

Combating Fraudulent Advertising for Fake Shops

This policy paper outlines the current challenges in tackling fraudulent advertising for fake shops, evaluates the implementation of the Digital Services Act (DSA) as a regulatory tool, and proposes concrete recommendations to improve platform accountability and enforcement.

Fraudulent actors exert a damaging influence on the Austrian e-commerce landscape. Through large-scale advertising campaigns, they divert visibility away from legitimate businesses, undermining fair competition and eroding consumer trust. Their practices not only mislead and harm consumers but also disproportionately impact local small and medium-sized enterprises.

Fraudulent Competition in E-Commerce

Online fraud has increased drastically in recent years. In 2024, the Criminal Intelligence Service Austria reported 31.768 cases of online fraud in Austria alone, marking a 50 % increase within five years.¹ A particularly prevalent form of this crime involves fake online shops, where consumers either receive no goods at all or products that differ significantly from what was advertised, despite full payment. 27 % of Austrian consumers state that they have fallen victim to fake shops and 17 % of retailers report that their legitimate online shops have already been copied by criminals. The sectors most affected include fashion, electronics, and travel.²

The negative consequences of e-commerce fraud extend beyond monetary losses. A lack of consumer trust remains one of the leading reasons Austrians abandon online purchases. While caution regarding unrealistic offers is generally advisable, the growing mistrust poses a particular challenge for small and medium-sized enterprises (SMEs) seeking to expand and establish themselves in the online market. Austrians rarely buy from unfamiliar online shops; nearly two-thirds consistently purchase from only one to three well-known providers.³

Fraudulent shops employ the same digital marketing tools as legitimate businesses, but often with greater reach and flexibility.⁴ Criminals register thousands of domains, exploit website vulnerabilities, and place hundreds of ads across search engines and social media platforms. Hence, the deceptive strategies of fraudulent shops undermine the visibility of legitimate retailers and distort fair competition within the online market.

The Digital Services Act: The Digital Services Act (DSA) requires Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) to provide public access to advertising libraries, enabling monitoring and investigations by researchers, journalists and the public (Art. 39 DSA). The DSA mandates that information such as ad content, who paid for it and target metrics be made transparent. Ad Libraries therefore serve as potential tools to detect and combat advertisements leading to fraudulent fake shops.

Gaps in Implementation & Enforcement of the Digital Services Act

Problems with the implementation of the DSA are becoming increasingly visible. Researchers criticize various ad libraries for not being DSA compliant. Common points of critique include difficult-to-use interfaces, a lack of search functionality, and insufficient information on ad performance and target metrics.⁵ Other issues include data delays, missing details for certain ad types, and limited search parameters - in some cases even a lack of vital information, such as product information and subject matter, impeding comprehensive analysis.⁶

While most advertising libraries provide information on reach or impressions, these metrics are not easily accessible and often lack explanations. Furthermore, links shown in advertisements that lead to online shops sometimes differ between what users see in the app and what appears in the ad library, making it difficult for researchers or journalists to trace fraudulent shops.

Following a critical review of TikTok's compliance with the DSA, the European Commission issued a preliminary assessment indicating that TikTok's advertisement library fails to meet DSA transparency requirements.⁷ TikTok reportedly fails to disclose sufficient information on ad content, targeting, and funding and its repository lacks adequate search functionality. Research by AI Forensics also showed that TikTok's advertising system allows advertisers to mask their true identity in the "For You Page" by operating under a chosen or automatically generated username.⁸ In parallel, the Commission has opened formal proceedings against Facebook and Instagram to investigate whether Meta complies with the DSA. These proceedings focus primarily on deceptive advertising, disinformation and insufficient mechanisms to flag illegal content.⁹

To increase transparency, a new access point for researchers via the DSA Data Access Portal, published by the European Commission in autumn 2025, should bring improvements regarding access to platform data.¹⁰ If these will materialize remains to be seen and tested.

Trusted Flagger: Trusted Flagger organizations are authorized under Article 22 DSA to identify and report specific types of illegal online content, while accounting for national legal contexts. Reports submitted by these organizations must receive priority from online platforms. Therefore, Trusted Flaggers are a central instrument in ensuring faster and more effective moderation of illegal content.

