

Is App-Install Fraud on the Rise?

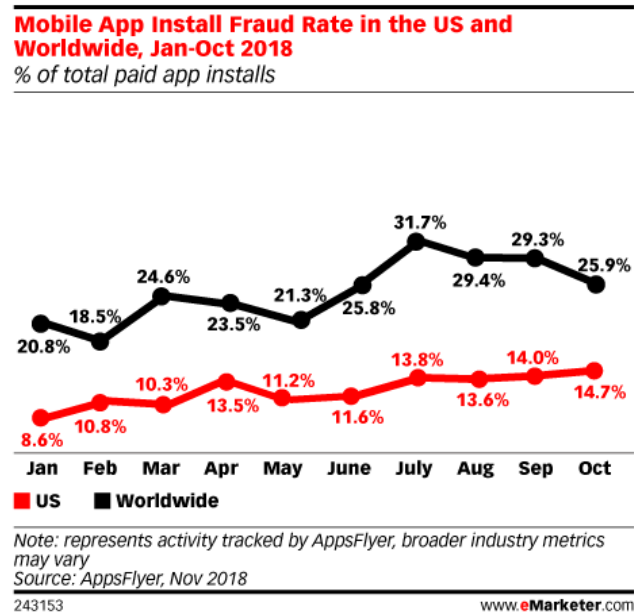
Article

Fraudsters are trying to make a buck off the ad dollars that **flow to mobile**.

Over the past 12 months, mobile attribution firm **AppsFlyer** analyzed 17 billion app installs across 7,000 apps worldwide. It found that the amount of install fraud roughly tripled. More than one-quarter of the installs that AppsFlyer analyzed in that timeframe were fraudulent.

“Fraudsters have become so sophisticated that they can essentially generate as much fraud as they want by faking installs,” said Shachar Guz, product manager at AppsFlyer. “They have

learned how to hack exposed software development kits [SDKs] and manipulate the system by mimicking real user behavior.”



eMarketer estimates that \$7.1 billion will be spent on mobile app install ads in 2018, up from \$6.5 billion last year. App-install fraud refers to the practice where a company falsely gets credit for getting a user to download an app.

“Many companies study app-install fraud where fake mobile devices install apps and get credit for the install,” said Augustine Fou, an independent ad fraud researcher. “Bad actors also take credit for organic installs [whereby] a user downloaded and installed the app because they wanted to, not because they saw an ad for it.”

Several companies have conducted research that indicates how expensive install fraud is for marketers. Mobile marketing analytics firm Adjust estimated that between July and September 2018, 13.7% of app installs were **rejected as fraudulent**. According to Tune, app-install fraud cost marketers **nearly \$2 billion** in 2017. DataVisor stated that for some ad networks, half of their app installs **are fraudulent**. Last year, Google **removed 700,000 malicious apps** from the Play Store, a 70% increase from 2016.

To get some clarity about the state of install fraud, eMarketer asked some ad fraud specialists about trends and tactics they’re seeing in the marketplace.

Shachar Guz, product manager, AppsFlyer: "There is so much money in the mobile and digital advertising ecosystem that bad actors will be incentivized to steal a piece of the pie."

Augustine Fou: "App install fraud has been crazy rampant all along. It is not on the rise."

Andreas Naumann, head of fraud, Adjust: "Currently, click injection and SDK spoofing are the two most vicious kinds of fraud, accounting for 47% and 24% of all rejected installs, respectively."

Stefano Vegnaduzzo, senior vice president of data science, Integral Ad Science: "Fraud is going to happen wherever the payout happens. If advertisers are paying per impression, then fraudsters will find ways to increase impressions. App-install fraud works in a very similar way. If advertisers pay per install, fraudsters will find a way to falsify the number of installations."

Praneet Sharma, CTO, Method Media Intelligence: "There are two reasons that persistent install fraud is on the rise: utilization of low-fidelity identifiers and spoofing of attribution tracking."