
THE INDIAN SOCIETY OF
ADVERTISERS

ABOUT THE ISA

- The Indian Society of Advertisers (ISA) is **the peak body representing advertisers across India for 70+ years**.
- ISA is one of the **founders of** Advertising Standards Council of India (**ASCI**).
- ISA is one of the three constituent bodies that **formed Broadcast Audience Research Council (BARC),** a pioneer body in TV audience measurement.
- ISA is also one of the **founding members of the World Federation of Advertisers (WFA)** that operates from Brussels.
- ISA's **mission** is to **safeguard the interest of advertisers by promoting efficient and effective Advertising Practices**

THE INDIAN SOCIETY OF ADVERTISERS

WE ARE THE INDIAN SOCIETY OF ADVERTISERS

THE INDIAN SOCIETY OF ADVERTISERS

Sunil Kataria
Chairman, ISA
CEO, Raymond Lifestyle

Tejas Apte
ISA Media Forum Chairperson,
General Manager-Media & DMC, South Asia, Hindustan Unilever

Ankit Desai
ISA Media Forum Co-Chairperson,
Media, Digital Marketing, and Brand PR Head (India and Global Centre of Excellence), Marico

FOREWORD

As the Indian advertising landscape continues to evolve, the need for a robust and transparent framework has never been more critical. The Indian Society of Advertisers (ISA) has been at the forefront of these developments, committed to fostering a media ecosystem that prioritizes transparency, efficiency, and the highest standards of practice.

We are proud to present the culmination of our efforts in the form of the ISA Media Charter Playbooks. These playbooks—focused on Brand Safety, Ad-Fraud, Viewability, and First-Party Data—represent the collective expertise, insights, and commitment of industry leaders and stakeholders. The creation of these playbooks has been a meticulous process, driven by our shared vision to safeguard the interests of brands, consumers, and the broader advertising community.

In an era where digital advancements and the proliferation of media channels present both opportunities and challenges, these playbooks offer a comprehensive guide to navigating this complex environment. They serve as a testament to our dedication to upholding the highest standards in advertising. We extend our deepest gratitude to everyone involved in the development of these playbooks—our members, partners, and industry experts—whose contributions have been invaluable.

We believe that these resources will empower advertisers to make informed decisions, enhance the effectiveness of their campaigns. With the launch of these playbooks, we reaffirm our commitment to safeguarding the interest of advertisers by promoting efficient and effective Advertising Practices.

LEGAL ADVISORY

The use of brand names, vendor names and/or company names in the ISA Media Charter (IMC) playbooks and/or any mention or listing of specific commercial products or services in these playbooks is solely for educational purposes and does not imply endorsement by the ISA, nor discrimination against comparable brands, products or services available in the market. ISA does not endorse or recommend any vendor/company and references to any vendor/company in the IMC playbooks are incidental and have been used with the consent of such vendor/company for illustrative purposes. ISA members are not obligated to follow the recommendations outlined in the IMC playbooks. Each member should independently evaluate which suggestions, brands, vendor or company is best suited to their specific business needs, policies, and values. The action plans presented in the IMC are intended as recommendatory and optional guidelines. While the IMC playbooks address various challenges within the digital advertising ecosystem and propose potential solutions for improved efficiency and effectiveness, members are encouraged to consult their legal counsel if necessary before implementing any suggestions. ISA makes no representations or warranties regarding the content or outcomes of the IMC playbooks

THE INDIAN SOCIETY OF ADVERTISERS

AD FRAUD PLAYBOOK

THE INDIAN SOCIETY OF
ADVERTISERS
Since 1952

ISA AD FRAUD SUB-COMMITTEE

Jaikishin Chhaproo
ISA Ad Fraud **Sub-Committee Head**,
Media & PR Head,ITC

Chintan Soni
CEO/Co-founder - mFunnel.ai
(Unit of Madison World)

