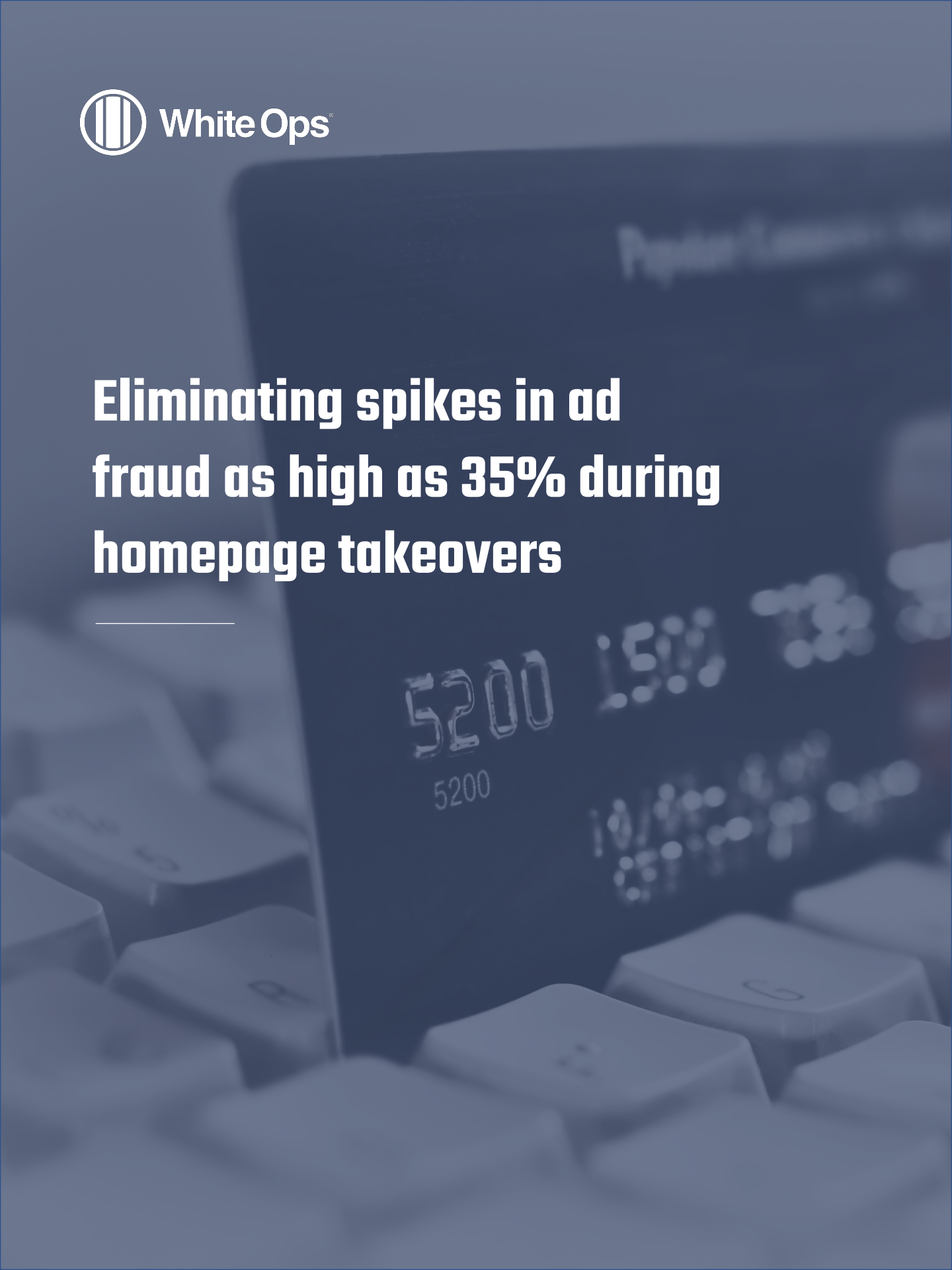
White Ops

Eliminating spikes in ad fraud as high as 35% during homepage takeovers



SUMMARY:

- A Fortune 100 financial services company couldn't figure out why one of its campaigns with a direct publishing partner was drawing surges in invalid traffic.
- They partnered with White Ops to find the source of the fraud.
- The publisher had deactivated its third-party verification system for all homepage takeovers without telling the advertiser.

THE CHALLENGE:

Sporadic fraud attacking a campaign

A Fortune 100 financial services company became frustrated with the high rates of SIVT it was receiving from a direct publishing partner. The problem was that the fraud would appeared in unpredictable surges, making it difficult to analyze and to prevent. The *average* rates of SIVT were low, but certain periods displayed unacceptably high rates. On one day, rates were seen at 3%; the following day, however, they skyrocketed to over 35%. For a company with a $35 million budget for digital media, this level of unpredictability was frustrating, and correcting it would likely be expensive.

