

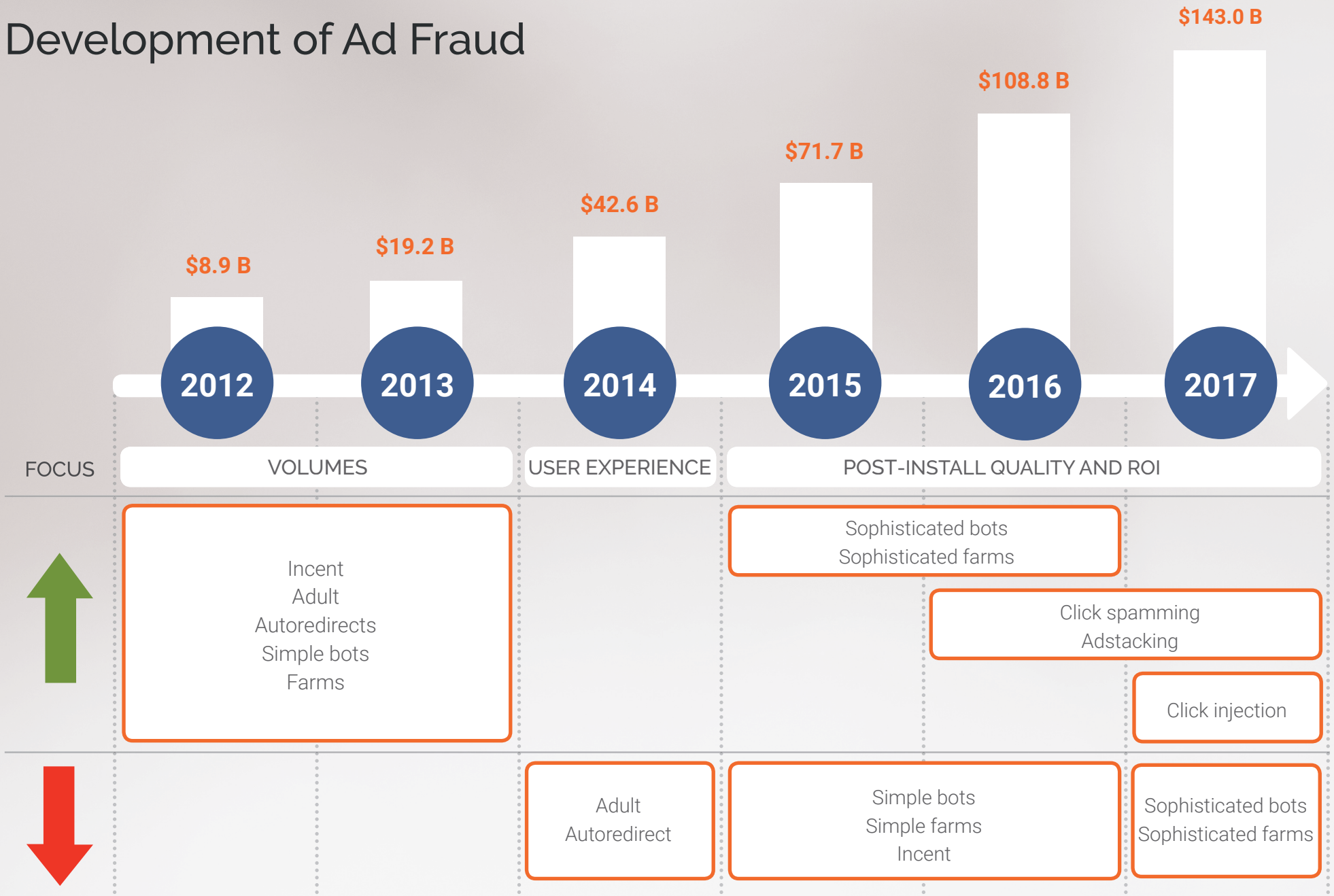
Back in 2012, when advertisers were focusing on growth and only looking for volumes, fraudsters found ways to deliver scale in a variety of ways: using incent traffic on non-incent campaigns, buying cheap traffic like adult or auto redirects, developing bots that emulated mobile devices and generating installs or investing into farms where people would be paid to install apps on mobile devices all day long.

Some of the techniques got rapidly identified by advertisers who started receiving complaints from their users who were being redirected automatically to the app store against their consent, or after they had seen an ad on an adult website. At that point, advertisers started to care more about user experience and worked hand-in-hand with networks to block such practices efficiently.

After this period of rush for volumes, shareholders and C-level executives realized they were investing huge amounts in marketing, but they were not necessarily getting the returns expected from their newly acquired users. It can be said that this was the moment that started the trends we are currently seeing in the industry; advertisers focus more on post-install quality and ROI.
At that moment, advertisers started sharing post-install data with networks more systematically. Simple bots and farms that were not able to replicate post-install behavior quickly became less relevant for fraudsters — they were getting flagged easily by advertisers and networks. Fraudsters, then, had to develop more sophisticated mechanisms to replicate real user behavior, by having their bots or farms engage with the app, even to a level where small in-app purchases were made. These bots and farms are identified most of the time now, since their user behavior replication is never perfect (e.g., through metrics such as no engagement after a certain period of time, unrealistically high engagement, etc.)

With rising expectations in terms of quality from advertisers, often comparing quality from organics and paid installs, fraudsters started to ask themselves: how can we deliver installs at scale with a quality similar to organics? The answer came rather easily: what is as good as organics, if not organics themselves? This is when organic theft techniques started appearing in the industry. We are talking here about click spamming, ad stacking and more recently, click injection. These three fraud mechanisms are now the big pie in the mobile fraud ecosystem, the techniques everyone is trying to detect and prevent efficiently. And it's not that easy, as we will see later in this ebook.

Development of Ad Fraud



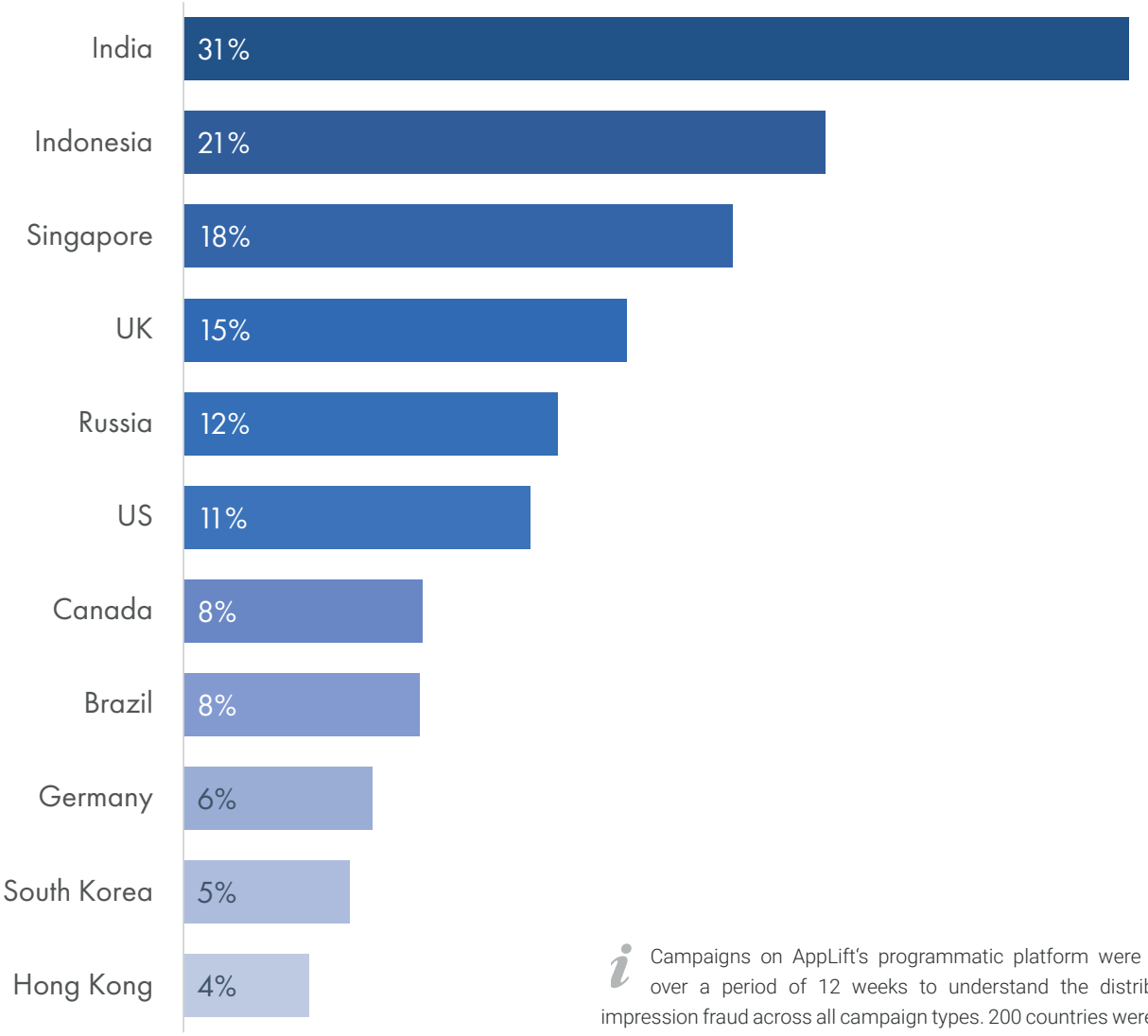
Insights Into Fraud Distribution: Current Trends

In the last two years, as an industry, we are better informed about ad fraud — its scope, faces and complexities — than we were in the years before when mobile advertising started to boom. Ad fraud exists in mobile where advertisers least expect it. To get an insight into the fraud distribution patterns, AppLift's fraud team studied impressions, clicks and conversions on the RTB platform over a period of 12 weeks and found the following trends:

Fraud Level by Country

We studied countries across the globe to understand the distribution of fraud levels and how markets stand against vulnerability of impression fraud on RTB. Some of the countries across those regions are represented in the heat map on the right. In particular, India and Indonesia, with a relatively young app market as compared to the Western countries, have considerably higher amount of fraud.

Fraud levels by country - % of Impression Fraud on RTB



i Campaigns on AppLift's programmatic platform were analyzed over a period of 12 weeks to understand the distribution of impression fraud across all campaign types. 200 countries were studied.

