Madison Media Matters

MADISON MEDIA
AUDIENCES | OUTCOMES | INTEGRITY

Media Newsletter | February 2020

Chintan Soni, GM, Madison Digital

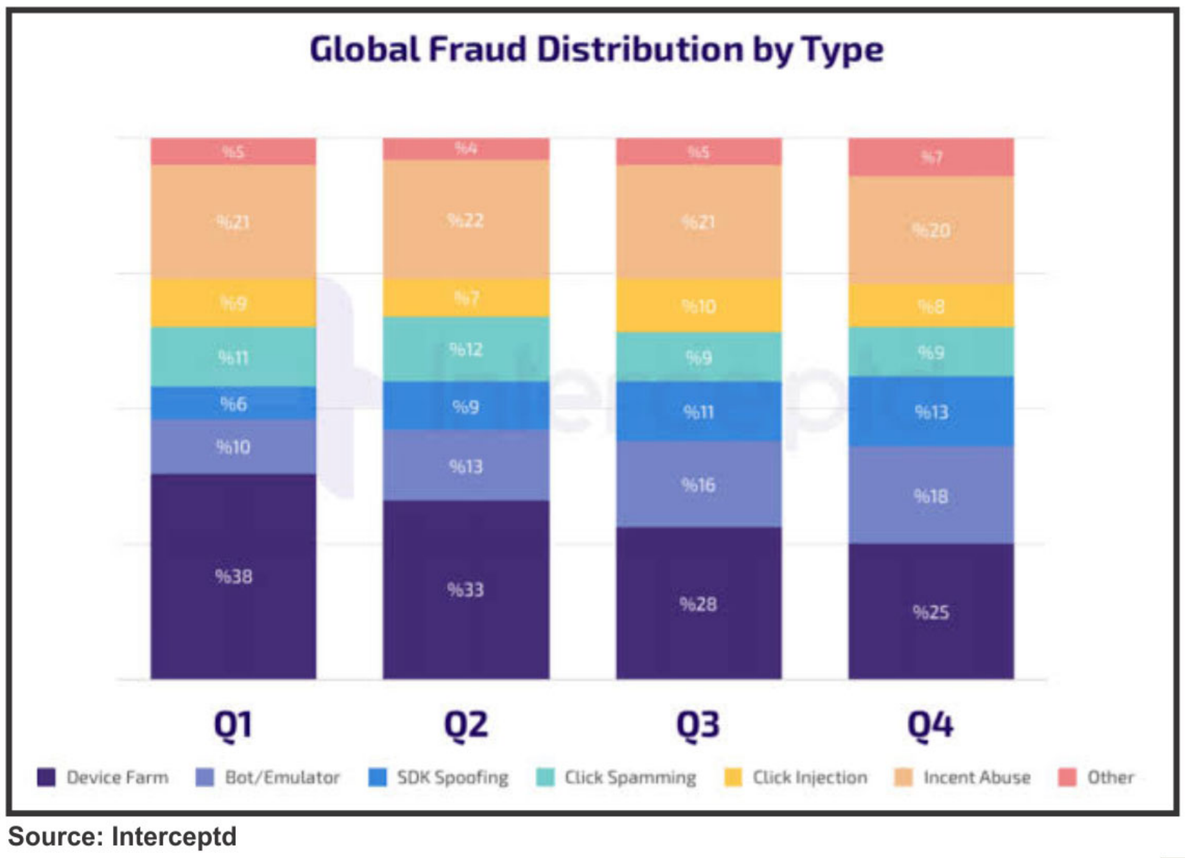
Demystifying and Preventing Ad Fraud in Digital

What is Ad Fraud?

Ad fraud is defined as where a fraudster in the online advertising space uses malicious methods/techniques to bypass required advertising funnels or rules and gains funds from another entity (an advertiser, agency, ad network or user). Ad fraud is a big threat not just to advertisers but also publishers as it steals their potential revenue.

