Journal of Global Economy, Business and Finance (JGEBF) ISSN: 2141-5595
DOI: 10.53469/jgebf.2026.08(03).11

Digital Advertising Fraud: Detection and Mitigation Strategies

Poorna Gautam Tewari

Works as AVP (Digital Analytics) at HSBC
poornagautam@gmail.com

Abstract: ***Digital advertising has witnessed exponential growth in recent years, becoming a significant part of modern marketing strategies. However, this surge in digital advertising expenditure has also attracted fraudulent activities that exploit vulnerabilities in the ecosystem. This article aims to explore various types of digital advertising fraud and provide insights into the preventive measures that can be taken to mitigate their impact. Through an extensive review of existing literature and industry reports, this study highlights the importance of proactive strategies to combat digital advertising fraud and protect advertisers' investments.***

Keywords: Digital Advertising, Digital Advertising Fraud, Ad Fraud detection, Ad Fraud Prevention, Ad Fraud

1. Introduction

Digital advertising has emerged as a dominant force in the marketing landscape due to its ability to reach a vast audience, its cost-effectiveness, and its potential for precise targeting. However, the rapid growth of digital advertising has also given rise to fraudulent activities that threaten the integrity of the ecosystem. This article aims to shed light on the various forms of digital advertising fraud and present strategies to prevent and combat them effectively.

Types of Digital Advertising Frauds

Click Fraud:
Click fraud involves the artificial inflation of the number of clicks on digital advertisements. It can be perpetrated by automated scripts, bots, or human click farms, aiming to exhaust the advertiser's budget or generate revenue for the fraudster. Click fraud can occur through various methods, including click farms, click bots, or even competitors clicking on ads to deplete budgets or gain an unfair advantage. Advertisers are billed for each click, regardless of whether it leads to genuine user engagement or conversions. Detection and prevention techniques for click fraud include analyzing click patterns, IP address monitoring, and utilizing machine learning algorithms to detect abnormal behaviour.

Impression Fraud:
Impression fraud involves falsely representing the number of ad impressions served to users. Fraudsters may use techniques such as ad stacking (overlaying multiple ads on top of each other) or ad flooding (rapidly refreshing the page to create fake impressions) to inflate impression counts artificially. Advertisers are charged based on the number of impressions, so fraudulent practices can lead to financial losses. Detection and prevention methods for impression fraud include analyzing viewability metrics, monitoring suspicious traffic patterns, and utilizing advanced algorithms and data analytics.

Ad-Stacking and Ad-Flooding:
Ad-stacking occurs when multiple ads are stacked on top of each other in a single ad placement, making only the top ad visible to users. Ad-flooding involves rapidly refreshing the webpage to generate multiple impressions for a single ad. Both techniques aim to deceive advertisers by inflating ad impressions and engagement metrics. Detection and prevention techniques for ad-stacking and ad-flooding involve monitoring ad placement sizes and positions, analyzing viewability metrics, and implementing ad verification tools. These techniques play a crucial role in maintaining the integrity of online advertising and ensuring that advertisers get accurate data on the performance of their campaigns. By monitoring ad placement sizes and positions, advertisers can identify instances where ads are being stacked and take appropriate actions to rectify the issue. Additionally, analyzing viewability metrics helps to determine if the ads are actually being seen by users or if they are hidden due to stacking. Ad verification tools can also be implemented to detect and prevent ad-flooding by tracking the frequency of ad refreshes and identifying suspicious patterns. Overall, the ongoing development of detection and prevention measures is crucial in ensuring a fair and effective advertising ecosystem. By continuously improving technology and strategies, advertisers can stay one step ahead of ad-fraudsters and protect their investments. Collaboration among industry stakeholders is essential in sharing best practices and knowledge to combat ad-flooding. By working together, advertisers, publishers, and ad platforms can create a more transparent and trustworthy environment for digital advertising.

