Content & Advertising Working Group

March 14th 2024

Anti-Trust Policy

- Anti-trust law prohibits agreements (written or implicit) between competitors that may negatively impact consumers or competitors and sharing of confidential information
- Anti-trust violations do not require proof of a formal agreement. A violation may be alleged based upon the mere appearance of unlawful activity.
- All meeting participants must abide by the following rules:
  - DO clearly identify the positive purpose of each project and follow it
  - DO NOT enter into agreements that restrict other parties' actions
  - DO NOT give rise to barriers to market entry
  - DO NOT discuss or exchange specific, confidential or commercially sensitive data on pricing, promotions and business plans
- Anti-trust laws do not prohibit petitioning the government, educating and informing the public, improving quality and safety standards, or protecting the public from fraud.

Agenda

MEF MOBILE ECOSYSTEM FORUM

01 Welcome

02 News

03 Report

04 Changes to the team

05 Members – what do you want to achieve?

06 Upcoming Events

07 Next Meeting

01 Your Content & Advertising Team

- NARAYAN **JAESINGH** (India)
- Partner of Industry Practice

- DARIO **BETTI** (UK/Italy)
- MEF CEO

- EWA **PEPPITT** (UK)
- Administrative Lead for Content & Advertising

01 Content & Advertising Working Group

MISSION
To Become the Industry Voice on How to Better Serve Customers Through Personalisation Whilst Protecting Consumer Trust in the Digital Era

DELIVERABLES: (NB. At this time these are ideas and it is up to you, MEF members, to ultimately decide the direction this – or any – working group takes when things get underway in 2022)

- Monthly forum for the review and discussions of new industry trends impacting all stakeholders viz. Consumer, Technology and Media / Content
- Whitepaper/reports/infographics/webinars/videos/social media to educate the market and stakeholders
- Creation of best practices for enhancing Digital Advertising, customer experiences across media platforms and Protecting Consumer Trust (Ad Fraud) (C&A Best Practice)
- Aligning Media, MNOs & D2C organisations with thought leader approaches for designing aspects of (i) Monetisation, (ii) Personalisation, (iii) Adoption and (iv) Ad-Fraud / Data Privacy innovations that are applicable multi country / geography

FOUNDER MEMBERS:
- Aegis Mobile
- Alchemy Telco
- AWG
- BICS
- BT
- Cheetah Digital
- China Mobile International
- Dexatel
- Direqt
- Dotgo
- Empello
- Enabld
- Engage Mobile
- Global Point View
- Globe Teleservices
- GMS
- Golden Goose
- imimobile
- Infobip
- Intis Telecom
- Kaleyra
- LANCK Telecom
- Mavenir
- Messente
- MCP Insight
- Mobilesquared
- Morethan160
- Ooredoo Group
- Out There Media
- PM Connect
- Sam Media
- TeleSign

02 The Asia Pacific Mobile market stabilises

AsiaPac

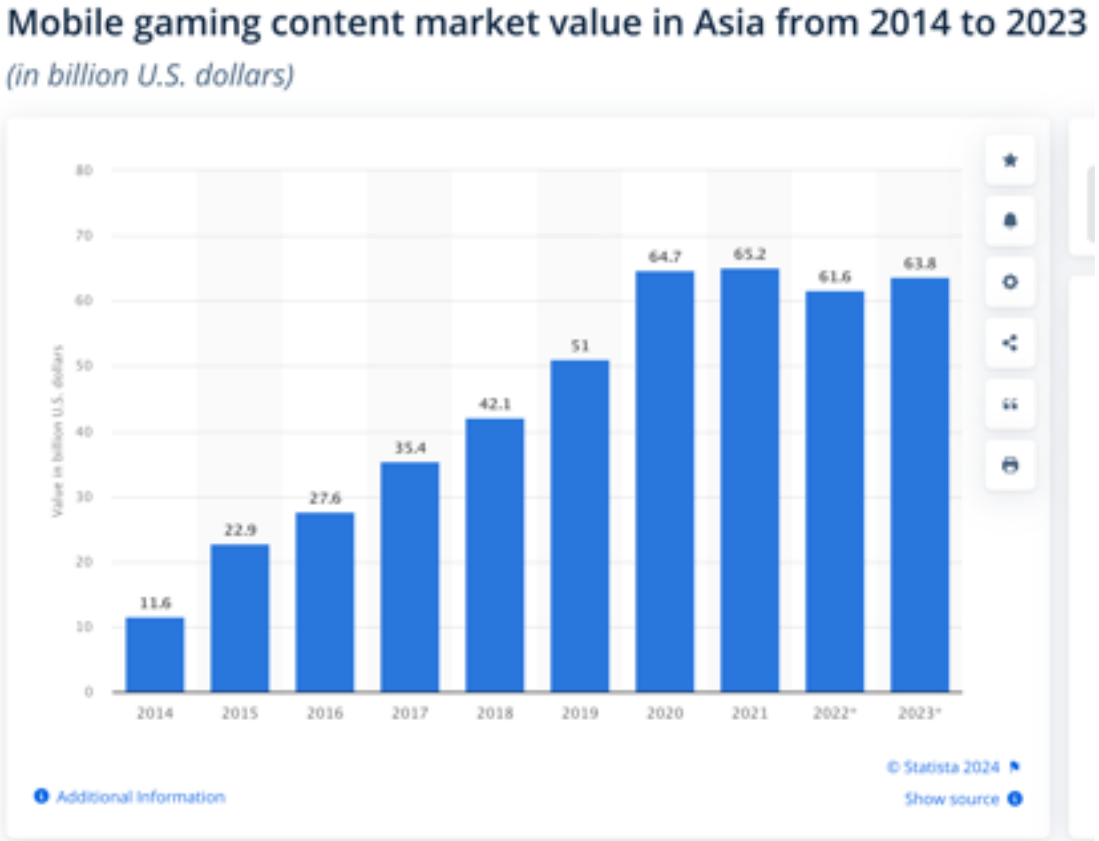
Displaying huge increases of value from 2014 onwards, the mobile content market in the Asia Pacific region was forecast to be worth close to 64 billion U.S. dollars by 2023, marking a slight decrease from the market's peak in 2021.

