

Fighting digital ad fraud

BY JOTHAM LIM

DIGITAL advertising fraud has been plaguing the advertising industry both locally and globally for the longest time, and it is expected to remain an issue in the foreseeable future.

According to estimates by the World Federation of Advertisers (WFA), the leading global trade body for advertisers, marketing spend lost to advertising fraud is likely to reach US\$50 billion (RM207.8 billion) annually by 2025. And that is just a conservative estimate. Without proper countermeasures in place, advertising fraud revenues may amount to US\$150 billion a year in the same time frame.

Also known as ad fraud, digital advertising fraud refers to impressions, clicks, conversion or data illegitimately acquired to earn revenue, or for other purposes of deception or malice.

Malaysian Advertisers Association (MAA) president Kadri Mohamed Taib says even though WFA highlighted these issues through a compendium released in 2016, ad fraud has continued to proliferate and shows no sign of abating.

"With tools such as click bots, pixel stuffing, malicious apps and more, ad fraud has evolved in such a way that it can impact every element of digital advertising, from evolving advertising mediums to leading the erosion of media investment across multiple platforms," says Kadri.

"Click fraud will become so rampant that it will cost advertisers more than US\$50

billion by 2025 globally. WFA advises brands to apply caution to digital investments until the advertising tech sector deals with the problem more effectively."

MAA is a trade body representing the interests of advertisers in Malaysia. It is also a member of the WFA. Its vice-president Claudian Navin Stanislaus points out that advertisers are the ones most adversely affected by the rising cases of ad fraud in the country.

"If you look at the entire ecosystem, the real victims are always the advertisers. This is because, despite the money we are spending on advertisements, they are not reaching the intended audience. So, everyone in the entire ecosystem still gets paid while the advertisers, who are paying for everything, don't get anything anything out of it," he fumes.

According to Navin, the thriving digital advertising industry is a key driver of ad fraud in Malaysia. The country's internet penetration rate is currently above 90%, a significant jump from 70.72% half a decade ago. This has attracted more advertising spend on the platform but, at the same time, it has attracted fraudsters as well.

"The more people switch to digital platforms, the more fraud cases there will be. This is because fraudsters do not [bother with] a platform that does not have viewers. If there were no viewers, advertisers would not be spending money there. And if there is no ad spend on the platform, there will be no way for fraudsters to benefit from it," says Navin.

In Malaysia, digital ads account for only about 25% of total advertising spend, whereas in the US, it accounts for 50%. But as digital ad spend grows in the country, so will the number of fraud cases, Navin notes.

There is another reason that ad fraud is so rampant: It falls into a legal grey area, as there is no law, whether locally or globally, to govern it, Navin points out. What this means is that even if the fraudsters are caught, it is difficult to prosecute them.

In September 2017, US-based e-hailing service Uber sought US\$40 million in damages from Fetch Media, alleging that the media agency had billed Uber for fake clicks on its online advertisements through a **pay-per-click model**.

This is an important lawsuit, says Navin, because it is the first of its kind and will set the precedent for future ad

fraud lawsuits. Uber withdrew its suit in late December that year, however, and was later countersued by Fetch Media for US\$20 million worth in unpaid bills. The case remains unresolved at the time of writing.

Navin says there are no similar lawsuits in Malaysia, and advertisers are left with little option but to resolve these issues privately. He adds that there should be regulations providing legal protection for advertisers against ad fraud.

"We have about 40 different regulations and codes governing advertising standards in Malaysia to protect consumers. Many of these affect the way we advertise, all of which we have to comply with," he says.

"Here, we have an actual problem that costs us money, and we are asking for regulation to help protect us. This will require a lot of effort not just from the government, but from international bodies as well."

Andrew Lee, president of the Association of Accredited Advertising Agents of Malaysia (4As), notes that ad fraud is widespread because of its low barriers to entry. Fraudsters are able to run their operations outside the country's borders and need only basic technical knowledge to operate.

Lee cites the example of streaming fraud. On the popular music-streaming app Spotify, artists are paid based on the total number of streams, or plays, of their content. The fraudsters would set up hundreds of free accounts to play their own content and the accompanying advertisements, illegitimately acquiring revenue.

PAY-PER-CLICK (PPC)

PPC is an internet marketing model, in which advertisers pay a fee each time someone clicks on one of their advertisements.

