UNDERSTANDING & MITIGATING AD FRAUD IN MENA

MAY 2025

iab mena

CONTENTS

02 INTRODUCTION

03 UNDERSTANDING AD FRAUD

04 TYPES OF AD FRAUD

11 DETECTION & MITIGATION

18 SELECTING ADTECH SOLUTIONS & MANAGING PERCEPTIONS

22 THANKS TO TASKFORCE

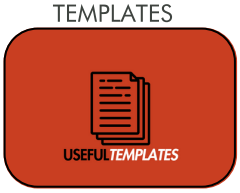
23 ABOUT IAB MENA

متوفر الآن باللغة العربية

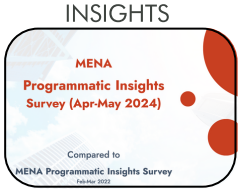
OTHER RELEVANT IAB MENA RESOURCES

ADTECH ECOSCAPE

ADTECH SELECTION TEMPLATES



PROGRAMMATIC INSIGHTS



ATTENTION GUIDE

Disclaimer

IAB MENA assumes no responsibility or liability for any errors or omissions in the content of this document. The information contained is provided on an "as is" basis with no guarantees of completeness, accuracy, usefulness or timeliness.

INTRODUCTION

IAB MENA estimates that the digital advertising investment in MENA reached $6,25Bill in 2023 and with growth rates well into double digits, digital advertising is likely to exceed $8Bill by 2026. But, equally ad fraud is growing both in terms of the overall impact on spend, and in new areas with new tactics. Some estimates suggest that as much as 20% of this spend is not reaching its intended audience due to deliberately fraudulent activity and is being siphoned off through a variety of means. That's a whopping $1,25Bill advertising investment potentially wasted in 2023, up to $1,6Bill by 2026! Ad fraud is quietly (and effectively) draining billions of dollars from advertising budgets. Fraudulent activities such as click fraud, impression fraud, app install fraud, and schemes targeting the entire ecosystem—spanning apps, Connected TV (CTV), and web—erode budgets, skew performance metrics, and diminish trust, ultimately undermining the effectiveness of digital marketing efforts.

This is not only a MENA challenge, this is a global phenomenon, but for a region with such significant scale and potential for digital expansion, tackling ad fraud is not just a financial necessity but a strategic priority for a sustainable industry.

All is not lost, with awareness of the challenge, there are many solutions to reduce this negative effect and increase the effectiveness of your investments. Firstly, we encourage all publishers to implement Ads.txt as a starting point. Launched in May 2017 by the IAB Tech Lab, the Authorized Digital Sellers project aims to tackle various types of ad fraud, most notably domain spoofing and illegal inventory arbitrage. Ads.txt is a simple text file that contains information about which companies are allowed to sell digital inventory on a particular domain. As it can be created and modified only by the webmaster of a domain, the information of the file is considered valid and authentic.

This guide, created collaboratively by the IAB MENA Adtech Taskforce delves further into the state of ad fraud in MENA, highlighting the various types of fraud, its financial impact, and actionable strategies businesses can adopt to protect their investments. By addressing this issue proactively, businesses can reduce lost revenue, enhance campaign performance, and contribute to building a more transparent and sustainable digital advertising ecosystem.