Dorab Ghadiali
Media Head,
Aditya Birla

Gautam Surath
COO, Performics

Gazal Bajaj
Media Head,
Nestlé

Karan Anand
SVP, IPG

Ravi Kiran
Principal Manager,
Media Planning, ITC

Sairam Ranganathan
Chief Digital Officer,
Wavemaker

Salil Sawant
Media Head,
Glenmark Pharma

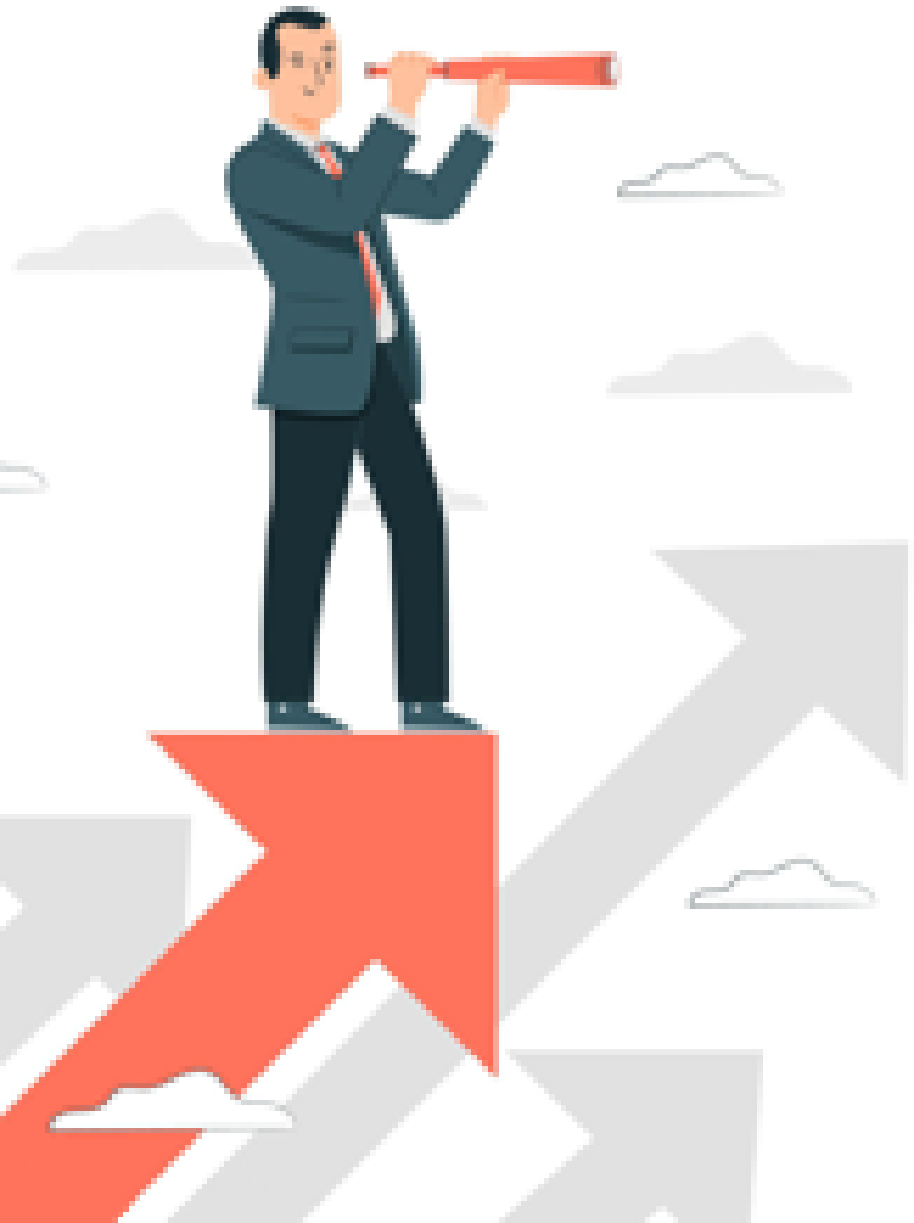
Savita Unnikrishnan
DGM-Media,
TVS Motors

Shashi Udyavar
Industry Head
(CPG), Meta

Shreya Godani
Media Measurement
& Marketing Head, ISA

Tejas Apte
GM, Media & DMC,
South Asia,
Hindustan Unilever

Vineet Nair
Media Head,
Amazon



VISION

Digital media fraud poses significant challenges to advertisers and the integrity of the advertising ecosystem. The ISA Ad Fraud Playbook empowers advertisers, agencies, and platforms with knowledge and strategies to detect, mitigate, and prevent digital media fraud, ensuring transparency, accountability, and effective media investment.

.

THE INDIAN SOCIETY OF ADVERTISERS

CONTENTS

THE INDIAN SOCIETY OF ADVERTISERS

SECTION 1

Understanding Digital Media Fraud: Types, Impact, and Advertising Challenges

THE INDIAN SOCIETY OF ADVERTISERS

What is **Digital Media Ad Fraud?**

Ad fraud is any deliberate activity that prevents the proper delivery of ads to the right people at the right time and place.

IMPACT OF AD FRAUD

Financial Losses and Inaccurate Performance Metrics:
Ad fraud wastes advertising budgets and distorts performance metrics, misleading advertisers about their campaign's effectiveness.

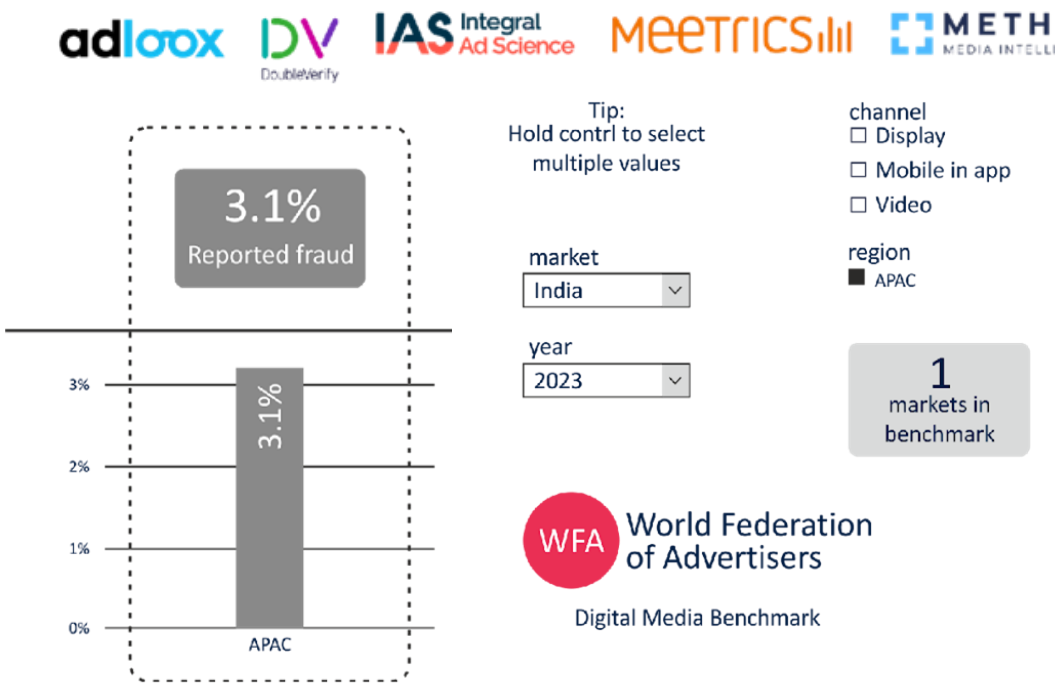
Diminished Brand Trust & Negative User Experience:
Ad fraud erodes consumer trust and harms brand reputation as consumers encounter fraudulent or misleading ads, leading to negative user experiences and ad-blocking behaviors.

