Protecting Users from Scam Ads

A Call for Social Media Platform Accountability

Revolut

JUNIPER RESEARCH

Executive Summary

How Big of an Issue Are Scam Ads on Social Media in Europe?

Scam ads have grown to become a large problem across social media platforms. Despite paid advertising being a regulated industry, scam ads continue to plague social media users. Not only does this diminish the value of their social media platform for users through intrusive ads, but it leaves users open to potential financial losses.

Furthermore, social media platforms are benefitting from scam ads. In 2025, it was estimated that they received nearly £3.8 billion in revenue from scam ads in Europe, despite the risk they pose to users.

What Are Social Media Platforms Doing Today?

Whilst social media users are those which fall victim to these scams, the onus to avoid these impacts does not solely rest on them. Social media platforms control the entirety of the ecosystem, including demand-side and supply-side markets, and the social media platform itself.

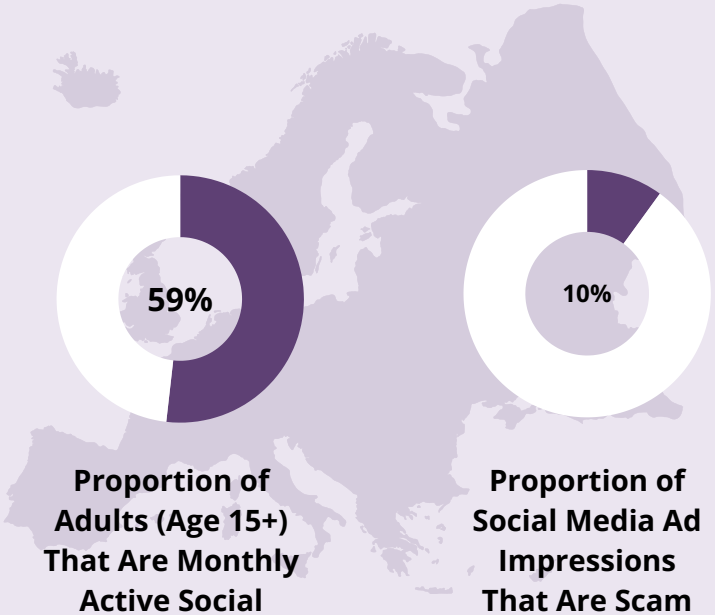
Social media platforms have acknowledged the impact of scam ads. They invest heavily in tools which monitor ad traffic; using AI and advertiser behaviour scoring. Additionally, they enable platform users to report scam ads.

Social Media Platforms Must Take More Responsibility

Social media platforms generate revenue from all ads on their platform; regardless of the authenticity of the ad itself. Whilst these platforms, such as Facebook and Instagram, also need to protect their users, the extent of this in comparison to maintaining and growing ad revenue is taken into consideration.

Leaked documents allege that leading social media platform developer Meta has directed its efforts toward hiding these scam ads from regulators and others, rather than prioritising the removal of scam advertisers from its platform.