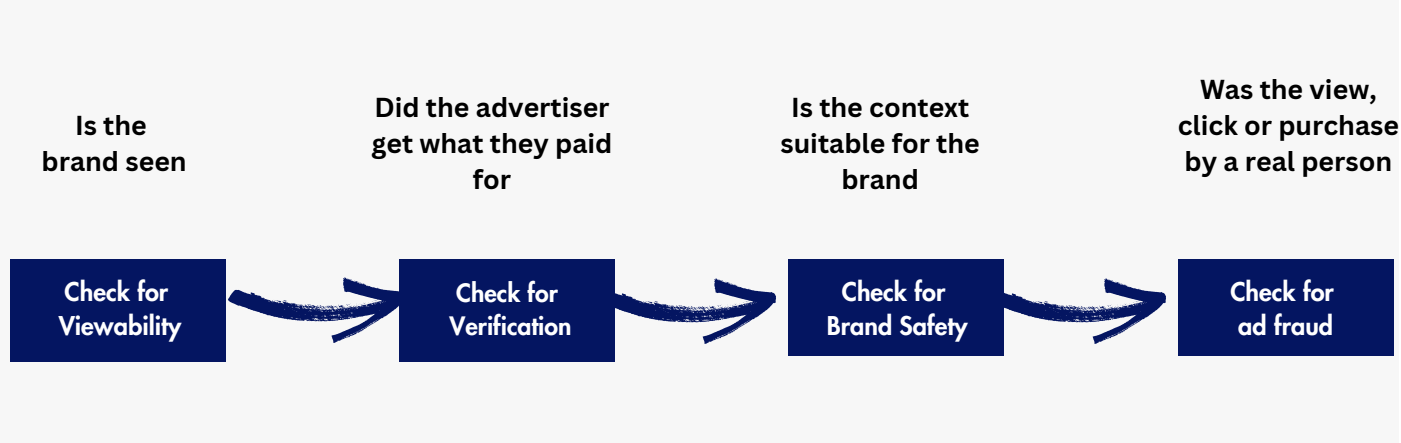
About Ads.txt

UNDERSTANDING AD FRAUD

To fully understand the role and extent that fraud plays within the ecosystem, it's best to consider ad fraud within a wider spectrum of media quality measures that drive better results. Consider how non-deliberate misrepresentation, such as viewability or other media quality measures are perhaps a low level misrepresentation, but have significant scale vs deliberate fraudulent activity such as domain spoofing, which may be more deliberate, harder to measure and thus less understood. Each is important in driving better quality and more predictable results for campaigns.

This paper aims to focus on the directly fraudulent activity seen in MENA, but is not exhaustive. Every attempt to mitigate fraud from activity should look to do so across the ecosystem. Consumer experience through responsible, honest and accurate advertising claims, through to ensuring brand suitability, viewability and other media quality measures should be considered alongside fraud detection and elimination.

Consider the spectrum below to see how brand safety, viewability and ad fraud detection work together to drive better results:



The removal of ad fraud from advertising campaigns has significant real world positive impacts on both KPIs and costs for advertisers. In essence, removing ad fraud allows advertisers to:

- **Maximize the effectiveness of their advertising budgets**
- **Gain a clearer understanding of their campaign performance**
- **Drive better results and achieve their marketing goals.**

TYPES OF AD FRAUD

TYPES OF AD FRAUD

Ad fraud, most often refers to invalid traffic (IVT), and is the fraudulent representation of online advertising impressions, clicks, conversions, or data events, in order to generate illicit revenue. These activities manipulate delivery channels, significantly impacting an advertiser's return on media investment, often jeopardising brand reputation.

Invalid traffic (IVT) takes two main forms:

General Invalid Traffic (GIVT):
Traffic generated by recognized industry crawlers, such as search engine bots, and traffic from bots exhibiting unnatural behaviour—like rapidly switching between websites every 10 seconds for extended periods—are often easier to identify.

Sophisticated Invalid Traffic (SIVT):
Invalid traffic that is significantly harder to identify, often necessitating sophisticated analytics, multi-layered collaboration, and extensive human intervention for accurate detection. This is often the most difficult to identify and combat.

Sadly, ad fraud or rather, fraudulent activity in advertising takes place throughout the ecosystem, many within lower funnel activities such as app downloads, cost per click/action activity all the way through to influencer fraud.

The following sections aim to identify many of these types of fraud and their potential impact on digital marketing investments. For navigation we have categorised them into:

- **Upper funnel**
- **Lower funnel**
- **CTV / FAST / OTT**
- **Retail Media**
- **Other (eg: influencers)**

This clarification is purely to make it easier to follow and more useful as a handy one pager you can use when considering individual planning types or channels. Thus, some fraud types may be represented in more than one category.

TYPES OF AD FRAUD - UPPER FUNNEL

These types of fraud involve generating illegitimate ad impressions to artificially inflate advertising costs. Perpetrators use various tactics like automated bots, non human traffic, or pixel stuffing to create false impressions, thereby misleading advertisers into believing their ads are being viewed by genuine users. This manipulation aims to deceive advertisers into paying for non genuine or non human traffic, resulting in wasted advertising budgets and skewed performance metrics. Examples of this category include:

