WEBINAR

Strategies to Prevent **Mobile Ad Fraud**

& Save your Marketing Budget

LIFTOFF   SmartNews   FreshPlanet

Meet the Panelists

Dennis Mink
VP Marketing

LIFTOFF

Andry Supian
Product Manager

LIFTOFF

Fabien Nicolas
Head of Growth

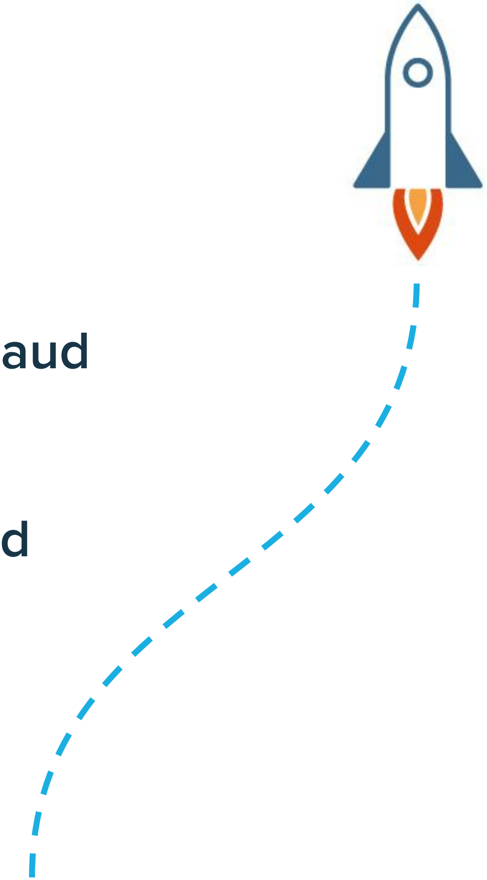
SmartNews

Shamanth Rao
VP of Growth

FreshPlanet

What We Will Cover

1. How big is the problem?
2. Most common types of mobile ad fraud
3. How Liftoff prevents mobile ad fraud
4. Q&A and strategies from panelists



> “Liftoff is a **performance-based, app marketing** platform helping companies drive adoption and **engagement** in mobile apps.”

amazon lyft match acorns King

Recognized as a top rated fraud-free mobile channel

OFFICIAL MEMBER

• CAAF •

COALITION AGAINST AD FRAUD

2017

SINGULAR FRAUD INDEX

MOST SECURE AD NETWORK

LIFTOFF

adjust

TUNE

KOCHAVA

AppsFlyer

How
BIG
is the
PROBLEM ?

In 2016, mobile advertisers lost over

$1B on fraudulent installs

Source: VentureBeat, 2016

This number more than doubled to

$2.6B in 2017

Source: VentureBeat, 2017

3 Main Types of Mobile Ad Fraud:

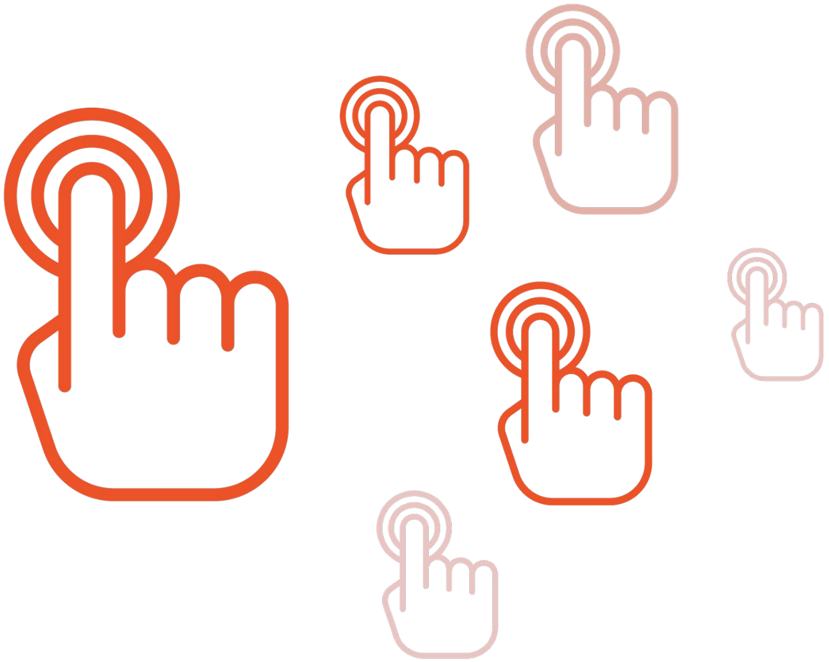
- ☒ Click Spam
- ☒ Click Injection
- ☒ Fake Installs

Click Spam

Click spamming occurs when a fraudulent app sends clicks in the background in hopes that one of the clicks will be attributed to an organic install.