Damaged Advertiser-Publisher Relationships:
Ad fraud strains relationships between advertisers and publishers, leading to disputes, contract terminations, and reluctance to collaborate.

THE INDIAN SOCIETY OF ADVERTISERS

Ad Fraud in India

India's rapid growth in digital advertising, driven by 5G expansion, affordable smartphones, and a vibrant digital ecosystem, makes it an attractive target for ad fraud. Low labor costs and the lack of a regulatory body allow fraudsters to operate easily.



Different numbers are quoted by different sources varying anywhere between 2% to 8%

THE INDIAN SOCIETY OF ADVERTISERS

Ad Fraud Can be Tracked by

IAS Integral Ad Science

DV DoubleVerify

nielsen

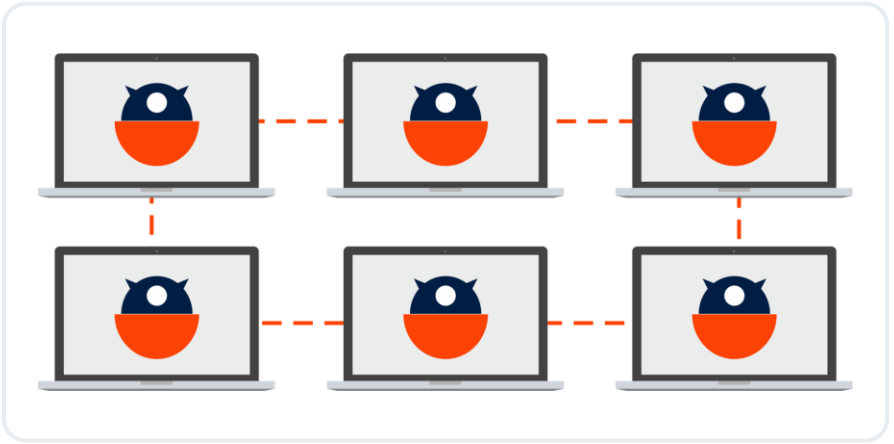
mFilterIt

THE INDIAN SOCIETY OF ADVERTISERS

Some Common **Types of Ad Frauds**

1. MALICIOUS BOTS

Also called ‘Click Fraud’, it is a broad category in which fraudsters use bots to generate large quantities of fake clicks on an ad, or fake visits to a website - resulting in wasted Ad Spends.



THE INDIAN SOCIETY OF ADVERTISERS

Some Common **Types of Ad Frauds**

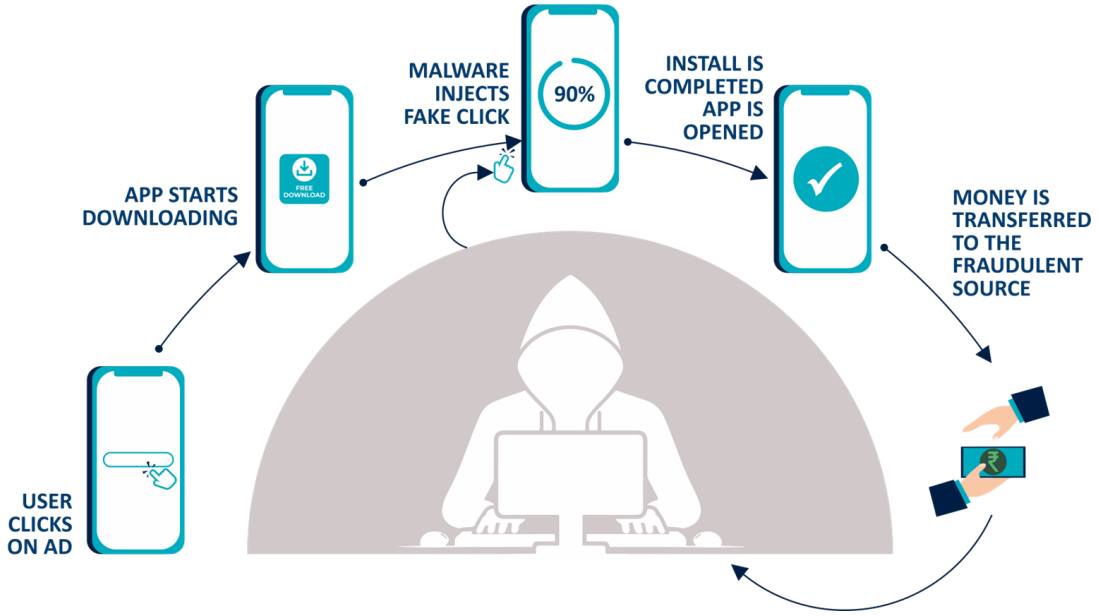
2. AD STACKING

Ad stacking is a type of display and impression fraud where mobile apps or websites stack multiple ads beneath one another in a single ad placement. While only the top ad is visible with its impression served, numerous advertisers are billed for the impression, because when a user clicks the top ad, a click will be registered for all ads on the stack.

