Billing Code: 6750-01-P

FEDERAL TRADE COMMISSION

16 CFR Part 461

RIN 3084-AB90

Rule on Impersonation of Government and Businesses

AGENCY: Federal Trade Commission.

ACTION: Advance notice of proposed rulemaking (“ANPRM”); request for public comment.

SUMMARY: The Federal Trade Commission (“FTC” or “Commission”) proposes to commence a rulemaking proceeding to prevent certain unfair or deceptive acts or practices by search engine, social media, and other digital marketplace platforms that further government and business impersonation scams to defraud consumers. The Commission is soliciting written comment, data, and arguments concerning the need for such rulemaking.

DATES: Comments must be received on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Interested parties may file a comment online or on paper, by following the instructions in the Request for Comments part of the SUPPLEMENTARY INFORMATION section below. Write “16 CFR Part 461—Impersonation Rule, Matter No. R207000” on your comment and file your comment online at *https://www.regulations.gov*, by following the instructions on the web-based form. If you prefer to file your comment on paper, write “16 CFR Part 461—Impersonation Rule, Matter No. R207000” on your comment and on the envelope, and mail it to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Hong Park (202-326-2158) and Elyse McNamara (202-725-3101), Attorneys, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION:

I. Overview

Every year, American citizens lose tens of billions of dollars to scams. In 2025, consumers reported losing approximately $16 billion to fraud, a 25% increase compared to 2024.[1] In our annual *Protecting Older Consumers Report*, the FTC estimated that the true cost of fraud in 2024, adjusted to account for underreporting, may be as high as $195.9 billion.[2] The top fraud reported by consumers to the FTC is impersonation—where an imposter pretends to be a real business, government agency, family member, or

---

[1] Fed. Trade Comm'n, *FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025* (June 15, 2026), https://www.ftc.gov/news-events/news/press-releases/2026/06/ftc-data-show-people-reported-losing-3-point-5-billion-imposter-scams-2025.

[2] Fed. Trade Comm'n, *Protecting Older Consumers Report 2024-2025*, at 28 (2025), https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf.

other trusted source to elicit money from the victim.[3] Last year, the FTC received over 1 million imposter reports, with consumers reporting nearly $3.5 billion in losses.[4]

Some of the most pernicious impersonation scams involve government and business impersonations. Consumers rely on government agencies and businesses on a daily basis to comply with the law (such as by paying tolls) and to conduct routine transactions (such as online bank transfers). Impersonation scams exploit this trust, often inflicting considerable harm on consumers while causing legitimate businesses to lose revenue and suffer reputational damage.

The Commission previously determined that these impersonation scams are prevalent in the U.S. economy and promulgated the Rule on Impersonation of Government and Businesses[5] ("Impersonation Rule" or "Rule") to address them. The Commission has vigorously enforced the Rule and other laws to stop these scams. Notwithstanding these efforts, however, scams—especially those perpetrated by foreign bad actors—continue to proliferate. In recent years, these scams have been amplified by search engine, social media, and other digital marketplace platforms that profit from optimizing online ads for third parties, regardless of whether the third parties are legitimate, while avoiding the social cost of the impersonation scams furthered by such

---

[3] *See* Fed. Trade Comm'n, *FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025*, *supra* note 1.

[4] Fed. Trade Comm'n, *The Big View: All Sentinel Reports, Top Reports 2025,* Tableau Public (July 28, 2026), https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports.

[5] 16 CFR Part 461; 89 FR 15017 (Mar. 1, 2024).

ad optimization.[6] The Commission now seeks public comment on whether it should address this misalignment of platform incentives, which is not covered by the current Rule, by initiating a rulemaking that would force such platforms to internalize the cost of optimizing fraudulent ads.

