forensiq by Impact

Guide to Mobile Fraud Prevention

Part 2:

Taming Install Fraud

Introduction

With the rise of mobile apps and the popularity of advertiser programs to promote app installs, spend in mobile performance campaigns has increased dramatically to about $7.5B1 today.

Unsurprisingly, bad actors have followed the money, creating new ways to defraud the ecosystem and take advantage of loopholes that inherently come with new environments. Mobile Marketer estimates that about $300M was lost to app install fraud in 2017.

Education is a necessary first step in fraud prevention, detection, and remediation. In this guide, we've distilled essential information on the two most common types of performance fraud on mobile:

1. mobile install fraud and
2. install attribution fraud (otherwise known as mobile affiliate fraud).

Performance marketers, agencies and networks should be especially vigilant about both types of fraud. We also advise you on what you can do about it.

Welcome to the second part of our Mobile Fraud Prevention Guide focused on mobile performance fraud. We hope this guide offers a quick but broad understanding of fraud in both areas and what you can do to reduce their impact on your business.

[1] eMarketer. US Mobile App Install Ad Spending, 2015-2017
[2] Study: App install fraud costs marketers up to $300M per year

Types of Mobile Install Fraud

Mobile install fraud mostly involves suspicious app installs where installers have no intention of actually using the app.

Install Farms

Install Farms employ hundreds of low-cost workers with real phones to install apps.

1. They install the app in order to claim CPI credit.
2. They delete the app.
3. They reset the phone in order to obtain a new Device ID.

Participants in the install farm then repeat the process over and over to capture more CPI revenue.

Sometimes, install farms will leverage device emulators in order to achieve better economics. Multiple device emulators can be run on a single desktop, increasing the fraudster's scale. Android devices are particularly susceptible, and because Android emulators are almost like full-function phones, the fraudster can delete the app, reset the emulator's device ID, and repeat, just like they would do with a real device.

Types of Mobile Install Fraud

Botnet Installers

Bad actors can often infect thousands or even millions of mobile devices through malware installed by malicious apps. These mobile devices form a mobile botnet, remotely controlled by the botnet operator, and can be used to commit install fraud at a large scale.

In order to avoid detection, bad actors will often avoid visible actions such as explicitly installing the app on the user's phone. Rather, they will choose advertisers with large CPI programs, and reverse-engineer postback codes that are sent by these apps from their tracking SDK to the SDK's servers. The botnet operator could then instruct their infected mobile devices to send out fake, manipulated postback signals to the same SDK servers to indicate that the install or post-install event has taken place.

Incentivized Installs

Individuals are offered incentives, such as mobile game power-ups, to install apps. However, these individuals have no interest in the advertised app and the advertiser pays for low quality installs. Incentivized installs are typically not fraud, but when they are mislabelled as non-incentivized traffic, then they are classified as fraud.

Techniques to Thwart Mobile Install Fraud

Install fraud is already a large problem, and it's bound to grow larger as malicious players in the mobile world upgrade their techniques. Fortunately, specialists like Forensiq have built up a significant arsenal of capabilities to thwart bad actors.

Device & App Reputation

A central fraud intelligence database is a must-have element of any serious mobile fraud detection service. The database should contain a comprehensive list of disreputable sources such as install farms, compromised devices and suspicious apps to ensure that your install traffic is as clean as possible, and to avoid chargeback conversations later on.

Device ID Lifecycle Analysis

Bad actors know that a good way to hide their activity from Device ID databases is to continuously reset their phone in order to obtain a new Device ID. However, careful monitoring of the ratio of new devices to existing devices makes it easier to identify suspicious sources where this type of behavior is prevalent.

Advanced Emulator Detection

Fortunately, there are a number of ways to distinguish real-world mobile device utilization from emulators. Close inspection of the hardware and phone configuration, such as motion and orientation analysis, makes it easier to discern legitimate installs from simulated installs.

Types of Install Attribution Fraud

Install attribution fraud focuses on unscrupulous partners or affiliates receiving revenue even though they played no part in prompting the app install.

