YOUR GUIDE TO AD FRAUD IN SOUTHEAST ASIA AND INDIA

AUTHORS

Kaixin Kang, Client Solutions Manager, LinkedIn

Rishi Bedi, Vice President, SEA, Japan and Korea, InMobi

Shane Dewar, Vice President, Media Operations, APAC, Essence

INTRODUCTION

Cybercrime is not an unfamiliar term to the general public, but most would associate that with data loss, email scams, or credit card fraud. However, there is another fraud that is even more common in our daily lives and one that those outside of our industry have little awareness of - ad fraud.

Ad fraud has been around almost as long as the internet space has been present. We have seen digital ad fraud transforming from simple deeds like over claiming impressions into more sophisticated activities that are even more malicious and very well hidden. In the recent IAB SEA+India Regional Brand Safety Landscape survey, we learnt that ad fraud is seen as a technical topic and understood better at senior management levels in the digital advertising industry of Southeast Asia and India. While ad fraud is not a new topic the sophistication of the modern day "white collar" criminals remains a constant threat to the digital advertising space.

There are more than 360 million internet users across Southeast Asia, making it a juicy target for fraudsters. Overall estimates of digital ad fraud vary widely as it is difficult to measure its true impact. However, according to TrafficGuard, an estimated $17 Million USD is lost to ad fraud every day in APAC. With Southeast Asia being one of the growing markets in the digital space and with a growth rate that far exceeds the technical expertise within the market, there's a gap in knowledge between junior and senior levels as well as inconsistencies in regards to ad fraud engagement and performance metrics.

This paper serves as a guide to the basic elements of ad fraud, with the aim of educating the reader and improving understanding of the unique challenges faced in the Southeast Asia landscape as well as some tips on how to face these challenges.

TYPES OF AD FRAUD

The landscape of ad fraud is continuously evolving and fraudsters are getting creative with their approach to mimic more real world consumer behaviours. Many newly discovered bot fraud methodologies are just old botnets using new fraudulent methods. The same culprits that used malware last year to generate nonhuman impressions can, this year, use fraudulent mechanisms to spoof desktop impressions as premium CTV. While bots are the most commonly known type of fraud, they are not the only species of fraud in the ecosystem. To understand this complex nether world, it is critical to distinguish between core types of ad fraud which are broadly classified as General Invalid Traffic (GIVT) and Sophisticated Invalid Traffic (SIVT).

GIVT broadly refers to traffic that is not generated by a human but can be routinely filtered by using blacklists or standard parameter checks. This generally means known, self-declaring bots or webspiders, known data center IP addresses and known browser user agents (i.e. if an impression has an unknown user agent, it's flagged as GIVT). In other parts of the world, IABs and other industry bodies have developed collaborative lists which are available to simplify the detection and management of such traffic. Many of the 3rd party verification platforms also have similar lists available. It's generally accepted across the digital advertising ecosystem that impressions generated by those on the GIVT lists are easily identified and hence are not billed.

Any proprietary Fraud/IVT detections that go beyond the definitions of GIVT are considered SIVT. SIVT broadly refers to traffic that requires advanced analytics, multi-point confirmation or human intervention to be identified as invalid. Below is a list of different types of SIVT -

BOT FRAUD

The most well known type of ad fraud, and in the IAB SEA+India's Regional Brand Safety Landscape, this was called out as the highest form of fraud witnessed in the region. This type of fraud occurs when bots masquerade as real human users. Serving impressions to bots is about as effective as serving impressions to cardboard cutouts of celebrities. One interesting nuance about bots and bot activity is that it is very short lived. Bots are known to live on average for 72 hours and produce the highest number of fraudulent impressions within the first 24 hours.

Infected devices are common, and many users do not know that they are affected and that their devices are controlled. This in turn creates 'Botnets', where these devices contribute to a network of devices that all run malicious software or malware and can be hijacked to commit ad fraud. As malicious software is placed on the devices of unsuspecting users, this means that they aren't aware that their device is being used to commit fraud. Botnets can siphon thousands of ad dollars through schemes like falsified websites or massively inflate traffic to legitimate websites.

SITE FRAUD

Site fraud is committed by bad actors who generate fraudulent quality views on websites with little to no traffic. The most common type of site fraud is impression laundering and domain spoofing.

- **Impression laundering:** similar to its distant cousin money laundering - conceals the actual URL where an ad appears by using 'front sites' that mask themselves as legitimate publishers, in order to monetize ad impressions that otherwise wouldn't be bought by brand advertisers.