Fake Shops on Social Media

Between January and April 2025, research conducted by the Austrian Institute for Applied Telecommunications (ÖIAT) identified several thousand online advertisements leading to a wide range of fraudulent fake shops pretending to sell branded products. Using specifically developed web-scraping tools and only three search terms, 1.567 advertisements related to the brand Birkenstock were found, linking to 59 different fake shops. These ads reached an estimated 6.5 million people across the EU. Approximately two-thirds of the fraudulent ads were reported and removed, while 621 remained active.

The brand Swarovski was also affected. In one notable scam, criminals advertised expensive binoculars at heavily discounted prices, falsely claiming a partnership with well-known retail chains such as Hofer, Billa and Lidl. Nearly 3.000 ads promoting this scam were identified, directing users to 41 fake shops. By September 2025, the number of fraudulent ads has risen to over 5.100. Although some individual advertisements were reported and removed by Meta, the majority remain online, and their number continues to grow. Similar fraud patterns have been observed across many other well-known brands.

Reporting these fraudulent advertisements at scale is not feasible under the current systems. Meta, for example, sets a limit of 20 URLs per report, making large-scale reporting impractical and overly resource intensive for Trusted Flaggers or other reporting organizations. Platforms should make use of automated detection and upload filters to proactively protect users from fraudulent advertisements. Recent reports claim that up to 10 % of Meta's revenue 2024 came from ads for scams and banned products.¹¹ Around 15 billion fraudulent advertisements (which Meta categorizes as "higher risk" in internal documents) are shown to users every day, earning Meta \$ 7 billion annualized revenue from "high-risk" ads alone. Therefore, Meta and other platforms have very little financial incentives to prevent scam advertisements, even if these are likely fraudulent.

6.5 mio
people reached

with 1.567 fraudulent Birkenstock ads linking to 59 different fake shops.

5.100

**ads promoting
fake retailers**

luring consumers with brands like Lidl, Billa and Swarovski.

\$ 7

billion revenue

does Meta earn annually from „high risk“ advertisements, profiting directly from harm.

Policy Recommendations

These findings illustrate a significant enforcement gap. While the DSA introduces transparency obligations, platforms' reporting systems remain inadequate to address the volume and recurrence of fraudulent advertising. To effectively combat fraudulent advertising and the proliferation of fake shops in the e-commerce sector, coordinated action is required across platforms, regulators, and enforcement authorities. The following recommendations address key gaps in transparency, accountability, and response mechanisms.

1 Enhance Platform Accountability & Transparency

- a. **Mandate advertiser verification through „Know Your Customer“ standards:** Platforms should be required to verify advertiser identities prior to publication, including business registration or VAT numbers, to prevent anonymous or fraudulent advertising activity.¹²
- b. **Ensure full transparency of paid content:** In line with the DSA, platforms must clearly disclose who paid for an advertisement and provide public access to this information in their ad libraries and directly on the platform.

2 Improve Response & Enforcement Mechanisms by Platforms

- a. **Allow bulk reporting of fraudulent advertisements:** Limits on the number of ads per report make large-scale reporting impractical and overly resource intensive.
- b. **Introduce automated flagging thresholds at account-level:** When a significant proportion of an account's ads are reported and confirmed fraudulent, platforms should be obliged to automatically review the account and, if necessary, suspend it.
- c. **Establish a maximum response time for Trusted Flagger reports:** Trusted Flaggers' reports must receive priority handling within a fixed timeframe (e.g. seven business days) to prevent prolonged exposure of users to fraudulent ads and other illegal content.
- d. **Enable direct communication between Trusted Flaggers and Platforms:** A direct communication channel would allow faster escalation of recurring scams and coordinated responses to emerging fraudulent patterns.

3 Ensure Functional Ad Library & Research Access

- a. **Provide tooltips, definitions and links near key metrics:** This would allow cross platform comparison, as definitions of key indicators would be explained and easily accessible.
- b. **Establish robust search functionality:** Ad libraries should allow keyword and advertiser searches as well as filtering and sorting of results.
- c. **Ensure full access to ad performance and targeting metrics:** Platforms must include detailed metrics in their advertisement archives, simply the information that ads have been targeted by age do not suffice.