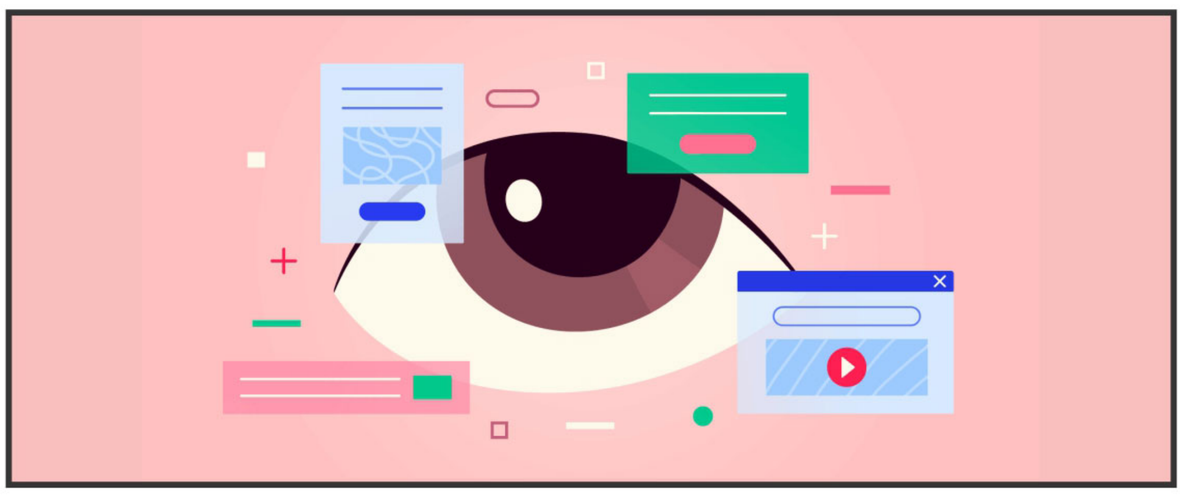
Facts and Figures

- Every 1 out of 4 clicks on online ads is a fraud click.
- 78% of marketers cite click fraud as their top concern (Adweek)
- Invalid Traffic (official name for Ad Fraud) in India is almost 6% for display and 4% for video. On average, clients who are not utilizing a measurement provider could be wasting at least 4% of their video budget to impressions that are not human and will never have the opportunity to pay attention to the ad. (MOAT)
  - However this is an average. It will go up/down basis the category you are operating in.



Source: Interceptd

- Viewability in India: Average viewability rates in India at the moment sit at around 60% for video and display (depending on the viewability definition that is being used by the brand/agency). This is 10% less than the Media Ratings Council recommended 70% viewability rate that brands should be holding publishers accountable to. (MOAT)



Source: Interceptd

Types of Ad Frauds:

Bots can mimic almost anything that a human can do.