Strength of Asia-Pacific gaming

It is known that the Asia-Pacific region makes up almost half of the games market revenue worldwide, with globally renown APAC gaming giants continuing to display huge revenues. Although many countries throughout the region have strong gaming industries, it cannot be denied that China leads the Asia-Pacific gaming sector. Not only does China reign in APAC, but China stands as the leading gaming market globally in terms of revenue, beating the United States to the top spot. Throughout the past decade, China, like many other Asia-Pacific countries, has exhibited huge increases in mobile game sales revenue.

The rise of mobile gaming

The mobile gaming sector in APAC has experienced a surge in users throughout recent years. Now more than ever, consumers, such as those in South Korea, are choosing to play mobile games rather than traditional games involving consoles. The rise in the number of smartphones is likely a main factor as to why the mobile gaming industry has seen dramatic growth. Increased smartphone ownership allows easier game accessibility for consumers, while making it easier for consumers to make in-game purchases. Thus, boosting the mobile gaming industry further.



02 Turkcell boosts edge content delivery

- Turkcell, working with Qwilt and Cisco, wants to improve streaming quality and data delivery for its 38.2m mobile and 3.1m fixed broadband subscribers
- Cisco and Qwilt announced a strategic partnership with Turkcell to enhance the quality of and capacity for digital content and applications. The aim is to improve streaming experiences and speed data delivery to Turkcell's 38.2 million mobile users and 3.1 million fixed broadband customers. It also supports the constantly growing traffic levels.
- Turkcell's adoption of Qwilt's Open Edge Cloud for Content Delivery platform is powered by Open Caching and enabled by Cisco's edge computing and networking infrastructure. The joint solution is embedded in and integrated with Turkcell's network edge.
-

Indian ministers calls for Direct to Mobile TV

- India Union Minister Anurag Thakur on Thursday made a strong pitch for exploring innovative broadcasting options such as Direct-to-Mobile to ensure a wider reach of content to all strata of society and also become self-reliant in the sector.
- Inaugurating the annual Broadcast Engineering Society Expo, Thakur also stressed the need to encourage indigenous research and development by nurturing scientific talent and fostering partnerships between industry and academia.
- "New Direct to Mobile (D2M) technologies offer exciting content possibilities for terrestrial broadcasting not only to television but also on handheld devices such as mobile phones, and notepads anywhere, on an anytime basis, and that too without the need for Internet," the Information and Broadcasting Minister said.
- "We must explore and embrace innovative options of broadcasting like Next Gen broadcasting which shall not only ensure wider reach to cater to all strata of our society but also catalyse ever-evolving user experience," the minister said.

South East: Mobile advertising trends

- Southeast Asia's smartphone penetration rate, which stands at a whopping 88.9%, presents marketers in the region with a goldmine of opportunities to reach, engage, and convert digitally-savvy audiences.