II. March 2024 Impersonation Rule and Proposed Means-and-Instrumentalities Provision

The Impersonation Rule prohibits the impersonation of government, businesses, and their officers or agents as unfair or deceptive acts or practices under section 5 of the Federal Trade Commission Act[7] ("FTC Act"), 15 U.S.C. 45. In December 2021, the Commission began its consideration of a rule to address impersonation fraud by soliciting public comment on an advance notice of proposed rulemaking.[8] The following year, the Commission determined it had reason to believe these acts or practices are prevalent in the U.S. economy and published a notice of proposed rulemaking ("2022 NPRM") formally proposing to promulgate a new rule.[9] In March 2024, the Commission finalized and promulgated the Rule, finding that consumer complaint data from the Consumer Sentinel Network, the Commission's enforcement record, data from a wide range of

---

[6] Firms that do not internalize the costs their activities impose on others can create harmful spillovers or "externalities." *See* R.H. Coase, *The Problem of Social Cost*, 3 J.L. & Econ. 1 (1960); *infra* notes 22-24 and accompanying text discussing negative externalities. Among other things, because many consumers who fall victim to impersonation scams blame the impersonated business or scammer—not the digital platform furthering the impersonation—digital platforms face little to no market discipline to correct the problem and have even less incentive to internalize the cost of scams, leaving the social harm unaddressed.

[7] 45 U.S.C. 41 *et seq*.

[8] 86 FR 72901 (Dec. 23, 2021).

[9] 87 FR 62741 (Oct. 17, 2022).

commenters, and other evidence in the rulemaking record supported its prevalence determination.[10]

During the course of that rulemaking, the Commission had also considered expanding the Rule to prohibit two additional types of unfair or deceptive acts or practices: first, the impersonation of individuals; and second, the provision of the means and instrumentalities used in prohibited impersonations.[11] However, after further consideration, the Commission did not adopt the proposed means and instrumentalities prohibition.[12] With respect to the impersonation of individuals provision, the

---

[10] 89 FR 15017 (Mar. 1, 2024).

[11] 87 FR 62741 (Oct. 17, 2022) (2022 NPRM); 89 FR 15072 (Mar. 1, 2024) (Supplemental Notice of Proposed Rulemaking "2024 SNPRM"). In the 2024 SNPRM, the proposed definition of "individual" was "a person, entity, or party, whether real or fictitious, other than those that constitute a business or government under this Part." 89 FR at 15077. The Commission initially proposed a means and instrumentalities provision in the 2022 NPRM. The 2024 SNPRM subsequently modified that proposal to read: "It is a violation of this part, and an unfair or deceptive act or practice to provide goods or services with knowledge or reason to know that those goods or services will be used to: (a) materially and falsely pose as, directly or by implication, a government entity or officer thereof, a business or officer thereof, or an individual, . . . ; or (b) materially misrepresent, directly or by implication, affiliation with, including endorsement or sponsorship by, a government entity or officer thereof, a business or officer thereof, or an individual . . . ." 89 FR at 15083.

[12] In the December 26, 2024 Initial and Final Notice of Informal Hearing, the Commission stated it "has decided not to proceed with the SNPRM's proposed means and instrumentalities provision at this time." 89 FR 104905, 104906 (Dec. 26, 2024). Commenters responding to the SNPRM proposal raised a number of concerns, including that the proposed language covering any means and instrumentality was overbroad and that the Commission should have introduced the proposal through an ANPRM instead of an SNPRM. *See, e.g.,* FTC-2023-0030-0059, FTC-2023-0030-0070, FTC-2023-0030-0082, and FTC-2023-0030-0092. Comments to the 2024 SNPRM can be found at https://www.regulations.gov/document/FTC-2023-0030-0031/comment. The Commission does not take a position on these issues. Regardless, the Commission's action here moots these commenters' concerns as any means-and-instrumentalities

Commission held an informal hearing in January 2025 and is still evaluating its options.[13]

III. Digital Marketplace Platforms and the Growing Threat of Impersonation Scams

Digital marketplace platforms ("Platforms")[14] have become essential infrastructure of the U.S. economy. They have achieved near-universal adoption in the United States, serving as a primary gateway through which consumers discover products and services, interact with businesses, and gather information.[15] Indeed, about 85% of

---

provision that the Commission considers in this proceeding will focus on ad-optimization practices by digital marketplace platforms and will therefore necessarily be narrower than the 2024 SNPRM's proposed provision covering *any* means and instrumentality. In addition, the Commission begins its consideration of any such provision through this ANPRM, not an SNPRM.

