The State of Mobile Fraud

Q1 2018

AppsFlyer

Key Findings

Fraud rising. Over Q1 2018, mobile app marketers were exposed to 30% more fraud (as compared to the 2017 quarterly average), reaching $700-$800 million worldwide. The share of fraudulent installs has also grown by 15%, tainting 11.5% of all marketing-driven installs.

Fraud comes in waves. When new protective measures are introduced, fraudsters adapt, which leads to new measures, and the cycle continues. Fraud has become a high stakes arms race as both sides are becoming increasingly sophisticated.

Bots are now the most dangerous threat. In September, we saw new kinds of bots emerge. By February, bots replaced device farms as the most popular form of attack responsible for over 30% of fraudulent installs.

Many apps are exposed. Fraud is not just about a few large apps targeted by advanced attacks. In fact, 22% of apps have over 10% fraudulent installs, while no less than 12% are significantly exposed with at least 30% fraudulent installs.

Shopping, gaming, finance and travel apps are the hardest hit. High payouts and verticals of scale suffer the worst financial loss. Shopping apps, with their high CPIs and huge scale are the most heavily hit vertical, with $275 million exposed over Q1 2018.

Android is more vulnerable to fraud, but iOS is also a target. With greater difficulty perpetrating device fraud on iOS, fraudsters resort mainly to click flood, where iOS is well ahead of Android. In all other types of fraud, Android rates are much higher.

Introduction

Fraud targeting mobile app marketers is evolving faster than ever. What once took fraudsters six months to develop can now take weeks or even days. The bad guys have gotten smarter, adapting much faster to anti-fraud measures. What's more, we see a significant increase in the rate of fraud and level of financial exposure.

In late 2017, Forrester reported that mobile fraud is among marketers' most pressing concerns. However, solid, data-backed information about mobile fraud is difficult to find. With fraud rates on the rise, we believe the time has come to share some deep, actionable insights in order to help reverse this disturbing trend.

On April 2nd, AppsFlyer launched a new annual initiative we call #FoolsNoMore. The #FoolsNoMore initiative includes a series of educational resources for marketers (including this report) that we hope will increase knowledge and awareness around this pressing issue. In this study, we will explore the current impact of fraud on the market and offer global findings and insights by category, country and platform.

Data Study Sample

9/2017-2/2018
Duration

6,000
Apps

10 Billion
Installs

Global Findings

30% Increase in Financial Exposure to App Install Fraud

The financial exposure of mobile app marketers to fraud is increasing at an alarming rate. Last September, we estimated that app install fraud would cost advertisers $2.2-$2.6B in 2017, or roughly $600 million a quarter. Over Q1 2018, this number grew about 30% to $700-$800 million.

A quick look at 2018 vs. 2017 yields the following insights, all of which explain the rise in financial exposure:

1) A 15% rise in the rate of app install fraud
2) A 10% increase in the cost of media
3) A 25% rise of non-organic installs

The financial exposure figure is based on cost per install data and 3rd party attribution market share estimates.

Estimated Fraud Exposure
Mobile App Marketing
(Q1 2018)

$700-$800
MILLION

Polluting the App Ecosystem

What are the odds that an app install you see in your reporting dashboard is fraudulent?

The answer: 11.5%. That means that out of 1,000 non-organic installs you pay for, 115 are not real. Simply put, that's money you are throwing away.

11.5%

Global Rate of
App Install Fraud (1-2/2018)

Market Perspectives

When it comes to mobile fraud, no advertiser, app exchange or network is immune. This includes the largest, most trusted suppliers. Everyone in the industry is dealing with click spam, hyperactive devices and other forms of fraud. Rather than blacklisting large groups of apps or entire networks, and potentially damaging the broader ecosystem, advertisers are better served to identify fraudulent bid requests upfront, before spending a dime, and avoid bidding on these fake bid requests in the first place.

This approach alone would save advertisers billions of dollars in wasted marketing budget which can be better spent marketing to real users.

