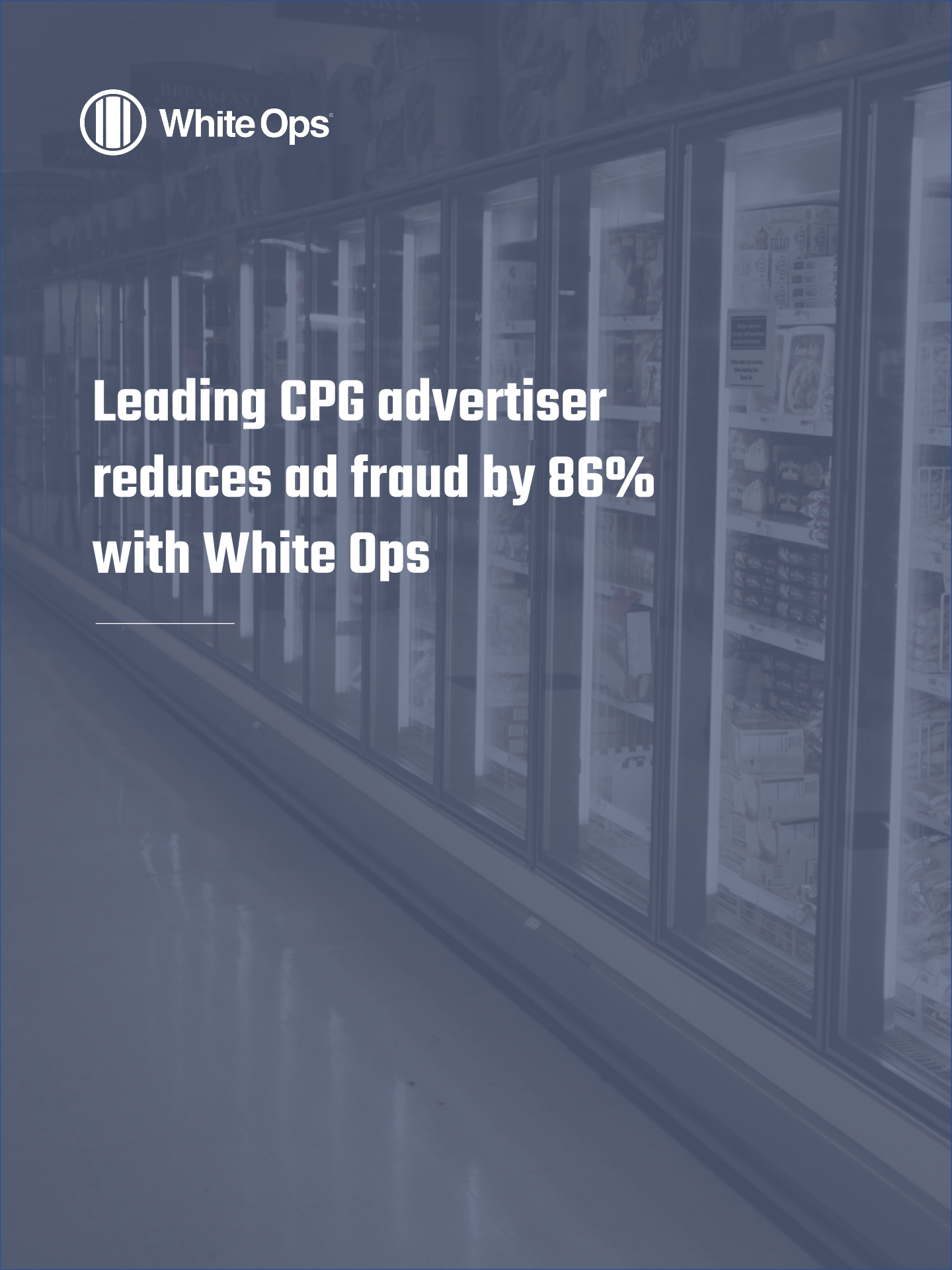
White Ops

Leading CPG advertiser reduces ad fraud by 86% with White Ops



SUMMARY:

- A top CPG brand believed its ads were protected against fraud because it had recently implemented a conventional pre-bid anti-fraud technology.
- However, after seeing suspicious activity the brand partnered with White Ops on an investigation and discovered an alarming 11% rate of fraud in the already-filtered traffic.
- Through vigilant hotspot analysis and regular blacklisting, the fraud rate has now dropped to 1.5%.