Type	Description	Impact
Ad Stacking	This form of display and impression fraud occurs when mobile apps or websites layer several ads on top of each other in a single ad spot. Only the top ad might be visible but the rest are not.	• Click / sale ratios undervalue the impact of digital ads • End users do not see the ads
Malicious Bots / Click Fraud / Click spamming	Fraudsters use bots to produce large numbers of false clicks on ads or fake website visits. Also called Click Fraud or click spamming.	• Advertisers end up paying for clicks not made by humans • Click / sale ratios undervalue the impact of digital ads • Advertisers overpay as bot-clicks cannot drive sales or brand impacts • Organic Stealing
Pixel Stuffing	Happens when ads are squeezed into individual pixels, often as small as 1x1 in size. The platforms have a check to detect this, but they might use combinations like -30x-140, 3x7, etc. to bypass the checks.	• Ads are not seen so no awareness is generated • Loss of ad budget

TYPES OF AD FRAUD - LOWER FUNNEL

The second main category of ad fraud, these refer to deceitful practices wherein fraudsters manipulate or create fictitious conversion events, such as form submissions, sales, or app installs, with the aim to unjustly claim advertising commission or inflate performance metrics. This fraudulent activity is typically executed through methods like click injection, fake form submissions, or utilizing bots to simulate genuine user engagement, thereby distorting advertisers' insights and wasting advertising spend on invalid traffic or interactions.

Type	Description	Impact
Click Injection	An advanced type of click utilizes malicious software on mobile devices to detect when other apps are being downloaded and rapidly generates fake clicks. Common on Android, they take credit for app installs or other conversion actions they did not genuinely influence.	• Advertisers pay for illegitimate actions • Miss-attribution of the final event • Organic stealing
Coupon & Cashback Fraud	Certain coupon and cashback sites post ads promoting fake, misleading, or fraudulent coupons and cashback offers, falsely claiming they come from well-known advertisers.	• Miss-attribution of the final event • Organic stealing • False communication
Incent Activity (Incentive)	Fraudulent affiliates conduct incent marketing campaigns on incentive-based platforms, where users download or use an app for a reward rather than genuine interest.	• Low install-to-event ratio • Higher attribution cost • These users can negatively effect the overall ROAS.
Lead Punching	Fraudsters submit fake leads or multiple leads from a single device to meet the CPL expectation of a campaign.	• Low conversion • High back-end cost • Loss of budgets to bad leads • Call center budgets impacted

TYPES OF AD FRAUD - CTV/FAST/OTT

Unfortunately newer channels like CTV , FAST and OTT are affected by fraudulent activity as a result of non-transparency of the placement or reporting limitations.

Type	Description	Impact
App Spoofing	Malicious apps disguise themselves as popular FAST channels to siphon ad budgets.	• Ads served on unauthorized or low-quality inventory • lack of transparency on where ads are flighted.
Device Spoofing	Running ads through fake CTV device IDs generated by botnets to simulate millions of "viewers" across FAST apps.	• Inflated reach metrics, fake audience delivery.
Ghost Ads	Ads "served" when TVs are off, or when apps run in background processes without user engagement.	• Zero visibility, wasted impressions.
Replay & Loop Fraud	Recorded ad sessions are replayed repeatedly to fake legitimate viewership.	• Artificial frequency inflation.
SSAI Manipulation 2.0	Fraudsters inject false ad requests via server-side ad insertion, making ads appear as legitimate impressions even when no viewer exists.	• Wastage due to invisible impressions.

TYPES OF AD FRAUD - RETAIL MEDIA

While Retail media fraud is typically included within the lower funnel type of fraud, as its new and growing category, we have called them out separately below.

Type	Description	Impact
Attribution Fraud / Hijacking	Fraudulent entities (or internal misconfigurations) manipulate last-click or view-through attribution models.	• Paying for fake performance • Retail MENA network claims credit through a cookie or impression.
Affiliate Hijacking	Redirecting legitimate traffic through fraudulent affiliate links to steal attribution and commissions.	• Paying illegitimate players not part of the plan.
Coupon & Loyalty Abuse	Fraudsters exploit digital coupons and loyalty programs by using automated scripts or fake accounts.	• Miss-attribution of the final event • Organic stealing • False communication.
Fake Clicks & Impressions	Automated bots generate clicks on sponsored product listings or banner ads to inflate engagement metrics.	• Paying for fake performance.
Fake Product Listings	Fraudulent sellers use ads to promote products that don't exist or never ship.	• Lack of transparency for both consumers and advertisers • Damages brand trust and inflates campaign performance metrics.