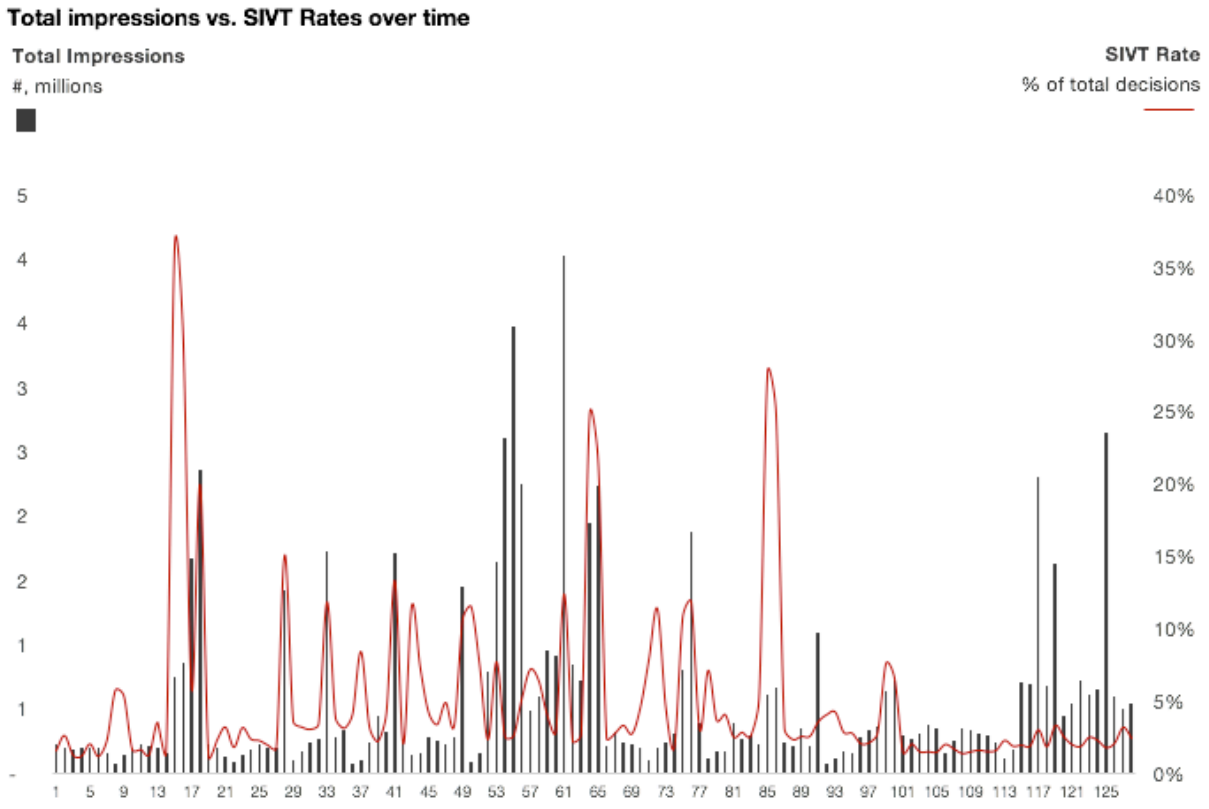
Unsure of what to do, the advertiser paired with White Ops to investigate the source of the non-human traffic.

THE SOLUTION:

Investigate & neutralize the fraud

Using FraudSensor, the financial services company collected detailed, impression-level analyses of the campaigns that drove the spikes in fraud. It became clear that the majority of non-human traffic arrived during a full homepage takeover.

Yet this information didn't fully explain the surge in bot traffic. A homepage takeover isn't necessarily more prone to fraud than any other type of campaign. With this information, the advertiser took the data to the publisher and received a surprisingly simple answer: the publisher had deactivated its third-party verification and blocking tools to fulfill 100% of the campaign impression requirements. The advertiser had been given no warning.

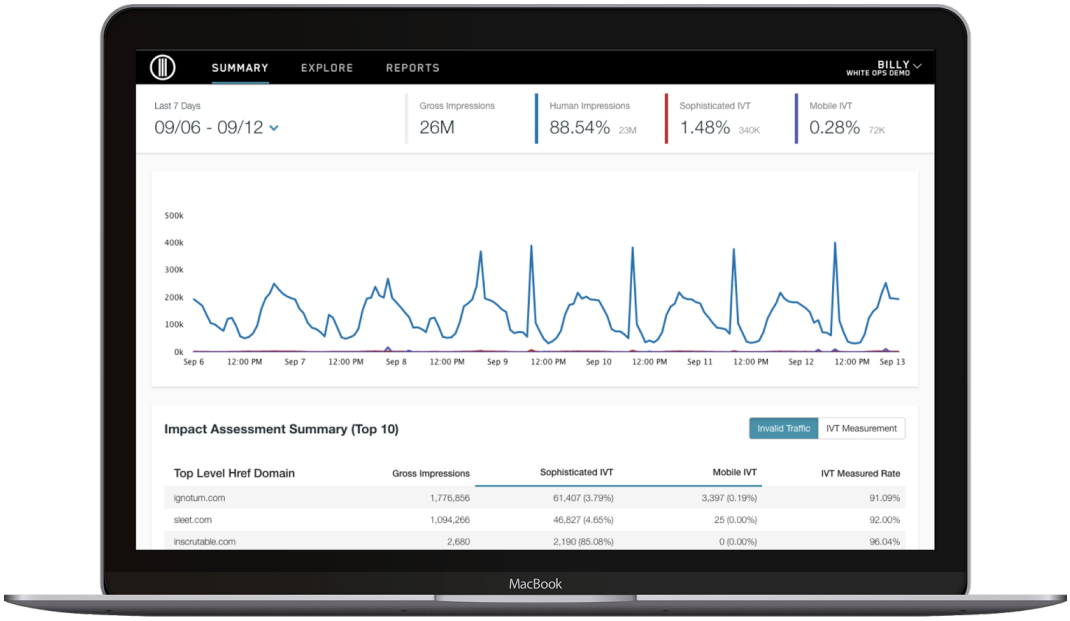


This is a prime example of why even direct buys are not immune to fraud. If the publisher practices any form of traffic acquisition or audience extension, there is a reasonable chance that bots with human-like behavioral patterns are infiltrating the publisher's domain.

The advertiser demanded that the publisher reactivate the anti-fraud tools. There was an immediate reduction in impressions from bots. Now the advertiser knows to demand verification software remain active during all stages of its campaigns.

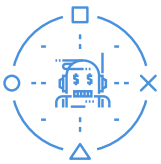
WHITE OPS FRAUDSENSOR

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