THE CHALLENGE:

Suspicious web activity

Although the CPG industry is one of the largest spenders on advertising overall — an estimated $225 billion each year — only a small percentage of the budget is spent on digital. Last year, the CPG industry spent an estimated $7.2 billion on digital advertising. This relatively small percentage is due to uncertainty about the effectiveness of the digital channel for consumer products — and that opinion only worsened when news of ad fraud hit the market.

But one leading CPG brand didn't want to cut digital without further testing. It began working with their brand safety partner to identify and counteract fraud. It wanted to ensure that its nearly $10 million digital budget was being used most effectively.

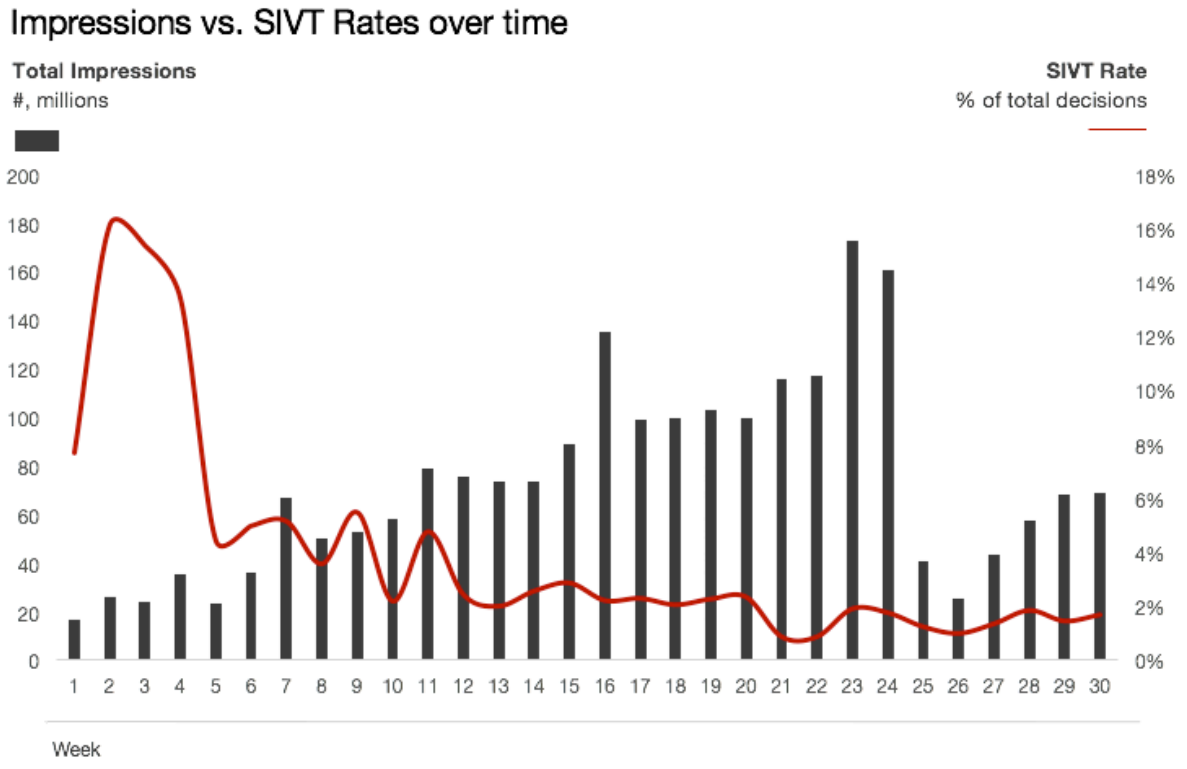
Despite being told by the partner that fraud rates were low, the brand was unconvinced. Some members of the team noted abnormal website activity and traffic sources. For example, they saw frequent visits for milliseconds to specific webpages in the middle of the night. Unconvinced that these were actions taken by real people, the advertiser approached White Ops for a second opinion.