The Drum

- **The future is live**
  - Live experiences are not just a passing trend in Southeast Asia but a cultural phenomenon deeply ingrained in the region's digital landscape. To miss this promising phenomenon is to miss connecting with millions of users in real time.
  - Particularly in Indonesia, the love for live experiences comes alive on the smartphone lock screen, where users clock 2 million watch hours a month (Glance platform data). Indonesians spend a significant amount of time engaging with their favorite content, and this is being utilized by Indofood Freiss.
  - The brand harnessed the power of live and reached 703k Indonesians on the smart lock screen. Perfectly timed messaging and an interactive approach are what enabled the brand to make an impact on its target audience. Besides this, effectively retargeting the viewers of the live stream and offering them an irresistible deal led Indofood Freiss to achieve 102% of its coupon redemption target.

- **Gaming is reigning supreme**
  - The mobile is the new console. With esports having become an official medal sport at the Asian Games, we see millions of smartphone users in Southeast Asia gaming, streaming, and competing from their "always-on" devices.
  - This demand for gaming on the go has also led to massive success for single-tap gaming in Indonesia, with the smartphone lock screen acting as the arcade for 7 million monthly active gamers (Glance platform data).
  - Single-tap esports is also seeing astonishing success. In February 2023, 1.67 million viewers from Indonesia joined the 12-day Goddess League live tournament for Mobile Legends Bang Bang. The six-day iFeL Southeast Asia Championship livestream also attracted 8.4 million views, a record 3 million+ more than YouTube and TikTok combined for the same tournament.

www.thedrum.com/open-mic/mobile-advertising-in-southeast-asia-2024-trends-and-what-they-mean-for-marketers

New Leader in puzzle games

FINANCIAL TIMES

Puzzle game 'Royal Match' dethrones 'Candy Crush' from top of app store

Istanbul-based developer Dream Games is on track to double revenue from its debut title despite a lacklustre year for mobile peers

- Puzzle app Royal Match, developed by a small team in Istanbul, has overtaken Microsoft-owned Candy Crush Saga as the most lucrative mobile game in the world, outshining other smartphone titles during a lacklustre 12 months for the industry. Royal Match became the biggest mobile game by monthly revenue globally in July and has held the top spot since then, according to Data.ai, which tracks consumer spending on Apple and Android app stores. Launched in 2021, it is the debut title from Dream Games, a Turkish start-up valued at $2.75bn early last year
- For more than a decade, King's Candy Crush Saga has been one of the world's most consistently popular games on any platform, hitting $20bn in cumulative revenue this year. Now part of Microsoft after its $75bn buyout of Activision Blizzard, Candy Crush has spent only six months outside the top 10 highest-revenue mobile games since it was released in late 2012, according to Data.ai

https://www.ft.com/content/1bb1ed54-821e-49bf-b12d-353b98fa9912

Apple in EU: opening stores

FINANCIAL TIMES

Apple rivals lobby EU over App Store dominance

Meta and Microsoft want Brussels regulators to extract more concessions that unpick iOS mobile software

FEBRUARY 21 2024

- Apple is coming under fire from rivals Meta and Microsoft who say its plans to open up its mobile software to comply with a landmark EU law fail to go far enough, as the iPhone maker faces unprecedented regulatory challenges from Brussels over the coming month. EU regulators, who are preparing to fine the tech giant €500mn in March over allegedly favouring its music streaming app against competitors such as Spotify, are also being lobbied to reject Apple's proposals to satisfy the **bloc's Digital Markets Act.** The growing backlash against Apple comes as it is forced to make some of the biggest changes to its business model in years, following concerns over the dominance of its App Store, which forms a large share of the company's $85bn-a-year services business. Apple announced last month it will make changes to its iOS mobile software in Europe, such as allowing users to download apps from other sources and access alternative payment systems. The changes were offered ahead of the EU's March 7 deadline for companies to declare how they will adhere to the DMA, which aims to tackle the market power of Big Tech groups. The proposal leaves developers with a dilemma: stick with Apple's existing ecosystem and fees, or leave permanently and face new terms. For those who choose to also build apps in alternative stores, Apple said it would cut the highest amount paid by companies using its App Store to sell digital goods and services from 30 per cent to 17 per cent.

https://www.ft.com/content/b4800998-5658-4068-b7f8-22a1f64c10ae

Content & Advertising Fraud Framework

Report prepared by the team

- First Draft ready
- Missing diagrams
- Looking for support in descriptions for diagram (visuals will be created based on those)

MEF MOBILE ECOSYSTEM FORUM

CONTRIBUTING MEMBERS

infobip

INTENTFUL® a gms company

MOBIBOX OUT OF THE BOX TECHNOLOGY

smadex by entravision

telecoming

INTRODUCTION

MEF's Content & Advertising Working group was established in 2022, uniting all stakeholders in the Content & Advertising ecosystem to support the deployment of best practices to limit fraudulent behaviours as well as enable the development of new advertising technologies and business models. Its collaborative cross-ecosystem working group is represented by senior executives from across Ad Tech, Content Production, Verification and Consumer Research teams.