Phil Crosby
Chief Product Officer

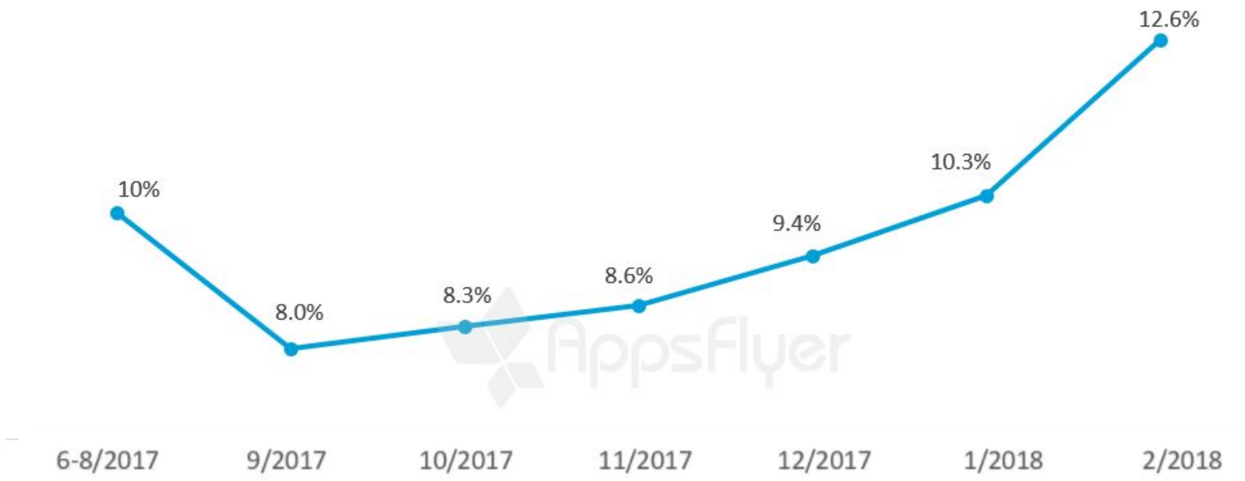
LIFTOFF

Fraud **Rising**

In this perilous game of cat and mouse, fraudsters are becoming increasingly sophisticated. When effective defenses are released, the bad actors are forced to adapt, and adapting they are, at increasingly alarming speeds.

The dip in September was driven by a drop in overall device farm activity. To make up for this loss, fraudsters doubled down on click flood, and began investing more in bot-based attacks. The bots wave and a resurgence of device farms are currently inflicting heavy damage. This is why we ended February at an all-time high with a 12.6% fraud rate. The next page shows how waves of different fraud types rise and subside.