Marketers use a last click attribution model to reward media partners for driving the install and bad actors game the model to steal credit for organic installs or from legitimate media partners.

Click Spoofing

When advertisers rely on their publishers to report click events, instead of tracking it themselves, they leave themselves exposed to Click Spoofing.

Click Spoofing occurs when malicious publishers report click events even when the user hasn't clicked on the ad. In fact, because malicious publishers can effectively "grade their own homework", nothing stops them from reporting click events even if a user has not been exposed to the ad.

Click Spamming

A common technique used by a malicious publisher is to have regular-looking apps hijack a user's device and generate hundreds of ads in the phone's background that are invisible to the user.

Click Spamming takes it one step further by actually triggering background click events to game brands' install attribution models.

Types of Install Attribution Fraud

Click Injection

Click Injection happens when a bad actor sneaks in app code that continuously monitors the user's Android phone for new installs. Fake clicks are sent just before the relevant installs are complete, effectively trying to claim the last click.

Malvertising

Malvertising occurs when bad actors inject malicious code into ads to trigger clicks to app stores. Malvertising requires bad actors to purchase impressions in order to distribute a malicious ad.

Malvertisers can damage honest publishers' reputations. The malicious ad can show up on that publisher's site and when a user visits that site, and as the ad renders on the user's device, the illicit click to the app store is triggered, often causing a poor user experience.

Techniques to Thwart Install Attribution Fraud

When bad actors attempt to game install attribution models, their perverse incentives lead to behavior that often gives them away.

Click behavior becomes irrational or improbable, and that makes it easier for specialists like Forensiq to detect.

Real Time Click Filtering

Expect vigilance from your fraud detection provider in identifying repeat offenders that generate fake clicks or installs to commit CPI fraud. Fraud detection providers often leverage machine learning to maintain the highest quality list of suspicious users, which can typically be accessed through real-time filtering APIs in order to keep bad actors out of your traffic.

Click Stuffing Detection

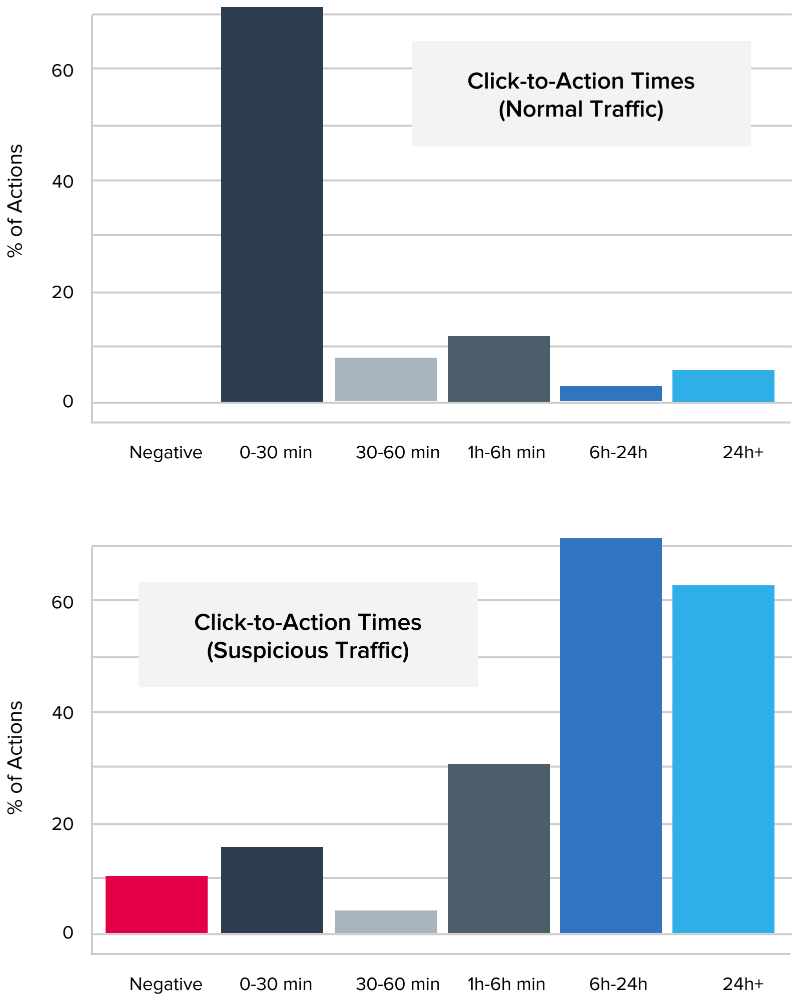
Fraudulent partners can illegitimately take credit for conversions through forced clicks generated using hidden iframes, browser toolbars, and pop-under windows. These illicit tactics divert revenue from high-quality referring partners and force advertisers to pay for organic traffic, which leads to inaccurate attribution and negative ROI. Techniques such as behavioral recognition, anomaly detection, and time patterns on the site can help identify when this is occurring.