Digital advertising has revolutionized the marketing landscape, leveraging online platforms to connect businesses with their target audience. With the rise of the internet, brands now have unprecedented opportunities to reach consumers through various channels, including social media, search engines, and display networks. This dynamic and data-driven approach enables precise targeting, personalized content delivery, and measurable results, making digital advertising an essential component of modern marketing strategies.

However, it is also imperative that across the entire ecosystem, all necessary actions are taken to prevent and mitigate fraud attacks to ensure the sustainability of digital advertising as a trusted marketing channel. Common understanding and awareness across the advertising ecosystem is essential.

This First Version of this Framework released in 2024 will set the foundations for the work of the Programme to develop best practice guidelines for the digital advertising industry.

As the Advertising & Content ecosystem continues to evolve, the working group regularly reviews the fraud framework to ensure that it remains current. New versions will undoubtedly come as the group meets to assess the ever-changing advertising landscape.

The framework is recommended for anyone buying or delivering digital ads

- Enterprises
- Digital Agencies
- Content Providers
- Consumers

The framework helps all stakeholders

- Understand why fraud exists
- Recognise the fraud types which affect the ecosystem today
- Identify the different stakeholders within the ecosystem
- Consider the impact of fraud on the whole ecosystem
- Learn what steps can be taken to mitigate and protect against fraud

CONTENTS

MEF MOBILE ECOSYSTEM FORUM

CONTENTS

BUSINESS SMS ECOSYSTEM

Mobile advertising has undergone a significant transformation, progressing from basic banner ads to a highly sophisticated ecosystem. Simple ads have given way to targeted advertising driven by advanced data analytics and machine learning. The rise of social media and mobile apps has expanded advertising opportunities, enabling personalised and engaging content. The ecosystem also contains parties which are not directly engaged within the end-to-end ad delivery, but provide support services such as testing, reporting or even the content itself being monetised through advertising. Here is an overview of the ecosystem:

CONTENT MEDIA

- OTTs
- Streaming App
- Gaming

TECHNOLOGY

- Agencies, Platforms
- Analytics
- Channels
- Service Providers

GOVERNANCE

- Regulation
- Data Privacy
- Ad-Fraud/ID Verification

CONSUMER

- Research / Framework Companies

ENTERPRISES

WHY DOES FRAUD EXIST

By definition, fraud is wrongful or criminal deception, intended to result in financial or personal gain, against an individual or organisation.

The global advertising ecosystem has grown and developed at different rates across different regions in order to meet demand, accommodate local requirements and to comply with legal and regulatory requirements. As such, the level of advancement and maturity of some countries compared to others means that the barriers to prevent fraud are lower in some countries than in others.

Fraud is indiscriminate. It can impact all parties within the business SMS ecosystem, either directly or indirectly and is carried out in order to achieve one or more of the following objectives:

Identity Theft
Obtaining information required to steal someone's identity

Data Theft
Obtaining information required to access personal and private banking or other financial accounts

Commercial Exploitation
To gain competitive advantage by exploiting gaps within the commercial structures of the ecosystem

Network/System Manipulation
To gain competitive advantage or perform illegal activities via the deliberate manipulation of ad delivery or the exploitation of system vulnerabilities to bypass protection measures intended to safeguard advertisers and consumers

IMPACTS OF FRAUD

The impact and consequences of fraud are felt globally.

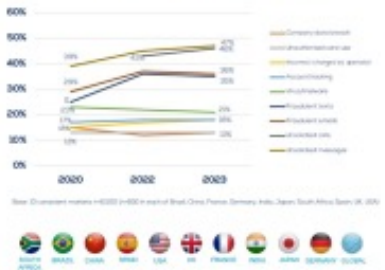
As these scenarios show, fraud within the Advertising ecosystem can have a significant and direct detrimental impact on individuals, in addition to the wider financial implications and reputational damage caused to parties who have a genuine commercial relationship with a victim.

In MEF's annual global consumer study which looks at the attitudes and behaviours of smartphone users in 10 countries, there was an upward trend of data harm from 2020 to 2023.