TYPES OF AD FRAUD - OTHER

The remaining types of fraud involve amongst others fraudulent use of websites, Apps or Influencers.

Type	Description	Impact
APK Fraud (APK is a file format that Android uses to distribute and install apps)	Distributing fake or malicious versions of apps through unofficial channels. Installs come from deprecated OS versions.	• Data security issues • Untrackable installs • Impossible to update apps
Domain spoofing	When a fraudulent website disguises itself as a legitimate, high-traffic site to deceive advertisers. By misrepresenting its domain, ads intended for reputable publishers, end up instead enriching fraudsters.	• Loss of ad budget • No source data
Influencers	Influencers misrepresent brands or misuse coupons to steal the attribution of a sale. eg: coupons given to the influencers land on coupon sites. This generates sales but has nothing to do with the influencer's reach.	• Overvaluing and therefore overpaying Influencers • False attribution
Made-For-Ads Sites (MFA)	Websites specifically built to attract clicks. They are often low-quality or irrelevant, designed to attract clicks and impressions without providing any real value to users.	• Loss of advertising budgets • Low conversions

DETECTION AND MITIGATION OF AD FRAUD

iab mena

AD FRAUD DETECTION: WEB

Practical methods to identify fraudulent activities on the web include; quick audits, behavioral red flags, traffic analysis, engagement metrics, and 3rd party verification tools. DSP's also have a role to play by providing transparent data, proactive fraud detection tools, brand-safe inventory and relevant 3rd party integrations. By implementing proactive fraud detection strategies, advertisers can safeguard their investments and maintain transparent, high-quality ad environments.

Pre-bid verification services from third-party verification platforms allow you to define your brand's risk tolerance, either by customizing settings or selecting from predefined options. Once activated, they evaluate every single ad impression in real-time before your ad is served, automatically blocking any that do not meet your brand safety criteria.

Compared to manual blocking, third-party pre-bid tools offer more advanced and dynamic protection, including real-time, page-level scanning. They not only reduce exposure to unsafe environments but also unlock higher-quality and more auctionable inventory by ensuring safer

Example suppliers in MENA who can support Web ad fraud detection and mitigation	DoubleVerify	IAS	mFilterit	Traffic Guard

Alternatively, you can do a manual process, following these 6 actions:

1 Identify & Define Threats to Brand Safety

- Classify threats based on risk tolerance:
  - High Risk: Fraudulent traffic, bot-driven impressions, domain spoofing, fake ad placements
  - Moderate Risk: Non-viewable impressions, misclassified inventory, low-quality traffic
  - Low Risk: Minor mismatches in audience targeting or misaligned contextual placements
- Define key risk factors that impact brand perception, engagement quality, and budget efficiency

2 Maintain a Dynamic Blacklist of Keywords, Websites & App

- Regularly update blacklists for high-risk websites, unverified apps, and unsafe keyword triggers
- Exclude unidentifiable domain extensions and AI-generated keyword insertion websites
- Blacklist content categories such as:
  - Discriminatory or controversial topics (political extremism, misinformation, hate speech)
  - Natural & manmade disasters (war zones, tragedies, crisis coverage)
  - Low-volume/non-secure web domains & apps (unverified publishers, uncertified ad networks)
  - High-risk inventory sources (VPN services, adult content, politically sensitive news)

AD FRAUD DETECTION: WEB

3 Implement Advanced Viewability Filters

- Utilize variable viewability thresholds based on:
  - Campaign objectives (awareness, engagement, conversion)
  - Ad format performance (video vs. display vs. native placements)
  - Time-in-view & interaction metrics rather than just ad visibility.

4 Apply Content Classification & Digital Content Labels

- Implement DSP and SSP-level filtering based on:
  - Brand Safety Segments: Exclude categories that conflict with brand values
  - Digital Content Labels (DCL): Ensure ads do not appear alongside inappropriate content
  - Contextual Relevance Filters: Target content that aligns with audience intent and avoids unsafe environments.

5 Select Reputable Inventory Sources & Partners

- Prioritize verified ad exchanges, direct deals, and premium publishers. For Retail Media, work with RMNs that provide full transparency on impression-level data and traffic sources
- Avoid open auction inventory with unknown or misclassified sources
- Leverage ads.txt & sellers.json validation to prevent domain spoofing and unauthorized reselling
- Monitor placement reports regularly to remove non-compliant publishers.