App Install Fraud Rate Trend



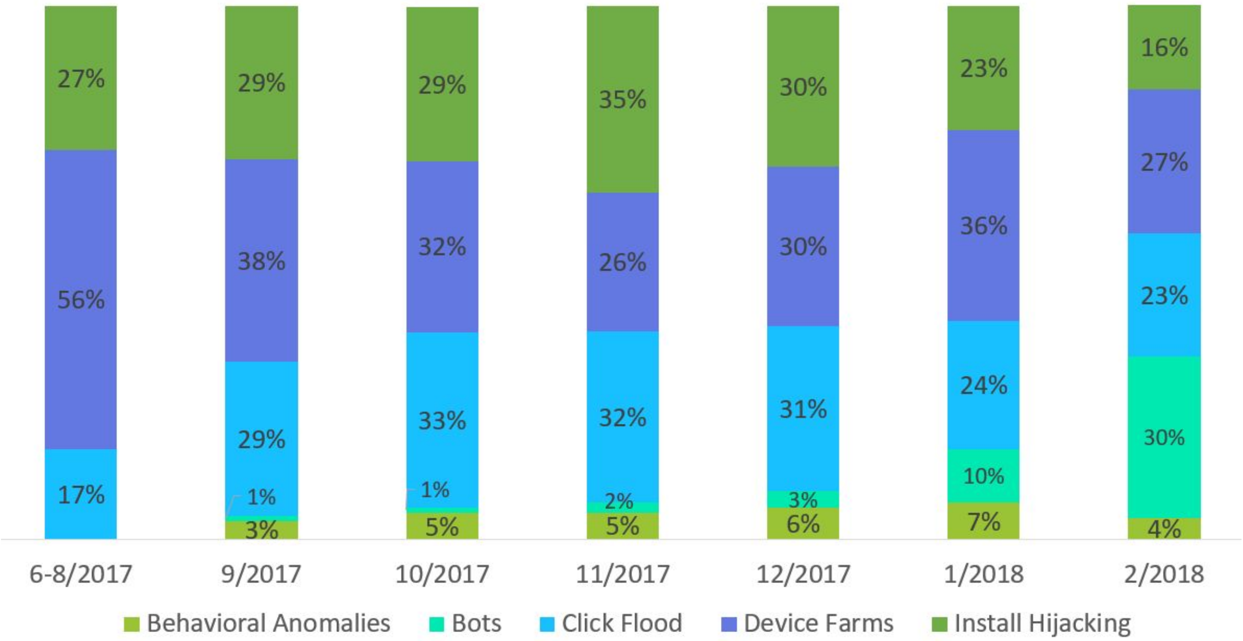
Fraud Comes in **Waves**

When looking at a month-by-month breakdown of fraud attacks by fraud type, we can clearly see the wave-like patterns of fraud.

Over the summer of 2017, device farms were responsible for an all-time high of 56% of fraudulent installs. The launch of Protect360 drove fraudsters to change their install patterns and invest in new forms of attack. As such, click flood rates jumped. Then we began experiencing a rise in bots trying to spoof our SDK on a minor scale around the world. Alarmingly, these new bots often came in tandem with new behavioral anomalies that are likely the result of advanced, programmatic bot attacks.

In February 2018, bots replaced device farms as the most popular fraud attack vector with 30% of fraud. Given the clear diversity and volatility of the fraud market, marketers are best served by multi-layered solutions that cover all of these tactics.

App Install Fraud Distribution By Type



Market Perspectives

Fraud impacts the entire ecosystem from ad networks and attribution platforms to advertisers and publishers. In order to adequately address the growing fraud problem, we all have a responsibility to share data and valuable insights, to build sustainable fraud protection and protect our industry.

When it comes to addressing mobile fraud, the entire team at Chartboost shares a deep sense of obligation to our publishers, advertisers and the industry. Preventing fraud in today's market is not easy. We have found that only by actively investing in fraud prevention measures, can we provide a healthy, trustworthy network. To find fraud, you must first run massive amounts of traffic data across machine learning algorithms, measuring hundreds of signals to identify potential pockets of fraud.

However, given the fragmented nature of our ecosystem, we cannot block traffic simply because it looks unusual. All fraud findings must be validated by experienced, human analysts. The challenge is, that as fraudsters are getting smarter, employing more sophisticated tactics, it is becoming harder to differentiate fraud from legitimate traffic. This is a challenge that we believe, must be met head-on by every player in the ecosystem.

Pepe Agell
VP of Corporate Strategy
Chartboost

Many Apps Have High Fraud Rates

The overall high rate of fraud is not the result of just a few large apps being targeted on a large scale. In fact, 22% of apps have over 10% fraud, while no less than 12% (that's hundreds of apps out of our sample of 2500 apps) were significantly exposed to fraud at rate of over 30%.

Distribution of Apps By Fraud Rate (1-2/2018)

More Than 1 in 10 Apps

Minimum

30%

Fraud Rate

Every App
is a Target

Many marketers mistakenly assume that the largest apps are the most heavily targeted by fraudsters.

However, we found no correlation between the size of an app (based on the number of its non-organic installs) and their rate of fraud. This means every app is a potential target, although larger advertisers obviously bleed the most cash because of their scale.

Fraudsters are obviously drawn to larger advertisers because of the size of their bounty. It appears bad actors are also drawn to smaller advertisers because they are easy targets, often with less knowledge and resources to fight fraud.

App Size / Fraud Rate Correlation (1-2/2018)

-0.04

= Not correlated

But Fraud Varies Significantly by Vertical, Region and Platform

Fraud Hits Where **CPIs Are High**

The financial exposure of fraud is based on either the scale of fraud, the cost of media or both. The high level of exposure seen among the Shopping, Finance, Travel, and Food & Drink verticals is the result of high payouts (40% higher than the average CPI).

The scale (and payout) in the shopping category is why this category is significantly exposed. In gaming, payout is much lower but the scale is massive.

Top 10 Financially Exposed Verticals
Q1 2018

Shopping	$275M
Gaming	$103M
Finance	$90M
Travel	$65M
Food & Drink	$63M
Utilities	$15M
Entertainment	$14M
Productivity	$8M
Lifestyle	$7M
Social	$6.5M

Fraud Targets
Payout and Scale

When fraudsters decide which country to target, they look at two primary factors: payout and scale. That's why they target, on the one hand, countries with relatively high CPIs (e.g., US, Japan, UK, Germany), and on the other hand, those with significant volume (e.g., India, Indonesia, Brazil).