[13] *See* Trade Regulation Rule on Impersonation of Government and Business, 2026 Regulatory Plan and the Unified Agenda of Federal Regulatory and Deregulatory Actions (July 2026), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202510&RIN=3084-AB71.

[14] As used herein, Platforms are public-facing websites or apps on which third parties offer goods, services, or opportunities through paid advertisements or other listings. These Platforms typically integrate ads for third-party products and services into the platform user experience, such as through posts on social media feeds and search engine results, and often embed hyperlinks into the ads for the interested consumer to use to contact the third party. Examples of Platforms include Google.com, Facebook.com, Amazon.com, Apple App Store, and LinkedIn.com.

[15] *See* Colleen McClain & William Bishop, *What we know about internet use, smartphone ownership and digital divides in the U.S.*, Pew Rsch. Ctr. (Jan. 8, 2026), https://www.pewresearch.org/short-reads/2026/01/08/internet-use-smartphone-ownership-digital-divides-in-u-s/#_What%E2%80%99s_the_current ("Nine-in-ten U.S. adults use the internet daily, including 41% who say they're online almost constantly. This is on par with what we found in 2023 and 2024."); Jeffrey Gottfried & Eugenie Park, *Americans' Social Media Use 2025*, Pew Rsch. Ctr. (Nov. 20, 2025), https://www.pewresearch.org/internet/2025/11/20/americans-social-media-use-

U.S. consumers shop online, with e-commerce Platform Amazon.com leading in online retail sales.[16]

A key driver of Platforms' expanding role in e-commerce is advertising. Platforms have revolutionized how advertisers reach consumers by offering ad-optimization tools and services that enhance an ad's effectiveness in engaging consumers. These tools and services can develop ad content, including through ad copy creation, image and video generation, ad enhancements, and product listing creation or enhancement. They can also use detailed consumer data—including the consumer's demographic profile, websites visited, and search history—to tailor the content and delivery of advertisements. For example, Meta offers its advertisers Meta Advantage+, a "suite of products that helps advertisers maximize performance by using AI to optimize campaigns in real-time and match ads to the people most likely to take action."[17]

2025/#changes-in-use-of-online-platforms (52% of surveyed adults said they used Facebook at least once a day; 48% reported using YouTube at least once a day); *Holiday Shopping 2025: US Fact Sheet*, McAfee (Nov. 11, 2025), https://www.mcafee.com/blogs/mcafee-news/holiday-shopping-2025-us-fact-sheet/ (97% of respondents use at least one social media platform); *State of Search 2025: Insights into American Online Search Behavior*, Claneo, https://www.claneo.com/en/state-of-search-us/ (last visited Aug. 19, 2026) (72% of surveyed respondents used search engines like Google, Bing, and Yahoo multiple times a week); U.S. Census Bureau, *Quarterly Retail E-Commerce Sales 1st Quarter 2026*, at 1-2 (May 18, 2026), https://www2.census.gov/retail/releases/historical/ecomm/26q1.pdf (e-commerce retail sales accounted for 16.8% of total retail sales in the first quarter of 2026, totaling over $300 billion).

16 *See* Xin Ou, *Online shopping behavior in the United States – statistics & facts*, Statista (Dec. 17, 2025), https://www.statista.com/topics/2477/online-shopping-behavior/#editorsPicks.