- **Domain spoofing:** when an illegitimate site masquerades as a legitimate site in order to win the ad dollars. The underlying users and impressions are real and spoofing as a premium publishers makes these impressions more valuable than they are in reality. This type of fraud affects both buyers and sellers of inventory; Advertisers think that they are buying premium inventory, but in reality the inventory does not exist on the premium site and there is no quality control over it. On the other hand, publishers lose credibility on their inventory.

Both kinds of fraud sound similar as they are misrepresenting domains; the difference is that domain spoofing is intentional misrepresentation of the domain by a low quality publisher who intends to monetise the ad slots, but declares itself as a higher quality URL to be served ads intended for higher quality inventory.

Impression laundering is more sophisticated. When you load a web page the user can only see one frame but in reality that screen the user sees is made up of several layers of frames called iframes. Impression laundering occurs when ads are rerouting through a series of iframes, resulting in the ad appearing on a lesser quality site than the one it was originally meant to appear on.

APP FRAUD

With a rapid increase in content consumption within in-app environments, advertisers now pay more attention to this channel, and as a result fraudsters have followed their way in. Global app fraud rates have seen a steady increase in recent years. Scammers use methods like hidden ads and app spoofing to defraud advertisers in the in-app space.

- **Hidden ads:** ads run silently in the background of an app and are invisible to the user, therefore providing no benefit whatsoever to the advertiser.
- **App spoofing:** a little more nefarious and occurs at the exchange level. Advertisers are duped into buying inventory from poor quality apps that are published on the exchange as premium apps.

NON-HUMAN DATA CENTER TRAFFIC

Nonhuman data center traffic impressions are those that originate from facilities used to house computer and server systems, e.g., traffic originating from a cloud-computing data center. While nonhuman data center traffic is not necessarily fraudulent traffic, it is often considered invalid in the industry because it represents impressions that are not served to a human user.

ADWARE/ MALWARE

These are impressions served by devices infected with a virus or malicious software that takes over a user's browser to generate ads. The most common types of Adware/Malware are:

- **Injected ads:** impressions independently inserted into the user's browser by adware and/or malware overriding or disrupting publisher-served impressions. The result is that there are constant ad calls on the page and the site is bombarded with ads - mostly on one top of another.
- **Hijacked devices:** impressions on apps or browsers infected with adware/malware, which are the usual entry point to becoming part of a botnet. These devices will mimic a user to generate a mix of injected ads and impressions appearing to originate from a publisher.

AD FRAUD IN SOUTHEAST ASIA AND INDIA

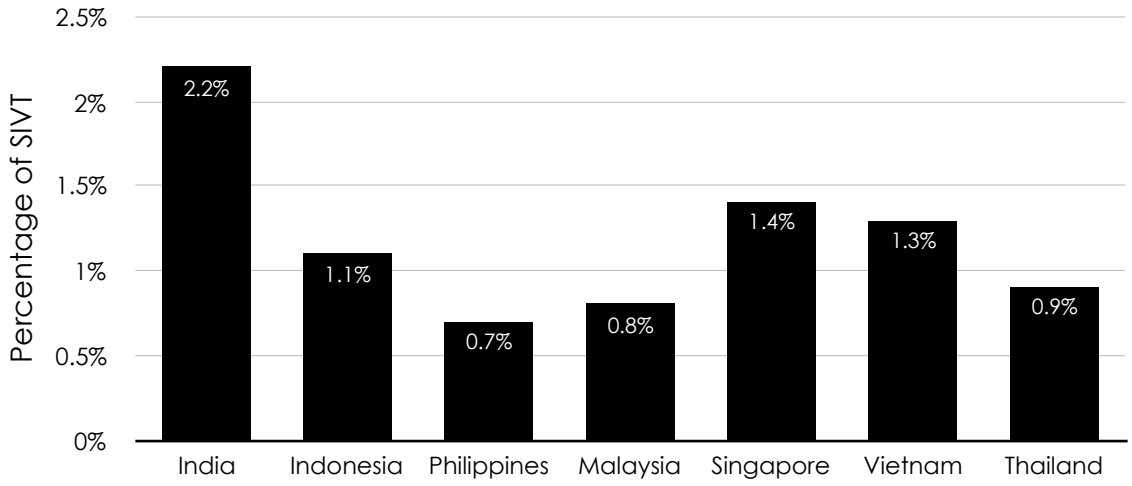
APAC's digital ad spend was projected to reach nearly half of all ad spend in 2019 according to forecasts by Dentsu Aegis Network at the start of the year. With the explosion of digital ad spending comes a huge potential for ad fraud.