Fraud Levels by OS

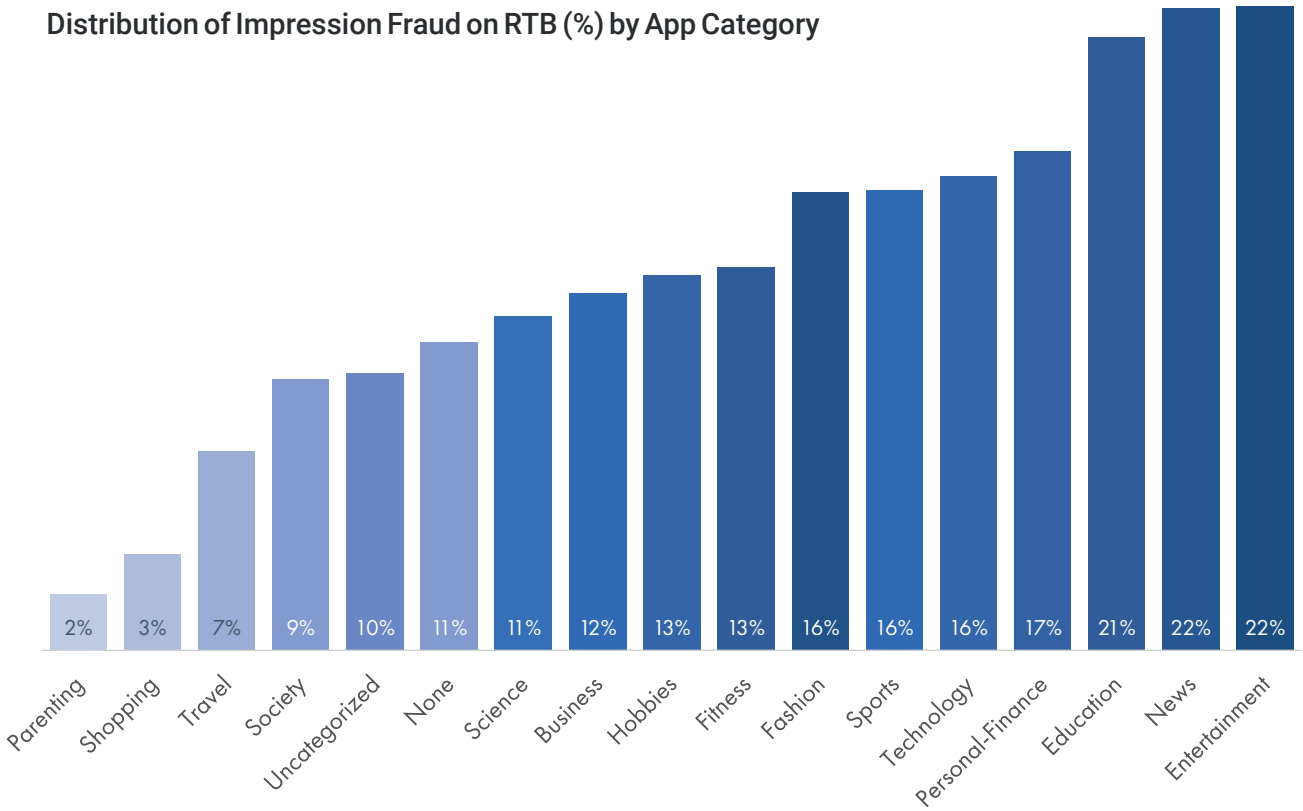
Overall, we did not find any significant difference in the amount of fraud across operating systems, both platforms are equally exposed to fraud.

Fraud Levels in App Categories

We examined the amount of impression fraud (%) on RTB that various app categories are exposed to globally, on both iOS and Android, and found the following trends. Some categories are more popular than the others (entertainment being the most common category for apps) and tend to attract publishers that serve fraudulent traffic for easy money.

i Campaigns on AppLift's programmatic platform were analysed over a period of 12 weeks to understand the distribution of impression fraud across app categories. Over 20 app categories were analysed over all campaign types and 200 countries.

Distribution of Impression Fraud on RTB (%) by App Category



The Typology of Fraud

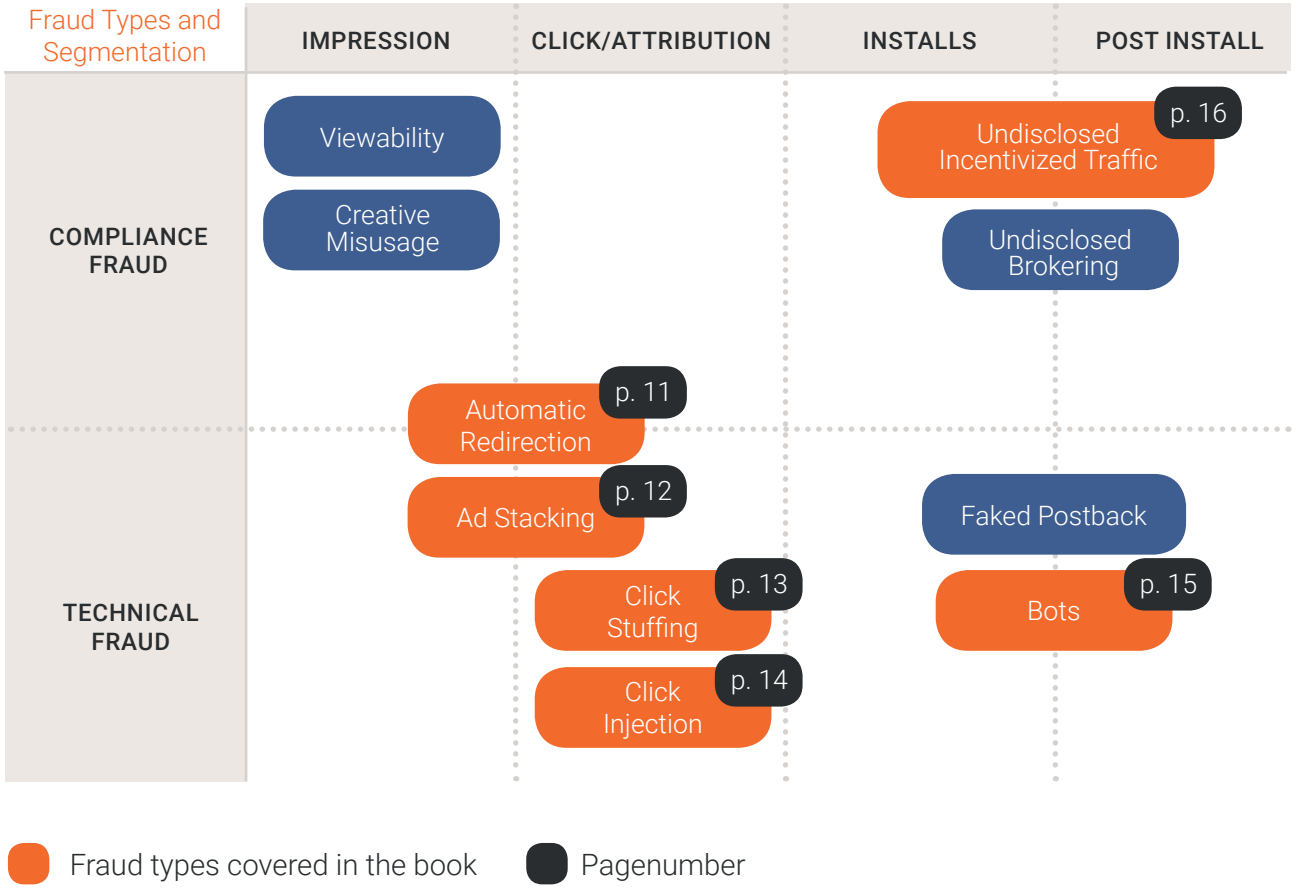
At any stage of the conversion funnel, it is possible to stimulate actions (impressions, clicks, installs, etc.). As we saw in the previous section, bots evolved as a common ad fraud tactic because of their simplistic action. New fraud types have emerged as fraudsters try to follow the money into what they perceive as lucrative and easy profits. The first step to better understand the motives behind each fraud type is to identify the different types of ad fraud that exist in the industry, the main characteristics of each, and the ways in which to spot the various forms. Once we know how to identify fraud, we can learn how to fight it.

Broadly, fraud can be categorized as either:

Compliance Fraud:
Deceitful tactics that do not directly require any specific kind of technology but aim to exploit platform vulnerabilities.

Technical Fraud:
Fraud committed through the use of technology to "game" the ad tech system.

For the scope of this eBook, we will be focusing on a few (of the many) fraud types in greater detail that stand to hamper advertisers and the industry as a whole. Below you will find a detailed matrix that gives an overview of the the most common ad fraud types, segmented as Compliance or Technical Fraud, at each level of the funnel (Impression, Click, Install and Post-Install). Follow the p. No. to deep-dive into the fraud type.



ATTRIBUTION FRAUD

While bots and undisclosed incentivized traffic generate fraudulent installs, attribution fraud exploits the weaknesses of the existing tracking models in order to claim installs that, under normal conditions, should be attributed to another publisher or be a part of organics. There are several variations of methods that allow fraudulent publishers to steal installs. In the following section we will focus on the main ones.

1 Automatic Redirection

The least sophisticated way to tag the device is just to send a user to the App Store/Google Play Store. This mostly happens on mobile web traffic, when users browse mobile web pages with advertisements. Fraudsters implement a click-tracking link in the impression pixel, so the click is triggered at the time when the banner is loaded, but not when the user actually clicks on the ad. Without any intention from the user to click on the banner, they get redirected to the app page and, even, if they decide not to download the app now, the device is already tagged by the tracking solution. Later on, if the user decides to download the app, the conversion will ultimately be attributed to the fraudster.

This type of fraud negatively affects not only advertisers that have to pay for organic users, but also heavily damages user experience for the publisher.