17 *Meta Advantage+ features*, Meta, https://www.facebook.com/business/help/2486309305148646 (last visited Aug. 19, 2026)

Similarly, Google offers tools that will "find the best performing ad combinations" from advertiser-supplied assets to optimize delivery and consumer response.[18] These capabilities benefit both businesses and consumers. But they also create serious risks: the same tools and services that rapidly generate and deliver highly-targeted ads are often readily available and easy for both legitimate entities and scammers to use.[19]

The root of the problem lies in how Platforms' incentives are structured. In economic terms, Platforms may be thought of as multi-sided markets that connect

---

(features include audience automation, ad creative automation, ad placement automation, and more). *See also* Jeff Horwitz, *Meta is earning a fortune on a deluge of fraudulent ads, documents show*, Reuters (Dec. 28, 2025), https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/ ("The [Meta] documents further note that users who click on scam ads are likely to see more of them because of Meta's ad-personalization system, which tries to deliver ads based on a user's interests").

[18] *How to set up your first Google Ads campaign*, Google Ads, https://business.google.com/us/google-ads/how-ads-work/ (last visited Aug. 20, 2026) ("Add your campaign assets and preview your keywords, images, logos, and videos in different ad formats. Google's AI will then find the best performing ad combinations to multiply campaign results for your goal."). *See also FTC v. Doxo Inc. et al.*, No. 2:24-cv-00569, 2026 WL 1429295, at *2 (W.D. Wash. May 21, 2026) (according to defendants' search engine optimization expert, the advertiser did "not manually dictate the precise order or static nature of the text in ad headlines" displayed on search engine platform; "rather, advertisers submit up to 15 ad headlines elements, three of which are dynamically assembled by the search engine platform").

[19] *See* Consumer Fed'n of Am., *The Scam Economy: The True Cost of Online Scams and Crimes in America*, at 3 (2026) https://consumerfed.org/media/legacy/post_32705/The-Scam-Economy_The-True-Cost-of-Online-Scams.pdf ("AI is supercharging these scams, social media platforms are enabling the spread, and data brokers facilitate targeting of victims, allowing criminals to reach consumers at massive scales while exploiting highly precise profiling."). *See also Creative solutions, bring your brand story to life*, Amazon Ads, https://advertising.amazon.com/creative-solutions (last visited Aug. 18, 2026) ("Amazon Ads creative solutions are a suite of tools and services designed to help advertisers of all types and sizes to bring their brand story to life. Our creative solutions include self-service tools as well as hands-on support across creative ideation and strategy, creative production and editing, ad policy, and creative effectiveness."); *supra* notes 17-18.

consumers on one side with sellers who may advertise on the other, and their incentive structure reflects their intermediary role. Currently, Platforms financially benefit from all paid advertisements posted on their platform, including scam advertisements.[20] As with other ads, Platforms can generate revenue from scam ads in multiple ways, including when Platform services are used to develop the ads, when the ads are posted on the Platform, or when consumers engage with the ads.[21] However, Platforms do not bear meaningful responsibility for the enormous social cost that results when consumers are victimized by scam ads that Platforms display and optimize.[22] These costs may represent negative externalities—costs that are not borne by the parties best positioned to reduce

---

[20] *See* Google, *How Google makes money with ads*, https://publicpolicy.google/article/how-google-makes-money-with-ads/ (last visited Aug. 20, 2026) ("If you find an ad useful and click on it to learn more, the advertiser pays Google."). *See also* Alphabet Inc., *Alphabet Announces First Quarter 2026 Results*, at 2 (2026), https://s206.q4cdn.com/479360582/files/doc_financials/2026/q1/2026q1-alphabet-earnings-release.pdf (Google and YouTube advertising alone generated over $77 billion in earnings in the first quarter of 2026—70% of Alphabet's total revenues that quarter); Investing.com, *Meta Q1 2026 slides: 33% revenue surge driven by ad momentum* (Apr. 29, 2026), https://www.investing.com/news/company-news/meta-q1-2026-slides-33-revenue-surge-driven-by-ad-momentum-93CH-4647470 (Meta's total reported revenue for the first quarter of 2026 was $56.3 billion, of which $55 billion was attributed to advertising); *Q1 earnings: Amazon CEO Andy Jassy discusses what's powering Amazon Ads*, Amazon News, https://www.aboutamazon.com/news/company-news/andy-jassy-amazon-ads-q1-2026-earnings (last visited Aug. 20, 2026) (reporting that Amazon Ads generated a revenue of $17.2 billion in the first quarter of 2026, which was up 22% year-over-year);*see also infra* notes 30-32.