Europe 2025



Proportion of Adults (Age 15+) That Are Monthly Active Social Media Users

Proportion of Social Media Ad Impressions That Are Scam Ads

Source: Juniper Research

993bn

Scam Social Media Ad Impressions in 2025 in Europe

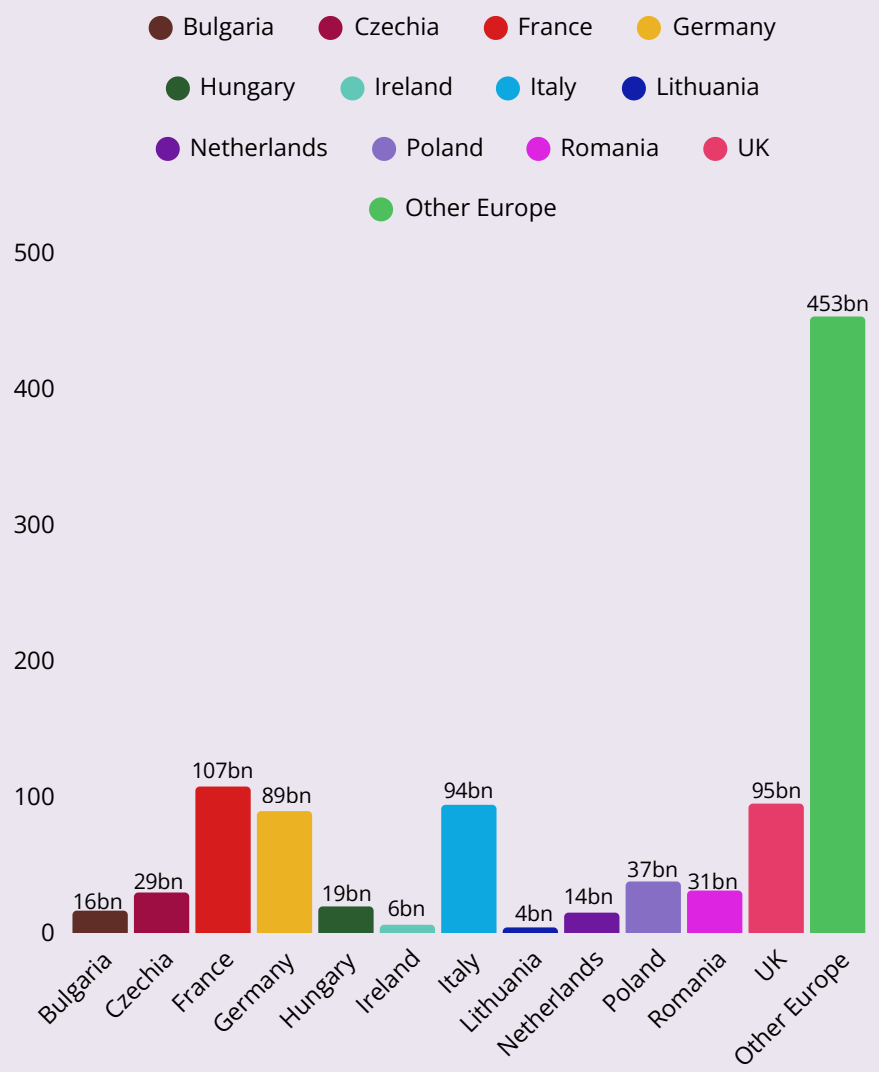
£3.8bn

(€4.4bn)

Social Media Ad Revenue from Scam Ads in 2025 in Europe

Source: Juniper Research

Total Scam Ads Impressions in Europe in 2025: 993 billion



Source: Juniper Research

Revolut

Scam Ads on Social Media

Scam ads are misleading digital ads that deceive users into engaging with fraudulent offers, solutions, or products. They use misleading promotions or endorsements; sometimes impersonating legitimate enterprises or retailers. The aim is to exploit social media users into making payments for fake products or investment opportunities.

Fraudulent players are attracted to social media platforms that are regularly engaged by a large number of users. These platforms are viewed as an ideal place for scammers to place scam ads.

The impact of scam ads on social media platforms has only become worse over recent years. As more scammers look to exploit the wide reach they provide, the platforms simply benefit from the additional advertising revenue.

In 2025, over half of the population of Europe are active social media users; representing over 430 million individuals. By 2030, there will be over 470 million people using social media platforms on a monthly basis. This is a notable entry point for scammers looking to financially benefit.

