AMERICAN MARKETER

Business at its best

MARKETING

Ad fraud is rapidly evolving and the threat is serious

February 28, 2019

Gil Meroz is vice president of innovation at AppsFlyer

By Gil Meroz

Ad fraud is a booming industry.

Late last year, the United States Department of Justice announced indictments in the federal government's largest ad fraud investigation to date a significant win against malicious actors, but merely one step in confronting a threat landscape that has evolved to reflect changing user consumption patterns.

The news came on the heels of a major investigative report in BuzzFeed recently exposing a massive scheme in which more than 125 applications and Web sites created fake traffic and defrauded advertisers of up to $750 million.

Beyond its scale, what is most alarming about the multibillion-dollar ad fraud industry is its sophistication.

No play-acting
Fraudsters are becoming increasingly skilled in their operations and deploying bots that effectively mimic the behavior of how real users interact with their smartphones and mobile devices, compounding the difficulty of rooting out fake activity.

How should advertisers respond to this proliferating threat?

Multi-layer security provides the only viable path forward for an industry facing a grave threat from the fraudulent activity of a few malicious actors, whose skill and revenue generation are disproportionate to their actual numbers.

The basic idea is simple.

Most of our homes feature several layers of protection. Some combination of locks, security codes, alarm systems, gates and even pets help thwart home invaders before they can cause harm.

Similarly, marketers' livelihoods in the age of massive fraud require a comprehensive approach to security and fortification from a fundamental awareness of the severity of different threats to the implementation of cutting-edge technologies that can analyze user behavior at scale, identify emerging patterns to flag suspicious activity, and technologies that can analyze user behavior at scale, identify emerging patterns to flag suspicious activity, and continuously enhance defense mechanisms that detect new types of fraud schemes and block attacks.

Failure to meet the ad fraud threat head-on will carry consequences that extend far beyond billions of dollars in stolen revenue each year.

Bots up
Fraud also contaminates crucial data and insights that businesses rely on to make decisions.

The longer the threat festers, the greater the strain will be on the resources, the relationships and trust between brands and their marketing partners. Deplete those resources and that trust among partners, consumers and in the information used to make data-driven decisions and business models collapse.

With bots now accounting for the bulk of mobile ad fraud and with estimates of "click fraud" pegged last year at around one fifth of all clicks on ads proactive measures to combat these malicious activities are sorely needed.

As bad actors continue investing heavily in computing power, acquiring apps to learn how real users behave and making real in-app purchases to boost their efforts at deception, fraudsters are pocketing increasingly large payouts from their schemes.

The savviest marketers will be vigilant by staying aware of the latest trends and vulnerabilities being exploited.

Additionally, they will leverage massive data sets and tools with machine-learning and artificial intelligence capabilities to identify threats and fight back.

Behavioral analysis can examine traffic to better understand intricate patterns and flag potentially problematic cases.

For example, do the devices from which a site's traffic comes tend to be static? That is a telltale sign of a "device farm."

Has there been an abnormal event, such as an app install taking place within seconds of an ad appearing?

Despite surging traffic, do a suspicious volume of users stop short of actually converting?

These are all red flags.

It follows, then, that marketers must ensure that they are intimately familiar with their key performance indicators (KPIs), otherwise they will have difficulty discerning between fraudulent and legitimate activity.

Advertisers should work to fraud-proof their KPIs as much as possible and each layer of protection from a heightened level of awareness to being smart about measuring the right metrics to leveraging the best technological tools available is crucial to battling the full gamut of fraudulent activity.

And if bold action is not taken? The costs will be astronomical.

Adds up
The billions already wasted in annual ad fraud will look like peanuts compared to what the World Federation of Advertisers forecasts for 2025: $50 billion in annual ad fraud, translating to some $137 million in fraudulent activity each day.

Given how rapidly the ad fraud menace has evolved a pattern that is sure to continue for the foreseeable future it is imperative that marketers act today to combat the most prevalent forms of ad fraud, identify potential weaknesses in their defenses, and build cultures of vigilance.

MOBILE AD FRAUD did not emerge overnight, and it will not be eradicated quickly, either. But it threatens to do irrevocable damage and sap billions of dollars in revenue much faster.

The sooner that stakeholders meet this challenge head-on, the better off all marketers, brands, and consumers will be.

Gil Meroz is vice president of innovation at AppsFlyer, San Francisco.

American Marketer is published each business day. Thank you for reading us. Your feedback is welcome.