[21] *See*, Consumer Fed'n of Am., *supra* note 19, at 19 ("For some scams and crimes, social media platforms directly profit via advertising revenue, revenue splits, and monetized content"); *How Google makes money with ads*, *supra* note 20.

[22] For example, Commission staff has reviewed Consumer Sentinel Network complaints about third parties perpetrating scams advertised on Platforms that do not mention the role the Platform tools/services played in optimizing the scam ad.

them—in this case, the Platforms.[23] The result is Platforms seeking to maximize their ad-related revenues with insufficient financial disincentive to avoid generating those revenues from scam ads.[24] In other words, Platforms internalize the revenue but externalize the risk.

Recent data, lawsuits, and press reports demonstrate the real-life impact of these misaligned incentives. Consumer data indicate that "scams perpetrated online [are]. . . more likely to result in a monetary loss" than those initiated by phone or text message,[25] with social media ranking among scammers' most frequently used contact methods and the costliest channel for consumers by total reported losses.[26] In 2025 alone, almost 30%

---

[23] The externalities—and corresponding costs—this proposal is addressing are what economists refer to as technological or non-pecuniary externalities, *i.e.*, a cost that affects another party's ability to produce or consume, without operating through prices or the price system. In other words, the price system does not internalize the externality through compensation or price adjustments. *See, e.g.*, Tibor Scitovsky, *Two Concepts of External Economies*, 62 J. Pol. Econ. 143 (1954).

[24] *See* Cristobal Cheyre, *Meta ad tools 'potent instruments' for scammers*, Cornell Chronicle (Nov. 6, 2025), https://news.cornell.edu/media-relations/tip-sheets/meta-ad-tools-potent-instruments-scammers ("Meta's response underscores a deeper failure of incentives: it bans only the most flagrant offenders while allowing others under suspicion to remain active, so long as they pay higher ad rates. This structure perversely rewards the most profitable scams – and ensures the platform takes a larger share of their proceeds.").

[25] Better Bus. Bureau, *2024 BBB Scam Tracker Risk Report*, at 26 (2025), https://bbbmarketplacetrust.org/wp-content/uploads/2025/02/2024-RiskReport-US.pdf.

[26] *See* Fed. Trade Comm'n, *Reported losses to scams on social media eight times higher than in 2020* (Apr. 27, 2026), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2026/04/reported-losses-scams-social-media-eight-times-higher-2020#ft1 (listing social media as the top fraud contact method based on total reported monetary loss; nearly 30% of people who reported losing money to scams in 2025 said the scam started on social media); Fed. Trade Comm'n, *Protecting Older Consumers Report 2024-2025*, *supra* note 2, at 25-26 ("In 2024, older adults filed more loss reports and reported losing more money in the aggregate to fraud that started on social media than to fraud

of consumers who reported losing money to scammers said the contact started on social media platforms, with reported losses reaching $2.1 billion.[27] Consistent with that data, public opinion research shows broad consumer consensus that online scams through Platforms are a national problem.[28] In parallel, the Commission has brought several recent enforcement actions against scams perpetrated on Platforms.[29] And State law

that reached them by any other method of contact"); Better Bus. Bureau, *supra* note 25, at 26-29 (36.2% of BBB survey respondents said that the scam incident they reported to the BBB that year involved social media, with roughly half of those incidents beginning when consumers responded to an advertisement or post); Horwitz, *Meta is earning a fortune on a deluge of fraudulent ads, documents show*, *supra* note 17 (internal May 2025 presentation by Meta's safety staff further estimated that the company's platforms were implicated in approximately one-third of successful scams in the United States).