Some Common **Types of Ad Frauds**

3. APP NAME SPOOFING

A sophisticated form of click spamming, click injection will use an app located on the user's device which "listens" to app installation broadcasts. These apps are usually junk apps that remain dormant until the installation broadcast wakes it up to hijack the user's device and generate clicks and steal credit for an organic install or non-organic install by another partner.



Some Common **Types of Ad Frauds**

4. PIXEL STUFFING

Pixel stuffing occurs when individual pixels are converted into ad space. An ad is inserted into a tiny space - often 1x1 pixel in size - which allows impressions to be recorded, even though the ad itself for all practical purposes is invisible to visitors.

Some Common **Types of Ad Frauds**

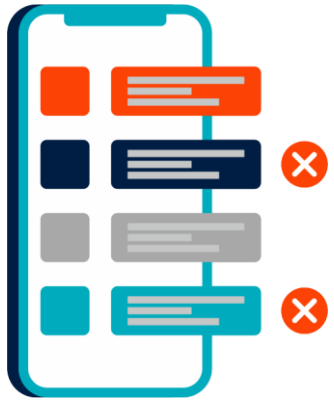
5. DOMAIN SPOOFING

Domain Spoofing occurs when a fraudster masquerades their fake site as a legitimate and, usually highly sought after site. They then trick advertisers into paying premium prices for low quality ad space.

Some Common **Types of Ad Frauds**

6. APP NAME SPOOFING

Similar to Domain Spoofing, App name spoofing occurs when the app on which ad impressions is generated is misrepresented. In this case, the app sends a bundled ID which is the identifier of the App.



Some Common **Types of Ad Frauds**

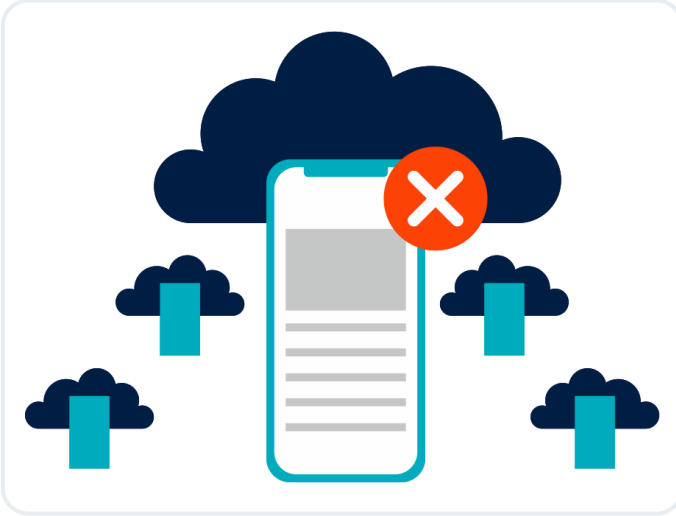
7. LOCATION FRAUD

Location fraud or Location / Geo Masking is where fraudsters send false location data so the ad serves somewhere outside the targeted region, which reduces the effectiveness of the campaign

Some Common **Types of Ad Frauds**

8. SDK (SOFTWARE DEVELOPMENT KIT) SPOOFING

SDK Spoofing also known as Traffic Spoofing involves creating a bot within an app that then initiates fake clicks and app installs. It can trick advertisers into paying for app installs- sometimes, for as many as tens of thousands – that didn't happen.



Other Types of Ad Frauds

1. INCENT ACTIVITY (INCENTIVE)

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.

2. LEAD PUNCHING FRAUD

Happens when advertisers are demanding 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 the advertiser call center dials the number guy on the other-side will dictate all the possible criteria to qualify the lead.

THE INDIAN SOCIETY OF ADVERTISERS

3. COUPONS & CASHBACK

Some coupon / cashback sites publish Ads of fake / misleading / fraudulent coupons & cashback offers in the name of renowned advertisers to get user traffic on their websites, impacting the brand image of the advertiser.

4. AD FRAUD IN EMERGING MEDIUMS

Connected TV: Includes device spoofing, running ads through secondary devices while the TV is off, and invalid server-side ad insertion (SSAI).

SECTION 2

Advanced Detection Techniques for Digital Ad Fraud

THE INDIAN SOCIETY OF ADVERTISERS

Advanced **Detection Techniques**

1. Traffic Analysis

- **IP ADDRESS MONITORING:** Identify suspicious IP addresses generating high volumes of traffic.

  Example: A platform flags an IP address generating thousands of ad clicks with no engagement, suggesting a click farm.

- **GEOGRAPHIC IRREGULARITIES:** Spot inconsistencies in traffic from unexpected geographical locations.