At a glance

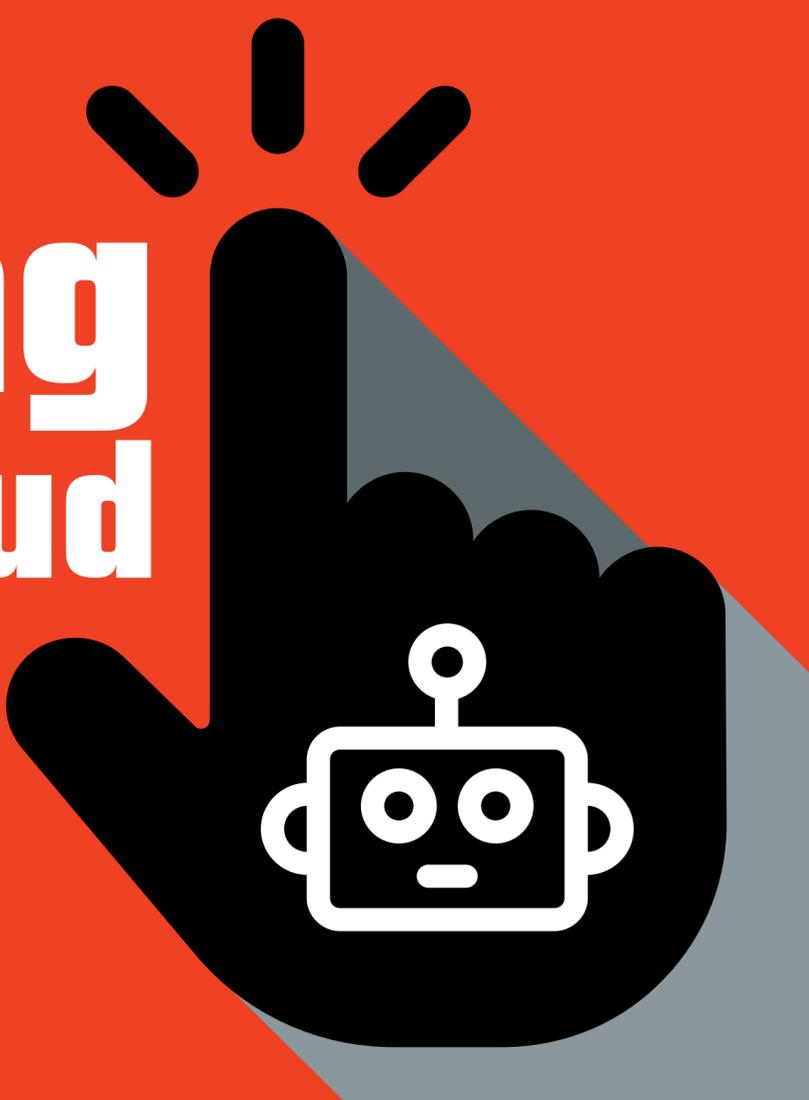
- 1 The amount of money lost to digital advertising fraud is likely to reach US\$50 billion (RM207.8 billion) annually by 2025 and this is a conservative estimate. This is likely to triple without countermeasures in place;
- 2 Digital advertising fraud is in legal limbo, as there is currently no local or international law that governs it directly; and
- 3 Two solutions to effectively combat digital advertising fraud would be to optimise advertising campaigns and use ad tech solutions.

44 With tools such as click bots, pixel stuffing, malicious apps and more, ad fraud has evolved in such a way that it can impact every element of digital advertising."

Kadri

44 Everyone in the entire ecosystem still gets paid while the advertisers, who are paying for everything, don't get anything anything out of it."

Navin



CHECKLIST TO MITIGATE DIGITAL ADVERTISING FRAUD

- 1 **Use verification and ad fraud solutions:** Use solutions that confirm the ads were delivered to the right place and to the right audience;
- 2 **Look for accredited fraud solutions:** Use solutions that have been accredited for both general and sophisticated invalid traffic (IVT);
- 3 **Mitigate the risk of paying for fraudulent impressions:** Ensure that the agency has agreed on contractual terms with publishers on make-goods for invalid traffic;
- 4 **Use pre-bid filtering to avoid fraud in programmatic buys:** Pre-bidding is a service that predicts the advertising viewability before making the placement bid;
- 5 **Be wary of deals that are too good to be true:** Focus less on low cost per mile (CPM) and more on key performance indices (KPIs) tailored to campaign goals; and
- 6 **Use exclusion lists for fraud:** Prepare or search for a list of fraudulent publishers and companies to avoid.

SOURCE: WFA

audience. So, no matter how fantastic your creative vision is, if nobody sees it, the advertising campaign has failed."

Lee says an enabler for ad frauds is programmatic buying, where ad slots are purchased automatically using a software application according to parameters set by the marketers.

Because these software applications automatically purchase advertisement spots based on the volume of traffic a website receives, fraudsters are able to artificially inflate their visitor figures using clickbots and extract dollars from the advertisers.

To resolve this issue, Lee explains that marketers should pay closer attention to the parameter settings, and optimise their campaigns by clearly specifying the publishers they wish their advertisements to appear in.