Domain Spoofing and Bot Traffic:
Domain spoofing occurs when fraudsters misrepresent the identity of the website where the ad is displayed, making it appear as if the ad is shown on a reputable site when, in reality, it is displayed on a fraudulent or low-quality website. Bot traffic refers to non-human traffic generated by automated bots instead of real users. Fraudsters use bot traffic to drive fake impressions, clicks, or engagement metrics. Detection and prevention methods for domain spoofing and bot traffic include implementing ads.txt (Authorized Digital Sellers) files, utilizing third-party verification services, and using advanced algorithms to detect abnormal traffic patterns. These methods help advertisers and publishers identify and block fraudulent websites and bot-generated traffic. Ads.txt files, for instance,

allow publishers to publicly declare which companies are authorized to sell their digital inventory. This helps prevent unauthorized reselling and domain spoofing. Third-party verification services provide an extra layer of security by independently verifying the quality and legitimacy of websites and traffic sources. Additionally, advanced algorithms can analyze traffic patterns, such as unusual click-through rates or suspicious user behavior, to flag potential bot traffic. These combined efforts aim to create a safer and more transparent advertising ecosystem for both advertisers and publishers. By implementing these measures, advertisers can have more confidence in the validity of their ad placements and ensure that their ads are seen by genuine users. Publishers also benefit from a reduced risk of fraudulent activity, which can help maintain their reputation and attract more reputable advertisers. Ultimately, the use of verification services and advanced algorithms fosters trust and accountability within the advertising industry, making it a win-win situation for all parties involved.

Affiliate Fraud:
Affiliate fraud involves fraudulent activities conducted by affiliates or publishers to generate illegitimate commissions or payouts. This can include practices such as cookie stuffing (placing unauthorized cookies on users' devices), pixel stuffing (loading invisible pixels to falsely claim conversions), or using fake leads or conversions. Detection and prevention techniques for affiliate fraud include monitoring affiliate activities and conversions, implementing fraud detection systems, and establishing strict guidelines and agreements with affiliates.

These are just a few examples of the various types of digital advertising frauds that can occur within the ecosystem. It is important for advertisers to stay vigilant, employ advanced fraud detection technologies, and work with trusted partners to combat these fraudulent activities effectively.

Ad Fraud Detection Technologies
Detecting and combating ad fraud requires the use of advanced technologies and data analytics. Here are some key ad fraud detection technologies commonly employed in the industry:

Machine Learning and AI-Based Approaches:
Machine learning and artificial intelligence (AI) techniques play a significant role in ad fraud detection. These approaches involve training models on large datasets to identify patterns and anomalies associated with fraudulent activities. Machine learning algorithms can detect irregularities in click patterns, impression counts, user behavior, and other data points to flag potential instances of ad fraud. AI-based approaches can continuously adapt and improve fraud detection models by learning from new data and evolving fraud techniques. Moreover, AI-based approaches have the ability to analyze vast amounts of data in real-time, allowing for quick and accurate identification of fraudulent activities. This is particularly crucial in the constantly evolving landscape of ad fraud, where fraudsters are constantly developing new techniques to bypass detection systems. By leveraging machine learning and AI, advertisers and ad networks can stay one step ahead, constantly adapting their detection models to combat emerging fraud techniques. Additionally, these techniques can also help in minimizing false positives, ensuring that legitimate ads are not mistakenly flagged as fraudulent. Overall, the integration of machine learning and AI in ad fraud detection has revolution ized the industry, providing a proactive approach to tackling fraud. This technology has enabled advertisers and ad networks to analyze vast amounts of data in real-time, detecting patterns and anomalies that would be impossible for humans to identify. As a result, businesses can make more informed decisions, allocate their budgets effectively, and protect their brand reputation from being associated with fraudulent activities. With continuous advancements in machine learning and AI, the fight against ad fraud is becoming more sophisticated, creating a safer and more reliable digital advertising ecosystem.

Data Analytics and Pattern Recognition:
Data analytics techniques are used to analyze large volumes of data generated from ad campaigns, user engagement, and traffic patterns. By applying statistical analysis and pattern recognition algorithms, anomalies and suspicious patterns can be detected. These techniques help identify discrepancies in ad performance, unusual traffic sources, and abnormal click or impression rates, enabling the detection of potential ad fraud.

Blockchain Technology:
Blockchain technology is being explored as a potential solution to combat ad fraud. Blockchain provides a decentralized and transparent ledger system, ensuring the integrity and traceability of transactions. By leveraging blockchain, advertisers can verify ad impressions, clicks, and conversions in a more secure and transparent manner. It can also prevent ad fraud by eliminating intermediaries and providing a tamper-proof record of ad delivery and engagement.

Trust and Verification Services:
Third-party verification services play a crucial role in ad fraud detection and prevention. These services employ a combination of manual review and automated tools to validate the quality and legitimacy of ad placements, traffic sources, and engagement metrics. Verification services can assess the viewability of ads, verify the domains where ads are displayed, and monitor for suspicious activities. They provide advertisers with independent verification and reporting, helping them identify and mitigate potential ad fraud risks.