  Example: An ad campaign targeted at users in India shows traffic from a remote region, indicating the use of VPNs or proxy servers.

THE INDIAN SOCIETY OF ADVERTISERS

1. Traffic Analysis (contd.)

- **FREQUENCY AND VOLUME ANALYSIS:** Check for unnatural patterns in traffic frequency and volume.

  Example: A new video on YouTube suddenly receives millions of views with no clear source, indicating the use of bots

- **USE SALES DATA TO TRACK SOURCE OF TRAFFIC AND IDENTIFY POTENTIAL ISSUES:** Exclude sources with no sales conversions / high returns. Additionally, analyze the sales data for each source to detect outliers in the cost per sale metric, as these may indicate fraudulent activity.

2. Behavioral Analysis

- **USER INTERACTION PATTERNS:** Study user interactions to identify non-human behaviour.
  Example: Systematic scroll patterns on a social media platform suggest non-human behaviour.

- **ENGAGEMENT METRICS:** Analyze click-through rates, time spent on pages, and interaction types.
  Example: A high click-through rate but low conversion rate on Google Ads may indicate click fraud.

- **MOUSE MOVEMENT TRACKING:** Monitor mouse movements for natural variances compared to bots.
  Example*:* Straight, rapid paths to the "buy" button on e-commerce sites suggest bot activity.

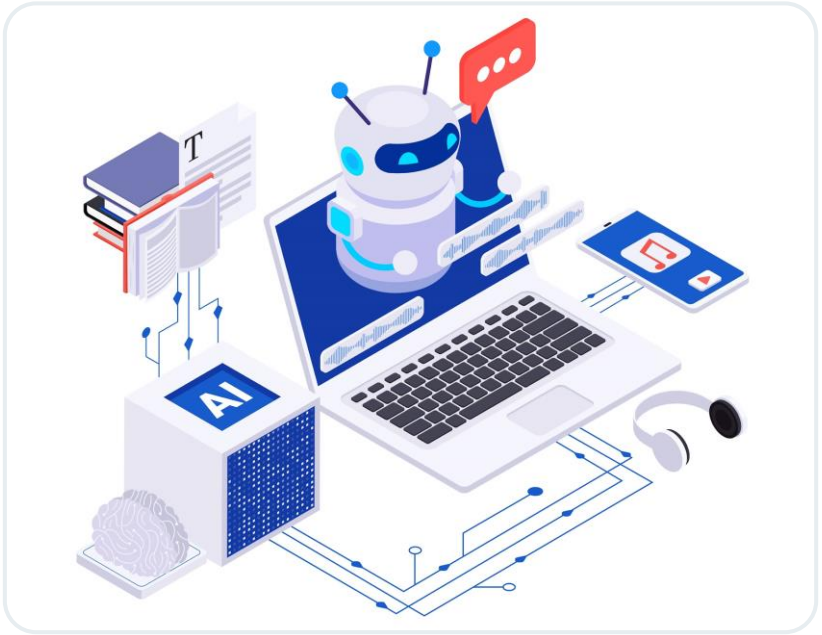
3. Ad Verification Tools

- **VIEWABILITY METRICS:**
  Example: Example: Implementing tools to ensure ads are actually viewed by real users, measuring parameters like ad visibility duration and screen position Tools like DV, MOAT can measure if an ad was actually viewable on the screen and for how long, ensuring ads are not being counted as 'seen' when they are not visible to the user.

- **CLICK VALIDATION:**
  Example*:* Example: Verifying the legitimacy of clicks on ads, distinguishing between intentional user clicks and automated or fraudulent ones. Ad verification companies can track the time between ad exposure and click, where a near-instant click on hundreds of ads might indicate automated clicking, hence fraud.

4. Machine Learning & AI

- **PATTERN RECOGNITION:** Use machine learning algorithms to identify fraud patterns.
- **PREDICTIVE ANALYSIS:** Predict potential fraudulent activities based on historical data.
- **ANOMALY DETECTION:** Automatically detect deviations from normal behaviour patterns.



5. Data Analysis & Reporting

- **REAL-TIME MONITORING:** Use tools for immediate detection of irregularities.
- **REPORTING SYSTEMS:** Establishing robust reporting mechanisms for in-depth analysis of traffic sources, user behaviours, and engagement metrics.

6. Cross-Platform Analysis

- **MULTI-PLATFORM MONITORING:** Monitor user activities across platforms to identify linked fraudulent behaviours.
- **CROSS-REFERENCING DATA:** Compare data from various sources to confirm fraudulent activities.

7. Collaborative Efforts

- **SHARING INTELLIGENCE:** Collaborate with other platforms to share insights and data on fraud patterns.

Proposed slide

8. Integrating Advanced Technologies

- **BIOMETRIC VERIFICATION:** Implement optional biometric methods, such as facial recognition or fingerprint scanning, to authenticate user interactions, particularly for high-value transactions. This ensures that the action is performed by an authorized user.

- **BLOCKCHAIN & DISTRIBUTED LEDGERS:** Utilize blockchain technology to create immutable records of ad transactions and user activities, preventing tampering with view or click counts. Leverage distributed ledgers to improve transparency and verification in ad delivery, enabling advertisers to track ad journeys and confirm genuine user engagement.