6 Continuous Monitoring & Fraud Detection Measures

- Exclude live-streaming inventory and freshly indexed pages that lack classification
- Conduct real-time monitoring of media metrics, such as:
  - Irregular traffic spikes
    - eg: sudden CTR or impression surges
    - eg: ongoing spikes for single source could indicate fradulent activity
  - Disproportionate conversion rates
    - eg: clicks not translating to installs/sessions
    - eg: high CTR with high bounce rate could indicate Bot traffic
  - Repetitive click injection patterns (geo-targeting fraud)
  - Attribution imbalances
    - eg: high post-view conversions vs. post-click interactions
    - eg: KPI increase that doesn't lead to an increase in real metrics (Orders/Revenue)
- Implement server-to-server integrations to maintain transparency in measurement
- Verify app installs using cross-platform validation (MMP vs. official app store data)
- Request SKU-level, channel-level, and placement-level transparency for Retail Media.

AD FRAUD DETECTION: APP

Fraud in mobile app advertising typically involves fake installs, fake ad impressions generated by bots, click injection, and SDK spoofing.

These 5 actions will help to detect fraudulent activity in app environments:

1 Secure Attribution & Measurement Integrity

- Use Server-to-Server (S2S) Attribution to prevent SDK spoofing
- Enable post-install analytics to cross-verify installs
- Compare Click-to-Install Time (CTIT) distributions for unnatural spikes
- Validate install sources and flag suspicious device IDs.

2 Strengthen App Install & In-App Event Validation

- Monitor high post-view conversion vs. post-click metrics to detect fraud
- Ensure ATT compliance (iOS) to prevent unauthorized tracking
- Track OS versions & user agents for outdated or jailbroken devices
- Match MMP & store data to verify install legitimacy.

3 Implement Pre-Bid & Inventory Filters for Ad Placement

- Whitelist premium inventory and verified publishers
- Exclude high-risk categories (VPN, incentivized traffic, low-quality apps)
- Monitor ad placements for bot-driven engagement.

4 Advanced Fraud Detection & Real-Time Monitoring

- Analyze Click-To-Install Ratios (CTIR) to detect click spamming
- Use AI-powered anomaly detection for IP clustering & bot patterns
- Monitor app uninstall rates & post-install engagement for irregularities
- Cross-verify in-app purchases vs. install volumes to detect fake users.

5 Device & Network Security Measures

- Prevent direct APK installs from third-party sources
- Block traffic from emulators, bots, and suspicious user agents
- Enforce frequency capping to reduce click flooding.

Example suppliers in MENA who can support App ad fraud detection and mitigation

Adjust | Appsflyer | mFilterit | Tapper AI | Traffic Guard

AD FRAUD DETECTION: CTV/FAST/OTT

CTV ad fraud has become increasingly sophisticated with methods like device spoofing and SSAI (Server-Side Ad Insertion) manipulation.

To protect CTV investments, advertisers must be diligent, proactive, and selective in their buying approach. The following 3 approaches help to identify and mitigate against fraud in CTV:

1 **Diligent Inventory Buying:**

- Going directly to the inventory publisher or buying with through PMP deals via DSPs
- Cross-referencing device IDs against legitimate CTV device lists.

2 **Selective Publisher choices:**

- Ensure publishers abide by industry standard and compliance (eg: IAB TechLab's Open Measurement SDK for CTV & TAG best Practices)