[27] Fed. Trade Comm'n, *Reported losses to scams on social media eight times higher than in 2020*, *supra* note 26. And independent analyses suggest the true monetary losses are far higher due to widespread underreporting. *Id.* (*citing* K.B. Anderson, *To Whom Do Victims of Mass-Market Consumer Fraud Complain?*, at 1 (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3852323 (finding only 4.8% of people who experienced mass-market consumer fraud complained to a Better Business Bureau or a government entity). *See also* Consumer Fed'n of Am., *supra* note 19, at 6-8 (considering various surveys and research to measure underreporting).

[28] Pew Rsch. Ctr., *Online Scams and Attacks in America Today*, at 16 (2025), https://www.pewresearch.org/wp-content/uploads/sites/20/2025/07/PI_2025.07.31_Scams_REPORT.pdf (62% of respondents said scams are a major problem on social media platforms, and 50% said scams were a major problem on shopping platforms). *See also* Utah Dep't of Com., *NEWS RELEASE: 42 State and Territory Attorneys General Urge Meta to Take Action Against Investment Scam Ads* (June 11, 2025), https://commerce.utah.gov/2025/06/11/42-state-and-territory-attorneys-general-urge-meta-to-take-action-against-investment-scam-ads/ (42 attorneys general sent a letter to Meta "urging the company to take immediate and meaningful action to address the proliferation of fraudulent investment advertisements").

[29] *See, e.g.*, *FTC v. Clickprofit, LLC et al.*, No. 1:25-cv-20973 (S.D. Fla. Mar. 3, 2025) (alleging that a company used Google advertisements to fraudulently induce consumers into purchasing e-commerce stores); *FTC v. Arise Virtual Sols*, No. 24-cv-61152 (S.D. Fla. July 3, 2024) (settling allegations that a company used Google to advertise unsubstantiated earnings claims); *FTC et al. v. Grubhub, Inc.*, No. 1:24-cv-12923 (N.D. Ill. Aug. 25, 2025) (settling allegations that a company used Google ads to make unsubstantiated earnings claims).

enforcers, consumer advocacy organizations, and private parties have recently filed legal actions against Platforms, alleging that Platforms have enabled and profited from scam advertisements.[30]

In late 2025, Reuters published a special investigative report detailing how these misaligned incentives operate at Meta. According to the report, Meta generates substantial revenues from providing powerful advertising tools that enable scammers to reach vulnerable consumers, often charging these scammers premium rates.[31] In fact, Meta allegedly earned an estimated 10% of its 2024 revenue—or $16 billion—by running

---

[30] *See, e.g.*, *People of the State of Cal. v. Meta Platforms, Inc.*, No. 26-CV-4934491 (Cal. Super. Ct. May 11, 2026) (alleging Meta knowingly facilitates and profits from billions of scam advertisements on its platforms, including through its provision of ad tools that create/refine fraudulent ads on its platforms); *Consumer Fed'n of Am. v. Meta Platforms, Inc.*, 2026-CAB-002643 (D.C. Super. Ct. Apr. 21, 2026) (alleging Meta misleads users about the steps it claims to be taking to fight fraud on its platform; while promising users that it is meaningfully fighting scams and removing scam content from its platform, Meta has instead allegedly adopted policies and practices that it knows allow scam advertisements to proliferate and simultaneously profits off those ads); *Bouck et al. v. Meta Platforms, Inc.*, No. 25-cv-05194 (N.D. Cal. June 20, 2025) (alleging Meta enabled stock investment scams via Facebook and Instagram with its ad content generation tools and ad-targeting tools, which are used to push scams to vulnerable users); *Forrest v. Meta Platforms, Inc.*, No. 22-cv-03699 (N.D. Cal. June 23, 2024) (alleging Meta played a role in creation of fraudulent ads that ran on Meta's platforms in which scammers impersonated plaintiff's endorsement of sham cryptocurrency investments).