The level of impact will vary by region and country because the global ecosystem operates within a complex set of legal, regulatory and commercial frameworks which differ by country and which may see a certain practice permitted in one country but not another. The enforcement of regulations or contracts can also influence how local markets operate and facilitate some types of fraud as parties seek to exploit gaps in these frameworks to bypass authorised and regulated routes to meet ill-advised demand for low-cost advertising, to gain commercial advantage or at worst, to commit theft.

As market opportunities grow within national and global enterprise communities, so does the significance and impact of fraud on the quality and reliability of services, on the ability for legitimate players to monetise services, and ultimately, on the continued growth of the sector.

REPORTED DATA HARMS OVER TIME - 10 CONSISTENT MARKET



The direct monetary losses being incurred by the industry through fraud are significant. However, the real impact of fraud on the global ecosystem extends beyond the direct financial losses incurred.

FINANCIAL IMPACT

- Theft from or the unsuspecting disclosure of personal or confidential information and data by a consumer can result in:
  1. Unknowingly authorising financial transactions
  2. Bank accounts being taken
  3. Damage to credit scores and personal financial status
  4. Bill shock as a result of illicit purchases
- Paid for ads not being displayed

REPUTATIONAL DAMAGE

- Brand damage caused by association to fraudulent activity

LOSS OF TRUST IN DIGITAL ADVERTISING

- Legitimate advertisements may be ignored if consumers believe them to be annoying, irrelevant or even intrusive
- Increased uncertainty amongst businesses, consumers and regulatory agencies about digital advertising will affect adoption rates for new services, sectors and markets and the long-term growth of the sector

CUSTOMER DISSATISFACTION

- Customer complaints are directed at the party with which a consumer has a direct relationship, namely a business
- Annoyance at the receipt of unwanted or irrelevant advertisements, including:
  1. Unsolicited 'prize draw' advertisements which claim that the recipient can claim a prize in exchange
  2. Overzealous marketing from an unknown sender or even a known brand innocuous messages masking something more sinister
  3. Inappropriate content displaying for minors

Content & Advertising Fraud Framework

UNFAIR MARKET ENVIRONMENT

- Businesses who do not participant in fraudulent activity are placed at a disadvantage and may become less competitive - legitimate companies lose business to less ethical ones

REGULATORY INTERVENTION

- Targeted regulatory controls introduced to address consumer harm can limit the flexibility of advertising solutions

FRAUD MAPPING

GRAPHIC WILL BE UPDATED HERE

This framework identifies 14 fraud types, each of which directly impacts on one or more of the four core communities within the Content & Advertising Ecosystem.

Some of the fraud types are highly complex and cut across a large proportion of the Advertising delivery chain

The solutions identified to detect and protect against fraud include commercial, technical and process, compliance and legal requirements and will need continuous cross-ecosystem collaboration to fully address all aspects of fraud in the Advertising ecosystem and be successfully implemented.

#1 CLICK SPAMMING

DEFINITION

Also referred to as click flooding, click spamming is a type of mobile ad fraud in which networks report a high number of fake clicks with the goal of receiving credit for the last click before a conversion.

CAUSE

Click spamming involves sending thousands or even millions of clicks to a Mobile Measurement Partner (MMP). Since the chance of misattribution is very low on a per-click basis, the high volumes increase the probability that the MMP will misattribute some clicks, resulting in a payout for the fraudsters. On top of stealing the advertiser's budget, click spamming can also result in skewing or distorting the advertiser's marketing data. This can result in marketers allocating more budget to these networks, when in fact they are not driving any real clicks, users, or conversions.

EXAMPLE

For example an app install:

- By attempting to take credit for the last click before a conversion, these bad actors are attempting to get paid by advertisers for the fraudulent clicks and ultimately steal an advertiser's marketing budget.
- A user unknowingly downloads a fraudulent app, which could be anything from a utility app like a calculator, a game, or any other type of mobile app.
- The app has code that will execute these spam clicks on ads in the background of the users mobile device without their knowledge.
- The ads that are clicked are then assigned to the developer of the fraudulent app, which can result in them getting paid for the clicks.

#1 CLICK SPAMMING

#2 CLICK INJECTION

DEFINITION

Click injection is a type of ad fraud where attackers inject fraudulent or unauthorized clicks on advertisements within mobile applications. This is generally done to manipulate click-through rates, inflate app and ad metrics, and ultimately generate illicit revenue from advertisers. Click injection is similar in concept to click hijacking, where a legitimate click is replaced by a fraudulent click as the last touch before an install or purchase event.