The US tops the financial exposure list because of both high payouts and massive scale even though fraud rate in the US is still lower than the global average. Overall, we found that the fraud rate in the US has increased by 30% (compared to the previous study).

To avoid detection, fraudsters cannot limit themselves to only one country where payout might be higher. Rather, they must spread out their traffic wherever campaigns are run.

Financial Exposure of the Top 10 Most Targeted Countries Q1 2018

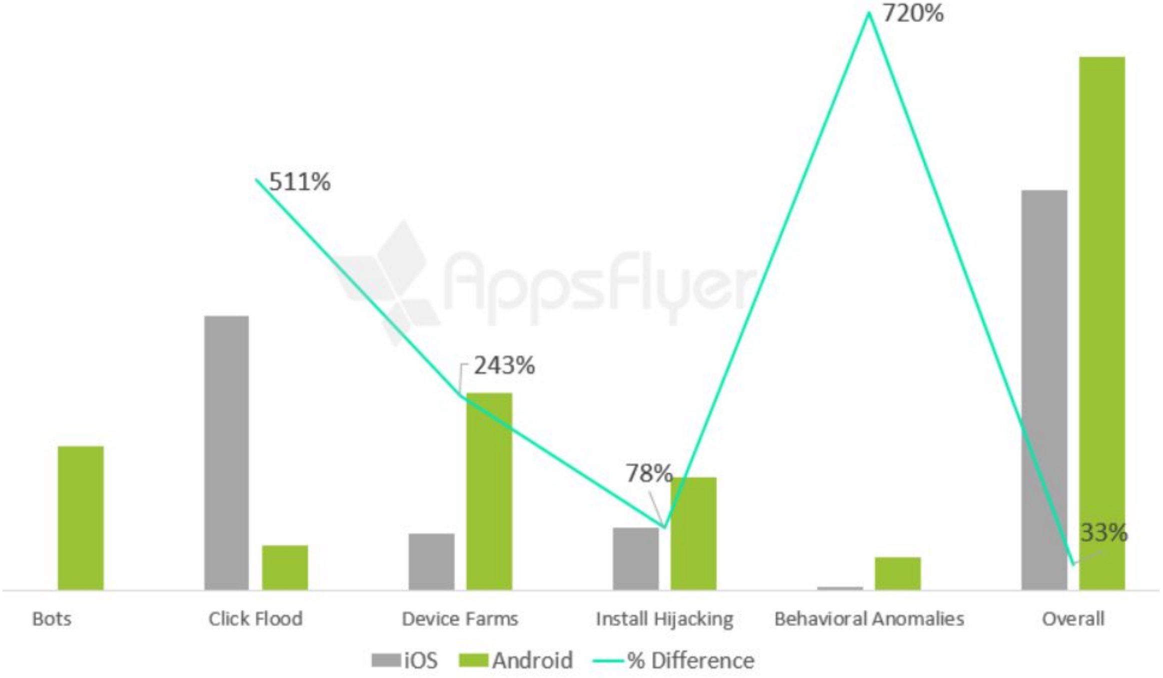
United States	$98M
India	$26M
Indonesia	$24M
Japan	$21M
United Kingdom	$16M
Brazil	$15M
South Korea	$12M
China	$10M
Taiwan	$7M
Germany	$7M

Android has more fraud but iOS is hit hard with Click Flood

The open Android OS is more vulnerable to attacks than the more locked down iOS platform. Because of its sheer scale, the overall amount of fraud perpetrated on Android is over three times that of iOS. However, when it comes to a fraud rate comparison, the difference between the platforms is only 33%.

Although app install fraud is harder to pull off on iOS, fraudsters are attracted by its higher payout. At present, many resort to click flood as it does not require compromising actual devices. As a result, the rate of click flood on iOS is more than five times that of Android. In all other fraud types, Android is well ahead, showing a far greater diversity of fraud.

Share of Fraudulent Installs By Platform



Market Perspectives

Mobile fraud is something every advertiser and publisher should be concerned with. It impacts all of us, from top to bottom. From a practical standpoint, advertisers should ask hard questions of their platform partners about what anti-fraud measures they can expect when ads are placed either programmatically or via managed service. Consider why certain apps and ad networks have a higher incidence of fraud and partner with those that take an active approach to minimizing fraud, thus maximizing their own advertiser ROAS.