User is viewing the page

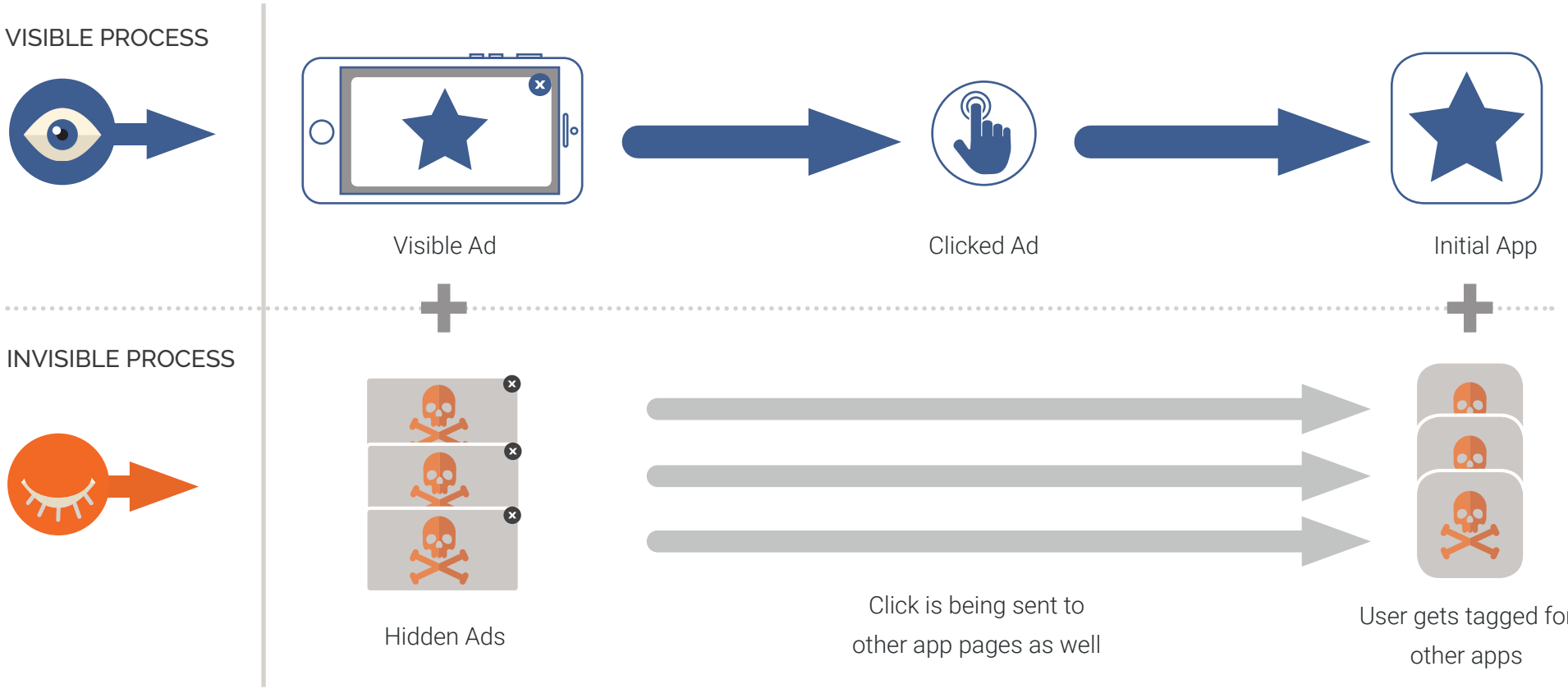
Malicious ad is being loaded (NO CLICK)

Automatic redirect to the app page

2 Ad Stacking

While in the case of automatic redirects users do not click on a banner at all, Ad Stacking requires users that are actually interested in the app to click on the banner. Fraudsters stack several invisible banners on top of each other, while only one of them can be effectively seen. Therefore, at the time of the click, it is sent not only to the original app page, but also to many different app pages as well.

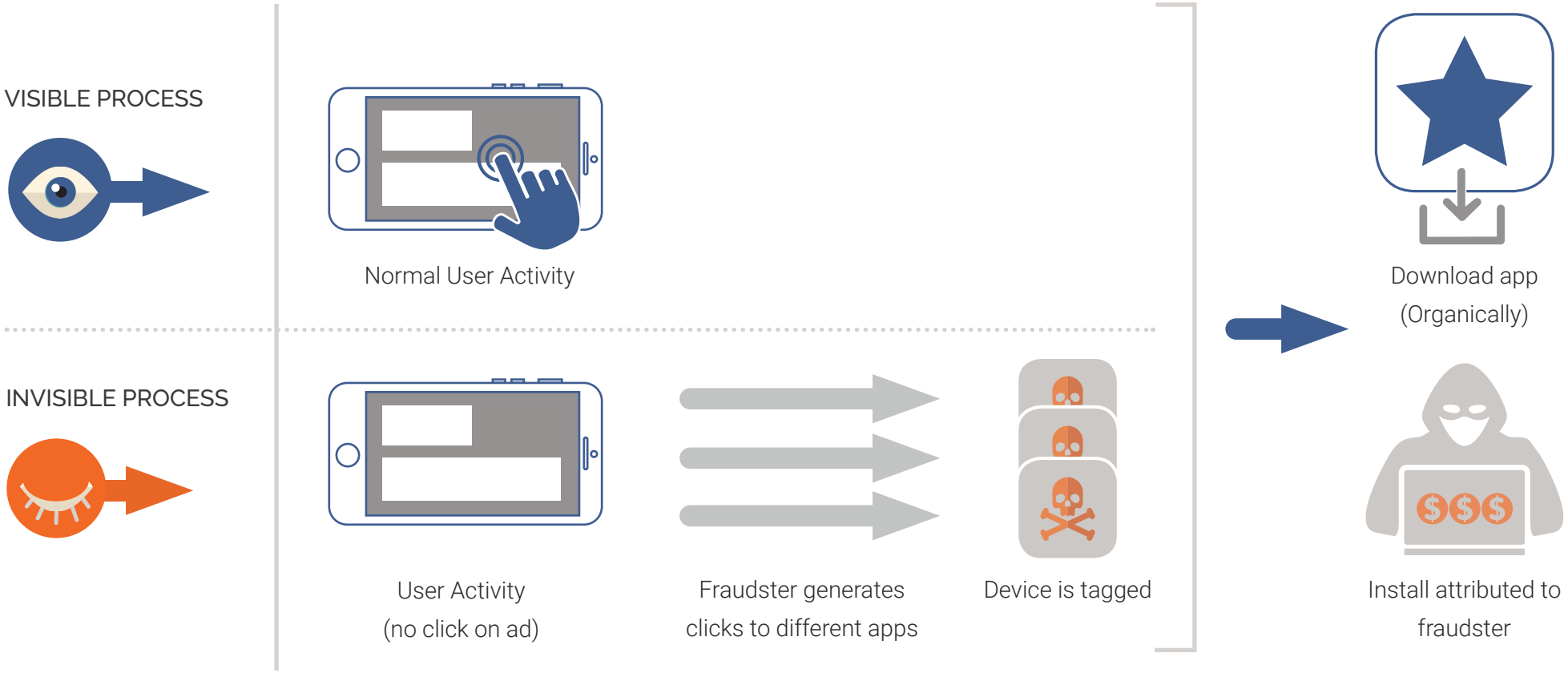
By doing this fraudsters not only minimize their costs (since they pay only for a single click), but also steal installs from advertisers/other legit publishers. A user clicked on one ad and this initial install should be attributed to the publisher, however, user's device is also tagged for other apps, and if he installs those apps later on, conversions will be attributed to the fraudster.



3 Click Stuffing

Cookie stuffing has been a common type of fraud on desktop — users receive third-party cookies after visiting a malicious web site that is not related to the advertised product, but in the end the conversion will be attributed to that media source. Similar technique of stealing installs is also used on mobile devices.

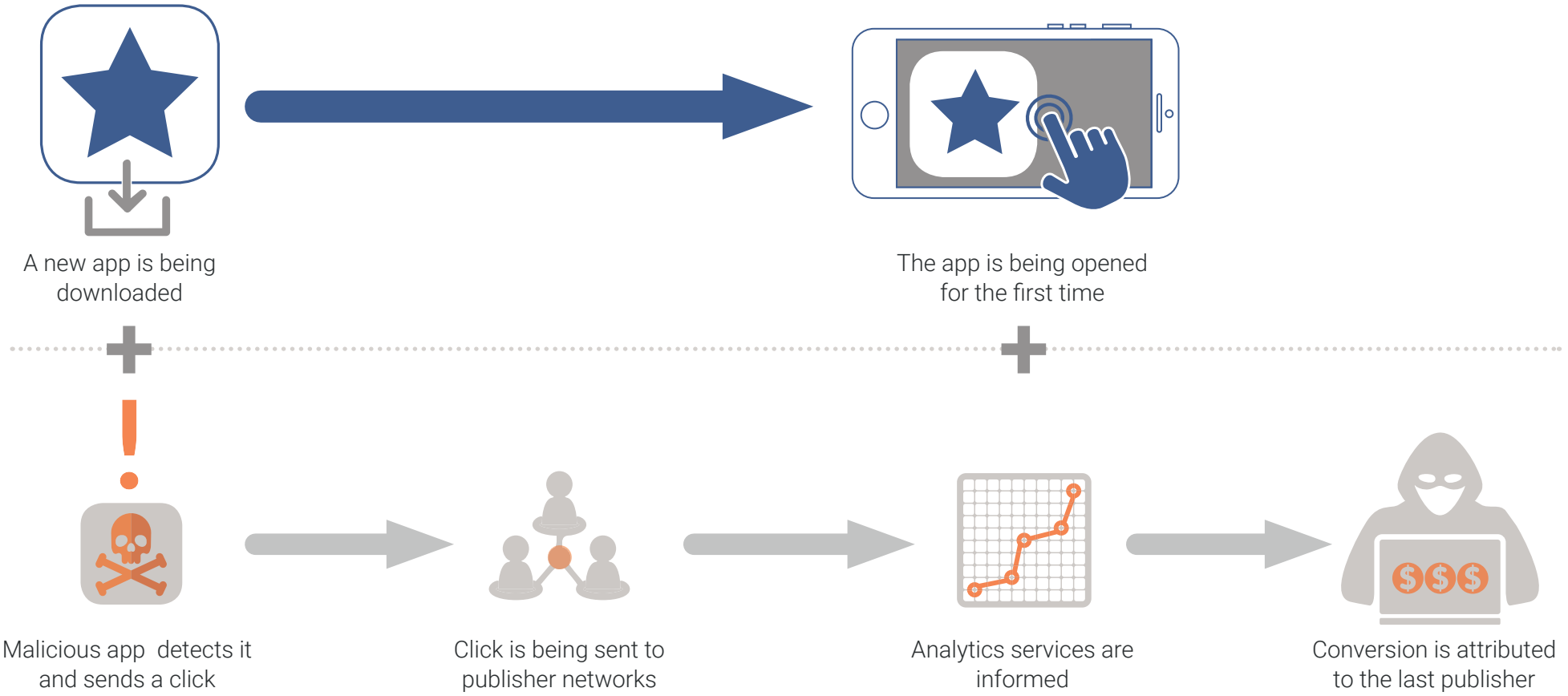
In mobile advertising, fraudsters try to emulate this in the form of click stuffing. Click-through is the most common type of attribution, therefore fraudsters generate clicks to different apps to tag the device, but there are no ads shown to the user. Clicks are generated in the background of a device without the user noticing, but if they try to install an app, this conversion will be attributed to the malicious media source.



4 Click Injection

This technique allows fraudsters to steal installs that should be attributed as organic installs or to other publishers by sending a new click from the device while the user is already downloading the app, so when the app is opened for the first time, the install is attributed to the fraudster.

To perform this click injection, fraudsters firstly need the user to install a malicious software (usually disguised as a useful app) that allows to monitor device's activity and detect when the user is about to install a new app. This trick is possible only on Android devices, where a malicious app can get permission to receive information about many actions performed on the device, in particular, about install of another app.