[31] Horwitz, *Meta is earning a fortune on a deluge of fraudulent ads, documents show*, *supra* note 17. The report analyzed various internal Meta documents, including an assessment that estimated users on Meta platforms were shown roughly 15 billion "higher-risk" scam ads per day, and that under Meta's policies, advertisers were typically banned only when automated ad review models reached at least 95% certainty of fraud, with lesser suspicions triggering higher pricing instead of takedowns. *See also* Jeff Horwitz, *Meta created 'playbook' to fend off pressure to crack down on scammers, documents show* (Jan. 5, 2026), https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/ ("As regulators press Meta to crack down on rogue advertisers on Facebook and Instagram, the social media giant has drafted a 'playbook' to stall them.").

scam advertisements.[32] Consequently, internal documents and other reports indicate that Meta has been hesitant to harm its advertising revenue stream by implementing more rigorous enforcement procedures against scam advertisers.[33]

The consequences of these misaligned Platform incentives are particularly concerning with respect to scam ads that impersonate trusted government and business entities. Consumers routinely turn to these trusted entities for transactions ranging from everyday purchases to banking to important government benefits. Once a consumer believes that a scammer is a trusted entity, the consumer may review the terms of the transaction with less scrutiny, leading to harm that is both immediate and far-reaching.

Consider these common examples. Scammers are using Meta's powerful ad-optimization and targeting tools to deliver Medicare-impersonation ads to seniors—a

---

[32] Horwitz, *Meta is earning a fortune on a deluge of fraudulent ads, documents show*, *supra* note 17.

[33] *Id.* (2023 internal Meta report allegedly uncovered that Meta ignored or incorrectly rejected 96% of roughly 100,000 valid weekly user reports of scam messages; some high-spending advertisers received leniency, with certain "High Value Accounts" accruing more than 500 strikes); Jeff Horwitz & Angel Au-Yeung, *Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook*, Wall St. J. (May 15, 2025), https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8 ("Current and former employees say Meta is reluctant to add impediments for ad-buying clients . . . [e]ven after users demonstrate a history of scamming, Meta balks at removing them."); Ctr. for Countering Digital Hate, *New Investigation Finds Meta Allowed Medicare Scammers to Generate More Than 215 Million Views on Ads, Mostly from Seniors* (May 12, 2026), https://counterhate.com/blog/meta-allowed-medicare-scammers-to-generate-more-than-215-million-views-on-ads-mostly-from-seniors/ ("Nearly every scam advertiser studied had ads removed for violations, averaging 151 removals each. One advertiser had 1,335 ads removed.").

group particularly impacted by such scams.[34] They are also using these tools to impersonate consumer brands—for example, impersonating McCormick Spice with fake "giveaway" ads on Meta platforms that redirect consumers to fraudulent websites.[35] Another common tactic, known as search-engine malvertising, involves scammers purchasing high-ranking sponsored placements on search engines for their deceptive ads that impersonate legitimate businesses, often incorporating the business's trademarks or brand names in the ads' text or associated web addresses that redirect users to imposter—or in some cases malicious—websites.[36] Search-engine malvertising is a popular method for travel and banking impersonation schemes: deceptive third-party hotel and booking

---

[34] Ctr. for Countering Digital Hate, *SCAMBOOK How Meta helps Medicare scammers target seniors*, at 10-11 (2026), https://counterhate.com/wp-content/uploads/2026/05/Scambook_CCDH_Final.pdf (watchdog report finding Medicare scammers promising "free" benefits, like groceries or money, paid Meta to run Medicare scam ads targeted at seniors on the Meta platform; "73% of ad impressions from top Medicare scammers were people over the age of 65"). The watchdog report also details that, in 2025, the top 30 known Medicare scammers on Meta generated around 215 million Medicare-scam impressions, earning Meta an estimated $12 million in ad revenue that year. *Id.* at 4. *See also* Fed. Trade Comm'n, *Protecting Older Consumers Report 2024-2025*, *supra* note 2, at 18-19, 22-25 ("Older adults were much more likely than younger adults to report losing money on tech support scams, prize, sweepstakes, and lottery scams, romance scams, and government impersonation scams."); Fed. Trade Comm'n, *Explore Age and Fraud Loss*, Tableau Public (June 30, 2026), https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic (comparing fraud loss reports, median reported monetary loss, fraud types, and payment/contact methods by age of reporter).