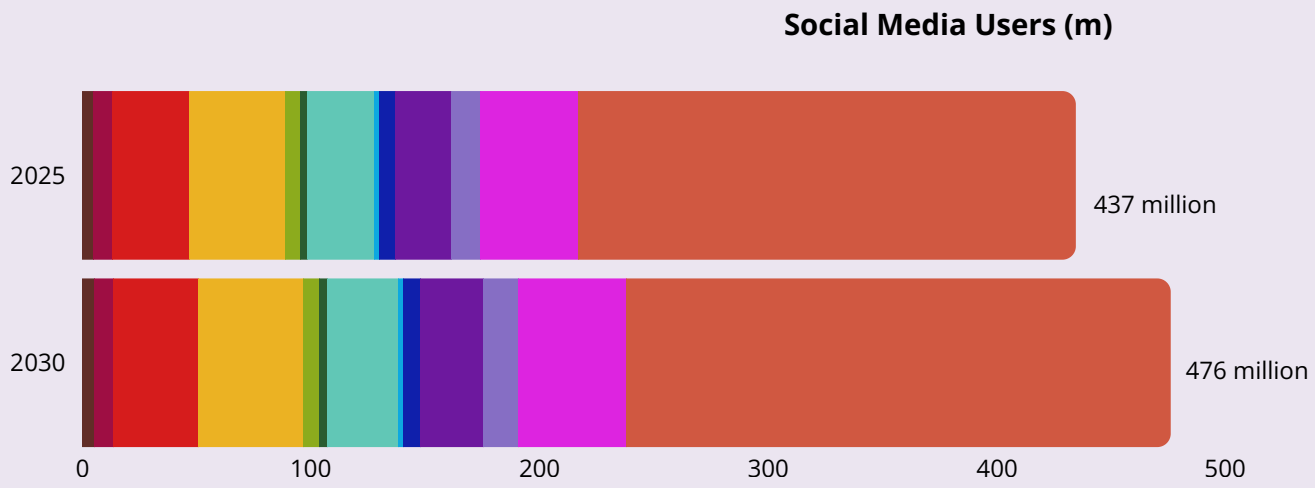
Additionally, social media platforms typically provide marketplaces or support payments that offer the perfect platform for scam activities; enabling direct payments which users often trust.

This has created an ecosystem which cultivates opportunities for scam advertisers. The majority of the responsibility to reduce these scam ads is on the social media platforms themselves, as they provide the solutions and ad services used by the scam players.

Social media users largely trust social media platforms and, by association, trust the content displayed. These platforms are often viewed as widely used and familiar.

However, the credibility of these platforms, such as Facebook and Instagram, is increasingly being questioned as scam ads continue to rise. Additionally, social media users assume platforms actively monitor harmful or scam activity. While social media platforms do monitor traffic for scam activity, it seems that their motivation to do so conflicts with these platforms' strategy to maximise ad revenue.

Regardless, this inherent trust can drive social media users into a false sense of security; leaving them vulnerable to financial losses through scam ads as scammers exploit platforms' credibility.



	2025	2030
Bulgaria	4.8m	5.1m
Czechia	8.0m	8.5m
France	33.9m	37.0m
Germany	42.1m	46.0m
Hungary	6.7m	7.2m
Ireland	2.8m	3.2m
Italy	29.6m	31.2m
Lithuania	2.2m	2.5m
Netherlands	6.7m	7.4m
Poland	24.5m	27.2m
Romania	13.0m	15.3m
UK	42.7m	47.3m
Other Europe	230.7m	253.7m

Source: Juniper Research

Juniper Research estimates that nearly 1 trillion scam ad impressions were delivered to social media users in Europe in 2025.

If the impact of scam ads is not addressed, the value of social media platforms will be increasingly diminished. It is in the best interest of platforms, such as Meta, to invest more substantially in processes that can better detect and block scam ads, and the advertisers looking to exploit social media platforms.

As can be seen in the graph to the right, if current trends were to continue, Juniper Research estimates there would be over 1.4 trillion social media scam ads in Europe by 2030. However, this growth could slow, or even decline, if social media platforms were to take more affirmative and transparent action in blocking scam ads.

In the short term, social media platforms may benefit in terms of ad revenue, however, this will damage social media platforms in the long run. As the value of their platforms is diminished by a high prevalence of scam ads, users will be more encouraged to move to alternative platforms.

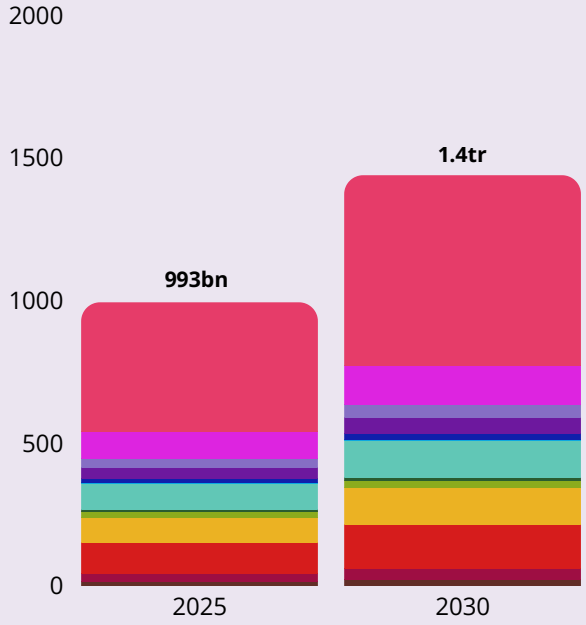
This growth in scam ads is driven by various factors including more connectivity, the growth of mobile-first economies, growing audience reach, and shifting priorities amongst digital advertisers. As a result, social media platforms are set to experience substantial growth in revenue in Europe.