THE INDIAN SOCIETY OF ADVERTISERS

SECTION 3

Influencer campaigns & ad fraud

Influencer Campaigns and Ad Fraud

How grave is the problem?

Nearly 2 out of 3 Instagram profiles in India have spurious or fake followers **over 60 percent.***

What are the influencer fraud types?

- **RAMPANT FAKE FOLLOWERS:** Influencers in India buy fake followers from various supplier sites worldwide. **Costs range from Rs 8 to Rs 50 per 1,000 followers.**
- **FAKE ENGAGEMENT:** Influencers also purchase fake likes and comments to mask the inactivity of fake followers, making fraud detection difficult for marketers.

*As per the numbers published by influencer marketing platform KlugKlug

THE INDIAN SOCIETY OF ADVERTISERS

Some Tools & Filters available for identifying quality influencers

Tools

- Klug Klug
- Qoruz
- Brand AI (Wavemaker)
- Influencer.in
- ClanConnect
- One Impression
- Pulpkey
- mFilterit
- Plixxo
- Winkl
- Animeta

Filters

- **Audience Demographics:** Age, Gender, Location, Interests
- **Influencer Characteristics:** Social Media Platform, Follower Count, Engagement Rate
- **Authenticity:** Detect fake followers
- **Growth Trends:** Analyse follower growth over time

Best Practices for Influencer Marketing

- **Engage influencers with the right audiences for your brand.** Find the right cohort in **gender mapping** for products suited to the right influencers.
- Identify **influencers based on audience credibility**, considering inactive and spurious followers.
- Go beyond the usual set of influencers. Use scaled platforms to **identify new, high-quality influencers** and use them like a media mix (micro, macro, nano, mega) in tandem.
- Implement real-time, **automated reporting** to ensure transparency and optimize future campaigns. This helps identify high-performing influencers and find "lookalike" influencers.

THE INDIAN SOCIETY OF ADVERTISERS

SECTION 4

Billing and Transparency

THE INDIAN SOCIETY OF ADVERTISERS

What to Track basis your Campaign Objective?

	Viewability	On Target	Human / Bot Traffic	Quality of Traffic	Valid Data
Awareness	✓	✓	✓		
Engagement	✓	✓	✓		
Lead	✓		✓		✓
Website Visit			✓	✓	
Conv.to sales			✓		✓

- Billing or make-good for digital ad fraud involves compensating advertisers for fraudulent or invalid activities that may have occurred during an advertising campaign.
- Handling billing or make-good for digital ad fraud requires a collaborative and transparent approach between advertisers and publishers to maintain a fair and trustworthy advertising ecosystem.

THE INDIAN SOCIETY OF ADVERTISERS

Context of Digital Fraud

- **Fraud Detection Systems:** Implement robust fraud detection systems to identify and filter out fraudulent activities in real-time.
- **Define Fraud Metrics:** Clearly define metrics and criteria for identifying fraudulent activities, ensuring a common understanding between advertisers and publishers.
- **Transparency & Communication:** Maintain open communication with publishers and share the regular reports with the benchmarks set. Transparency builds trust.
- **Refund or Credit Policy:** Establish a clear refund or credit policy outlining the conditions under which compensation will be provided for ad fraud before the start of the campaign.
- **Mutual Agreement on a Verification Process & Protocols:** Implement a verification process to investigate and confirm instances of fraud.
- **Timeframe for Claims:** Set a reasonable timeframe in which an advertiser would report suspected fraud and submit claims for compensation.
- **Documentation & Proof:** Provide publishers with detailed documentation and proof of fraudulent activities to support your claim.
- **Stay Updated:** Continuously update and improve fraud detection mechanisms to stay ahead of evolving fraudulent tactics.

THE INDIAN SOCIETY OF ADVERTISERS

SECTION 5

Ad Fraud Case Studies

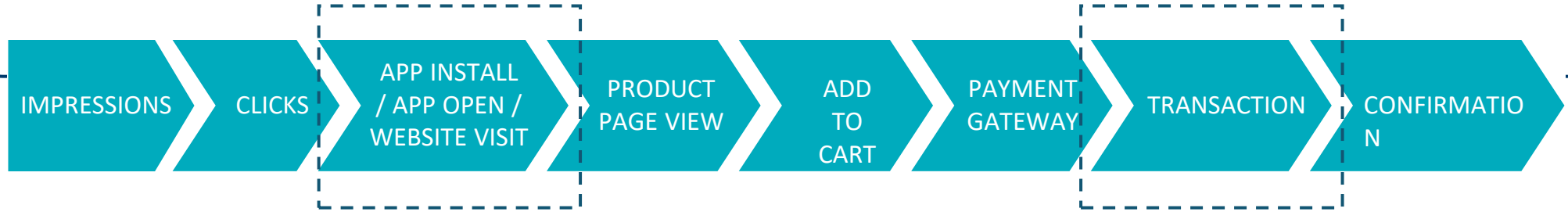
THE INDIAN SOCIETY OF ADVERTISERS

Leading QSR Brand in India

How ~5-8% of investment behind ad-fraud can bring in 50-60% efficacy in your ROI Metrics.