THE SOLUTION:

Investigate & neutralize the fraud

The brand placed White Ops FraudSensor JavaScript tag on its ads and began tracking fraud. Unfortunately, the brand's suspicions were confirmed. White Ops identified over 11% invalid traffic among the otherwise "human" traffic that the other provider had verified.

Because White Ops' technology looks beyond simple anomalous behaviors, it was able to identify the traffic that looked human, but was actually automated.



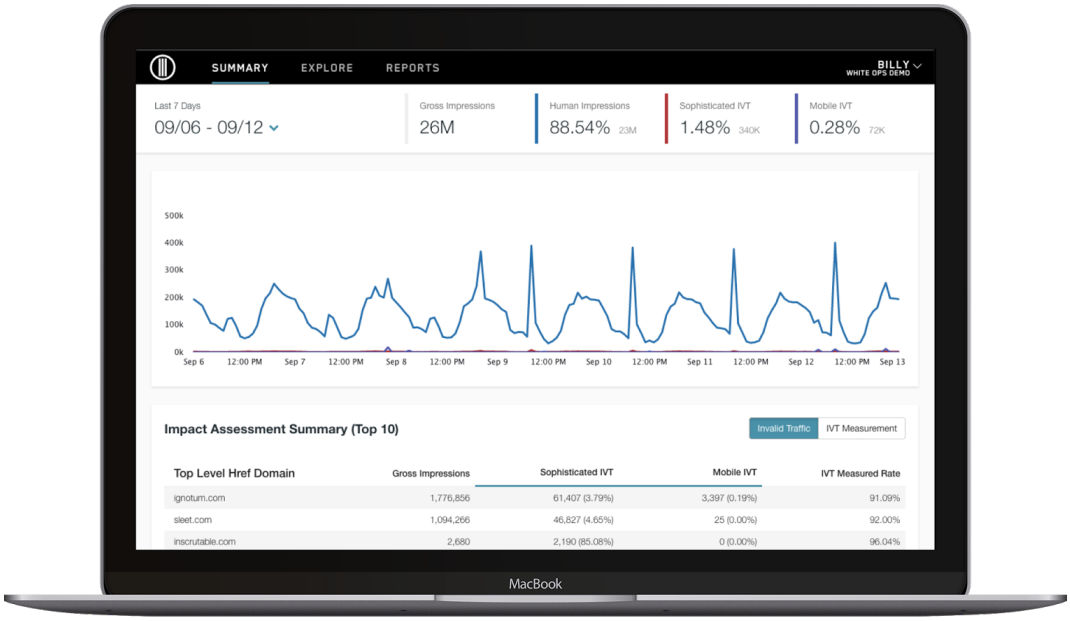
With a better handle on the real fraud threat, the CPG company began working with White Ops to eliminate the most fraudulent sources. Through hotspot analyses — a series of investigations that analyze the data in progressively more detailed ways — the brand was able to identify the source of the fraud and blacklist over 1,500 suspicious domains.

Within a few weeks, the SIVT rate fell by over 86%, effectively neutralizing the bot problem. The company has been able to maintain an average fraud rate of 1.5% and therefore returned nearly $2 million to their digital media budget.

By gaining visibility into the scale of its bot problem, the CPG company was able to determine how to fight fraud within its ecosystem and rebuild trust in digital. The company has subsequently invested more in its digital advertising strategy.

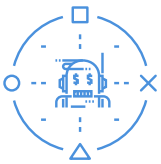
WHITE OPS FRAUDSENSOR

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