Furthermore, we always recommend that advertisers look at fraud as part of their overall ad optimization strategy, rather than just a single point of failure in a campaign. Strategic optimization can further reduce fraud's negative impact on ROAS. Given the state of fraud in the real world, optimizing away from those trafficking heavily in fraud can help offset their initial loss.

Most of all, remember that fraud should be an ongoing conversation with any ad platform or network. Fraud can shift rapidly, and it's important for conversations around this challenge happen regularly between the advertiser and their partners.

Eric Dickinger
VP Growth
ADCOLONY

Understanding Protection

- **The Scale Challenge**
  Fraudsters are continuously improving their ability to mimic legitimate traffic. Identifying fraudulent activity and validating a new fraud signature requires a massive amount of data. Few companies have the data and expertise needed to manage the problem and stay protected without a third-party provider.

- **Blocking and Transparency**
  Finding fraud after it has already been attributed is not ideal. However, automated blocking often obscures data for both marketers and their network partners. As a marketer, you should understand the ROI of every investment, including fraud protection.

- **Protection is Insurance**
  Fraud comes in waves, impacting nearly every app that invests in user acquisition. Though it comes as no surprise that businesses with serious fraud challenges see strong ROI from anti-fraud investments, many marketers are now investing in fraud as an insurance policy. This proactive investment incrementally improves their performance data integrity today and provides the coverage needed when the next big wave hits.

What Can You Do?

There are a number of practical ways you can keep your business protected against mobile fraud. Here are our best practices.

1. **Keep Your SDKs Up To Date**
   Running the latest SDK version ensures that you have the latest security updates.

2. **Pay Attention to Your Data**
   Anomalies in your data such as large discrepancies between App Store numbers and your reporting platform, or significant changes in conversion rates may be due to fraud.

3. **Get a Fraud Assessment**
   General trend data (such as this report) is a great way to quantify your potential exposure. If you are working with AppsFlyer, contact your success manager for a detailed assessment of your fraud exposure and where your business is most vulnerable.

4. **Stay Transparent**
   Set your fraud terms with each of your providers and media sources before campaigns begin to avoid the headache of reconciliation negotiations.

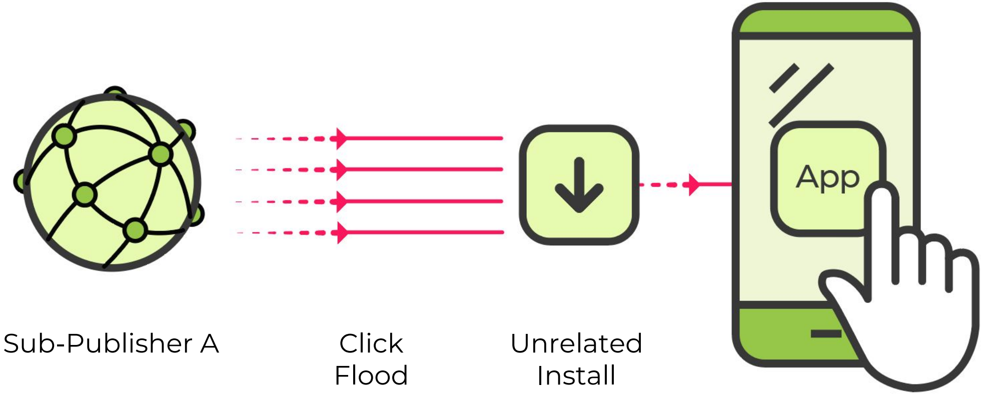
Understanding Fraud

HOW IT WORKS

In click flooding, fraudsters send a “flood” of false click reports from, or on behalf of real devices.

When the actual device downloads the app, the sub-publisher is falsely credited with the install.

Click Flooding



Sub-Publisher A

Click Flood

Unrelated Install

Sub-Publisher A Is attributed

PROTECTION

Protect360 uses signals including click-to-install time (CTIT), conversion rates and multi-touch contribution rates to identify and block click flooding at its source, in real-time.

Market Perspectives

Fraud protection used to be as simple as blocking of basic IP address spoofing. This has since evolved into ever-more sophisticated detection capabilities associated with bot farms and click injection.