CAUSE

Click injection creates a negative cycle in which the advertiser continues to pay someone else for users they would have acquired in the normal way (or at least through other marketing channels). It grabs organic traffic, tags it without the user's knowledge, and then demands credit for it. This spoils the accuracy of the marketer's data and interferes with making accurate decisions.

EXAMPLE

- User A has a fraudulent app installed on her device – usually through a third-party app store. The fraudulent app is often a very basic app with some ads.
- When User A downloads a new e-commerce app to her device, all existing installed apps on her device are notified of this download event. This is a particular loophole with Android devices. iOS devices are less susceptible to click injection.
- If this e-commerce app is running an install advertising campaign, the fraudulent app could be participating too and therefore has the tracking codes. The download event triggers the fraudulent app to report a click from User A.
- Ads attribution services start tracing clicks in reverse chronological order when the new e-commerce app is opened the first time. The fraudulent click has all the correct matching on device IDs and track code, and will therefore be determined as the last-touch click. Fraudsters will then be rewarded the ad dollars associated with User A's install.

#2 CLICK INJECTION

#3 AD INJECTION

DEFINITION

Ad injection is the practice of modifying web pages on the client side, by a third-party application, in order to present the user with its own ads. The result is that the third-party app monetizes the user browsing sessions, instead of the publishers.
In cyber-security speak, ad injection is a man in the browser attack (MITB) that targets ads serving and revenue. Ad injection is a sub-niche of "adware", software that's designed to generate ad impressions.

CAUSE

Ad injectors were most commonly implemented as browser extensions, which were easy to develop, maintain and distribute. After Google started to ban ad injecting extensions, implementation shifted towards applications who used questionable techniques, from changing DNS and / or proxy settings in order to modify ads traffic, or injecting DLL into the browser in order to achieve MITB and modify ads.

EXAMPLE

- Imagine visiting a website that's ad-free, but suddenly, pop-up or banner ads appear out of nowhere – that's ad injection in action. Alternatively, you might click on a link, expecting to see specific content, only to end up on a page swamped with ads.
- Ad injection can even happen in less obvious ways like ads disguised as authentic content or hidden in obscure corners of a webpage. Not only do these tactics diminish the user experience, but they can also inflict reputational and monetary damage on a website.

#3 AD INJECTION

#4 PIXEL STUFFING

DEFINITION

Pixel stuffing works by cramming advertisements of standard dimensions into tiny spaces. These spaces can be as small as 1x1 pixels, making them virtually undetectable. Several of these advertisements can be stuffed into one webpage.

CAUSE

In pixel stuffing, the crammed ads are not visible to the user, but just by visiting the infected site, an impression is registered and reported as a real view. Fraudsters use this technique to trigger impressions from a much higher number of ads, then there is room for on a publisher's website

#4 PIXEL STUFFING

GRAPHIC WILL BE UPDATED HERE

#5 DOMAIN SPOOFING

DEFINITION

Domain spoofing is a type of cyber-attack where an attacker creates a fake website or email address that appears to be from a legitimate organization or individual. The goal of domain spoofing is usually to deceive the user into divulging sensitive information such as usernames, passwords, credit card details, or other personal data.

CAUSE

Domain spoofing is a significant problem in the digital advertising industry. It can deceive advertisers into believing their ads are being displayed on reputable websites, leading to wasted ad spend, damaged brand reputation, and lost revenue for publishers. It is a prevalent type of ad fraud and has become increasingly sophisticated, making it challenging to detect and prevent. Advertisers believe their ads are showing up on premium websites for the right audience. However, the fraudsters will show them up on low-quality websites for the bots (or, sometimes, a random audience).

EXAMPLE

- The Financial Times (FT.com) ran an audit in 2017 and found that FT.com had been spoofed, and fraudsters via these spoofed domains were selling display inventories on 10 ad exchanges and video ads on 15 exchanges. FT.com doesn't sell video ads programmatically at all.
- The money will never reach the publisher as the website is theirs. The publisher estimated the fraudsters were making over $1.3 million monthly, claiming they were the Financial Times.
- Estimated Loss: $1.3 Million Per Month.

#5 DOMAIN SPOOFING

GRAPHIC WILL BE UPDATED HERE

#6 AD STACKING

DEFINITION

Ad stacking refers to a type of mobile ad fraud in which the fraudsters "stack" or hide ads beneath the primary ad that is displayed to users. The reason that fraudsters use ad stacking is that while only the top ad will be seen by the user, advertisers that have multiple ads stacked beneath will still have to pay for the fake impressions.

CAUSE

Advertisers typically pay ad networks either on a cost-per-thousand (CPM) or cost-per-click (CPC) basis, depending on whether they're paying for impressions or clicks. In either of these advertising models, fraudsters are able to steal ad budgets with ad stacking by having them pay for ads that were never actually seen or clicked on by the user.

