

SPONSORED BY SCAMMERS

What this complaint is about and why it matters for consumers

Consumers spend more time online and increasingly rely on digital payment services in their daily lives. As their digital presence grows, so do fraudulent practices, with online advertising emerging as a major vector for scams. Whether watching videos, following friends, scrolling or reading the news, consumers are routinely exposed to increasingly sophisticated fraud schemes, leading not only to financial harm – i.e. in 2024, consumers suffered financial losses up to EUR 4.2 billion – but also to a loss of trust in digital and financial markets.

Under the EU’s Digital Services Act (DSA), online platforms are required to mitigate risks stemming from fraudulent contents by providing (among other things) transparency about the ads and advertisers on their interfaces, easy ways to report scams and by ensuring that scammers are removed from the platform.

Between December 2025 and March 2026, BEUC and 13 consumer organisations conducted large-scale evidence-gathering in 13 countries. The findings show that financial scams remain widespread on Meta, TikTok, and Google, and that platforms systematically fail to take effective corrective actions. In many cases, consumer groups found alarming discrepancies between what platforms claim to do and the reality of what is happening on their interfaces. Therefore, consumer organisations filed this complaint with the European Commission and the competent national authorities in May 2026 and highlighted breaches of Art. 16, 20, 23, 24, 25, 34, 35 and 39 DSA.

Our demands to the European Commission and competent national authorities

Consumer organisations call on the European Commission and national Digital Services Coordinators (DSCs) to:

- € Launch, or where applicable accelerate, investigations into Meta, TikTok, and Google’s DSA compliance and the measures taken by these platforms to mitigate risks related to financial scams.
- € Require Meta, TikTok, and Google to bring their practices into immediate compliance with the DSA.
- € Impose fines and, where appropriate, periodic penalty payments in cases of continued non-compliance.
- € Where platforms propose commitments to change their practices, ensure that interested third parties are given a meaningful opportunity to submit their views on those commitments.

Results

The figures presented below provide a snapshot of reported ads and contents.³⁰ Additional examples of scams flagged by consumer groups can be found in the accompanying Annex.

In a nutshell, consumer groups found that:

- Meta rejected nearly 43% of the submitted ads.
- TikTok only removed 21% of the submitted ads. In 37% of the cases, TikTok claimed that the ad was removed before they could review it.
- Google removed 60% of the submitted ads.

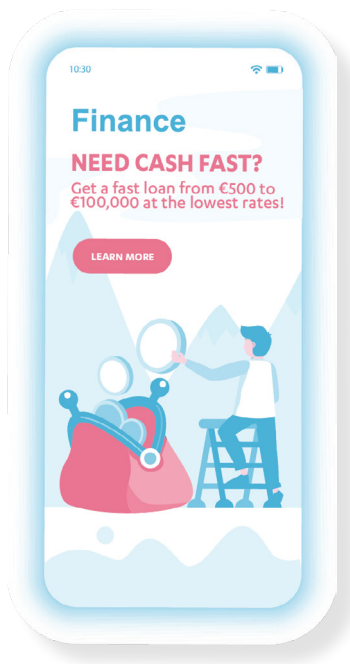
	Total number of notices submitted against fraudulent ads	Total number of ads taken down by the platform after notices	Total number of notices rejected by the platform as not considered fraudulent	Total number of ads ignored by the platform	Total number of ads removed before review
Meta	503	146	216	90	51
TikTok	360	79	74	73	134
Google ¹	30	18	7	5	0
Total	893	243	297	168	185

¹ For an explanation of the low number found on Google, please refer to p. 11 of the report

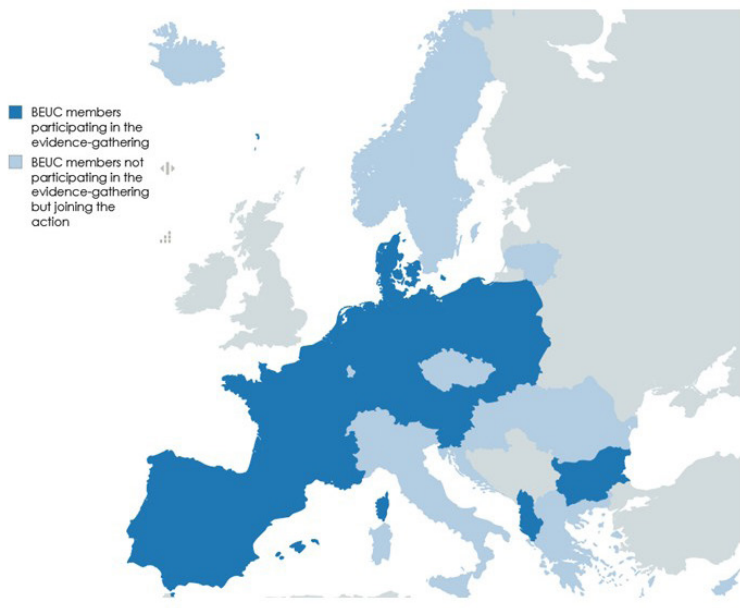
The toxic mix: when payment frauds meet the platform economy

In 2025, a survey on digital payments conducted by consumer groups in 10 European countries revealed that 22% of adults and 18% of teens had been victims of frauds or security breaches in the last 5 years.² In parallel, online advertising has become a major driver for payment frauds. It enables fraudsters to reach millions of consumers across Europe and beyond. A study conducted by the Austrian E-Commerce Trust Mark found that 54.7% of respondents reported seeing fraudulent or suspicious ads on platforms such as Facebook, Instagram, and TikTok.³

Reports have also revealed how online platforms might benefit from fraudulent ads. In December 2025, Reuters obtained confidential material which showed that about 10% of Meta’s overall annual revenue (approx. EUR 15 billion) comes from running ads for scams and banned goods. This includes fraudulent e-commerce and investment schemes, loans, gambling, and sale of banned medical products. According to the report, many of the fraudulent ads came from marketers whose behaviour was suspicious enough to be flagged by Meta’s internal warning systems. However, Meta seemed hesitant to crack down in ways that could harm its business interests.⁴



Consumer groups participating in the action



BEUC Members participating in the evidence-gathering

BEUC members not participating in the evidence-gathering but joining the action

2 BEUC, 'FREE, EASY AND SECURE', www.beuc.eu/sites/default/files/publications/BEUC-X-2025-085_What_consumers_expect_from_the_digital_euro-copy.pdf, p 3 (accessed 14 April 2026).
 3 Österreichisches E-Commerce-Gütezeichen, 'Von betrügerischer Online-Werbung umgeben: Zumindest jede zweite Person in Österreich betroffen', www.guetezeichen.at/blog-detail/betruegerische-online-werbung-jeder-zweite-betroffen/ (accessed 31 March 2026).
 4 Reuters, 'Meta is earning a fortune on a deluge of fraudulent ads, documents show' (2 November 2025), www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/ (accessed 13 April 2026). The article continues that "a small advertiser would have to get flagged for promoting financial fraud at least eight times before Meta blocked it, a 2024 document states".