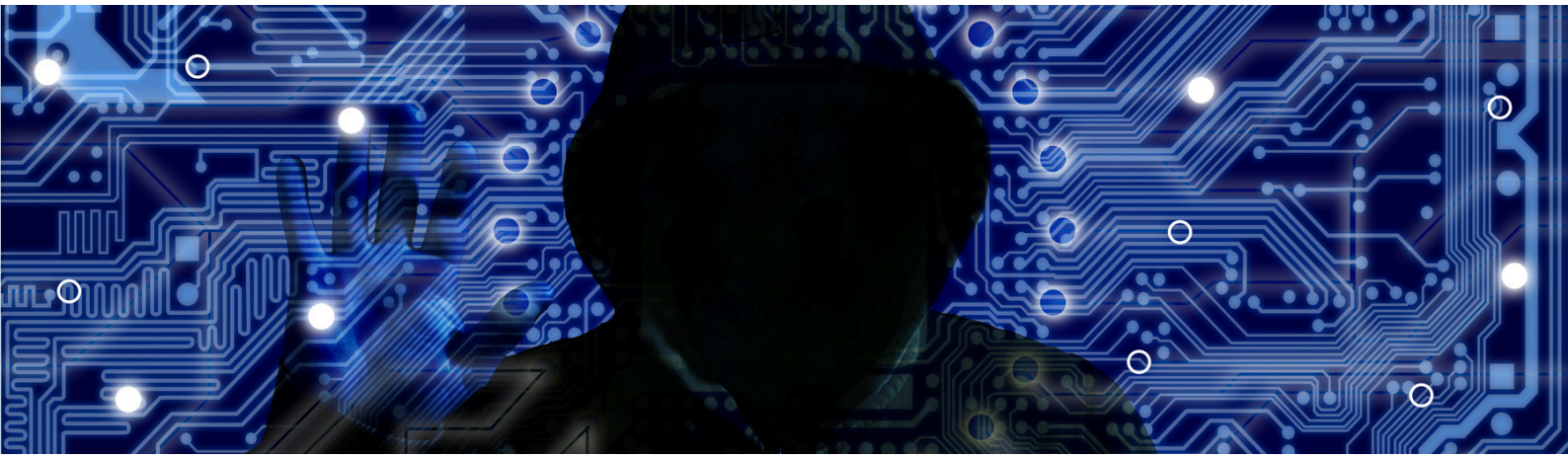
3 **Proactive Verification and Monitoring:**

- Set up real time dashboard integrated with Publisher/DSP log level data along with third party verification tool data to observe and compare against historical or industry standard benchmarks
- Monitor for SSAI manipulation by ensuring server-to-server transparency.

Example suppliers in MENA who can support CTV ad fraud detection and mitigation

DoubleVerify

IAS



AD FRAUD DETECTION: RETAIL MEDIA

Ad fraud in Retail Media Networks (RMNs) is an emerging concern as brands increasingly shift budgets to retail platforms. As these ecosystems grow, so do the risks associated with invalid traffic (IVT), fake impressions, and misattribution.

The following 4 approaches help to identify and mitigate against fraud ion Retail Media Neyworks:

1 **Demand 3rd-Party Verification**

Use ad verification tools for viewability, IVT, and brand safety (if the RMN allows it).

Push RMNs to integrate with verification partners; some top RMNs now support this.

2 **Focus on First-Party Outcomes**

Track sales lift, ROAS, and customer acquisition using first-party CRM data.

Use clean rooms or CDP integrations to verify conversions independently.

3 **Run A/B Holdouts**

Compare test vs. control groups to isolate incremental impact.

This helps identify inflated or misattributed performance.

4 **Audit Traffic Sources**

Scrutinize traffic origins, especially if you're running on offsite RMN extensions (e.g., programmatic inventory).

High CTR + low conversions = red flag.

Request SKU-level, channel-level, and placement-level transparency.

Work with RMNs that provide full transparency on impression-level data and traffic sources.

AD FRAUD DETECTION: MANAGED SERVICE

When using a managed service for campaigns, it can sometimes be more complicated to identify fraudulent activity due to limited visibility on the details of campaign metrics and performance, while the service provider should be preventing fraud as a matter of course, there are a few key considerations or checks you can put into place to reduce the probability of fraudulent activity in your campaigns.

1 Ad Server & Tracking Security

- Ad server integration is mandatory in web environments to ensure proper attribution
- Enable built-in fraud prevention measures in Mobile Measurement Partners (MMPs)
- Only buy inventory from measurable and authenticated sources (eg. HTTPS-secured domains, ads.txt-verified publishers).

2 Ensuring Media Metrics & User Behavior Alignment

- Maintain a healthy correlation between click data and user engagement
- Watch for red flags, such as:
  - Millions of clicks but disproportionately low installs or sessions
  - Abnormal attribution patterns (high post-view conversions with low engagement)
  - High app uninstall rates immediately after install
- Cross-verify install numbers between MMP dashboards & official app store data
- Ensure app tracking includes ATT requests (iOS) and OS-level version tracking.

3 DSP Transparency

- Even in managed models, some DSP's can provide log-level transparency, curated marketplaces, and buyer-controlled safety layers.