EXAMPLE

If a user clicks or views the top ad and there are other ads stacked beneath, this means that a click or impression will be reported for every ad in the stack. Ultimately, by stacking ads, fraudsters are stealing ad budgets from advertisers and increasing the ad revenue for publishers that may be involved in the scheme.

#6 AD STACKING

GRAPHIC WILL BE UPDATED HERE

#7 DEVICE FARMS

DEFINITION

Device farm is a type of mobile ad fraud that drains advertising spending by having fraudsters manually carry out actions (such as clicks, installs, and other forms of interaction) on your ads or mobile apps. More specifically, Device Farms are real-world places where a lot of devices are stored together to execute mobile click fraud.

CAUSE

Device Farm or Click Farm or Phone Farm is a traditional form of fraud that continues to make up a sizeable portion of mobile ad fraud because it is a relatively easy form of the crime. The farms are just a huge group of gadgets that have been programmed to carry out some operation, like an install, and then repeat this action repeatedly. Resultantly this depletes display-based marketing efforts by repeatedly clicking on mobile advertising.

EXAMPLE

Fraudsters connect to several publishers, constantly monitor all available apps/games which need paid traffic sources, and target them for fraud. Then they perform analysis to determine the expected KPI for good traffic quality. Finally the device farm operator gets these parameters: how to download the targeted apps/games and what post-install events to perform afterward for each. More complex device farms use "matrices", which automate operator work and perform the same actions across multiple devices simultaneously.

#7 DEVICE FARMS

GRAPHIC WILL BE UPDATED HERE

#8 GEO MASKING

DEFINITION

The practice of disguising the true geographic origin of web traffic or ad interactions to deceive advertisers or ad networks. This type of fraud is particularly relevant in online advertising, where the value and cost of ads can vary significantly based on the location of the audience.

CAUSE

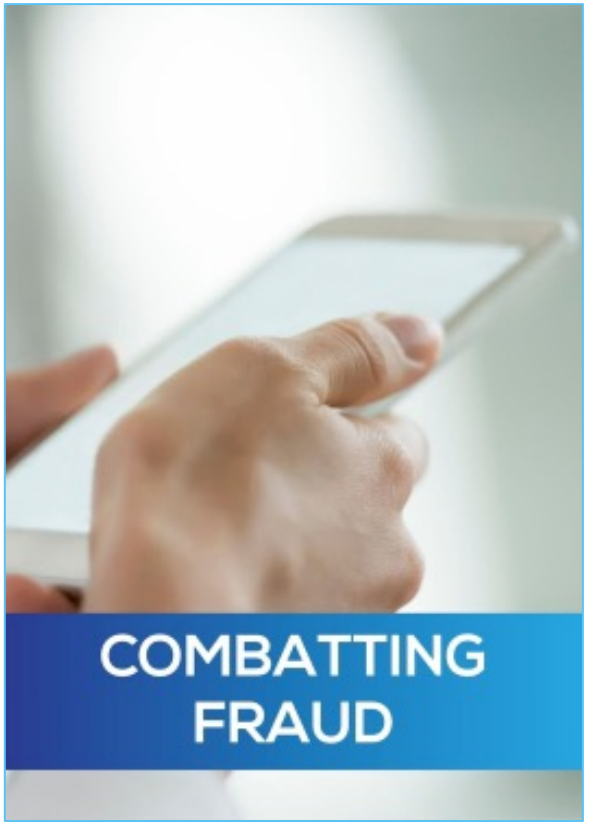
By geo masking, fraudsters can trick advertisers into believing that the traffic is coming from these high-value regions, thereby earning more revenue fraudulently. Furthermore, it distorts the true performance of the ad campaigns. The advertiser might believe they are effectively reaching their target audience in a specific region, while in reality, their ads are being seen elsewhere.

EXAMPLE

- Proxy Servers and VPNs : Fraudsters employ proxy servers and virtual private networks (VPNs) to disguise their actual location. Routing their traffic through servers located in the desired target area, they can mimic the location data of legitimate users.
- Spoofing GPS Data : Fraudsters can manipulate GPS data to make it appear as if they are physically present in a specific location, even when they are miles away.
- IP Spoofing : Altering the source IP address in network packets to appear as if they originate from a specific location. This way, fraudsters can trick ad campaigns that rely on IP-based targeting.
- Device Fingerprinting: By altering device parameters such as time zone, language settings, and system information, fraudsters can imagine a user being in a different location.