Despite the DSA's potential, platform compliance remains inconsistent. Preliminary findings by the European Commission and multiple independent studies highlight persistent shortcomings in ad library accessibility, transparency, and responsiveness to Trusted Flaggers. Addressing the issues is essential to ensure that the DSA effectively protects consumers from fraudulent advertising and businesses, especially SMEs, from criminal competitors in the e-commerce sector.

References

- [1] Bundesministerium für Inneres und Bundeskriminalamt. 2025. „Polizeiliche Kriminalstatistik 2024 - Entwicklung der Kriminalität in Österreich“.
- [2] Putz, Nina, und Gerald Kühberger. 2025. Sicherheitsstudie 2025. Sicherheitsstudie. Handelsverband, Bundeskriminalamt.
- [3] E-Commerce Gütezeichen. 2022. „Aktuelle Studie: Ein Drittel aller Online-Käufe scheitert am Vertrauen“. OTS.at, November 10. https://www.ots.at/presseaussendung/OTS_20221110_OTS0028/aktuelle-studie-ein-drittel-aller-online-kaeufe-scheitert-am-vertrauen-bild
- [4] UNODC. 2019. „Organized Crime / Cybercrime Module 13 Key Issues: Criminal Groups Engaging in Cyber Organized Crime“. // www.unodc.org.
- Liu, Xiang, Sayed Fayaz Ahmad, Muhammad Khalid Anser, u. a. 2022. „Cyber security threats: A never-ending challenge for e-commerce“. *Frontiers in Psychology* 13. <https://www.frontiersin.org/articles/10.3389/fpsyg.2022.927398>.
- Zumstein, Darius, Carmen Oswald, und Claudia Brauer. 2022. Onlinehändlerbefragung 2022 : Erfolgsfaktoren und Omnichannel-Services im Digital Commerce. 79,application/pdf. <https://doi.org/10.21256/ZHAW-2432>.
- ÖIAT. 2021. „Wege in Fake-Shops. Studie zu Produkten, Preisen und der Kund:innenansprache von Fake-Shops. Deliverable 2.1“.
- [5] Alexander Hohlfeld, Anna Semenova, Martin Degeling, Greta Hess, und Kathy Meßmer. 2024. „Tik-Tok, DSA O’Clock?“ Auditing Tik Tok, Februar 21. <https://tiktok-audit.com/blog/2024/Tik-Tok-oclock/>.
- Louise Beltzung. 2024. Ready or Not - How Prepared Are Advertising Libraries for the DSA? ÖIAT.
- [6] Auer,Valentine, Julia Krickl, Irem Hölzl, und Louise Beltzung. 2025. #KeineWerbung? Schleichwerbung und problematische Marketing kommunikation auf TikTok. Studie. ÖIAT. <https://research.oiat.at/tiktok>.
- [7] European Commission - European Commission. o. J. „Commission Preliminarily Finds TikTok’s Ad Repository in Breach of the Digital Services Act“. Text. Zugegriffen 30. Oktober 2025. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1223.
- [8] Entrena-Serrano, Carlos, Martin Degeling, Salvatore Romano, und Raziye Buse Çetin. 2025. „TikTok’s Research API: Problems Without Explanations“. Version 2. Preprint, arXiv. <https://doi.org/10.48550/ARXIV.2506.09746>.
- [9] European Commission. 2024. „Commission Opens Formal Proceedings against Facebook and Instagram under the Digital Services Act“. Text. April 30. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373.
- [10] <https://data-access.dsa.ec.europa.eu/home>
- [11] Horwitz, J. (2025). Meta is earning a fortune on a deluge of fraudulent ads, documents show. Reuters. <https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/>
- [12] Ian Moss. 2025. „Is a Global Consensus on Tackling Digital Ad Fraud Finally within Reach?“ New Digital Age, Oktober 16. <https://newdigitalage.co/technology/is-a-global-consensus-on-tackling-digital-ad-fraud-finally-within-reach/>.

The research in this paper was conducted within the ACR research projekt StopFraud.

Contact

Julia Krickl
krickl@oiat.at

Imprint

Austrian Institute for Applied
Telecommunications (ÖIAT)
Ungargasse 64-66/3/404
1030 Vienna, Austria

www.oiat.at
office@oiat.at

