White Ops

Home goods retailer uncovers 88% fraud in campaign due to audience extension

SUMMARY:

- A home goods advertiser contracted a large video campaign to run over a holiday weekend.
- Despite having partnered with a well-known publisher, the campaign returned an 88% rate of SIVT.
- Thanks to an investigation with White Ops, the advertiser was able to secure remediation for the fraudulent traffic.

THE CHALLENGE:

An unexpectedly fraudulent campaign

Nothing is quite as frustrating as when a carefully planned campaign goes totally awry. This is exactly what happened to a national home goods advertiser that launched a major campaign over a holiday weekend. To maximize reach and spend, the brand partnered with a well-known publisher.

There is a belief in the industry that ads purchased through PMPs or direct buys are more resistant to fraud than other buys. So when the team learned — during a regular audit with White Ops — that nearly 90% of impressions from their campaign came from bots, they were extremely distraught. Uncertain of what could have gone wrong in the carefully planned campaign, the retailer reached out to White Ops to investigate.

THE SOLUTION:

Watch out for audience extension sites

Using White Ops FraudSensor and its transaction-level reports, it became clear that 90% of the campaign traffic originated from audience extension sites. To make matters worse, the traffic sourced from the audience extension sites was 97% non-human. Together, this yielded a fraud rate of 88% across the entire campaign.

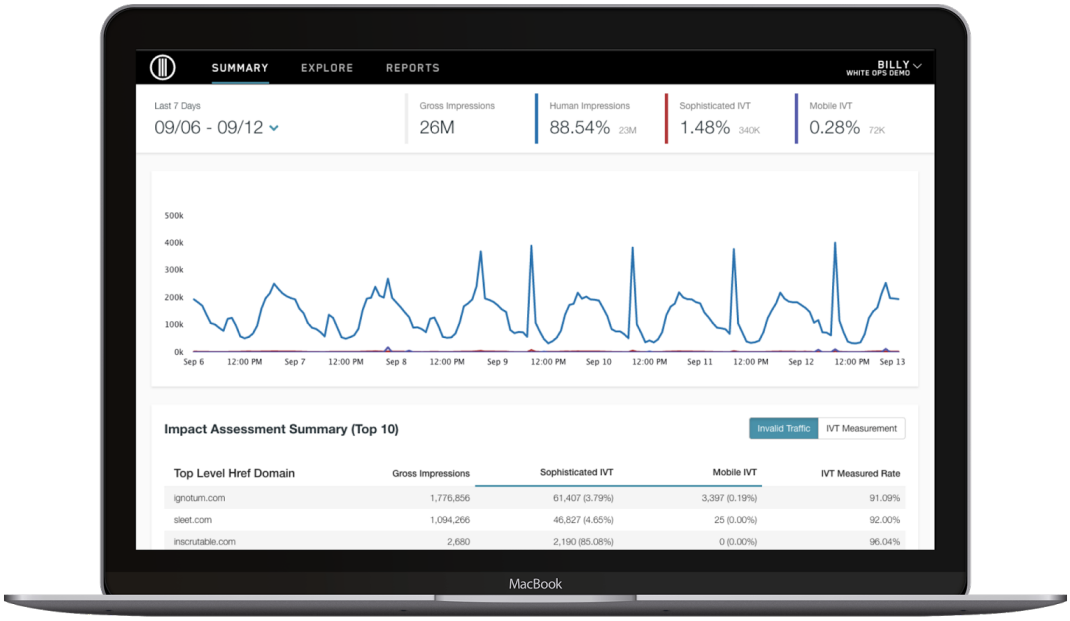
If a publisher uses an audience extension site to secure traffic at the end of a campaign, there is a good chance that bots will operate on these sites to perpetrate further fraud.

A publisher may pass the ad along to an audience extension site to fulfill campaign requirements, but these sites sometimes have little oversight from the parent publisher and may resort to purchasing traffic from suspicious sources to help the publisher meet their demands. This purchased traffic is often filled with bots, many of which are advanced enough to steal human users' cookies, which makes it easier for them to get picked up by retargeting campaigns and steal even more.

To meet the high demand of the holiday weekend, the brand had partnered with the publisher in order to access quality-owned and operated websites — but this goal failed to be met. Needless to say, the advertiser was displeased. However, armed with the data from FraudSensor, the brand was able to secure remediation from the publisher.

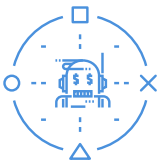
WHITE OPS FRAUDSENSOR

FraudSensor provides scalable bot detection and reporting to give you unprecedented visibility into the sources of fraud.



Gain visibility

Get insight into the scale and source of your bot problem to find the cybercriminals that hide in plain sight.



Detect & respond

Simply knowing you have a bot problem isn't enough. Ensure you use your data to prevent fraud in the future.

Streamline workflows

Automate reporting and share data with approved parties to help save time and improve your fraud fighting efforts.


White Ops