- **Click spamming**: Simulating a high number of clicks from real devices in order to get the credit for organic installs to be made legitimate. This shows ad budget squandered on organic users who are already highly-engaged. It generally creates long CTIT (click-to-install-times). Click injection and CTIT anomaly – a fraudulent app creates fake clicks when app installs are taking place, claiming the attribution for the install. CTIT tends to be short.
- **Lead Punching:** Ad Frauds happening in CPC (cost-per-click) or CPL deals are common and we have the set protocols of detecting/blocking such frauds with ML + manual monitoring. This does not end there. At Madison, we have noticed huge pile up of ad frauds happening in performance marketing campaigns.
  - Lead punching fraud happens when advertisers demand down the funnel metrics like cost per walk-in, cost per qualified lead, cost per PAN/Aadhar verification.
  - Fake leads are being filled up and when an advertiser call center dials the number, a person on the other-side will dictate all possible criteria to qualify the lead. Madison has found a way to block such ad networks.
- **App Fraud:** Frauds happening on performance based marketing campaigns i.e. CPI (Cost Per Install), CPR (Cost Per Registration), CPT (Cost Per Transaction)
  - SDK (software development kit) spoofing – hackers create a bot within an app which then pings clicks, installs, and engagement to the MMP (mobile measurement partner) which registers them as genuine users. On an average, an app would have approximate 18 integrated SDKs which can be spoofed.
  - Device farms – The use of real devices to click on ads and install apps, after which they are reset and the process begins again. This creates a suspicious pattern, which can result in ad fraud detection.
  - Bots/emulators – using the same principle as device farms, except using devices which are not real, making the resetting process easier, though leaving behind a similar suspicious pattern.
- **Web Fraud:** Bots will technically be able to deliver on any of the following metrics. They are programmed to trigger the action for which an advertiser has agreed to get billed.
  - CPC/ CPV – Cost Per Click/ Visit: Campaigns run on cost per click/visit and affiliates are paid on number of users clicked/visited on the advertisers' webpage. Payout is low, but volumes are high.
  - CPCV – Cost Per Completed View: In a video campaign, affiliate partners are paid once a user watches the complete ad. Payouts are relatively higher than CPC/CPV. However, volumes are also high.
  - CPL/CPA - In CPL campaigns, affiliates are paid once a user completes the lead. Payouts are much higher than CPV or CPCV but volumes are relatively lower.
- **Brand Safe Content:** Your ads could be shown on doorway pages or on content related to Profanity, Tragedy, Derogatory, Weapons, Violence, Alcohol, etc. This will continuously grow if not handled carefully.
- **Incent Activity:** Fraudulent Affiliates run non-incent marketing campaigns over incent platforms where the user downloads or uses the app for a certain incentive rather than an actual interest in the app. Incent abuse – incentivizing users to click and install apps. To help hide the high click-to-install conversion rate that results from this, fraudsters might send a high level of fake clicks to help mitigate the suspicion.
- **Coupon & Cashback:** Some coupon/cashback sites publish Ads of fake/misleading/fraudulent coupons & cashback offers in the name of renowned advertisers in order to get user traffic on their websites, which impacts the brand image of the advertiser.
- **Viewablity:** It's a big concern in digital. A viewable impression is a standard measure of ad viewability defined by the International Advertising Bureau (IAB) to be an ad which appears at least 50% on screen for more than one second for display and 2 seconds for video.

- In all programmatic buys, we are implementing all 17 standard brand safety filters to avoid exposure to unsafe brand zone.
- We do thorough monitoring of all the metrics and parameters through the entire digital funnel - right from the impression to final conversion and highlight any suspicious activity happening anywhere.
- In every campaign we execute via DV360, the following categories are excluded:

Profanity	Tragedy	Derogatory	Downloads & sharing
Weapons	Violence	Alcohol	Drugs
Politics	Religion	Transportation accidents	Adult
Shocking	Suggestive	Tobacco	Gambling

- Use Ads.txt Authorized Digital Sellers for web (ads.txt) is an IAB initiative to improve transparency in programmatic advertising by allowing publishers to identify who is authorized to sell their inventory. Declaring authorized sellers in an ads.txt file helps protect buyers from counterfeit inventory. We at Madison by default exclude non-participating inventory on new campaigns.
- Employing Reverse IP Lookup (when required): We have found that identifying the culprits of click fraud through a reverse IP lookup has proven to be quite effective. Most businesses have static IP addresses and these are easily identifiable. We use our marketing automation tool to produce the reports and once identified, exclude the bad IPs from our campaign.

How Third-party Verification Can Help

- MOAT Measurement for advertisers is not only a platform that allows the brand to understand how viewable, brand safe and verified (ad fraud free) the impressions are across campaigns but also a way for brands to gain deeper insight into creative performance and ad effectiveness to more accurately calculate ROI across digital channels.
- Video platforms such as YouTube, SonyLiv and HotStar traditionally hold very high viewability rates. However, even though the ad can be classified in-view, does it mean that that a user is paying attention to the ad? Can they hear the brand message or be influenced by the music? Do they watch the video to the end or just click out of the ad after a certain period of time? These are all questions that a brand and agency should ask and answer to optimize Creative and Media strategy.