Step 1: Defining Granular KPI is the Most Important

- Irrespective of the campaign type/objective, it's important to know which KPI is most important for your business.
- Based on that KPI, you need to identify granular KPIs that needs to be optimized to achieve your final goal.
- In this case while end goal i.e. sale is important, the consumer journey has been broken in to various parts.
- Based on this journey, the advertiser has defined validation / optimization criteria at a different stage of the funnel as below:



THE INDIAN SOCIETY OF ADVERTISERS

Setting Lead Indicators

- Unusual peaks in the number of clicks or impressions.
- Reduced page views and higher bounce rate during peaks in impressions or clicks.
- Checking Analytics data like Google Analytics, Adobe etc. and looking at the age and gender section to see whether the traffic is from in-target audience.
- No increase in the number of conversions during peaks in impressions or clicks.
- For sales campaigns, check the customer details (if it's the same phone number placing the order multiple times, check for average order values, if order is placed and returned in 7 to 10 days).
- For app installs, check if the installs are coming from fake device, device, incorrect region, blacklisted IP's etc.

Partners worked with

- mFilterIT, P360 for app installs and orders validation for our 2 app's
- Nielsen for In-Target Reach

Result: The advertiser invested approx. 5-8% of media cost in deploying these tools / technologies. In return they saw seen 50-60% fake / fraudulent orders getting mitigated which translated into pure efficiency.

Tackling Ad Fraud in CPG Programmatic Buying

Background: CPG marketers, early adopters of programmatic buying, leveraged it for campaign scalability and cost efficiency. However, they faced significant challenges, including the risk of buying impressions that reach non-human audiences, especially in unfiltered programmatic environments. Programmatic buying, with its multiple transaction layers, is particularly vulnerable to ad fraud. Marketers often push for ultra-low eCPMs, inadvertently inviting fraudulent impressions.

Solution: Pre-Bid Fraud Protection - A prominent CPG brand partnered with IAS to combat ad fraud. IAS implemented pre-bid ad fraud protection, eliminating fraudulent inventory before bids were placed. By setting risk thresholds with programmatic buyers, IAS ensured high-quality ad space while protecting against GIVT and SIVT fraud. Continuous monitoring and weekly tracking reports helped maintain low fraud levels.

Result: The CPG brand achieved a 7.9% reduction in fraud, maintaining levels around 1.3%. This strategy prevented over 32.2 million fraudulent impressions, allowing the brand to focus on valuable ad spaces. The partnership with IAS demonstrated the effectiveness of pre-bid optimization in reducing ad fraud and improving campaign quality.

Source : IAS

Frequency Cap Fraud

Frequency capping violation by Publishers

Device ID (As on 15th June'23)	Counts
2a7d52fa-bc10-485a-bb23-b7baf5334d2f	135
fc7a14a1-c53e-4043-bf3e-cdb8314e90e7	92
eff39288-cded-4629-beb5-e6fd1f522e12	90
922a4add-7030-4a36-9d6c-0ccc0f41a2a5	84
f1033370-87b0-4df3-b925-611b717fbf72	80
1c7bff12-968a-4fd6-ab5a-d6bec0672c07	75
d61e1a32-73cf-46c7-87d2-2d04913823de	68
bb2b8562-30ed-42b9-ac91-804d29b8ccaa	68
f3b7042c-8b5f-4efa-8958-1fb62d68219e	61
4900da9f-e479-4573-a599-3adbefa3dde6	60

Device ID (As on 15th June'23)	Counts
7fc25405-27ca-4e2f-8c5c-f37b291d7426	57
7969f983-9eef-4cfc-8e6b-e00af79fb5ef	56
e16413bf-f47c-4eb5-9e9bb-b4af20338e00	55
53092592-311c-4fd5-82cd-2d7636d533d3	53
68ebb213-f0d3-472e-9ae1-9c8442e02ef5	51
c7735966-021-4c77-9b1a-a5fd4b8ae706	50
286963c5-6130-462a-99e6-4934cff86289	49
b5e1653f-e1aa-4619-863b-539f2f4a534e	47
b7232264-8c05-403a-8cb5-9c34c52a7cfo	47

Device Repetition or Frequency Mapping is a compliance fraud wherein the same user is being shown impressions multiple times.
Thresholds: More than 2 in the whole month.
Whereas the sample shown in the left, clearly indicates the violation of the frequency cap set up by the client. This will affect the reach of the ad being served.

Total Impressions = Total Frequency* Reach

Frequency Cap: The number of times viewers are exposed to the same ad during a campaign.
Reach: The number of people exposed to a given medium at a given point in time, i.e. target audience.
If the same ad is being exposed more than 50 times to a user, this affects the reach of the campaign and hence only a limited number of users are being targeted for that particular campaign, thus affecting the marketing/sales funnel for the client.