However, if social media platforms do not address the growing number of scam ads displayed to their users, concerns will persist as to how social media platforms are sacrificing the safety of their users for additional ad revenue.

Logically, as the number of users grows, so does the attractiveness of the platforms to scam advertisers. It provides greater reach, and a larger number of legitimate social media ads in which they can hide their scam ads.

Therefore, social media platforms must assume that, as their platforms grow, so will the ad impressions to users, and so will the number of scam ads displayed to their users. Whilst revenue will increase, so will the risk to their end users.

Scam Ad Impressions on Social Media (bn)



	2025	2030
Bulgaria	16bn	22bn
Czechia	29bn	41bn
France	107bn	153bn
Germany	89bn	128bn
Hungary	19bn	27bn
Ireland	6bn	8bn
Italy	94bn	129bn
Lithuania	4bn	5bn
Netherlands	14bn	21bn
Poland	37bn	54bn
Romania	31bn	48bn
UK	95bn	137bn
Other Europe	453bn	665bn

Source: Juniper Research

The average social media user in Europe sees over 190 scam ads per month over the platforms they use.

By 2030, this is expected to rise to 250 scam ads per month; driven by increased usage of social media platforms.

1 in 10 ads shown to social media users in Europe in 2025 was a scam.

The Impact on Users

Scam ads erode trust among social media users through advertising fake products with attractive deals or investment opportunities. When users are successfully deceived, they not only lose money, but also risk exposing sensitive financial and personal information to scammers. For example, financial scams, such as crypto scams, can appeal to social media users; owing to their get-rich-quick nature.

Beyond financial harm, social media platforms must consider the impact that scam ads can have in eroding confidence in their ecosystems. If scam ads are not reduced, users will become wary of legitimate ads; eventually reducing engagement from enterprises and demand for ad space on their platforms.

Additionally, victims often experience emotional distress, such as feeling embarrassed or violated, which may not only discourage engagement with ads, but also with future online interactions over their platforms.

Whilst there is some degree of responsibility on a social media user to detect and avoid scam ads, social media platforms must do more to block ads before they are displayed to the user.

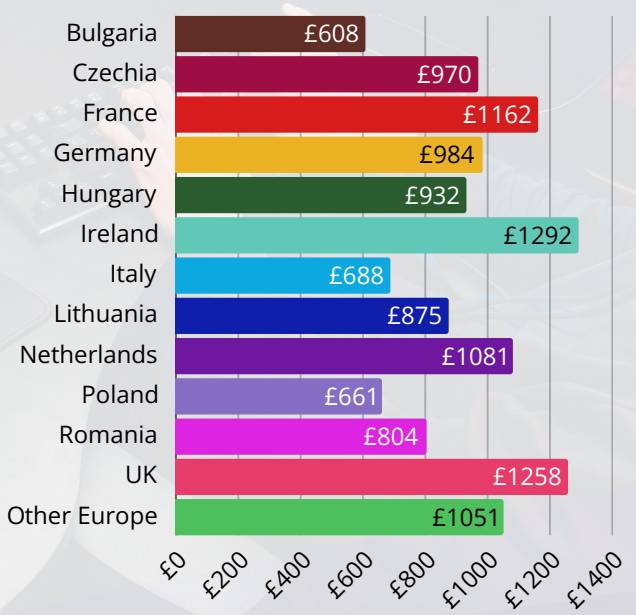
Indeed, the sophistication of scam ads is bridging the gap between ads from legitimate brands and scam ads that often impersonate them. This is making it more likely that the average social media user falls for a scam ad; thus, contributing to the growth of losses to social media scam ads in Europe.