SELECTING ADTECH & MANAGING PERCEPTIONS

ADTECH SELECTION

When considering the Adtech partner to monitor and mitigate against ad fraud, it's important to consider the type of ad fraud you are most interested in addressing. While some solutions offer integrated approaches covering a range of use case, others specialise in specific areas. As such, part of the evaluation is to establish which areas are most important and whether these require multiple solutions, or can be addressed through integrated solutions.

By accessing this template, you are able to consider all the needs you may have, prioritise those you're most interested in and thus make an informed decision on the right mix of suppliers for your needs, from verification through to the different types of ad fraud. Considerations when selecting an Adtech partner are to consider to what extent each partner provides satisfactory detection and reporting of the following:

- Overall solution
- Ad fraud (eg: invalid traffic)
- App fraud
- Viewability
- Brand Safety and Suitability.

Naturally considerations should also include:

- Ease of Use
- Reporting Quality
- Integrations
- Cost.

Download Template

MANAGING PERCEPTION

By removing ad fraud there will be an impact on reported performance, which needs to be fully understood to avoid misattribution of effects. When ad fraud is effectively removed, the impact on CPX (e.g. CPI, CPA) is generally a decrease when looking at the "true" or "effective" cost, but reported metrics may signal an increase.

Ad fraud inflates metrics, as when fraudulent installs or actions occur, advertisers pay for them, even though they provide no real value. This artificially lowers the apparent CPI and CPA. These low numbers are misleading. They don't reflect the actual cost of acquiring a real user or customer.

A low CPI or CPA, may hide the fact that a large portion of those installs or actions are from bots or fake users. Marketing budget is being wasted.

By eliminating fraud, advertisers stop paying for worthless installs and actions. This means the raw CPI and CPA numbers might initially appear to rise, as the "fake" low numbers are removed. However, the effective CPI and CPA—the cost of acquiring a genuine user or customer—will actually decrease. In other words, advertisers are now paying for real results, which in the long run, is more cost effective.

The CPI or CPA might be slightly higher, but they represent real, valuable installs or actions. ie: Better real-world ROI.

Real-world Impact on KPIs:

- Increased Return on Advertising Spend (ROAS)
- Improved Conversion Rates
- More Accurate Data and Analytics
- Enhanced Customer Acquisition Quality
- Better Campaign Optimization.

Real-world Impact on Costs:

- Reduced Ad Spend Waste
- Lower Customer Acquisition Costs (CAC)
- Savings on Resources
- Improved Budget Allocation.

THANKS TO CONTRIBUTORS

THANKS TO THE TASKFORCE

IAB MENA Taskforces include subject matter experts from our membership to drive and execute specific initiatives and tasks. They are the primary collaboration and networking opportunity for members to drive real insight and collective progress across our industry.

The Adtech Task force focuses on driving knowledge of the Adtech ecosystem, helping to deliver a more robust local marketplace by supporting the development and growth of the ecosystem while maintaining standards and global best practices.

Thanks to the following member companies who actively participated in writing this guide

ArabyAds

bidease

DoubleVerify

digital media services
a Choueiri Group Brand

INMOBI

GoWit

MiQ

mFilterIt

OMG OMNICOM MEDIA GROUP

PUBLICIS MEDIA

ABOUT IAB MENA

The Interactive Advertising Bureau (IAB MENA) is the regional voice and thought leader of the region's interactive marketing and advertising industry, committed to building a sustainable future for digital advertising in the region.

Our members number in excess of 75 companies that represent the full spectrum of the MENA digital advertising industry and include:

- Advertisers
- Agencies
- Measurement Companies
- Publishers
- Research Companies
- Sales Houses
- Technology Platforms

Our Vision

To be the catalyst for growing the MENA digital advertising economy by nurturing the community, accelerating knowledge sharing and establishing accountability standards that cultivate trust and credibility.

Our Mission

Positively influence corporate leaders & policymakers to value diversity & inclusion as a key currency for the growth of the digital economy in MENA through awareness initiatives and enabling thought-starting conversations between our members and partners.

Collaborate with the industry on the development of unbiased digital learning and development programs to expand the market's understanding of how digital best practices drive their business success.

Become the authority in setting up the standards of measurement, research & attribution for the industry for the benefit of industry growth, trust and sustainability.

Inspire innovation and partnerships to support the development of a world-class, contemporary ecosystem of marketing solutions and services in MENA.

*For more information go to **iabmena.com***

iab mena