Click-to-Install Time Analysis

Bad actors that inject their fake clicks into advertisers' attribution models often exhibit unusual click-to-install time durations. A careful examination of this data often reveals improbable or unrealistic click-to-install timing that should be treated with suspicion.

Distribution of Clicks-to-Install

In addition to looking at individual click-to-install timing, it is also helpful to look at the data in aggregate. Examining the distribution of click-to-install durations for bad inventory sources often yields highly unusual distributions when plotted on a time-based histogram. This data lets you assess the mobile attribution risks associated with your media partners.



Suspicious sources of click traffic exhibit unusual histograms of click-to-install duration. For example, the source above shows a distribution that is heavily weighted towards unusually longer durations than what is typically observed from more reputable sources.

Proactive Steps for Addressing Install Fraud

All parties in the ecosystem have a role to play in reducing bad actors' ability to exploit the CPI market.

Supply-side players that do their part in maintaining clean traffic should be rewarded with more clients and longer-running campaigns. Demand-side players save money, which can be redirected to optimal sources that drive even higher performance.

When considering the actions you can take, it's useful to think in terms of a framework for proactive fraud handling that consists of tactics around prevention, detection, and remediation.

- **Prevention**. As a participant in the CPI landscape, you will want to prevent highly suspicious click and install events from entering your system. Prevention means blocking high risk clicks and installs before their traffic gets to your systems.
- **Detection**. Real-time click or install blocking is effective but can be technically challenging. Even without real-time click and install blocking, it is still important to evaluate your traffic sources after the fact, based on the amount of high-risk clicks and installs they send your way.
- **Remediation**. Once you have a sufficient amount of data available from your prevention and detection efforts, institute processes to further optimize traffic quality by methodically evaluating your sources on an ongoing basis.

Proactive Steps for Addressing Install Fraud

Prevention

Do your due diligence when choosing the partners you allow into your program. Manually approve each applicant. Visit their website, read their content and call them on the phone to ensure they align with what you're selling.

Talk to your fraud detection specialist to leverage real-time filtering to eliminate fraudulent installs from install farms, or fraudulent clicks from compromised devices. Adjust your attribution models and proactively block payouts from your high-risk suppliers.

Score every click and install event; new types of install and attribution fraud constantly emerge. It pays to remain vigilant on a continuous basis.

Consider only rewarding partners when the users engage in some revenue-generating activity post-install, and not for the install event alone.

Detection

Always evaluate the level of risk for each of your media sources' click and install events. If you were not able to block payouts to sources that delivered high-risk clicks or installs, request chargebacks for those events.

Remediation

Work with your provider to determine a threshold for install or click fraud. Monitor sources that consistently exceed the threshold, issue chargebacks, and consider expelling them from the program if install fraud rates or install attribution fraud rates do not improve.

forensiq
by Impact

About Forensiq

Forensiq is your digital armor. Sophisticated detection methods, including machine-learning algorithms, identify and block fraud so that you can eliminate costly, ineffective marketing spend and keep your ad inventory safe.

At the same time, we know fraud is a never-ending battle. Malicious actors never stop looking for new ways to exploit your vulnerabilities. For this reason, our obsessed team of data scientists continually innovates technologies and strategies to protect your marketing investments.

Contact sales@impact.com to learn more!

impact