How to detect:

- Extremely low click-to-install and post-install conversion rates
- High amounts of duplicate clicks from the same user on the same ad-media
- Flat distribution of click-to-install time



Click Injection

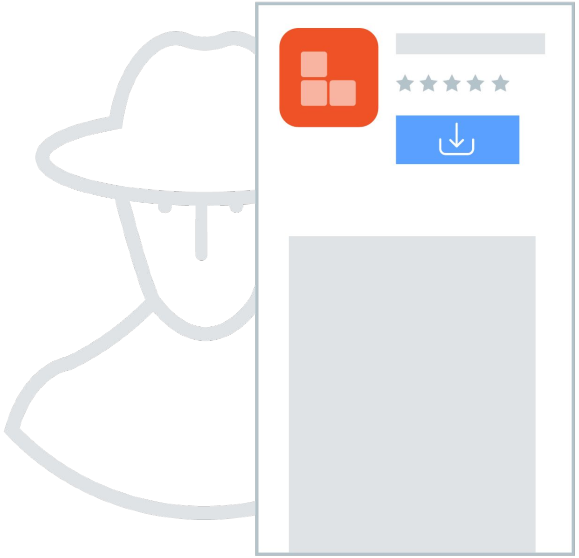
Click injection is a sophisticated type of mobile fraud that only occurs in Android devices. When an organic install happens, the perpetrating app sends a fraudulent click report, effectively stealing the "last-click" attribution.

How to detect:

Extremely short click-to-install time

Fake Installs

A fake install is accomplished by using device emulation software in virtualized environments to make it appear as if an install or post-install event occurred.



How to detect:

Devices coming from anonymized / masked IP addresses

How LIFTOFF Prevents mobile AD FRAUD ?

3 Key Technologies for Preventing Fraud

Bad Bid Request Filtering

Bad bid request filtering, which detects 10 different types of fraudulent traffic

2 Billion Fraud Free Devices

A database of over 2 billion verified fraud free mobile devices

Post-install Optimization

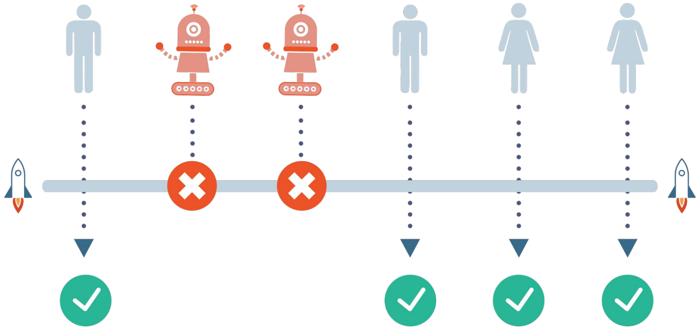
Campaign optimization for post-install engagement

10 Types of Suspicious Bid Requests

- **Bid request rate too high**
- **Poor performing app names**
- **Blank device ID**
- **Too many source apps**
- Non-standard device ID formatting
- App Store ID missing
- App Store ID invalid
- Source app blacklisted
- Invalid IP address
- Blacklisted IP address

87%

Definitions of Top 4 BAD BID REQUESTS



✖ Bid request rate too high

A device ID that makes an abnormally high amount of bid requests a day

✖ Poor performing app names

App names containing certain keywords that are historically poor performing

✖ No device ID

Automatically exclude bid requests with a missing or invalid device ID or App Store ID

✖ Too many source apps

If a device ID is seen in too many source apps we deem the user to likely be fake

Q&A

Submit your questions!

“Tell us about your first experience dealing with mobile ad fraud.”

“What are some of the biggest obstacles you face when dealing with fraud?”

> What tools and services have you used? What worked well or not so well?

> “MMPs (attribution tracking services) all offer fraud detection solutions. What experience do you have with MMP fraud prevention tools?”

“Who do you believe is responsible for curbing mobile fraud? Ad networks and exchanges? DSPs? MMPs? The government?”

“What are 3 concrete suggestions you can offer other marketers who have less experience with fraud?”

Thanks!

You can find more information at www.liftoff.io