The increasing sophistication of these scam ads and growth in user losses necessitate stronger platform accountability and user education. Social media platforms must create robust detection and enforcement; as scam ads will only continue to undermine consumer trust and contribute to user losses.

Additionally, the prevalence of these user losses is high in all countries. For example, the research estimates that approximately 14% of social media ad impressions in Bulgaria were scam ads in 2025; notably high.

Conversely, Poland, whilst on the lower end of the spectrum, still experiences more than 6% of social media as scam ads in 2025. This still accounts for more than 1 in 20 ads.

Average User Losses per Scam in 2025, Europe



Source: Juniper Research

Not only is the number of scam social ads increasing, but the average loss per successful attempt is also rising. Scammers are becoming more inventive in the ads they display, and AI has accelerated the rate at which scam ad content is created.

Additionally, more 'lucrative' scam tactics, such as investment scams, are becoming increasingly popular amongst those creating scam ads. Not only is this contributing to the rise in losses per successful scam, but it is contributing to the growth of the overall number of scam ads on social media. The sheer number of advertisers and ads across the ecosystem necessitates intervention from social media platforms to block scam advertisers. Given the scale of social media traffic, AI is already necessary to effectively tackle scam ads - which social media platforms have confirmed they are using today.

Meta publicly affirmed its commitment to combatting scam ads on the platforms it owns, Facebook and Instagram, in December 2025. Prior to this announcement, Meta has implemented tools that block specific types of scam ads, including AI-based facial recognition software that can detect the unauthorised use of images in ads. It also provides enhanced brand protection by enabling legitimate enterprises to report scams which infringe on copyrighted or trademarked material.

But this raises one notable question. If social media platforms such as Meta have the tools necessary to combat scam ads, why is the value of losses to scam ads still rising?

Meta announced it had removed 134 million scam ads in November 2025 so far that year; reducing user complaints by 50% over the previous 15 months. It attributed this reduction to AI detection tools and advertiser verification solutions; notably for ads in the financial sector. Meta announced that it removed 12 million accounts linked to scam ads in the first six months of 2025. However, some outlets, such as Reuters, have reported that efforts from Meta could have done more to tackle scam ads. Instead of blocking scam ads, the company only removed keywords to make these scam ads harder for regulators and journalists to find.

These leaked internal documents raise questions surrounding these announcements. The documents have unveiled a 'playbook' from Meta which minimises the visibility of public ad library searches in certain countries.

The documents allege that Meta targeted keywords related to known scam ads, then removed ads which matched that keyword in order to hide them from regulators, journalists and users. This implies that, instead of looking to solve the issue and reduce scam ads, Meta's priority was to hide the problem.

Meta has implemented tools that block specific types of scam ads, including AI-based facial recognition software that can detect the unauthorised use of images in ads. It also provides enhanced brand protection by enabling legitimate enterprises to report scams which infringe on copyrighted or trademarked material.

Social Media Platforms Must Share Responsibility

Social media ad revenue has grown vastly over the last few years; benefitting social media platforms substantially. However, as previously mentioned, social media platforms generate 10% of their ad revenue in Europe from scam ads. This raises a conflict of interest. While social media platforms have a responsibility to protect their users, they do benefit from ad revenue; regardless of whether or not ads are scams.

Juniper Research estimates that social media ad revenue in Europe will grow from £38 billion (€44 billion) in 2025 to over £84 billion (€98 billion) by 2030; a substantial growth of 120% in just five years.

Social media platforms have the primary responsibility of reducing both the prevalence and subsequent impact of scam ads. They control the infrastructure, algorithms, and ad approval processes that enable scam content which leads to users' financial losses.

Platforms cannot shift any blame to users or regulators, and must decide to prioritise user safety over the revenue gained from these scam ads.

Every day of continued inaction puts their platform users at risk of financial harm from scams, and will erode further trust in their services. From now on, social media companies must be the ones to take ownership of the issue of scam ads.