In a media quality report published by Integral Ad Science, advertising fraud made up 6% to 11.9% of non-optimised advertising spend as at 2H2019, and the figure is increasing yearly. Optimising the advertising campaign can, however, reduce the advertising fraud rate to between 0.5% and 1.1%.

"For example, if I were to create an advertising campaign without specifying where the advertisement should appear, it will then rely on the bot to make the decision. Out of a RM1 million budget, a portion may go to a random app where nobody sees the ads," Lee says.

"But, realistically, you cannot completely ignore programmatic buying and rely on manual media buying. There will always be a need to have programmatic buying because of benefits such as audience retargeting. What marketers can do is to have a blacklist — websites or these apps that I don't want my ads to appear in."

Lee adds that the Communications and Multimedia Content Forum of Malaysia (CMCF) has a blacklist of unscrupulous websites with pirated content, fake news and the like, which is sent to advertisers and media agencies to warn them not to place advertisements on those sites.

"The idea is to starve them of advertising revenue, so that there is no way for them to continue to fund their operations. They survive because, right now, advertisers around the world are supporting them unknowingly."

While ad fraud is a growing concern among advertisers, president of the Media Specialists Association (MSA) Chanchal Chakrabarty says Malaysia has one of the lowest risk rates of ad fraud in Southeast Asia. Even lower, he claims, than Singapore.

"This is because the local publisher landscape in Malaysia is not large. There are very few local competitors, and the majority of digital advertising happens on only two major players — Facebook and Google," says Chanchal.

"Therefore, Malaysia is not a very fertile ground for fraudsters. Ad fraud generally happens in markets where the local publisher ecosystem is large but does not have the capability or the tech to create clean inventory."

MSA is a trade body that primarily represents the interests of media agencies in Malaysia. Chanchal explains that ad fraud is actually part of a larger industry challenge in the form of

AD-STACKING

Ad-stacking is an ad fraud tactic in which digital advertisements are stacked on top of each other, which registers as multiple views instead of a single view.

PIXEL STUFFING

Pixel stuffing is an ad fraud tactic in which an advertisement is shrunk to the size of a single-pixel or a small size, and is counted as a view despite not being legible.

BAV — brand safety, ad fraud and viewability.

In brand safety, marketers try to ensure that advertisements do not end up on non-brand-friendly platforms such as terrorist or pornographic websites. In terms of viewability, at least 50% of the advertisement must be displayed for at least two seconds to be classified as viewed as per industry standard, according to Chanchal.

He says despite the low fraud risk in Malaysia, the country still struggles with brand safety and viewability. Several ad fraud tactics, such as **ad-stacking** and **pixel stuffing**, are also linked to an advertisement's viewability. Fortunately, there are several ad tech solutions in the market that help address the BAV challenge.

Integral Ad Science (IAS) and DoubleVerify are services that analyse and verify the value of digital advertising placements, to ensure that the advertiser gets the most bang for its buck. IAS, for example, has an advertising quality scoring system that assesses the quality of an advertisement placement using multiple metrics.

"To avoid ad fraud, you need the technology. However, the majority of local advertisers do not use these solutions," says Chanchal.

"These solutions are generally adopted by only global advertisers, such as Unilever's Procter & Gamble, which has its own programmatic buying unit. But if you are buying advertising spots through advertisement exchanges, the majority of them do not use these tech solutions."

He adds that many trusted programmatic buying units or some trusted advertisement exchanges have these technologies integrated into their system and they are accessible to advertisers.

Chanchal believes that if the entire advertising industry were to adopt these solutions and make them the default option, ad fraud cases would drop dramatically. He warns, however, that there is a limit to the effectiveness of such tools.

"It's like a flu shot, which will help you cover only a few flu strains, never all of them. Even if you take a flu shot, you can get the flu because it might be from a different strain," he explains.

"The same goes for ad fraud. The space is constantly evolving and fraudsters are always in the process of coming up with new tactics. Even if you have the tech, you cannot be 100% sure you can avoid all possible types of ad fraud. Therefore, these tech solution providers are also constantly evolving and coming up with ways to defeat these new tactics. It's a cat-and-mouse game."

Chanchal encourages advertisers to purchase advertisement spots directly from trusted and reputable publishers instead of through advertising exchanges, where there is a higher risk of falling victim to ad fraud.

MSA has also been active in conducting supply summits, where publishers are gathered and taught global best practices on how advanced markets have improved their advertisement inventory.

"As an industry, we currently lack caution. That is why the use of these fraud detection solutions is so low, and that is the first thing that needs to change. If advertisers are cautious about this, good money will be placed behind quality advertising space," Chanchal adds.

44 No matter how fantastic your creative vision is, if nobody sees it, the advertising campaign has failed."

Lee



44 The space is constantly evolving and fraudsters are always in the process of coming up with new tactics."

Chanchal