#8 GEO MASKING

GRAPHIC WILL BE UPDATED HERE



COMBATTING FRAUD

Fraud in the mobile content ecosystem can have far-reaching consequences since it undermines the trust and integrity of the entire mobile ecosystem. We are dedicated to supporting the fight against mobile fraud and offer the following advice:

1. Trust in Premium and Transparent Inventory
One of the primary steps in combating mobile fraud is to trust in premium and transparent inventory for your advertising campaigns. Advertisers are encouraged to partner with platforms that exclusively use client-provided ads. Utilizing solutions that offer real-time access to inventory forecasting and dynamic filtering capabilities empowers advertisers to make precise volume estimates based on various dimensions, including exchange, carrier, publisher name, ad size, OS version, and more. Dependence on transparent inventory sources significantly reduces the risk of fraud.

2. Emphasize the Quality of Supply
Maintaining quality supply sources is critical in the fight against mobile fraud. Advertisers should diligently vet their supply partners and prioritize working with those who uphold high-quality standards. Prioritizing supply quality creates a safer environment for campaigns, minimizing the likelihood of fraudulent activity.

3. Implement Advanced Targeting
Advanced targeting plays a pivotal role in achieving accurate results and reducing fraud. Utilizing sophisticated targeting options, such as geographical targeting by countries, operators, and IP levels, enables precise audience reach while minimizing exposure to fraudulent traffic.

4. Utilize Multi-Dimensional Reporting
In the fast-paced world of mobile advertising, timely action is crucial. Multi-dimensional reporting is a key component in fraud detection and mitigation. Implementing comprehensive reporting systems that offer insights across various dimensions, including campaign performance, traffic sources, and user behavior, is vital for effective fraud prevention.

5. Prioritize Premium Content and Banner Quality
Collaboration with content providers or merchants offering premium content and the enforcement of stringent banner quality policies ensure a superior user experience and optimize performance.

GLOSSARY

Phishing
The act of misleading a user by presenting to be a known and trusted party to gain access to online systems, accounts or data such as credit card, banking information or passwords for malicious reasons.

Spam
A broad term for an unsolicited ad, namely, whether the message has been sent with good intentions or maliciously.

Traffic
A common term used to refer to the delivery of ads.

Malware
A common term used to refer to the movement of messages, e.g., "the [SMS] traffic has been successfully delivered.

Identity Theft
The fraudulent practice of using another person's name and personal information in order to obtain credit, loans, etc.

ABOUT THE PROGRAMME

Established in 2020, MEF's Content & Advertising Programme is a worldwide, cross-ecosystem approach to promote a competitive, fair and innovative market for mobile Content & Advertising between businesses and consumers.

Programme participants represent different regions and stakeholder groups working collaboratively to:

- Produce and publish best practice frameworks, papers and tools to accelerate market clean-up and limit revenue leakage
- Educate buyers of Content & Advertising solutions
- Promote mobile advertising as a premium and trusted marketing channel
- Drive knowledge across the ecosystem of new platforms, technologies and procedures to address the evolving content landscapes
- Develop the value-chain to support new use cases and business

FOR FURTHER INFORMATION ON THE FUTURE OF MESSAGING PROGRAMME AND TO GET INVOLVED PLEASE VISIT:

WWW.MOBILEECOSYSTEMFORUM.COM

MEF MOBILE ECOSYSTEM FORUM

Established in 2000, the Mobile Ecosystem Forum is a global trade body that acts as an impartial and authoritative champion for addressing issues affecting the broadening mobile ecosystem. As the voice of the mobile ecosystem, it provides its members with a global and cross-sector platform for networking, collaboration and advancing industry solutions. The goal is to accelerate the growth of a sustainable mobile ecosystem that delivers trusted services that enrich the lives of consumers worldwide.

04 Anzelle Robertson

Anzelle used to oversee Business Development and Carrier Relations in Sub-Saharan Africa at SAM MEDIA

Skilled at identifying unique opportunities to solve tangible problems digitally, Anzelle's background in law means she has a strong focus on regulatory compliance and a firm understanding of the legal landscape governing VAS, PSMS, DCB and M-Wallets on the continent.

Anzelle has served on the Board of the South African regulatory body for VAS and Mobile Payments, WASPA, and remains an active member of various industry organisations and regulators, championing the uptake of Direct Carrier Billing as go-to payment method for digital content. Anzelle is an Attorney of the High Court of South Africa and an alumnus of the University of the North-West. A proud woman in mobile, she is passionate about empowering others like her.

05 Members – what do you want to achieve?

Content & Advertising Online event in June 27th?