Social Media Platform Revenue From Scam Ads (£m)

	2022	2025
Bulgaria	£39m/€46m	£59m/€69m
Czechia	£78m/€92m	£119m/€139m
France	£233m/€273m	£362m/€422m
Germany	£240m/€283m	£375m/€438m
Hungary	£27m/€31m	£41m/€48m
Ireland	£17m/€20m	£27m/€32m
Italy	£209m/€246m	£317m/€370m
Lithuania	£8m/€10m	£13m/€16m
Netherlands	£37m/€44m	£58m/€67m
Poland	£93m/€109m	£147m/€172m
Romania	£36m/€43m	£60m/€70m
UK	£276m/€324m	£430m/€502m
Other Europe	£1.1bn/€1.3bn	£1.8bn/€2.1bn

Source: Juniper Research

Social media platforms generate substantial revenue from ads. If scam advertisers were blocked, then social media platforms would experience diminished revenue.

By blocking scam ads, social media platforms are protecting their end users from potential scams.

The sheer scale of social media ad traffic means that social media platforms will need to spend significant sums to block scam advertisers.

By reducing scam ads, social media platforms increase the value of their platform. In the long term, they will benefit from being able to charge a premium to advertisers.

Next Steps for Social Media Platforms

Scam ads over social media have grown to become a significant threat to users in Europe. Scammers exploit social media users through evolving tactics; often causing financial losses and distress. The biggest burden of how to reduce this impact lies with social media platforms.

Why Social Media Platforms Must Want to Reduce Scam Ad Impacts

Social media platforms are the primary enablers of these scam ads, as they control the ecosystem in which these ads are distributed, displayed, paid for, and approved. Given they control such a large part of the ecosystem, the burden of reducing the impact of scam ads lies with social media platforms.

Whilst they may initially suffer from a reduction in ad revenue from their platform, they gain something far more important – more protection for their users. In the long run, users will view social media platforms with less scams as of higher value. This will attract more users and better advertisers to their platforms.

Indeed, these are the individuals which suffer the financial losses arising from scam ads, while social media platforms benefit from the revenue. If the value of the platform decreases, eventually social media platforms will begin to see a reduction in users as they seek alternative platforms which do not suffer from the impact of scam ads.

The recent growth in scam ads must be considered a systemic issue. While these platforms generate significant revenue from scam ads, it is clear that they must take action and start prioritising the safety of their users.

The primary goal of social media companies, as with all other service providers, is to protect their users and revenue through providing the most valuable services. This is most notable as the competition for digital services grows.

Regulators also play a key role in defining compliance and enforcing frameworks that provide protection for social media users. While initiatives such as the EU's Digital Services Act aim to enforce accountability, regulation can be a key driving force in driving greater accountability from social media platforms.

However, social media players must not allow other bodies to take the lead in implementing regulations that protect users from scam ads. Social media platforms must be the stakeholder that drives the conversation, and action around frameworks that identify and block scam ads on platforms.

Social media platforms must want to reduce the prevalence of scam ads first. Whilst there has been public commitment to tackling scam ads, some social media platforms are allegedly taking a different approach privately.

Platforms must move beyond merely committing to tackling scam ads. Moving forward, there needs to be more decisive action, a much higher degree of transparency, and more technologies put in place to protect social media users. These efforts must be led by leading companies such as Meta.

How Do Social Media Platforms Reduce Scam Ads?

Scam ads over social media have grown to become a significant threat to users in Europe. Scammers exploit regulatory loopholes and conflicts of interest to deceive social media users; often causing financial losses and distress. The biggest burden of how to reduce this impact lies with social media platforms.

Today, platforms employ a wide variety of technologies to detect and block scam ads. However, these solutions rely heavily on technology that automates the identification of suspicious activity; given the substantial amount of traffic sent over social media platforms.

This approach does have drawbacks. Whilst there is a higher degree of automation, this increases the chance that potentially high-risk ads slip through the identification process. This will ultimately lead to consumer losses and diminished value of a social media platform.

In addition, many social media platforms have introduced manual advertising verification processes. This verifies the identity of the advertiser, rather than the content of the scam ad itself. Whilst more costly in terms of time, it has proven effective at tackling scam ads for financial services and investment opportunities. Meta has expanded these identity checks to other types of fraud owing to its effectiveness.

Lastly, social media platforms must work more closely with regulators and law enforcement to reduce scam ads. This must be done before more legislation is put in place that enforces new solutions to be adopted.