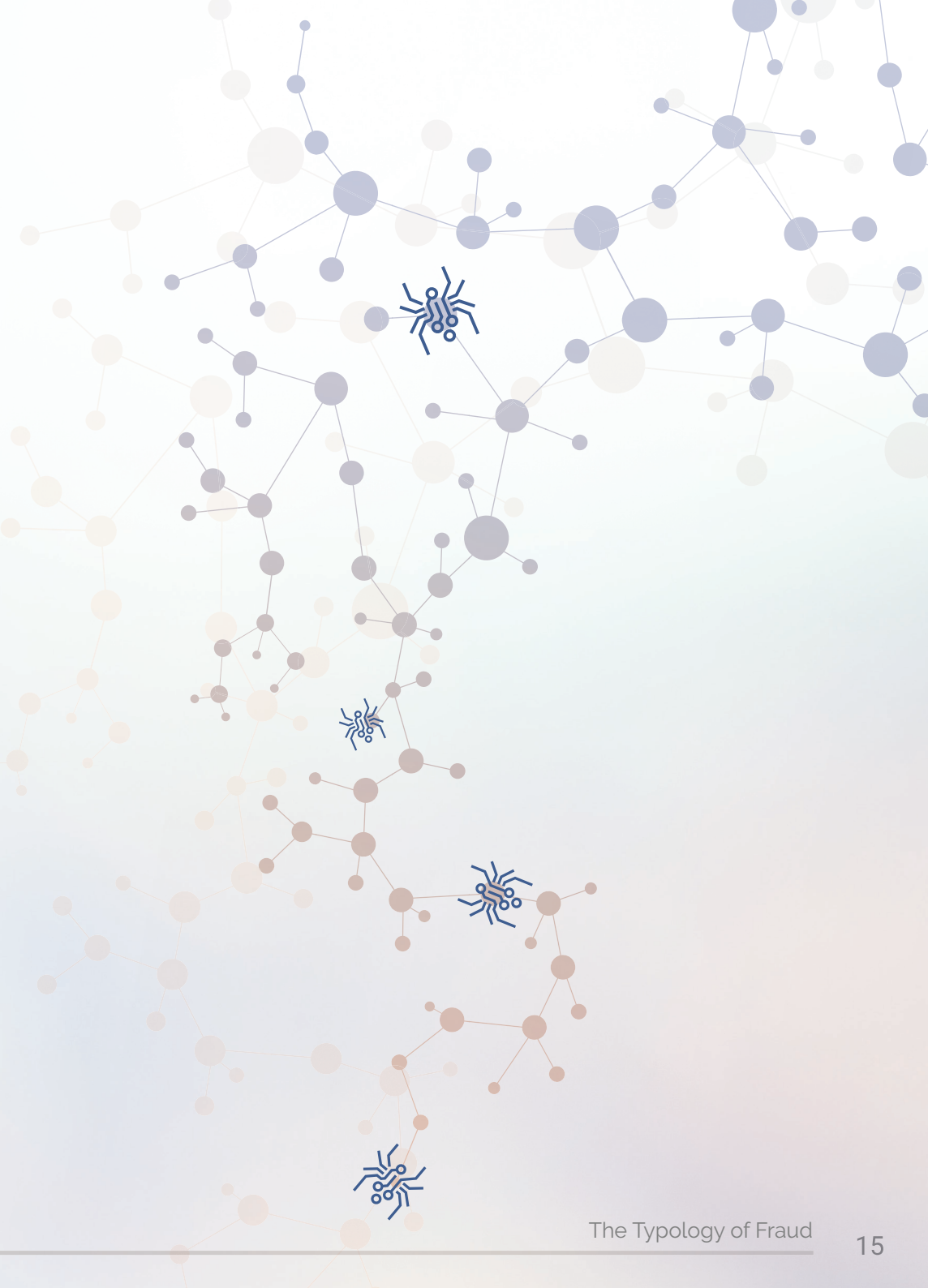
INSTALL FRAUD

1 Bots/Emulators

Bots are one of the common types of ad fraud: they mimic human behavior in order to fake actions, leading to fraudulent impressions, clicks, installs, and post-install events. Instead of promoting apps and looking for real users, fraudulent publishers use bots to emulate devices and deliver installs that do not bring any value to the advertisers. Typically, fraudsters use hosting solutions and VPNs to imitate users and make advertisers believe that the traffic is coming from real devices; in reality that is far from the truth.

There are several ways to spot bots, but the best way is to analyze in-app behavior after installs. Most of the time, installs made by bots don't generate any actions within the app.

This type of fraud can be recognized relatively quickly, so in order to keep making money, fraudsters develop more and more sophisticated workarounds. For campaigns with high premiums, fraudsters can even configure bots that are able to perform not only some early in-app actions, but also make purchases. Those types of bots are extremely hard to detect, since they are programmed to look exactly like real users. Only deeper analysis of their long term behavior will help to reveal the fraudulent nature.

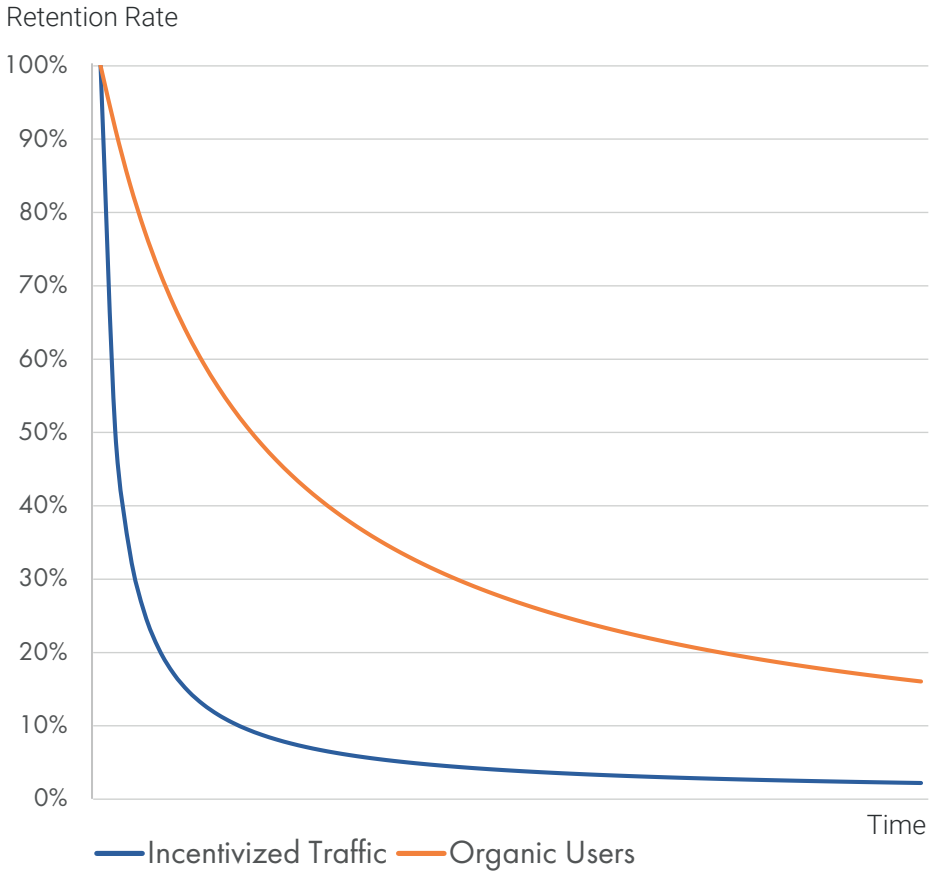


2 Undisclosed Incentivized Traffic

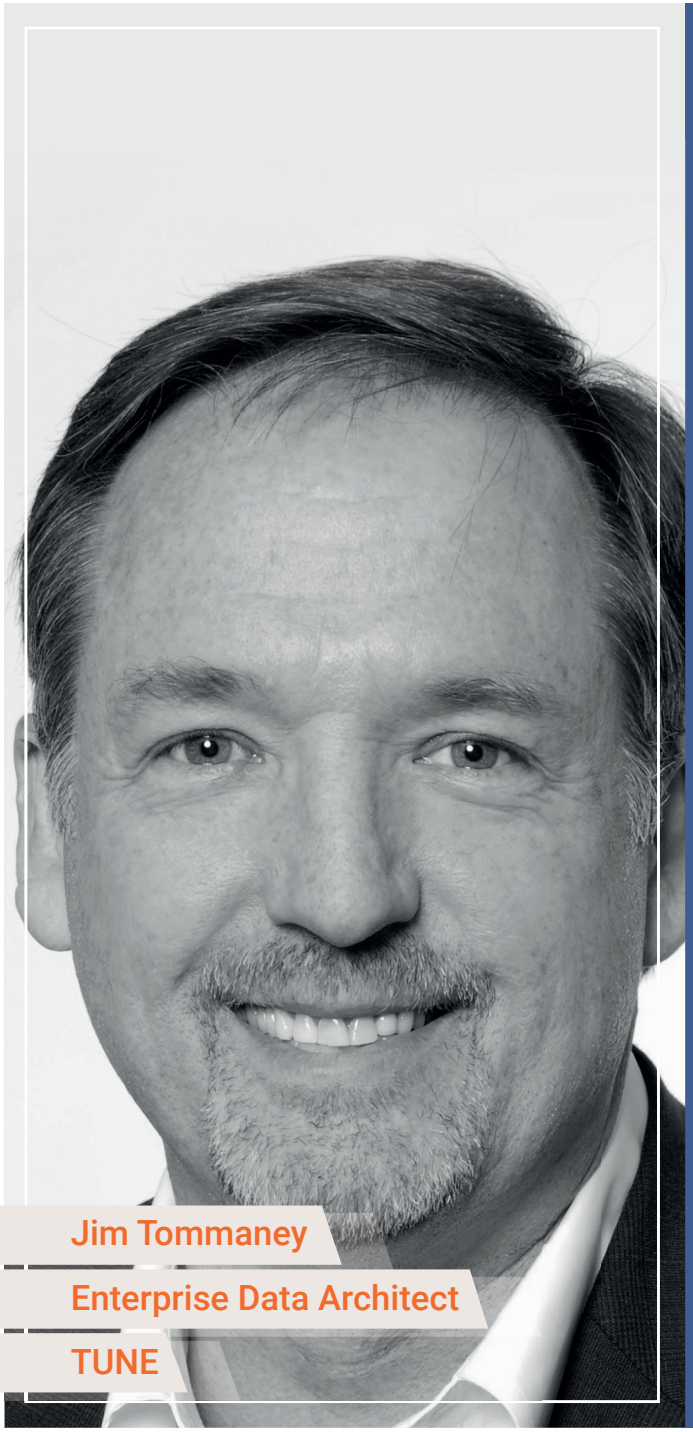
Incentivized installs are not a fraudulent tactic per se, but passing off incentivized traffic for non-incent traffic is. In the case of fraud, some fraudsters try and send incentivized traffic to non-incentivized campaigns, such that the advertiser gets low quality traffic but is nevertheless charged at premium rates.

