KOCHAVA

Kochava Audit Catches Fraud other Tools Missed

VERTICAL: GAMING

SOLUTION: FRAUD AUDIT

THE CHALLENGE:

A major mobile app gaming company with hundreds of titles in the top charts became concerned after seeing abnormal performance in some of their campaigns. High click-through-rates and low user quality raised concerns about possible ad fraud that their own tools weren't correctly detecting. They hoped to mitigate fraudulent traffic to get cleaner data, which would allow them to strengthen their campaigns and improve return on ad spend (ROAS).

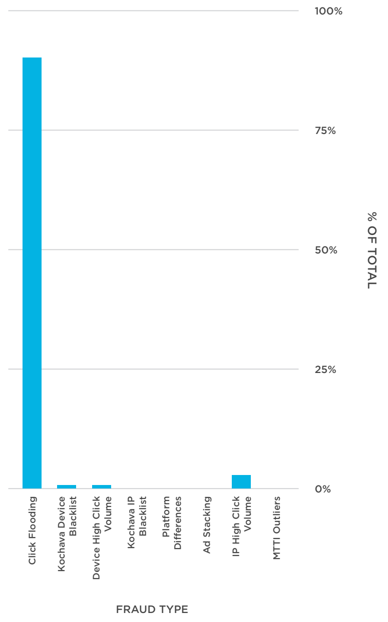
THE SOLUTION:

The gaming company enlisted Kochava to perform an independent fraud analysis on attribution data captured by their internal system for a specific app over the period of one month. To do this, Kochava used their internal fraud detection algorithms that focus on outlier detection and pattern identification. Click and attributed install data from the app publisher were used to establish baseline norms. Kochava data science and client analytics teams performed a detailed analysis and consultation, providing a comprehensive report of the findings.

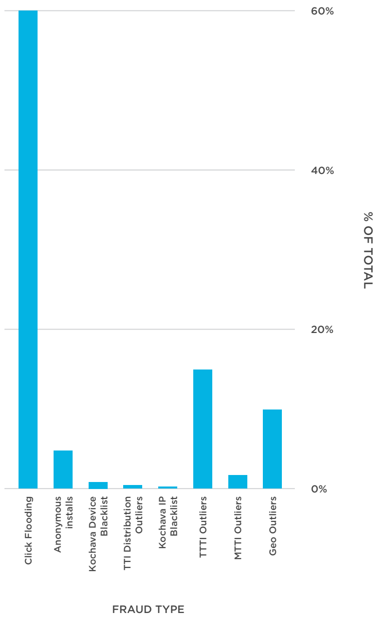
THE IMPACT

The Kochava Fraud Audit found many measurable quantities of fraudulent transactions. Click flooding accounted for the largest volume of false attributions at over 60% of all installs analyzed, followed by time-to-install (TTI) outliers, and click-to-install geo outliers. As for clicks, over 90% of all the clicks analyzed were flagged as fraudulent. In total, over 190,000 misattributed installs were reported—driven by over 400 million fraudulent clicks. The company was able to take action on the findings and swiftly cleaned up their media mix.

CLICK FRAUD



INSTALL FRAUD



> *"This has truly changed how we're looking at performance from our partners and we will be applying these fraud learnings to our future relationships."*
>
> —User Acquisition Manager

TAKEAWAYS

190 THOUSAND MISATTRIBUTED **INSTALLS** UNCOVERED

400 MILLION FRAUDULENT **CLICKS** UNCOVERED