Unfortunately, fraud prevention is a project that never truly reaches completion. It is imperative that advertisers and publishers alike maintain dedicated resources to ensure both standards & technology, as well as to maintain brand safety and transparency. It's also critical that advertisers work closely with partners like AppsFlyer, as their much broader view of the market enables them to detect and address new fraud variants more quickly than any one advertising or app publishing platform can do on their own.

In my personal experience, I attribute much of Tapjoy's growth and success to our continuing investment in identifying and routing-out new fraud schemes as they emerge.

Paul Longhenry
SVP of Strategy and Business Development

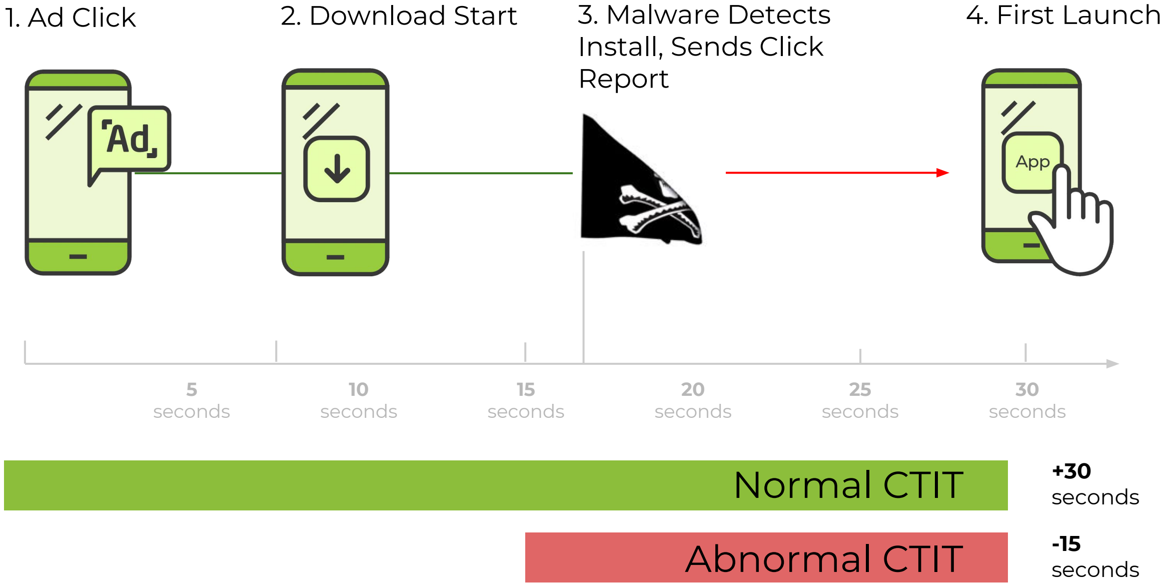
Tapjoy

HOW IT WORKS

Install hijacking is a type of fraud where fraudsters “hijack” credit for an install.

Common techniques include sending false click reports or injecting false referrer data.

Install Hijacking



PROTECTION

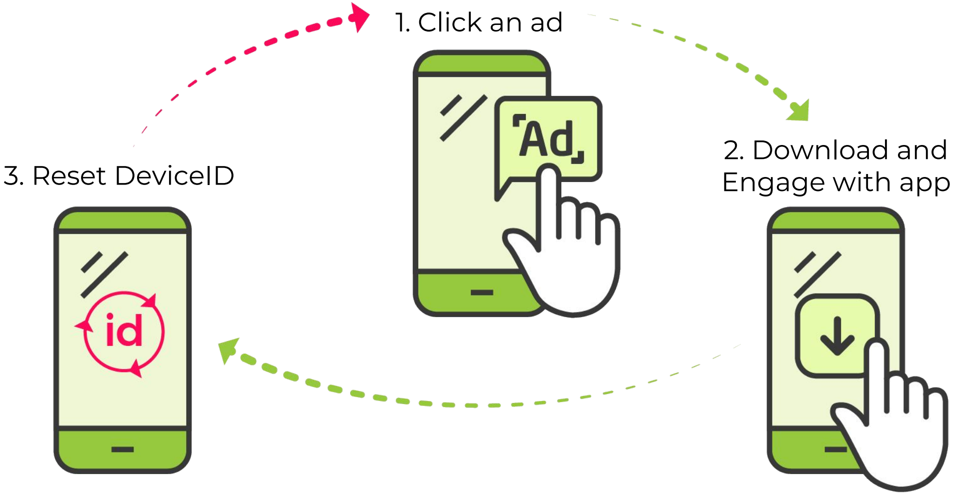
Protect360 uses multiple signals including short CTIT, referrer mismatching, and multi-touch distribution patterns to identify and block install hijacking in real-time.