There are services that encourage users to perform specific actions to receive a reward: mostly in-app bonuses such as additional points within the game or in-app currency, but it can also be real money. Those incentivized actions can be very different. Sometimes users are asked to view an advertisement, participate in a survey, or install an application, which is the main point of interest for mobile user acquisition. While this type of traffic generates installs from real users, their behavior is very different from average or organic users. Usually such users are incentivized to perform a particular action after they install the app, so advertisers do see some in-app activity from those installs. However, since the main incentive for such users is to get rewards from downloading the app, they tend to stop using the app after they performed the requested action.

Retention rate (%) - Incentivised vs. Organic Users in Time - Concept



i Incentivized traffic shows significantly lower retention levels than organic traffic.



Jim Tommaney

Enterprise Data Architect

TUNE

Industry View: TUNE

Ad tech fraud has become a significant issue in the mobile ecosystem, especially with the advent of advanced click-fraud techniques. Click spamming, click stacking, and click injection have combined to destabilize the industry.

There has been a significant uptick in click fraud (spamming, stacking, click-injection, etc.) as the overall ecosystem has grown. Companies with brand presence will have significant ongoing organic downloads and typically aggressive paid campaigns. This high-volume of activity combined with the simplicity of some click spamming methods makes click-fraud very lucrative.

Critical to fighting fraud is the ability to detect and eliminate bad traffic sources quickly. Any delays in identification and elimination raises (at least) three costs:

a) The absolute cost of wasted spend.
b) The missed opportunity cost of investing in sources that deliver real growth.
c) The overhead in attempting to build a case for credit of claw-backs.

Smarter big data systems, that execute and analyze faster, in a way that allows for identification/elimination of fraud sources is critical. Next day (or next week) actionable recommendations are core to avoid being overwhelmed by fraud.

In addition to faster, more actionable systems, the next most critical gap is around quality data input. Certified Partner Programs that enforce correct labeling of traffic sources lead to quality output from these systems.

Fraud Detection: Main Metrics

AppLift's fraud detection team carefully examines the campaign data and tracks actions to identify, prevent and fight any potential fraud at various levels. These fraud detection metrics rely on sophisticated pattern-detection and heuristics to combat the above fraud forms, which are otherwise hard to detect on a surface level.

Based on our learnings and experience, we illustrate below the metrics that can be used to identify each type of fraud, employing practical use cases to show pattern behavior. However, these metrics should be carefully studied before concluding the presence of any fraudulent activity, as not all patterns are necessarily fraudulent in nature.

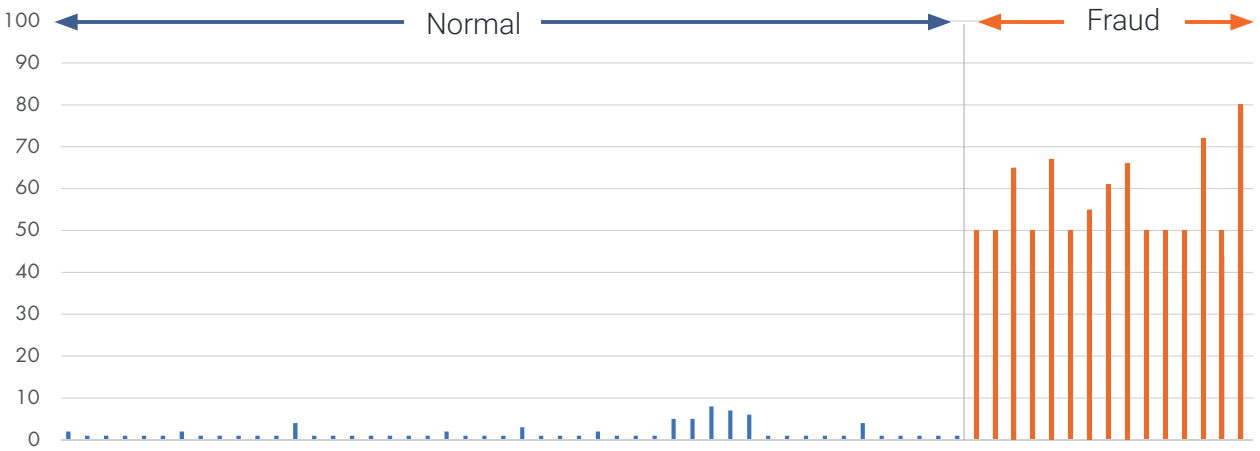
BOTS/EMULATORS

As bot traffic represents a substantial share of fraud that we see in the market, many different indicators can be deployed to allow us to identify such types of fraudulent activity:

1 IP Filtering and Blocking

A vast majority of users tend to not use anonymizers, therefore, if it is detected that the traffic is coming from proxy IPs, instead of going through the tracking link, it is redirected to the app page.
In the below chart you can see the plotted installs and their IPs, both for fraud-free and fraudulent traffic. On the left side, in case of fraud free traffic, we see many IPs and most of them are unique, with usually not one conversion per subnet. We also see some occasional groups of installs that share the same/similar IPs. Those usually represent cases when users utilize the same WiFi spot, but it also may be a sign of mobile carriers rerouting and grouping the traffic of their clients. The main idea here is that while it's totally normal to see installs from the same IP/subnet, high share of installs coming from similar IPs is very unlikely, and it is a sign of suspicious traffic, visible on the right side of the chart (fraudulent traffic). Fraudulent publishers that generate bot traffic tend to use different hosting solutions to deliver traffic, therefore those installs are usually manufactured from similar IPs.

Number of Installs Per Subnet



i Normal traffic is characterized by a large number of installs that come from different IP addresses, while fraudulent installs usually come in batches from a narrow range of IPs.

2 Analysis of Devices

Information about the device also helps to detect fraudulent activity by implementing algorithms to monitor traffic coming from different sources, in order to identify cases of potentially strange activity. When employing device information as a detection metric, an analysis of the distribution of devices and shares of different OS versions from every media source can help to spot any anomalies.

It can be normal to see a high number of installs from devices that use new versions of OS, in comparison to devices with older versions. However, in the example to the right, Publisher 5 will be marked as suspicious by our algorithm. The traffic in this case comes only from devices with three different OS versions, which is very different than a range of OS versions from the rest of publishers.

In some instances, it is possible that media buyers target specific OS versions due to better conversion rates. Hence, when using the OS version distribution as a metric, it is important to use it in combination with other patterns and not as a sole indicator of fraudulent activity.

OS version	Publisher 1	Publisher 2	Publisher 3	Publisher 4	Publisher 5
4,1	0,7%	0,6%	0,0%	0,7%	0,0%
4,2	0,8%	0,4%	0,0%	0,4%	0,0%
4,3	0,7%	0,3%	0,0%	0,1%	0,0%
4,4	16,1%	15,6%	21,0%	12,5%	0,0%
5	8,5%	6,9%	17,5%	10,2%	29,0%
5,1	11,8%	10,1%	6,0%	5,8%	0,0%
6	47,0%	51,8%	54,8%	42,1%	45,0%
7	14,4%	14,3%	0,8%	28,2%	26,0%
7,1	0,1%	0,1%	0,0%	0,1%	0,0%

i Fraudsters tend to send traffic from only a few OS versions and normal traffic usually comes from a variety of OS versions.

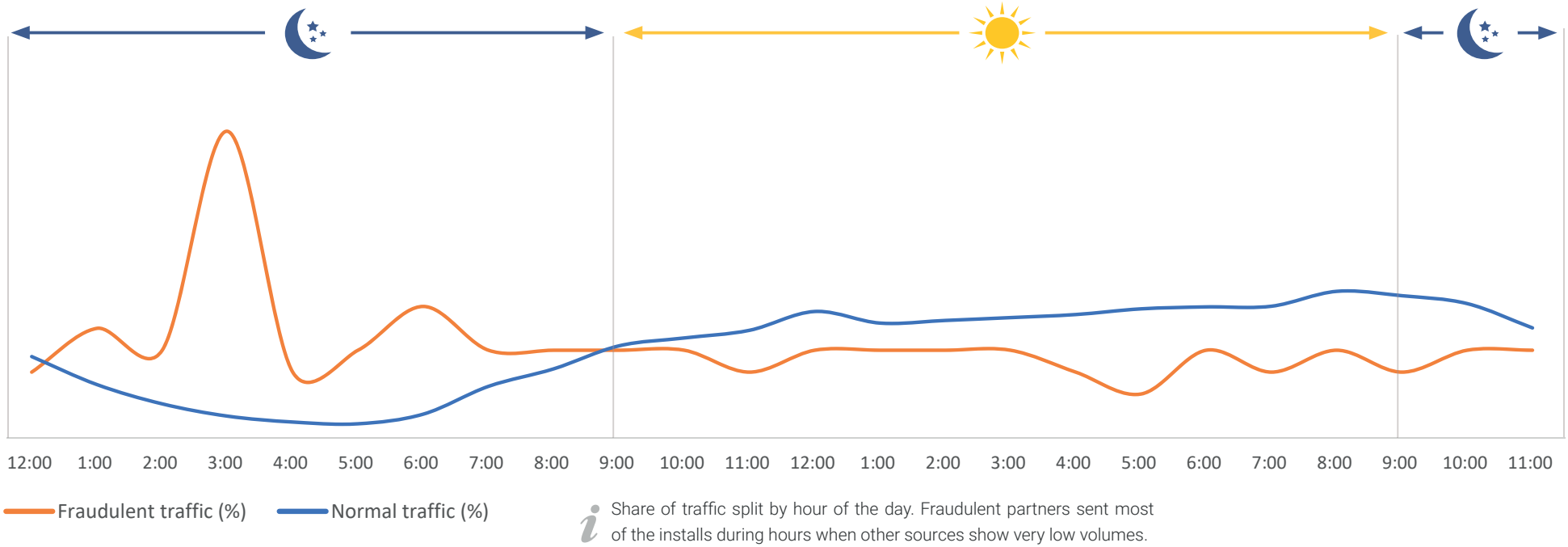
3 Intraday Distribution of Installs

Further useful information about the traffic can be obtained with the analysis of install times. Typically, people use mobile phones during the day. Therefore, we expect that most of the installs should be made during daytime hours. On the graph below, you can find the normal distribution of traffic by hour of the day, as well as traffic from one publisher that delivered fraudulent installs.