THE INDIAN SOCIETY OF ADVERTISERS

Hourly ADID Repetition

Device ID: 0ee4abea-b344-463f-87f9-0257beda5f68

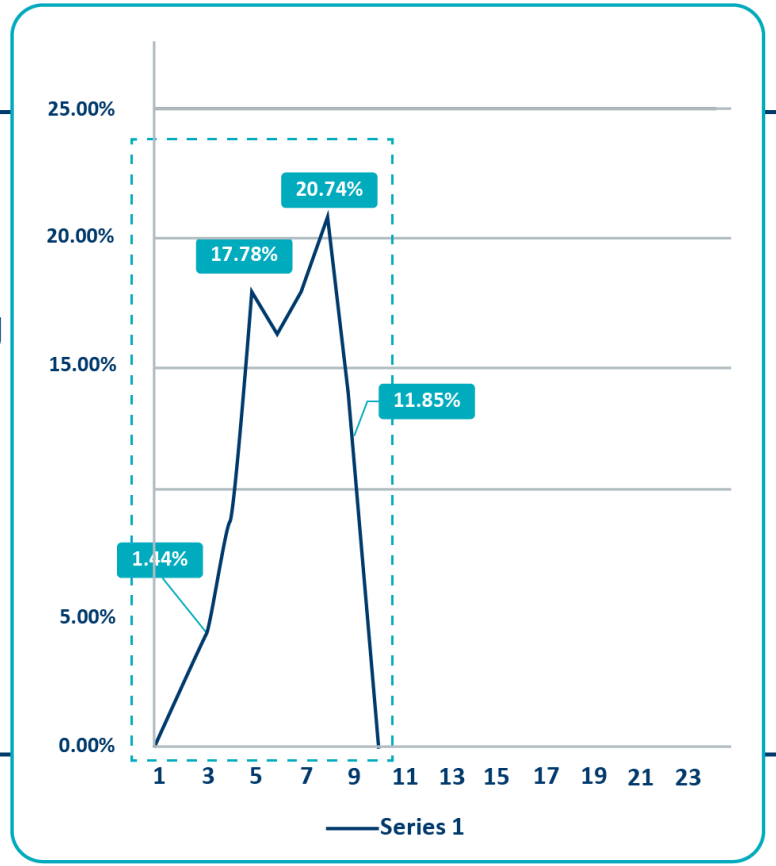
Date	Hour Of The Day																							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
17-06-2023	1	0	0	16	10	10	20	13	14	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18-06-2023	0	0	0	0	0	0	1	10	10	16	5	9	10	8	5	1	14	4	5	7	9	2	1	3
19-06-2023	1	0	0	0	0	5	18	14	4	9	5	9	5	0	0	0	0	0	1	0	0	0	0	0
20-06-2023	1	2	0	0	0	4	6	8	3	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0

Device ID:4b3c8be2-fe92-4443-aaab-48d24aadcb7f

Date	Hour Of The Day																							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
17-06-2023	14	10	9	12	18	13	12	12	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18-06-2023	11	4	13	13	12	14	14	12	8	0	7	11	0	0	0	0	0	0	0	0	7	2	1	1
19-06-2023	0	0	0	0	0	8	12	15	13	9	12	2	0	0	0	0	0	0	0	0	0	0	0	0
20-06-2023	1	3	5	2	5	7	7	13	7	2	6	5	0	0	0	0	0	0	0	0	0	0	0	0

Impression Fraud Explained

Fake User - Frequency Cap Violation
Condition: If the Device ID / GAID / ADID is greater than 2 (taking previous records of the same ADID as well into consideration), mark the records under Device Repetition fraud check.
A total of 106 Impressions were recorded from the same device ID: 4b3c8be2-fe92-4443-aaab-48d24aadcb7f.
The ad was served to the same person or device 106 times within the same time frame. This malicious activity is aimed at depleting the budget



THE INDIAN SOCIETY OF ADVERTISERS

SECTION 6

Industry Action Required

THE INDIAN SOCIETY OF ADVERTISERS

Individual Advertiser

1. **Vendor and Partner Vetting**
   - Use accredited fraud solutions for both General and Sophisticated Invalid Traffic (IVT).
   - Work with a Demand-Side Platform (DSP) offering a fraud-free guarantee.
   - Demand transparency into inventory and traffic, including sourced traffic and audience extension.

2. **Performance Measurement**
   - Measure fraud across all campaigns to understand anti-fraud performance.
   - Focus on real Key Performance Indicators (KPIs) tailored to campaign goals, rather than relying on low Cost Per Thousand (CPMs).
     Design a performance incentive structure based on results, as the future of marketing is paying for performance.

3. **Transparency and Communication**
   - Request transparency into where programmatic advertising is served.
   - Maintain open communication with publishers, sharing regular reports and benchmarks.
4. **Know Your Metrics**
   - Identify digital, business, and brand metrics to recognize anomalies.

     Example: If your click volume increases by 500% and your Click-Through Rate (CTR) triples but your lead volume remains flat, there may be a problem.
5. **Establish High-Quality Partnerships**

   Reduce the number of affiliate partners and allocate spend to high-quality media.
6. **Pre-Bid Filtering**
   - Implement pre-bid filtering to avoid fraud in programmatic buys.
   - Use exclusion lists to prevent ad placements on known fraudulent sites.
7. **Closely Monitor Your Campaign**
   - Combine data from attribution solutions with close monitoring to detect increased activity from bots.
   - Identify when and what to block, such as keywords, domains, geographic locations, and times of day.

Joint Industry Body

Advertisers, Media Agency & Digital Platform Association

1. **Standardization and Guidelines**
   - Refer to common criteria and metrics for identifying fraudulent activities to ensure consistency across the industry.
2. **Collaborative Efforts**
3. **Technology and Innovation**
   - Share intelligence and data on known fraud patterns and sources within the industry.
   - Adopt industry-standard fraud detection tools & methodologies for a unified approach.

By implementing these strategies, individual advertisers and industry bodies can create a more transparent, accountable, and effective advertising ecosystem, significantly reducing the impact of ad fraud

THE INDIAN SOCIETY OF ADVERTISERS