Device Farms & DeviceID Reset Fraud

HOW IT WORKS

Device farms are locations full of actual mobile devices clicking on real ads and downloading real apps, hiding behind fresh IP addresses.

Over 2017, fraudsters started regularly resetting their DeviceIDs to avoid detection.



PROTECTION

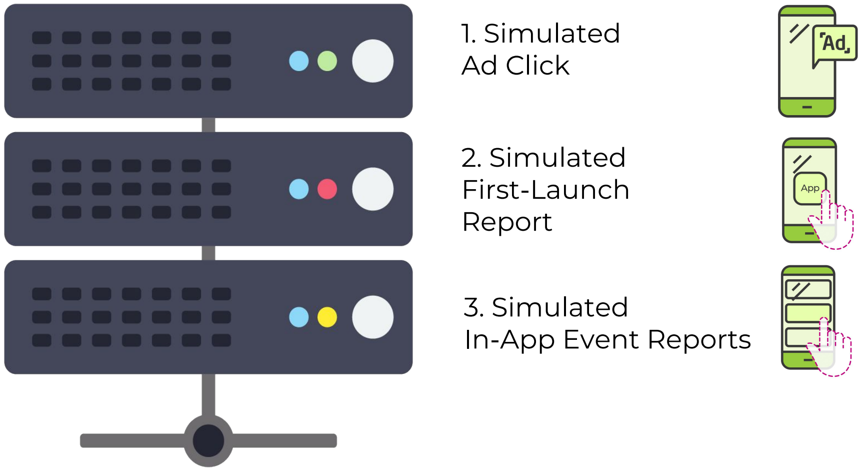
DeviceRank maintains active ratings for over 5.5. billion devices, automatically blocking device farms. Sub-publishers trafficking concentrations of devices “new” to the database are blocked in real-time.

Bots

HOW IT WORKS

Bots are malicious code that run a set program or action. While bots can be based on real phones, most bots are server-based.

Bots aim to send clicks, installs and in-app events for installs that never truly occurred.



1. Simulated Ad Click
2. Simulated First-Launch Report
3. Simulated In-App Event Reports

PROTECTION

AppsFlyer's unique scale allows Protect360 to identify both highly targeted and widely distributed bots operating at both lower and higher volumes, blocking bots in real-time.

Market Perspectives

The Unity team takes publisher fraud seriously and has rigorous systems for detecting and blocking fraudulent activity. We leverage the deep and broad data visibility across our entire network, which includes over 19,000 developers and 119,000 individual games.

We have found that fraud solutions cannot be naive, trusting basic one-size fits all sets of rules across every scenario. At Unity, we leverage various machine learning approaches to determine the type and quality of the traffic from each publishing game. Networks and advertiser must actively recognize artificial traffic, whether it is by invasive human actions or automated traffic from scripts or bot networks, in order to block fraud at the publisher level.

Paul Bowen
Vice President

unity

Behavioral Anomalies

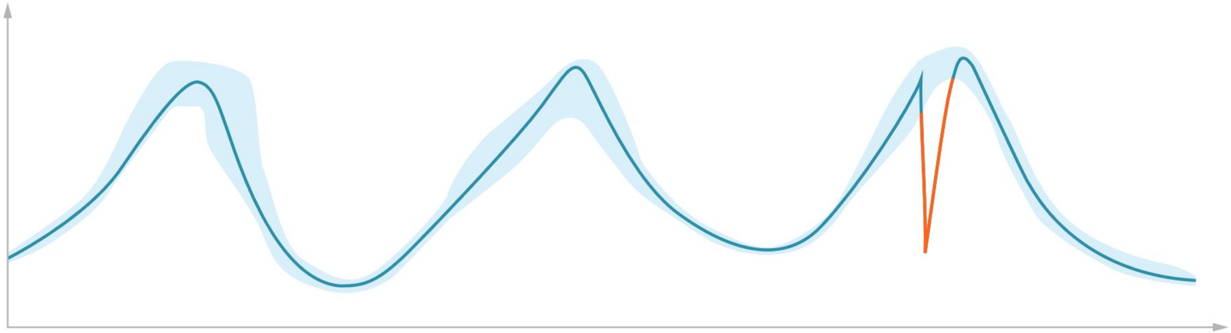
HOW IT WORKS

As bots and malware have become more advanced, some have developed the ability to simulate a limited set of functions, sending seemingly legitimate click, install and in-app event reports.

