Adjust Releases Latest Mobile Fraud Insights Reveal Fraud Rates Nearly Doubled Compared to 2017

Damage Pegged at $4.9 Billion; Some Advertisers Losing Up to 80% of Ad Budget

San Francisco and Berlin - May 10, 2018 - Berlin-based global mobile measurement leader Adjust today published new data findings on mobile ad fraud and released a comprehensive international mobile fraud guide. Adjust measured 3.43 billion app installs and 350+ billion events, processing and analyzing 125 terabytes of data per day from 20,000+ apps over January, February, and March of this year. As the most used mobile fraud tool in the industry, Adjust's goal was to shine a light on how much fraud is currently present in the global mobile ecosystem and to track its effect on the industry in 2018.

It's no surprise that mobile fraud is on the rise. Compared to 2017, mobile ad fraud rates almost doubled, with 7.3% of all paid installs rejected by Adjust's Fraud Prevention Suite. The following new Adjust data insights show what type of fraud drove app installs being rejected:

- SDK Spoofing 37%
- Click Injection 27%
- Faked Installs 20%
- Click Spam 16%

According to eMarketer, mobile ad spending in 2018 will grow 20% to more than $75 billion in the U.S. The research firm also estimates that mobile advertising will rise by 23.5% year over year in 2018. Damage from mobile ad fraud in 2018 could be in the billions, with a +7.0% paid install rejection rate, the damage can be pegged at approximately $4.9 billion.

"Naturally, the fraud rates we see in active rejections only show the level of fraud prevented for advertisers who actually chose to protect themselves. Yet, the aggregate amount of preventable fraud is significantly higher. The number of unreported cases of advertisers being victims of mobile ad fraud is undoubtedly a much high number," says Adjust's Fraud Specialist, Andreas Naumann.

Last year, the Games category was hardest hit, experiencing 35% fraud rates. The next category that fraudsters attacked was e-Commerce, which experienced 20% fraud rates. In 2018, however, there has been a dramatic shift. e-Commerce is now the most affected vertical, accounting for two-fifths of the total installs rejected by Adjust. The other top mobile app categories most affected after e-Commerce are Games with 30% followed by Travel apps with 10 percent.

Fraudsters' New Scam Du Jour: SDK Spoofing

The dramatic rise in these latest fraud numbers can be explained by the latest form of Ad Fraud - SDK Spoofing. The most difficult to detect of all fraud schemes, SDK Spoofing has rapidly gained momentum and become fraudsters' preferred scam du jour. Adjust's initial investigation found that SDK Spoofing is globally distributed across all markets and is attributable to 37% of all rejected installs. The app categories hit hardest by SDK Spoofing are:

- Games 29%
- E-commerce 27%
- Food & Drink 17%

Single campaigns experienced up to 80% of all installs attributable to SDK Spoofing. This means that some advertisers could be losing 80% of their ad budget! For some individual advertisers, the loss could easily be in the tens of millions.

Click Injection: iOS versus Android

This Q1 2018 mobile fraud findings shows that the Adjust's Fraud Prevention Suite rejected twice as many app installs on Android versus iOS devices, meaning that twice as much fraud occurs on Android mobile devices. Besides the sheer amount of Android devices sold vs. Apple's mobile devices another explanation for this is the second biggest source of fraud: Click Injection. This fraud type only occurs on Android devices yet is attributable to 33% of all rejected installs. App categories hardest hit by Click Injection are:

- E-commerce 51%
- Games 23%
- Travel 8%

"When Adjust spearheaded our industry-wide initiative, the Coalition Against Ad Fraud (CAAF), it was a first step to bring together key players in the mobile ecosystem to collectively fight fraud. Yet, the ongoing status quo of ignoring widespread mobile ad fraud by some remains the weakest link and biggest challenge for our industry in 2018. Aligned on one goal, Adjust's next step is to help educate the market about all the different fraud types used, so all players can undertake a stronger defense and implement effective countermeasures to fight fraud head-on," noted Christian Henschel, CEO and Co-founder of Adjust.

Raymund Bautista, Head of Strategic Partnerships at InMobi

"As a founding member of the Coalition Against Ad Fraud (CAAF), InMobi is proud to fight alongside Adjust on the front lines in the ongoing battle against advertising fraud," said Raymund Bautista, Head of Strategic Partnerships at InMobi. "Ad fraud is a real threat to the mobile industry and InMobi is dedicated to building trust between brands and advertising platforms by taking a stand against these malicious activities. Only by embracing collaboration and transparency together will we have the opportunity to eliminate fraud once and for all."

Andry Supian, Product Manager at Liftoff

"Click spam comes from many sources generating fake or low intent clicks. Historically, Liftoff would measure the click-to-install conversion rate (CTI), and block publishers that generate an extremely high number of clicks with a low conversion rate. Recently though, we discovered that a small number of devices drive a disproportionate amounts of clicks, greatly eroding the average CTI for a publisher. In response, Liftoff now detects and blocks click spam per device instead of blocking entire publishers. By being more precise in the way we evaluate and filter our supply, we can decrease fraud without compromising campaign scale."