Here's a summary of the approximate volume of SIVT detected in SEA and India for a 6 month period in 2019, derived from data provided by Integral Ad Science and DoubleVerify specifically for this whitepaper.

With a growing digital population and explosion in smartphone penetration in the region, brands are spending exponentially in digital, particularly in the In-App channel, giving more reasons for fraudsters to be active.

Besides being the 2nd largest digital consumer base in the world after China, India's digital consumers and media spends are also growing at breakneck speeds. This explosive growth has a direct impact on the growth of content consumption and digital ad spends. The ongoing battle for e-commerce market share, just to name a major vertical, makes it lucrative for fraudsters to use this opportunity to make as much revenue from the ecosystem.

FRAUD LEVELS BY COUNTRY



Source: Integral Ad Science and DoubleVerify figures for a 6-month sample in 2019

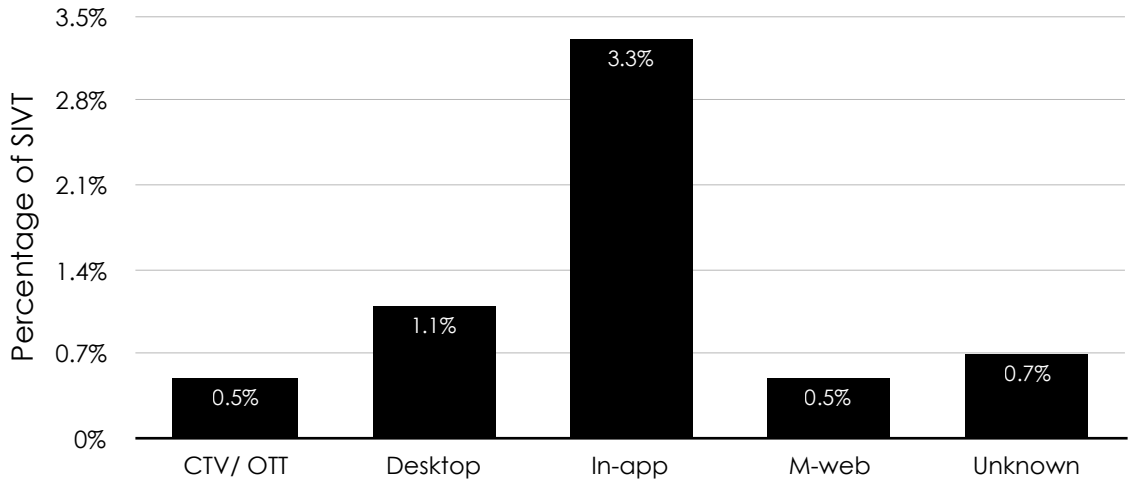
Indonesia and Vietnam, as the two fastest growing digital economies in Southeast Asia also show the second and third highest rates of SIVT , indicating that fraudsters are following the money and momentum.

Generally speaking, the most common types of fraud in the region are not surprising:

- Bots and non-human traffic designed to mimic users and inflate audience numbers.
- Domain spoofing, a specific form of app or site fraud where HTML or an ad request that attempts to represent a site, device, etc. other than the actual placement. This tricks advertisers and ad exchanges into thinking the inventory is legitimate. This is also called domain laundering.
- Incentivised browsing, when a human user may be offered payment or benefits to view or interact with ads or generate traffic on ad-supported sites.
- Proxy Server Traffic that is routed through an intermediary proxy device or network where the ad is rendered in a user's device where there is a real human user.

Being one of the regions with the highest mobile penetration, it's natural that mobile fraud is abundant in Southeast Asia and India. In a recent study released by DoubleVerify, mobile ad fraud, especially In-app fraud, tops the charts among the different device channels in APAC.

FRAUD LEVELS BY CHANNEL



Source: Integral Ad Science and DoubleVerify figures for a 6-month sample in 2019

The study also showed that common ad tech tools like keywords, contextual targeting and whitelisting, which are easily adopted and implemented on digital campaigns, have helped to lower the percentage of ad fraud on web publishers. Limitations on mobile in-app ad fraud verification tools - added to the constant release of new apps - means that it's technically challenging to lower the percentage of ad fraud in the in-app environment. With 90% of Southeast Asia's 360 million internet users primarily connecting to the internet through their mobile devices, it's no wonder that the in-app environment is a key target for fraudsters.