Some additional metrics to look for in video campaigns:

- **Exposure Time:** the amount of time in seconds and hours the user watched the video
- **AVOC%:** audible and visible on complete rate
- **Visible at Complete Rate:** the % of impressions where the user watched the video 'in-view' to the very end, but didn't have the audio turned on
- **Audible till completion:** the % of impressions where the user listens to the audio till the end of the video, but not in-view
- **Relevancy on OTTs/YouTube:** Protecting Brand Image: With our machine learning based algorithm, we keep on identifying the blacklisted and inappropriate channels where advertisers would avoid showing their ads, thus protecting the brand image
- **Micro Segmentation/Relevancy:** Understand nuance of a channel to improve targeting with a relevant creative. E.g. A sports channel will have higher probability of relevant viewers for sports apparels & shoes
- **Micro Influencer Channel Selection:** Basis analytics and data-driven approach, advertisers can target the most relevant video channels. Channels are added and excluded from the relevant list basis performance on YouTube/OTTs
- **Intelligent Creative Selection:** Monitoring latest trends in YouTube/OTTs and finding the best possible ways to reach to the right customer regularly for each category of ads

Advice for Advertisers

- **Always Use Trusted Networks** or if you don't trust the network you are dealing with, deploy at least one or more ad verification methodology that can help minimize the risk of ad fraud. Once implemented, make sure you work with a DSP that offers a fraud-free guarantee to ensure you are paying not burning your money on fake impressions/clicks.
- **Establish Fewer But Higher-Quality Partnerships:** In any push for campaigns with zero fraud, here's how to start: Encourage

your agency or internal team to reduce the number of affiliate partners with which your organization works. Run campaigns through limited number of platforms and allocate your spend in high-quality media.

- **Know Your Metrics:** Knowing your metrics is a vital step in identifying ad fraud. If you can't identify the issue, you cannot combat it. Knowing your digital, business and brand metrics are really important like CTRs, bounce rates, session time, conversion rates, visits to lead, lead to walk-in etc. will allow you to identify anomalies when they occur. For example, if your click volume increases by 500% and your CTR triples, but your lead volume is flat, there may be a problem.
- **Build A Robust Programmatic Tech Stack:** There are many faces of ad fraud, including viewability, bot traffic and completion rates. Select the right programmatic technology provider that includes thorough fraud detection solutions, such as prebid filtering for invalid traffic and built-in viewability measurements.
- **Pay for Performance, Not Clicks:** The future of marketing is paying for performance. Clients want outcomes. As a client, you should design a performance incentive structure to be paid based on results. It's a win-win situation for both parties.
- **Closely Monitor Your Campaign (Or Hire Someone):** The majority of digital ad frauds are performed via manipulation in the way attribution is done. Marrying data from attribution solution along with close monitoring of increased activity from bots will help you understand if you're a victim of ad fraud, as well as know when and what to block such as keywords, domains, geographic location, times of day, etc.

Madison's Partnership

Madison has a partnership with all leading verification services:

MOAT DoubleVerify IAS Integral Ad Science adloox

Cost

Approximate cost to implement third-party verification services i.e. DoubleVerify | MOAT | IAS | AdLoox

Brand Safety	Display Viewability	Video Viewability	Fraud & Invalid Traffic
₹3.55 - ₹ 5.5 CPM	₹ 6.40 - ₹ 8.5 CPM	₹ 10.66 - ₹ 15.5 CPM	₹ 3.55 - ₹ 6.4 CPM

Contact

For more information, contact

Vishal Chinchankar: vishal.chinchankar@madisonindia.com | +91 98673 30055 or
Chintan Soni: chintan@madisonindia.com | +91 98928 87544