YOU'VE BEEN 'AD

Grant Simmons *advises best practices for ad fraud protection*

Ad fraudsters operate by deceiving digital advertising networks for financial gain. This usually involves manipulating performance metrics through deceptive tactics such as fake impressions, clicks and conversions. Not only does this hamper the effectiveness of campaigns, it also drains ad budgets by diverting money towards fraudulent activities instead of reaching intended audiences.

Research indicates that 22 percent of all digital advertising spend in 2023 was attributed to fraud, amounting to $84-billion. This figure is anticipated to rise to $172-billion by 2028. The shifty and intricate nature of ad fraud makes it difficult to detect and can allow deceptive behaviour to go unnoticed for long periods of time, causing significant financial ruins. A high-profile example of this is multinational tech company Uber, which fell victim to ad fraud and was forced to process over 58-billion records to uncover false marketing campaign results. The organisation then had to find a way to recover millions in damages. To address these risks and prevent similar incidents, businesses should consider the importance of adopting proactive and comprehensive strategies among advertisers.

FRAUD BLOCKLISTING CAN BE USED TO PROTECT CAMPAIGNS ACROSS DIFFERENT APPS

First and foremost, companies need to understand the various forms that ad fraud can take. Domain spoofing, for instance, entails disguising poor-quality or fake websites as premium ones to trick advertisers into bidding on their inventory. Ad injection takes place when unsolicited or unauthorised ads are incorporated into genuine websites using browser extensions, ransomware and network proxies. Click fraud happens when false clicks are produced on an ad with the help of bots or malware, while impression fraud involves inflating the number of times an ad is displayed through bots, illegitimate sites and hidden pixels.

Dealing with each type of ad fraud requires a certain degree of finesse. Advertisers need to harness state-of-the-art detection technologies that can quickly spot and inhibit fraudulent conduct. For example, fraud blocklisting can be used to protect campaigns across different apps. This strategy involves creating and maintaining a comprehensive list of known fraudulent entities, such as suspicious IP addresses, domains or app IDs. Any traffic that goes against the installed blocklist is regularly flagged and excluded from being counted as a valid conversion. This helps advertisers to swiftly react to new fraud patterns and ensure that only genuine interactions are considered, which keeps the accuracy of campaign performance data intact.

Setting guidelines for campaign traffic also plays an important role in safeguarding the integrity of advertising initiatives. Marketers can define criteria based on factors such as device type, location and campaign dates to ensure that traffic aligns with their standards. This helps to prevent any discrepancies or irregularities from being overlooked.

Tackling risks such as SDK spoofing, where false data is transmitted to mimic user interaction, is another highly recommended strategy. Detecting and preventing deceptive data in this context allows advertisers to avoid making payments for conversions, thereby guaranteeing that their marketing budget is allocated towards authentic user engagement.

Advertising fraud is a surprisingly complex issue that calls for equally complex solutions, while the cost of mobile ad fraud is rising exponentially each year and fraudsters aren't showing any signs of letting up in their attempts to steal from ad budgets. The growing sophistication of ad fraud schemes means relying solely on basic detection methods is no longer sufficient to combat increasing threats. In order to shield campaign successes and reserve budgets, advertisers must employ a comprehensive strategy that combines technology, transparency and continuous oversight. When following practices such as blocklisting, configuring advanced traffic rules and accurately detecting spoofed data, advertisers can considerably reduce the risk of ad fraud and get the most out of their marketing efforts ●

Research indicates that 22 percent of all digital advertising spend last year was attributed to fraud

Grant Simmons is VP at Kochava Foundry.