Nonetheless, it's a common trend that ad fraud prevails globally, not just in Southeast Asia and India region, and it's not going to just disappear. Fraudsters are getting smarter and faster. There are no tools for us to remove it completely, and it is having a huge impact in both campaign performance and ad spends. Despite understanding all these, combatting ad fraud is often seen as optional rather than a necessary arms race.

INDUSTRY BARRIERS IN ADOPTION ACROSS SOUTHEAST ASIA AND INDIA

As digital ad spend grows at a rapid pace in the Southeast Asian and Indian market, the incentives for malicious agents to innovate and find new fraud mechanics are growing too. The combined region is a key target for fraudsters due to its size, growth rate and relatively low investments in technical tools or talent. This underlines a far greater need for digital marketers to deploy fraud detection and prevention measurements, however the adoption of tools and measures to curb fraud has been significantly low in the region, as shown in the IAB SEA+India Regional Brand Safety Landscape survey. There are various factors contributing to this:

- **Low awareness in the industry:** there is a general lack of awareness around sophisticated ad fraud within the wider digital marketing industry, and ad fraud is largely understood only at more senior levels on the brand and agency side. The aforementioned survey by IAB SEA+India confirmed that there are significant inconsistencies in the understanding of ad fraud and revealed that it is not considered as an essential skill or area of understanding. The survey revealed that whitelisting is still the most commonly used fraud prevention method, which is not sufficient for detecting sophisticated fraud.

- **Technical challenges:** ad fraud is still considered to be a technical area of expertise across our industry. The same IAB SEA+India survey revealed that only about half of the industry really has an appreciation and understanding of ad fraud in their roles. This means that it is a topic where expertise is reserved to those in more technical roles, adtech platforms or senior positions at agencies. Brand managers, media planners and client-facing staff at platforms in the ecosystem do not have the same exposure or in depth understanding of the complexities of fraud and the corresponding tools available to combat each of these fraud types.

- **Misplaced success and cost metrics:** increasing ad spend on digital channels has resulted in a surge in 'bad actors' that lure marketers into buying fraudulent inventory. These ads normally perform well, showing high click-through rates (CTRs) and high viewability as compared to genuine sources of inventory. These misunderstood success metrics drive marketers to focus on quantity (reach and engagement) more than quality - meaning they often end up overlooking the threat of ad fraud.

- **Media to Verification cost ratio:** battling fraudsters with the help of advanced tools from 3rd party measurement platforms requires a deep appreciation of the impact of fraud on overall media spends before a cost decision can be made. In mature markets where media CPMs can be significantly higher than in our region, the cost of verification is a much smaller proportion of the overall media cost. In our region, media CPMs can be much lower and hence the verification costs are looked upon as an additional overhead. Inconsistent approaches, a lack of understanding coupled with a notion of additional costs, becomes a barrier to adoption of ad fraud verification tools.

- **Inconsistent measurement benchmarks:** the IAB SEA+India survey revealed that there are significant inconsistencies around the basic understanding of different types of ad fraud. Ad fraud is considered an area of technical expertise and intermediaries, i.e. adtech platforms and agencies, are expected to take the lead in detecting fraud through third party vendors. Ad fraud is also understood better by the more senior employees at these organizations, and as mentioned above, only half of the survey respondents from these organizations indicated having experience with fraud in their roles. As a result, it is mostly 3rd party verification technology providers who invest effort into spreading awareness of ad fraud across the industry, using their own insights and benchmarks. This has the effect of leaving the industry with inconsistent messaging about definitions and measurement definitions. The absence of a common voice or standard benchmarks around definitions and measurement increases the inconsistency across the ecosystem resulting in lower adoption of these tools.

WHAT ARE THE WAYS TO COMBAT AD FRAUD?

So how can we work together as an industry to combat ad fraud, in all its many forms? Especially as the recent IAB SEA+India Regional Brand Safety Landscape survey highlighted the fact that a limited amount of respondents had experience with ad fraud, and that instead it is covered by the more-technically-orientated members of companies?

A first step might be to break the myth that ad fraud is not a necessary skill or area of understanding needed across many functions. Ad fraud impacts the entire ecosystem – and although there is no catch-all solution – we at the IAB SEA+India believe it is an industry-wide responsibility to drive further education and increase discussion around it to tackle it.

There are a number of ways that ad fraud can be prevented, and the good news is that there is quite some overlap with techniques being used to tackle other areas of brand safety, so these will be more familiar ground for those to whom ad fraud is relatively new.