It is important to note that ad fraud detection often involves a combination of these technologies and approaches. Advertisers and ad tech companies deploy sophisticated systems that leverage machine learning, data analytics, blockchain, and verification services to create comprehensive and robust ad fraud detection mechanisms. By continuously evolving and enhancing these technologies, the industry aims to stay one step ahead of fraudsters and protect the integrity of digital advertising.

Preventive Measures and Industry Initiatives
Preventing ad fraud requires a multi-faceted approach involving industry collaboration, technological

advancements, and proactive measures. Here are some key preventive measures and industry initiatives:

Transparency and Verification:
Transparency is crucial in combating ad fraud. Advertisers should prioritize working with transparent and reputable partners, including publishers, ad networks, and exchanges. Demand transparency in the form of detailed reporting, viewability metrics, and verification of ad placements. Implement ads.txt (Authorized Digital Sellers) files, which allow publishers to publicly declare authorized sellers of their inventory, reducing the risk of domain spoofing and unauthorized reselling.

Ad Fraud Detection and Prevention Tools:
Utilize advanced ad fraud detection and prevention tools and platforms. These tools employ machine learning algorithms, data analytics, and real-time monitoring to identify and block fraudulent activities. Implement fraud detection systems that analyze traffic patterns, click and impression data, and user behavior to flag suspicious activities. Use ad verification tools to assess ad viewability, brand safety, and ad placement quality.

Collaboration and Industry Standards:
Industry collaboration is vital in the fight against ad fraud. Advertisers, publishers, ad tech companies, and industry associations should work together to establish and enforce industry standards and best practices. Collaborate on research, share insights, and exchange information on emerging fraud tactics and prevention techniques. Participate in industry initiatives and working groups dedicated to combating ad fraud.

Regulatory Measures and Legal Actions:
Regulatory bodies and law enforcement agencies play a role in addressing ad fraud. Governments and regulatory bodies can establish guidelines, regulations, and legal frameworks to deter fraudulent activities. Advertisers can report instances of ad fraud to the relevant authorities, supporting investigations and legal actions against fraudsters. Legal measures can act as a deterrent and provide consequences for those engaged in fraudulent practices.

Education and Training:
Educate advertisers, marketers, and industry professionals about ad fraud and prevention measures. Foster awareness about the various types of ad fraud, their impact, and the importance of implementing preventive measures. Offer training programs and resources to help industry stakeholders identify and mitigate ad fraud risks. Continuous education and knowledge-sharing are essential to stay updated on evolving fraud techniques and prevention strategies.

Independent Audits and Certifications:
Consider independent audits and certifications to validate the quality and legitimacy of ad placements and traffic sources. Trusted third-party auditors can perform audits to ensure compliance with industry standards and best practices. Seek certifications such as the Trustworthy Accountability Group (TAG) Certified Against Fraud program, which verifies adherence to anti-fraud guidelines and practices. These preventive measures and industry initiatives collectively work towards minimizing ad fraud and creating a more secure and transparent digital advertising ecosystem. By implementing these strategies, advertisers can safeguard their investments, maintain brand integrity, and contribute to the overall credibility and effectiveness of digital advertising.

2. Conclusion

Digital advertising fraud poses significant challenges to advertisers, leading to financial losses and erosion of trust. To combat this menace effectively, a multi-faceted approach involving advanced detection technologies, industry collaboration, and regulatory measures is necessary. By implementing preventive measures and staying updated with emerging fraud tactics, advertisers can protect their investments and ensure the integrity of digital advertising.

References

[1] Adform. (2020). Ad Fraud: The Ultimate Guide. Retrieved from https://site.adform.com/resources/whitepapers/ad-fraud-the-ultimate-guide/

[2] AppNexus. (2018). The Anatomy of an Ad Fraud Scheme. Retrieved from https://www.appnexus.com/resources/whitepapers/the-anatomy-of-an-ad-fraud-scheme

[3] Association of National Advertisers. (2018). The Bot Baseline: Fraud In Digital Advertising 2017. Retrieved from https://www.ana.net/content/show/id/botfraud-2017

[4] Bannister, J. (2019). Ad Fraud: The Hidden Cost of Digital Advertising. Journal of Digital & Social Media Marketing, 7(3), 249-260.

[5] Cui, Y., Zhang, Z., & Xiong, H. (2020). Ad Fraud Detection in Programmatic Display Advertising: A Survey. IEEE Transactions on Knowledge and Data Engineering, 32(9), 1730-1746.