The full expert fraud guide is available free for download:
https://www.adjust.com/resources/insights/sources-of-error-white-paper/

The Great Fake Out: Other Top Fraud Types

Click Spam (a.k.a. organics poaching) happens when a fraudster executes clicks for users who have not made them. It captures organic traffic, brands it without detection and then claims the credit for the user later. Nearly everything is real (user, device, organic install). The only thing fake is the ad engagement. Yet the party that stole the attribution of a legit install, without having displayed the ad, will be the one paid.

Top categories hit are:

- E-commerce at 38%,
- Games at 29%, and
- Food & Drink at 7 percent.

Fake Installs are fabricated users that only exist to trigger installs based on fraudulent advertisements. Normally they can be spotted through a high level of installs with an instant drop-off after the click. Users, devices, and ad engagement are fake and usually come from data centers or VPNs. On a traffic flow sample of over, 400 million installs over 17 days, Adjust estimated that $1.7 million was paid to fraudsters faking installs.

Top categories hit are:
Gaming at 42%,
E-commerce at 14%,
Entertainment at 14 percent.

About CAAF

Since the start of CAAF, many companies and partners have joined. Adjust actively collaborates with participants to inform and educate the market. The mission is to have participation along the entire ad tech supply chain to effectively protect the industry from perpetual fraud, racketeering and losses.

About Adjust

Adjust is the industry leader in mobile measurement and fraud prevention. The Berlin-based company provides high-quality analytics, measurement and fraud prevention solutions for mobile app marketers worldwide, enabling them to make smarter, faster marketing decisions. With Adjust’s open-source SDK, app marketers can measure and analyze user behavior, user acquisition, marketing ROI, and much more. Adjust’s platform proactively keeps datasets clean through its Fraud Prevention Suite, verifies in-app purchases in real-time, and provides streamlined reporting for clear, actionable, and comparable metrics. Adjust is a marketing partner with all major platforms, including Facebook, Google, Snap, Twitter, Naver, Line, and WeChat. Dynamic Adjust Integrations are used by over 1,200 leading networks and analytics providers worldwide. In total, more than 20,000 apps have implemented Adjust's solutions to improve their performance.

Adjust is the only attribution company to meet stringent EU privacy standards and is fully compliant with GDPR. For more information, interested parties can visit www.adjust.com.

Additional input for the press

Reason why the install was rejected

- SDK Spoofing 37%
- Click Injection 27%
- Faked Installs 20%
- Click Spam 16%

Most affected Verticals (in total):

- E-commerce 43 %
- Games 29%
- Travel 10%

SDK Spoofing

SDK Spoofing is probably the most difficult to detect of all fraud schemes. Through a fraudulent app, fraudsters have access to the device of real users and use these to trigger legitimate-looking fake installs. The devices used actually exist and are credible as install sources. Everything seems real: the connection, the device data, the device. But there is no interaction between the user/device and the intended ad, and most important there is no actual install. The fraud attack goes undetected by the end user and can affect anyone's device at any time. The performance of the campaign will look great, but only in the statistics. The advertisers lose money and the end users are unaware that they've been party to a scam.

Alarming signs: if the SDK version and app version of installs coming through don't match the latest version you've released.

SDK Spoofing - Most affected vertical

- Games 29%
- E-commerce 27%
- Food & Drink 17%

Click Injection

Only appears on Android and is a sophisticated form of click-spamming. Nearly all data is real, except for the last ad engagement. By having access to an Android app on the device of a real user, the fraudsters can trigger a click right after the install completes and before the first app open. The fraudster will receive the credit for the install. This is because the attribution method is almost always based on the last click (last ad engagement).

Alarming signs: attributions to clicks after the user decided to download the app.

Click Injection - Most affected vertical

- E-commerce 51%
- Games 23%
- Travel 8%

Click Spam

Also known as organics poaching, click spam is a type of fraud which happens when a fraudster executes clicks for users who have not made them. It captures organic traffic, brands it without its knowledge and then claims the credit for the user later. Nearly everything is real - you see installs from real users on real devices who behave normally after the install - because these are real users who organically downloaded the app. The only thing fake is the ad engagement. Instead, the party that would be paid for the install actually stole the attribution of a legit install, without having displayed the ad. The performance of the campaign looks great, but the data will be inaccurate. It also threatens the certainty of acquisition decisions. If an advertising network is claiming organic users and these users perform well within an app, the advertiser will obviously decide to invest in that channel to acquire more of the same type of users.

Alarming signs: paid installs from certain sources behaving eerily similar to organic counterparts. A flat distribution of installs over the length of the campaign and low to extremely low conversion rates.

Click Spam - Most affected vertical

- E-commerce 38%
- Games 29%
- Food & Drink 7%

Fake Installs

These are completely fabricated users that only exist to trigger installs based on fraudulent advertisements. Normally they can be spotted through a high level of installs with an instant drop-off after the click. Users, devices, and ad engagement are fake and usually come from data centers or VPNs. On a traffic flow sample of over, 400m installs over 17 days, Adjust estimated that $1.7m worth of installs were being paid to fraudsters faking installs.

Alarming signs: a high level of installs with an instant drop-off after the click.

Fake Installs - Most affected vertical

- Gaming 42%
- E-commerce 14%
- Entertainment 14%