Estimated Click Fraud Rate

34%

Estimated Install Fraud Rate

16%

Top 3 Click Fraud Types

Click Flooding

Click flooding is one of the more common methods fraudsters use to cheat the last-click attribution model used in the industry. Fraudsters are flooding the ecosystem with clicks to steal attribution of organic installs. Click flooding also takes advantage of the fingerprinting (probabilistic) method of attribution which uses a combination of IP address and user agent when a device ID is not available. By creating fake clicks that do not contain unique identifiers, such as a device ID, fraudsters increase their chances of stealing attribution including attribution of organic installs.

Platform Differences

If ads for a particular OS platform are sending clicks on devices from a different platform, this may be indicative of bot farms generating fraudulent traffic.

IP w/ High Click Volume

Large volumes of clicks are observed for an app from a single IP address are flagged as potentially fraudulent as they are likely programmatically generated. It is highly unusual to have large volumes of clicks come from a single IP address.

Top 3 Install Fraud Types

Click Flooding

Click flooding is one of the more common methods fraudsters use to cheat the last-click attribution model used in the industry. Fraudsters are flooding the ecosystem with clicks to steal attribution of organic installs. Click flooding also takes advantage of the fingerprinting (probabilistic) method of attribution which uses a combination of IP address and user agent when a device ID is not available. By creating fake clicks that do not contain unique identifiers, such as a device ID, fraudsters increase their chances of stealing attribution including attribution of organic installs.

Abnormally Clustered Traffic

Abnormally distributed traffic identifies cases where click traffic is systematically and evenly spread across many publishers. In these cases, fake clicks are manufactured to steal attribution of organic installs or a scheme to conceal the true identity of the publisher displaying the ad.

Anonymous Installs

Analysis of anonymized install outliers identifies installs driven from IP address networks using various forms of anonymization. These include IPs associated with virtual private networks (VPNs), web hosting services, proxies, and Tor. Installs from these types of IP addresses do not reflect typical human behavior and usually signify fraudulent activity. Installs from publishers exhibiting a significantly high percentage of installs from anonymized sources are considered suspicious and flagged for review.