The only way to address these advanced techniques is to analyze their behavioral patterns.

Example

Normal Distribution of In-App Activity



PROTECTION

Protect360 utilizes supervised machine learning to validate behavioral anomalies. Sub-publishers trafficking in this fraud are blocked in real-time.

Appendix

Vertical Breakouts

Shopping

- #1 hardest hit category: $275 million in financial exposure over Q1 2018
- #2 share of apps with a high fraud rate: 30% with at least 10% fraud, 22% with at least 20%, and 17% with more than 30%
- 35% higher rate of fraud in Q1 2018 vs. Q4 2017
- #1 highest number of fraudulent installs from bot attacks
- #1 highest number of fraudulent installs rejected through behavioral anomalies
- #1 highest number of fraudulent installs from install hijacking attacks
- #2 highest number of fraudulent installs from device farm attacks
- #2 highest number of fraudulent installs from click flood attacks

Travel

- #1 share of apps with a high fraud rate: 38% with at least 10% fraud, 32% with at least 20%, and 27% with more than 30%
- #4 hardest hit category: $65 million in financial exposure during Q1 2018
- 15% higher rate of fraud in Q1 2018 vs. Q4 2017
- #3 highest number of fraudulent installs from bot attacks
- #2 highest number of fraudulent installs rejected through behavioral anomalies
- #3 highest number of fraudulent installs from install hijacking attacks
- #5 highest number of fraudulent installs from device farm attacks
- #3 highest number of fraudulent installs from click flood attacks

Market Perspectives

Marketers rely heavily on networks and affiliates to drive not only high-quality users but also scale. When you are looking to grow your user base, no one solution out there can drive all the consumers necessary for a healthy and profitable ecosystem. This means advertisers have to trust their partners do all they can to ensure the ROI is there. Identifying and preventing fraud is something, unfortunately, all marketers are forced to face.

Understanding your network partners' approach to managing fraud and the systems they put into place to identify early-stage data anomalies should be a critical step in building your marketing plan. Networks who rely heavily on direct SDK integrations with publishers leads to a closer relationship to the inventory. These direct integrations make it easier to identify potentially fraudulent publishers at the onset.

However, curation of publishers is not the end all be all. Robust fraud detection systems which look at user behavior at every stage of the impression funnel, all the way through to post-install-events help to identify suspicious behavior. This may not be immediately identifiable based purely on the user base or ad requests, particularly as we see more sophisticated ad farms springing up. This is why you may see the majority of fraud coming from long-tail publishers. Publishers who pass all business and data mining vetting, still need to continue to be manually evaluated based impressions, clicks, installs, and ROI for every user. Most importantly, it is critical to continue to modify identification methodologies in order to adapt as fraudsters are becoming more and more sophisticated.

Colin Behr
VP of Business Development

Vungle

Gaming

- #2 hardest hit category: $103 million in financial exposure during Q1 2018
- #8 share of apps with a high fraud rate: 21% with at least 10% fraud, 13% with at least 20%, and 10% with more than 30%
- #1 highest number of fraudulent installs from click flood attacks
- #2 highest number of fraudulent installs from install hijacking attacks
- #5 highest number of fraudulent installs from bot attacks
- #3 highest number of fraudulent installs rejected through behavioral anomalies
- #3 highest number of fraudulent installs from device farm attacks

Finance

- #3 hardest hit category: $90 million in financial exposure during Q1 2018
- 250% higher rate of fraud in Q1 2018 vs. Q4 2017
- #5 share of apps with a high fraud rate: 23% with at least 10% fraud, 20% with at least 20%, and 15% with more than 30%
- #1 highest number of fraudulent installs from device farm attacks
- #2 highest number of fraudulent installs from bot attacks
- #5 highest number of fraudulent installs rejected through behavioral anomalies

Food & Wine

- 500% higher rate of fraud in Q1 2018 vs. Q4 2017
- #5 hardest hit category: $63 million in financial exposure during Q1 2018
- #4 highest number of fraudulent installs from device farm attacks
- #4 highest number of fraudulent installs from bot attacks
- #7 highest number of fraudulent installs from install hijacking attacks