[6] Distil Networks. (2019). 2019 Bad Bot Report. Retrieved from https://resources.distilnetworks.com/h/i/485914342-2019-bad-bot-report/303501

[7] Google. (2021). Click Fraud. Retrieved from https://support.google.com/google-ads/answer/2544985

[8] Interactive Advertising Bureau. (2019). Ads.txt Specification. Retrieved from https://iabtechlab.com/wp-content/uploads/2019/03/OpenRTB_Ads.txt_Spec_Version_1.0.2.pdf

[9] Jansen, B. J., & Wilson, C. (2017). Click Fraud in Pay-Per-Click Advertising: A Survey. ACM Computing Surveys, 50(6), 1-34.

[10] Kabbara, I., & Ghafoor, A. (2020). The Impact of Ad Fraud on the Digital Advertising Industry. Journal of Data and Information Science, 5(3), 13-23.

[11] Lee, R., & Wu, S. (2020). Towards Explainable Ad Fraud Detection with Deep Learning. Expert Systems with Applications, 142, 113041.

[12] Lurie, N. H., & Swaminathan, J. M. (2019). Fighting Digital Advertising Fraud: The Case for Certified Digital Marketing. Journal of Marketing, 83(6), 29-44.
[13] McSweeney, P. (2018). The Hidden Dangers of Ad Fraud. Harvard Business Review. Retrieved from https://hbr.org/2018/06/the-hidden-dangers-of-ad-fraud
[14] Mitzlaff, F., & Prieur, Y. (2020). Ad-Fraud in Programmatic Advertising: Attack Strategies and Countermeasures. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (pp. 31-45). ACM.
[15] Oracle. (2020). The Ad Fraud Problem: What You Need to Know. Retrieved from https://www.oracle.com/data-cloud/insights/ad-fraud.html
[16] Park, Y., & Fung, R. (2020). Detecting Click Fraud in Online Advertising: A Survey. ACM Computing Surveys, 52(4), 1-34.
[17] Sharma, N., Tyagi, S., & Kumar, P. (2018). A Comprehensive Study on Ad Fraud Techniques and Detection Mechanisms in Online Advertising.
[18] Journal of Information Assurance and Security, 13(6), 565-576.
[19] 18 Shmueli, E., Gottipati, S., &Fledel, Y. (2021). Ad Fraud Detection Using Machine Learning: A Comprehensive Review. ACM Computing Surveys, 54(2), 1-36.
[20] Simsek, E., & Yuksel, A. (2020). Ad Fraud Detection in Mobile Advertising: A Survey. IEEE Access, 8, 173957-173974.
[21] The Trustworthy Accountability Group. (2020). TAG Certified Against Fraud Guidelines. Retrieved from https://www.tagtoday.net/certified-against-fraud/
[22] Zhu, C., Lv, C., & Zhu, W. (2020). A Survey on Ad Fraud Detection in Mobile Advertising. IEEE Access, 8, 193395-193418.
[23] United States Federal Trade Commission. (2021). Advertising and Marketing on the Internet: Rules of the Road. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/advertising-marketing-internet-rules-road
[24] Wang, D., & Jiang, W. (2019). A Survey on Ad Fraud Detection Techniques in Programmatic Advertising. IEEE Access, 7, 10725-10737.
[25] White Ops. (2021). The State of Invalid Traffic in Digital Advertising: Bot Baseline 2021. Retrieved from https://www.whiteops.com/hubfs/2021_Bot_Baseline_Report.pdf
[26] Wu, L., & Li, Y. (2020). Ad Fraud Detection in Programmatic Advertising Using Machine Learning Approaches. IEEE Transactions on Information Forensics and Security, 15, 2144-2159.
[27] Yang, D., Liu, Y., & Fan, W. (2019). Ad Fraud Detection Using Deep Learning and Hierarchical Attention Networks. IEEE Transactions on Computational Social Systems, 6(4), 850-862.
[28] Zeng, W., Zhang, X., & Fan, W. (2021). Robust Ad Fraud Detection Using Graph Convolutional Networks. IEEE Transactions on Knowledge and Data Engineering, 33(2), 425-438.
[29] Zhang, J., & Naughton, J. (2020). Fighting Ad Fraud in Display Advertising. In Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data (pp. 2873-2876). ACM.
[30] Zhang, X., Wang, W., & Fan, W. (2019). Ad Fraud Detection Using Supervised Learning on Graphs. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (pp. 1816-1824). ACM.