Be More Transparent

Social media platforms must release information on their efforts to combat fraud; holding themselves accountable to reducing scam ads.

Invest in Manual Identification

Automated identification, via AI, cannot fully combat scam ads. Manual intervention is needed to verify the advertisers themselves.

Prioritise User Safety

All efforts in reducing scam ads must target protecting users, including removing scam advertisers from the ecosystem and blocking scam ads.

Be Agile Against New Tactics

As new technologies block scam ads, new tactics will evolve to evade this detection. Social media platforms must be quick to respond.

Rebuild Trust Amongst Users

As social media platforms reduce scam ads, they must promote their efforts amongst users to increase user trust in their platforms.

Out of all of the players in the ecosystem, social media platforms carry the most responsibility for reducing the impact of scam ads.

This must be achieved through transparency in their ad approval processes, use of AI, and regulatory compliance.

Despite the lost revenue from removing scam ads, and the increased cost of doing so, social media platforms must protect the value of their platforms and reduce risk of financial losses for their users.

About Juniper Research

Juniper Research is a leading global analyst firm, established in 2002 and based in the UK, that specialises in providing market intelligence, analysis, and strategic insights for high-growth sectors within the digital ecosystem; focusing on areas such as Fintech, Telecoms, IoT, Smart Cities, and Sustainability.

Juniper Research offers syndicated and bespoke research, market forecasting, and data-driven insights to help businesses navigate digital innovation and make informed strategic decisions in competitive tech markets.

About Revolut

Revolut is a global fintech, helping people get more from their money. In 2015, Revolut launched in the UK, offering money transfer and exchange. Today, more than 70 million customers around the world use dozens of Revolut's innovative products to make more than a billion transactions a month.

Across our personal and business accounts, we give customers more control over their finances and connect people seamlessly across the world.

Methodology

Juniper Research began to size the social media advertising market through publicly available data released by leading social media platforms in Europe. We leveraged internal data for metrics such as population, adult population, social media users, and social media accounts to initially size the market. We define a scam ad on social media as a deceptive paid post that misleads users into giving money, personal information, or account access by falsely advertising products, services, or investment opportunities.

Juniper Research does not classify platforms as social media companies when user accounts and content sharing are secondary to the platform's core value proposition. As such, our social media definition excludes video-streaming services (such as YouTube, DailyMotion, and Twitch) and mobile messaging applications (including WhatsApp, Viber, and Telegram).

Instead, our analysis focuses exclusively on platforms where social interaction, content discovery, and algorithm-driven feed engagement form the primary user experience. The social media platforms within scope for this study include: Facebook, Instagram, TikTok, Snapchat, X (formerly Twitter), and LinkedIn.

This dataset, analytical framework, and the accompanying whitepaper have been developed independently by Juniper Research, using our established forecasting methodologies, and have been commissioned by Revolut. Roles and responsibilities were clearly defined. Juniper Research is responsible for all data modelling, sizing, and analysis.

Revolut commissioned the research, but did not influence the data, underlying methodology or conclusions. To ensure analytical integrity, the dataset and outputs have additionally undergone an internal peer review within Juniper Research.

As part of Juniper Research's forecasting approach, we used verified industry data on social media advertising volumes to estimate the number of ads displayed to users across these platforms. Publicly available cost-per-mille (CPM) figures were then incorporated into our forecasting model to determine the scale of advertising exposure. We also used open-source datasets to assess the prevalence of scam advertisements and estimate associated consumer losses. While this model uses the best available evidence, it is important to note that scam activity is frequently under-reported or undetected, meaning all loss estimates are presented on a best-efforts basis.

To further strengthen the robustness of the projections, Juniper Research employed a multi-layer, bottom-up market modelling approach, combining:

- *platform-level ad-impression estimates taken from external sources*
- *cross-validation against historical scam-ad prevalence figures; sense checked against various forms of other fraud*

This whitepaper includes comprehensive pan-European data and forecasts, with detailed country-level segmentation across the following 11 markets: Bulgaria, Czechia, France, Germany, Hungary, Ireland, Italy, Lithuania, Netherlands, Poland, and the United Kingdom.