THINK ABOUT HOW YOU BUY

One of the findings from the IAB SEA+India Regional Brand Safety Landscape was that the most common tool to prevent fraud, selected by 76% of respondents, was whitelisting – a list of pre-agreed, specially curated domains on which a brand's advertising campaign can run across. Although, as with many areas of brand safety, it isn't perfect or fail-safe, whitelisting is probably one of the most accessible (and arguably the cheapest) way of preventing ad fraud. Whitelisting means you can avoid publishers with non-transparent inventory on unknown or unfamiliar sites.

Leveraging private marketplace (PMP) deals takes this one step further as buying inventory in an "invitation-only" manner with known publishers has been shown to generate lower volumes of ad fraud than inventory bought on the open exchange. As PMPs are direct deals with brands (or their agencies) and publishers, contract terms could be added denoting that the brand will not pay for any fraudulent impressions.

Although some large agency groups often already include these terms in their contracts as standard to protect clients in this region, based on numbers from third-party ad verification technology, measuring, and ultimately mitigating ad fraud, is the responsibility of everyone in the ecosystem. Therefore publishers and platforms should also be leveraging this technology to monitor and adapt to what they see. This is particularly important for publishers in areas such as video which sees huge volumes of spend (and which continues to increase year on year) to ensure they prevent the loss of revenue to bad players.

RECONSIDER HOW YOU MONITOR CAMPAIGN PERFORMANCE

It's important to avoid campaign KPIs that are easy to fake – such as click-through rate (CTR). This is because certain metrics, such as clicks are more easily faked via bad actors such as Bots. Data available in your ad server or on-site analytics can help you identify when ad fraud may have occurred by revealing major fluctuations in performance – for example if you see your CTR has increased by 2000x, but your volume of sales remains flats; or you see a huge increase in CTR, but your web analytics shows an increase in bounce rate, it's possible that ad fraud has occurred. Knowing your campaign performance benchmarks, seasonality effects or the impact of changes in sales messaging can make spotting these anomalies easier.

Campaign performance measures that are more difficult to fake involve using more qualitative data, such as surveys or brand panels.

Instead of "old school" methodology on campaign measurement, will be useful for brands to move to real "Business Outcome" based result that could take clicks, fill up forms, brand engagement, store visit and finally to the purchase process. This represents better value on media investment and at the same time prevent fraud from deepening as fraud click or impression only can generate metrics such as CTR but it takes real user to generate transaction value.

LEVERAGE 3P VERIFICATION TECHNOLOGY

Companies such as DoubleVerify, Integral Ad Science and Oracle Data Cloud (Moat) have market-leading technology and tactics available to help protect brands against ad fraud. Their technologies can mitigate against the risk at both the "pre-bid" stage (assessing if an impression is likely to be IVT before buying that impression via a Demand Side Platform programmatically) as well as at the "post-bid" stage (which can support programmatic and non-programmatic means of buying inventory). These partners can share reports which highlight which inventory sources have high rates of ad fraud, even allowing some management by exception with alerts being sent when significant spikes are detected. These reports can then be used to create a blacklist of fraudulent domains, that can be removed from future campaigns.

WHAT'S NEXT?

In the digital space, fraud has not been monitored or regulated - meaning that the digital space is one where fraud gets rewarded easier as there is a lower barrier of penetration and lower chance of getting caught.

Southeast Asia and India face unique challenges in ad fraud, and it is clear that mobile in-app fraud is one of the key areas we need to look into. With the market's growth rate far exceeding the ability to keep up with new fraud mechanics in the space, and technical challenges and limitations in the region, this is a constant battle. On top of that, an emphasis on click-related KPIs and low media cost further compounds the opportunities for fraudsters.

On top of the current digital media, new media channels like connected TV are on the rise in Southeast Asia, and with new technology comes new potential loopholes for fraudsters to exploit. Currently, there is no data and learnings for Southeast Asia and India on how to address fraud, so we need to be reactive in finding an approach to fraud on these new media channels.

Beyond understanding the potential treat that ad fraud has as well as the limitations we have, the industry also needs to understand that there are many ways to combat ad fraud and it takes the entire ecosystem to do so. Both the supply side and the demand side needs to take up the responsibility to create awareness. Publishers need to ensure that the inventory that they supply conform to industry standards. On the other hand, advertisers need to take into consideration the bigger picture, and demand for better quality inventory.

Interestingly, throughout the industry, there are no fixed benchmarks for ad fraud rates. We want to drive all advertisers, publishers and ad tech platforms to have an open conversation of the level of ad fraud that they are willing to accept. Ad fraud will never be completely stamped out, but we all need to learn how to set and understand acceptance levels.