For normal traffic, we see that most of the installs are made between 10:00 AM and 10:00 PM, when people are generally active on their phones. There are also some installs at night, but they represent a very small share of all traffic.

If we look at the traffic that was identified as fraud, we can see that there is a very flat distribution of installs with an abnormal spike at 3:00 AM. This is another metric that can be used to identify suspicious traffic. However, it should be applied very carefully, especially for traffic that is coming from countries that operate on several different time zones: USA, Canada, Australia, Russia, etc.

Normal vs Fraudulent Traffic During a Day



i Share of traffic split by hour of the day. Fraudulent partners sent most of the installs during hours when other sources show very low volumes.

UNDISCLOSED INCENTIVIZED TRAFFIC

Conversion Rates

In comparison to normal traffic, incentivized traffic tends to have significantly higher Click-to-Install conversion rates. While incentivized traffic may very well be used to achieve many advertisers' goals — for example for large burst campaigns to increase visibility of apps in the store — some fraudsters take advantage of it and deliver incentivized installs on non-incent campaigns. Information about hourly conversion rates can be used to identify this type of non-compliant traffic. However, fraudsters tend to disguise incentivized traffic by mixing it with other sources of installs to conceal abnormally high conversion rates. On a publisher level conversion rate may look normal, but after digging deeper into sub-publishers it is much easier to find out if the publisher delivers incentivized traffic or not.

Incentivized traffic has substantially lower retention rates than normal installs; most of the time users will only open the app once for a conversion to be registered. Therefore, looking at the activity of users in the app will also help to identify this type of fraudulent traffic.

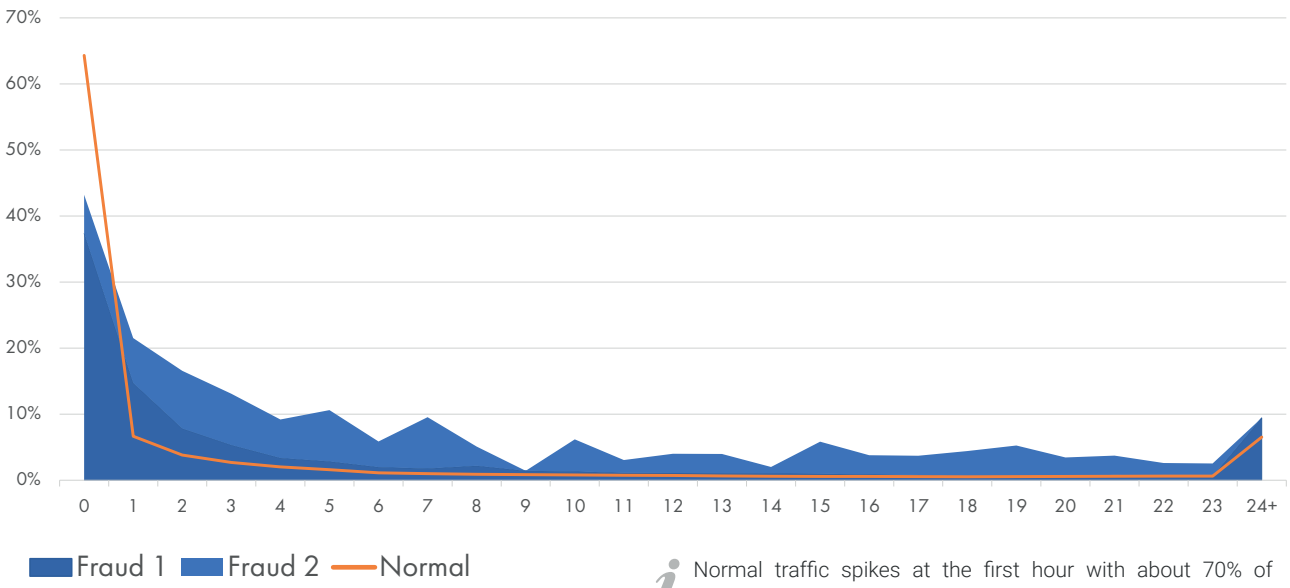
ATTRIBUTION FRAUD: AUTOMATIC REDIRECTION/AD STACKING/CLICK STUFFING

Click-To-Install Time

Attribution fraud, in general, is related to misattribution of installs in one way or another. Therefore, the techniques that are used to identify this type of fraud also have a lot in common. Fraudsters are essentially trying to tag devices in order to get credit for installs made by these devices. It is gambling of some sort: fraudsters believe that eventually a user will download something, however, there is also a chance that they sent all those clicks for nothing.

The time when the user downloads an app does not depend on the time when the fraudster generated a click to tag the device, which is very clearly shown on the graph below: distribution of installs is very flat and there are almost as many users that installed the app more than 19 hours after the click as users who installed the app during the first hour after the click.

Click-To-Install Time (in hours) - Normal vs Fraud



i Normal traffic spikes at the first hour with about 70% of installs coming during the first hour. Distribution of traffic from fraudulent publishers tends to be more flat with much heavier tail.

However, in reality there are not so many cases when we can see such clear distinction.

Even for fraudulent traffic we will see that most installs come within the first several hours after the click. To be sure that the installs will be attributed to fraudsters, they send new clicks to "refresh" attribution windows for the device.

There are other issues that affect the Click-To-install-Time (CTIT) distribution, such as the actual size of the app. The heavier the app, the more likely we will see a flatter distribution, since it takes more time for users to download and install the app. Because it takes a bit of time, users may not want to wait for an app to download, so they'll continue with other activity and then open the app much later. This can lead to very long CTITs, which are perfectly normal. When evaluating these KPIs marketers need to be aware of these other influencing factors.

CLICK INJECTION

Short Click-To-Install Time

In theory click injection can be spotted very easily: since the clicks are generated after the user has started downloading the app, CTIT for this install should be remarkably small. If a publisher delivers significant amounts of installs with small CTITs (several seconds), it may signal that the publisher is doing click injection.

However, there can be another explanation for such short (in some cases even negative) CTITs: Asynchronous clicks. In this case, clicks are sent not from the end user, but from a server. Asynchronous clicks are used by publishers to improve user experience. Usually users who click on an ad are redirected to the app store through the browser which slows down the process and increases risk for the publisher that the user interrupts the redirection without converting. When they use Asynchronous clicks, publishers pass click data from their servers and redirect the user straight to the App Store — instead of it being passed by the end user. Due to the slight delay when that information is sent by the publisher's server - potentially after the download started, it is possible to have installs with short/negative CTIT.

Fraud Detection Metrics: Summary

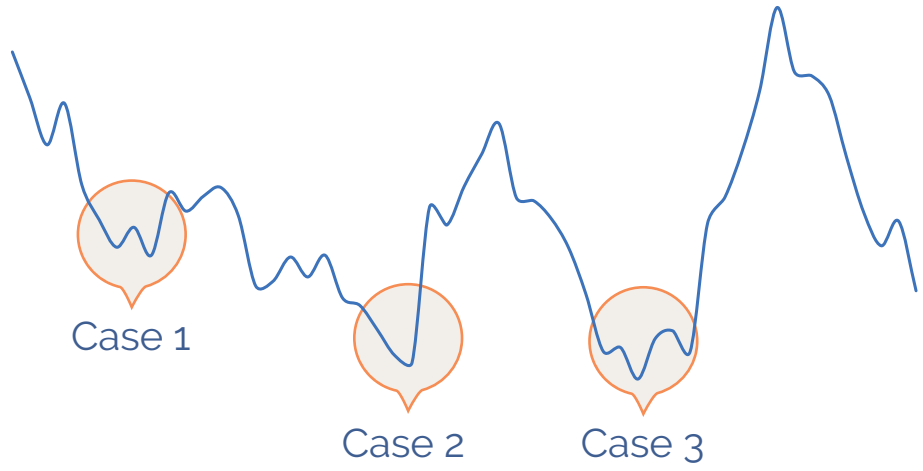
Looking at one metric in isolation is not enough to identify fraud. Only a combination of metrics will allow for justification of whether or not the traffic is fraudulent. However, it is worth noting that any suspicious pattern does not necessarily mean fraud. In some cases, the above metrics such as repetition of IPs, hourly distribution, or Click-To-Install-Time may be legitimate. Once suspicious patterns are detected, correlations need to be studied carefully to arrive at a conclusion of whether the trends show fraudulent patterns or not. While machine learning algorithms can help ad tech companies to detect suspicious patterns, a dedicated human effort is required to study and interpret confirmation of fraudulent patterns.

Case Study: Using AppLift's Pattern-Detection Technology to Detect Fraud

We want to illustrate fraud detection at Applift using a campaign of one of our main partners: Miniclip. While we aim to deliver a high amount of installs for their campaigns, we also analyze how well those installs perform in terms of their KPIs. Having proper KPIs that appropriately reflect users' activity and engagement is a crucial point in assessing the quality of the traffic. For new titles, identifying patterns based on user behaviour is more challenging, as there is not enough data to support this analysis, but for well-known titles it is a lot easier and helps us to prevent and fight fraudulent sources in a timely manner.

On the graph below you can see the development of the KPI by day:

ROAS 3-Day Moving Average (in %)



We constantly monitor and optimize traffic delivered by our publishers, however, we also work on getting new ones to promote apps. Unfortunately, not all players in the market deliver legitimate installs and it negatively affects the performance of advertising campaigns. Therefore, our main goal is to identify those fraudsters as fast as possible. During our collaboration we have faced some issues related to fraudulent traffic that we identified and stopped. Let's take a deeper look.

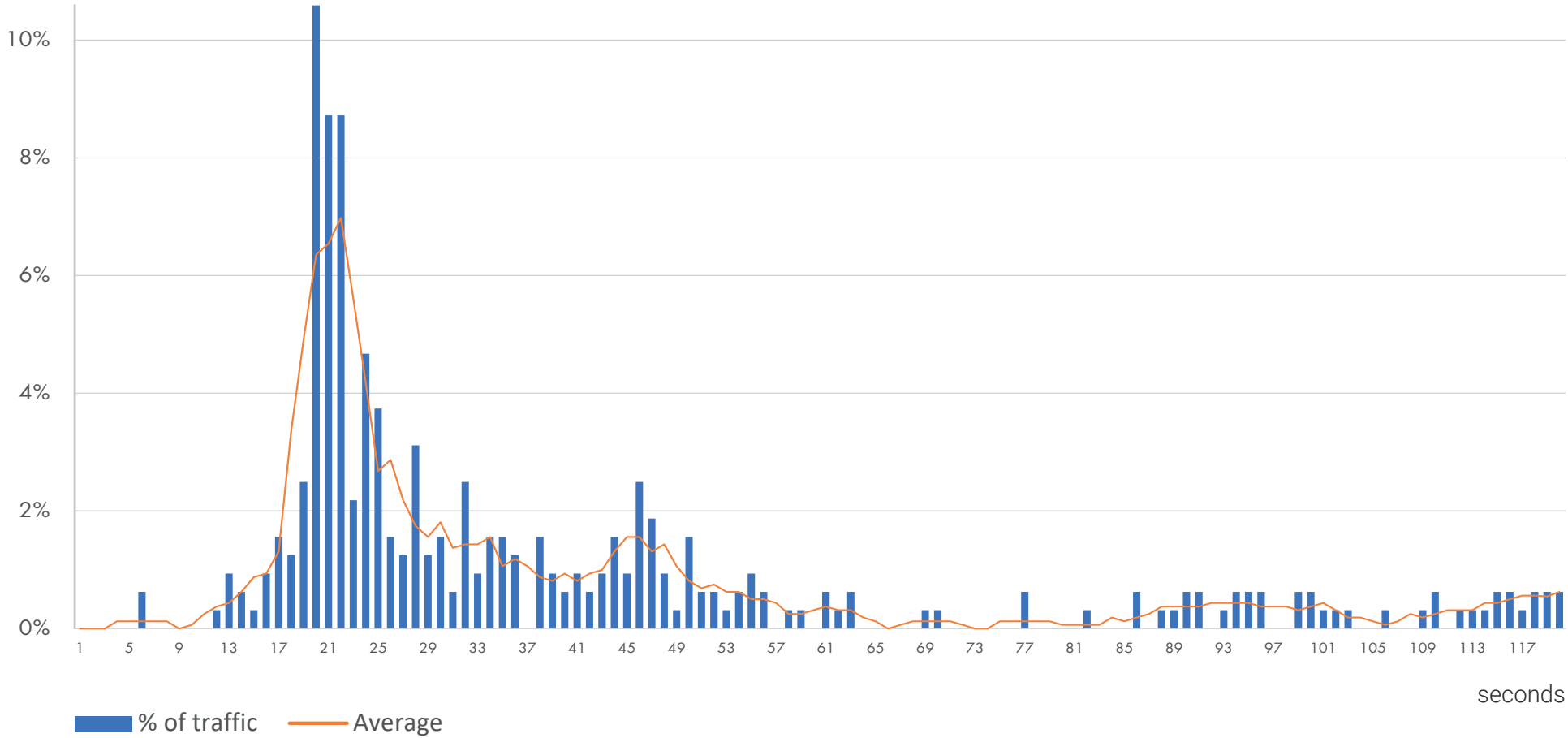
Case 1

We identified a publisher that delivered an unusually high share of installs coming from Wi-Fi and, in addition, many installs from the publisher had repeated IP addresses with an average of 1.52 conversions per install. This metric is significantly higher than we see across other publishers. We suspected that the partner delivered non-legit traffic, which was confirmed by extremely low in-app engagement of the installs.

Case 2

Here we identified a media source that had very strange patterns in Click-to-Install Times: 80% of installs came within the first 5 minutes after the click and with median CTIT below 50 seconds:

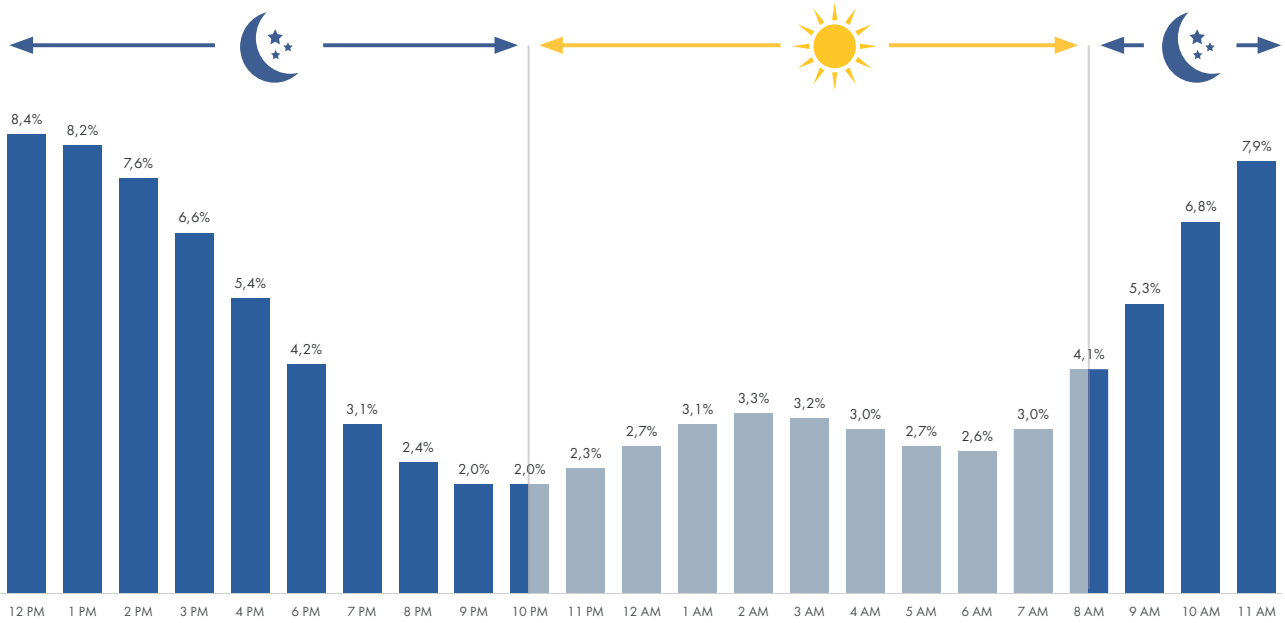
Another strange factor was a very high click-to-install conversion rate of around 5%. It was apparent that the media source was delivering fraudulent traffic since there were no real users behind those conversions, and the app was opened only once to claim a conversion.



Case 3

One publisher delivered a significant portion of installs at night, while other publishers had very small amounts of installs coming during those hours. On the graphs below you can find a distribution of installs from this publisher split by hours of the day:

Distribution of installs - by hour of the day



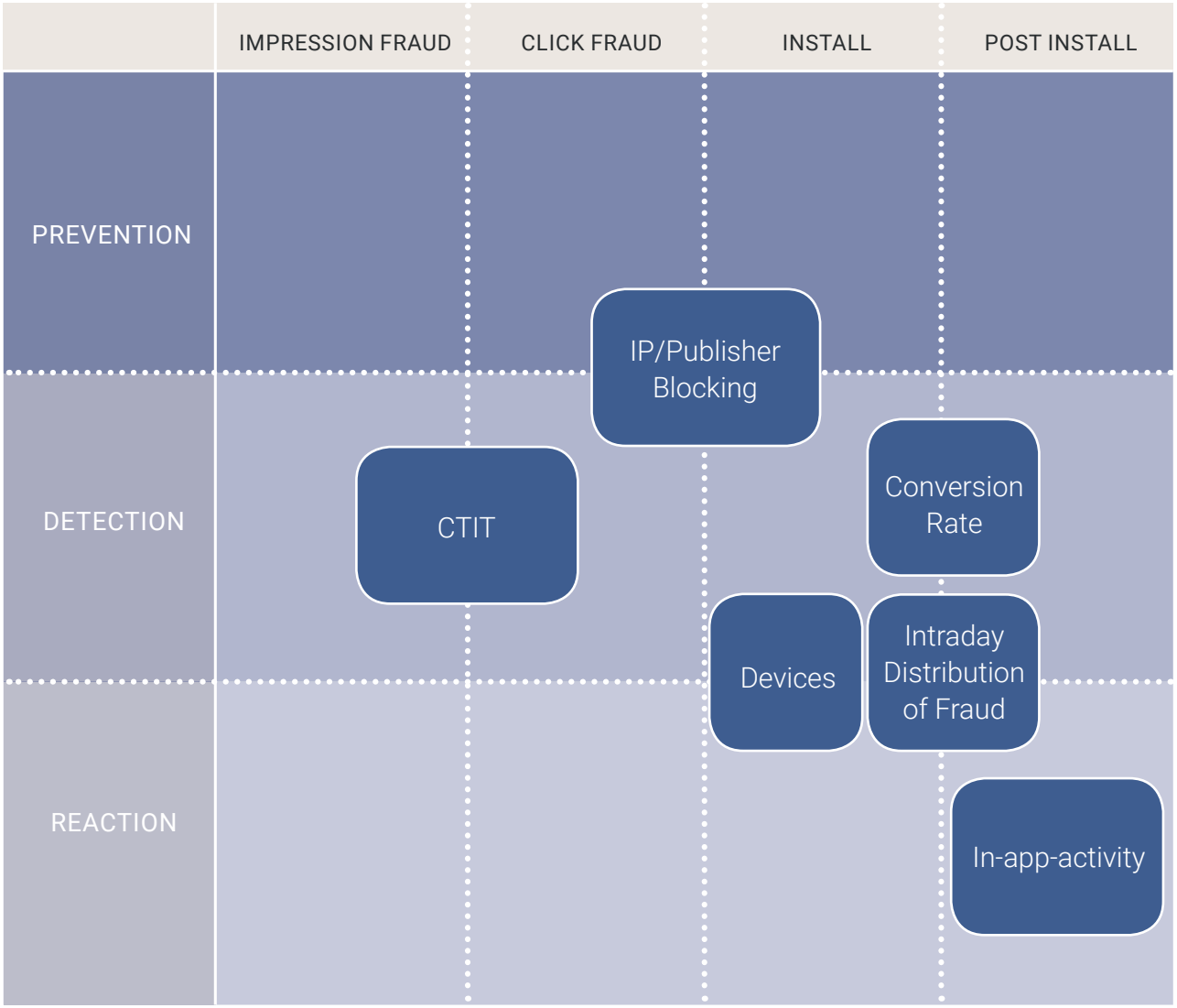
We still can see that most of the installs came during daytime hours, but this distribution differs substantially from what we usually see across publishers. Moreover, installs delivered during those hours had close to zero in-app activity after the install as well. After deeper investigation, we found that the publisher was sending legit installs during the day, but it was mixed with the addition of fraudulent bot traffic.

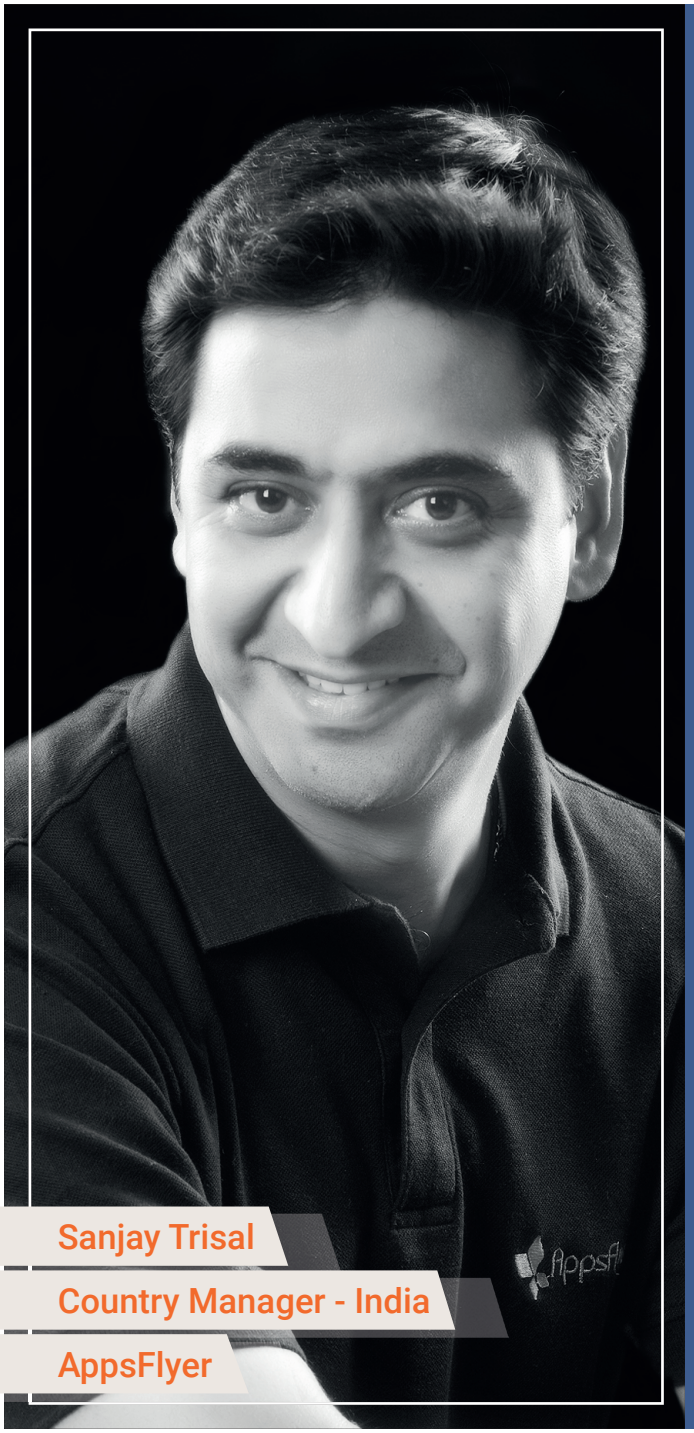
"We have a great working relationship with the team at AppLift. Eradicating ad fraud is a major concern for all players in the industry today, and most particularly the advertisers. We have been able to stay on top of fighting fraud by working closely together with the team at AppLift to significantly reduce marketing waste."

Jonathan Winters
Head of User Acquisition
Miniclip

AppLift Fraud Fighting Matrix

Fraud fighting requires a combination of technology, data and people. We have developed a fraud-fighting table summarizing the metrics elaborated above at various levels as a handy guide for the readers of this eBook. The matrix below depicts the different means of fighting fraud by combining the stages of prevention, detection and reaction.





Sanjay Trisal

Country Manager - India

AppsFlyer

Industry View: AppsFlyer

With fraud hitting center stage, the industry is fighting back. And everyone has a role to play.

One of the problems in this space is a lack of experience. Many players across the ecosystem focus exclusively on real-time protection (blocking fraudulent traffic from entering one's dashboard via different mechanisms). Although an important weapon, those with experience know that this alone is not enough. Not all fraud can be blocked in real-time, especially when fraudsters up their game to find cracks in the wall — which they are doing at an increasingly high rate.

Advanced fraud detection, therefore, is another equally important weapon in the arsenal. At its core, after-the-fact detection is centered on the ability to pinpoint bad traffic that evaded real-time protection through various means, like hiding behind limit ad tracking (LAT), device ID reset marathons, and the use of real devices that generate high volume fraudulent installs (fraudulent devices), as well as real devices that generate both real and fraudulent transactions (we call them suspicious devices). Detecting these advanced classes of fraud require massive, fresh databases and the application of next generation AI-driven anomaly detection solutions. These multi-layered statistical analyses can detect and flag new trends with remarkable speed and accuracy.

What role do different players in the ecosystem have? To clean up our space, much is dependent on changing the mindset on the media side. They need to understand that it is in their best interest to fight fraud. Sure, when we identified fraud for our clients, media sources lost money. And that's never an easy thing to accept in such a fiercely competitive and unstable space.

Unbiased and independent attribution providers like AppsFlyer have an extremely important role to play, with a commitment to never do anything such as selling solutions or data to affiliate networks, ad networks or DMPs/Collectives. From this unique vantage point, we have an extensive view across the entire ecosystem, enabling us to build a massive database that extends both vertically and horizontally across networks, channels, publishers and sub-publishers, which empowers AI-driven machines to be far more effective in detecting polluted data.

10-Step Approach to Fighting Fraud

Mobile fraud is ubiquitous and, to some degree, unavoidable. Nonetheless, advertisers can minimize the risks by becoming more aware of the target KPIs of the app and working closely with the ad networks, publishers and attribution partners.

We have outlined a ten-step approach as a starting point for advertisers to help fight fraud:

1

UNDERSTAND THE TARGET KPIS OF THE APP:
Advertisers can play an integral role in early fraud detection by having a process to monitor traffic and KPIs to detect any suspicious activity.

2

BACKGROUND ANALYSIS:
Know where the risks are. Make sure you understand the different types of fraud and how to detect them. Diversify the sources of information — networks, media sources, fraud detection companies, and publishers are all your friends in staying informed about how to identify fraud. Do not rely on one source; make sure to get the full picture to educate yourself on not just identifying fraud, but also interpreting heuristics to detect fraud.

3

INCENTIVES AND MANAGEMENT STRUCTURES:
Set the highest standards of quality with your UA managers to focus not only on bringing installs, but legit installs. Incentivizing UA managers only on volume may push them to close their eyes on fraud.

4

WORK WITH ATTRIBUTION AND TRACKING PARTNERS:
If you do not have resources to tackle fraud internally, work with a fraud solution offered by main measurement partners such as AppsFlyer, Kochava, TUNE, and Adjust.

5

SET UP AN INTERNAL INFRASTRUCTURE:
Build a scalable internal infrastructure with your Business Intelligence teams to easily and quickly understand and analyze patterns. By having a scalable infrastructure (a combination of technology and people) that can process the huge amount of campaign data coming in, you can help to take timely actions to fight and prevent fraud at various levels.

6

SELECT YOUR SOURCES:

Before beginning campaigns, advertisers must ask their partners about their approach to fraud and choose businesses that have robust prevention measures in place. Be sure to work with only those partners who take the most proactive stand against fraud.

7

IMPLEMENT GUIDELINES AND TARGET METRICS:

Set up a process to implement campaign management guidelines with all your supply sources. Be careful, though, as you might miss inventory opportunities if you inaccurately define target metrics or range.

8

MEASURE CONTINUOUSLY:

Once you have developed an understanding on what patterns can be used to identify different types of fraud, build a set of data and calculate metrics based on patterns across all different inventory sources. Define corridors for your target metrics and each pattern that you will be focusing on based on the analysis. Take into account individual factors of your app that may lead to different empirics than general market averages.

9

EXCEPTION MANAGEMENT:

The amount of data being generated is huge. Set up a system in which certain patterns trigger alerts or actions automatically. For ad publishers and DSPs, monitoring traffic and campaign-related KPIs for suspicious patterns is of critical importance. For example, if you observe an unusually high app-install rate, that the time between click and app install is uniform for every user from the same traffic source, or that the time between click and install is inexplicably short, that should raise a red flag.

10

IMPLEMENT A FEEDBACK LOOP AND INCORPORATE LEARNINGS:

Be proactive. Should you identify a worrisome traffic pattern before your supplier, share as much data as possible so that your partners can learn from the incident.

Meridith Miller

Head of Commercial Partnership

MoPub

Industry View: MoPub

The entire mobile industry is battling against the fraudsters together, but generally there's still a lack of transparency and collaboration across supply sources. To advance the industry forward, it's worth considering how we can collectively work better together to share best practices, fraud findings, and even data. This isn't an easy topic to navigate given the sensitivities with data and privacy, but it's a conversation we need to have the courage to start.

We believe fighting fraud is one of our core responsibilities as a supply source. As one of the largest mobile in-app supply source for marketers, we have a commitment to our demand partners to provide high quality supply for their advertising spend on our inventory. We have taken a three pronged approach to fight fraud — Process, Product, and Partnerships.

The biggest trend we've seen this year is a move towards more standardization and commitment to compliance of those standards. Industry initiatives like TAG are a great example of this, and we think there will be increased adoption of efforts like this as advertisers continue to demand higher standards on where their campaigns run. It's reasonable to expect that fraudsters will always be something we need to combat in digital, but both supply and demand sources are no longer willing to turn a blind eye.

Conclusion

The tolerance towards fraud is rapidly decreasing as the industry has become more aware of the risks that play out due to ad fraud in its various forms. Since 2012, ad fraud has evolved to appear in various iterations that seek to harm the growth of mobile ad tech, manifesting in a three-pronged problem — operational, financial and trust/reputation issues.

Over the last two years, great progress has been made on identifying low quality traffic coming from bots, click farms and incent. It has now become difficult for fraudsters to run campaigns at scale with these methods. But attribution fraud (click spamming, ad stacking, click injection) is still a reason for worry because of its sophisticated nature, making it hard for advertisers to trace if they don't have mature detection technologies and processes.

The industry needs to ask itself not only how to identify fraud, but more importantly, why fraud is happening. Each player needs to develop their own initiatives, depending on their knowledge, to detect patterns, study heuristics, and share that knowledge. Ad exchanges, intermediaries, publishers, and attribution partners now have a bigger role to play in mitigating fraud compared to some years ago. The industry must join forces and fight the common enemy, otherwise ad fraud will remain a cat-and-mouse chase.

About AppLift

AppLift is a leading mobile ad tech company that empowers mobile app advertisers to take control of every stage of the app marketing lifecycle. AppLift's programmatic platform, DataLift 360, enables advertisers to launch their apps as well as grow and retain quality users from one interface. With DataLift 360, app marketers can programmatically access all major mobile ad inventory worldwide and control their campaigns through a single proprietary technology platform, which provides advanced data integration as well as extended targeting and audience management capabilities.

AUTHORS & CONTRIBUTORS

Evgeny Makarov

Senior Traffic Quality Manager

Diksha Sahni

Content Marketing Manager

Clément Névoret

Director Business Operations

Stefan Benndorf

Managing Director

Mangat Modi

Senior Software Engineer