[35] Horwitz & Au-Yeung, *supra* note 33.

[36] *See* N.J. Cybersecurity & Commc'ns Integration Cell, *Beware of SEO Poisoning and Malvertising* (July 17, 2023), https://www.cyber.nj.gov/Home/Components/News/News/225/. *See also* Fed. Bureau of Investigation, *Public Service Announcement: Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users* (Dec. 21, 2022), https://www.ic3.gov/PSA/2022/PSA221221 (warning consumers of cyber criminals' use of "search engine advertisement services to impersonate brands and direct users to malicious sites").

portals use Google Ads to appear above genuine hotel websites and steer consumers to lookalike reservation portals[37]; meanwhile, according to industry sources, scammers frequently use search-engine ads to impersonate legitimate banking institutions and obtain placement at the top of sponsored search results for consumer banking searches.[38] Given the pervasiveness of these impersonation scams, the FTC and other government agencies have brought law enforcement actions targeting Platform-enabled business and

[37] *See People of the State of Cal. v. BookOnline.com, LLC, et al.*, No. CGC26639469 (Cal. Super. Ct. July 29, 2026), available at https://media.api.sf.gov/documents/2026-7-29_People_v_BookOnline_Complaint.pdf (alleging booking portals GuestReservations.com and BookingOnline.com used Google and other search engines to rank their impersonation ads above genuine hotel websites and funnel consumers to lookalike booking portals with considerable rate markups, up-front payment requirements, and inflexible cancellation policies); Better Bus. Bureau, *BBB Scam Alert: How to avoid scams when booking a hotel online* (May 2, 2025), https://www.bbb.org/article/scams/28768-bbb-scam-alert-how-to-avoid-scams-when-booking-a-hotel-online.

[38] *See* U.S. Dep't of Just., *Justice Department Announces Seizure of Stolen-Password Database Used in Bank Account Takeover Fraud* (updated Dec. 30, 2025), https://www.justice.gov/opa/pr/justice-department-announces-seizure-stolen-password-database-used-bank-account-takeover (scammers delivered fraudulent advertisements through search engines, including Google and Bing, that imitated the sponsored search engine advertisements used by legitimate banking entities and sent consumers to malicious websites that impersonated legitimate banks).

government impersonation scams,[39] and issued alerts urging consumers to be vigilant for impersonation scam advertisements on Platforms.[40]

Beyond harming individual consumers, these impersonation scams undermine the conditions that markets need to function efficiently. Efficient markets allocate a society's scarce resources to the most valued uses by allowing consumers to discover and choose among competing sellers, thereby channeling consumer spending to firms that produce goods and services that consumers value, and away from firms that do not. Markets can, however, only perform this important role efficiently when material information is transparent and consumers trust the market enough to engage. Information asymmetries—when a buyer has less information than a seller—can hinder consumer

---

[39] *See, e.g.*, Complaint, *FTC v. MediaAlpha, Inc.*, No. 2:25-cv-07263 (C.D. Cal. Oct. 16, 2025) (alleging defendant impersonated the government by placing deceptive search text ads on search engines like Google when consumers searched for government-related health care terms or State-run marketplaces); Complaint, *FTC v. Doxo, Inc., et al.*, No. 2:24-cv-00569 (W.D. Wash. Apr. 25, 2024) (alleging defendants use misleading search ads to impersonate consumers' billers); Complaint *FTC v. Mercury Marketing, LLC, et al.*, No. 1:25-cv-02021 (D. Md. Jun. 24, 2025) (alleging defendants impersonated substance use disorder clinics in Google search ads to deceptively route consumers trying to call those clinics to defendants' clinics); Complaint *FTC v. Innovative Partners LP*, No. 0:26-cv-60976 (S.D. Fla. Apr. 7, 2026) (alleging defendants impersonated government and large insurance companies by deceptively using government-related URLs and names in online advertisements, including search engine advertisements).

[40] *See, e.g.*, Off. of the Att'y Gen. Conn., *Attorney General Tong Warns Connecticut Against Investment Scams on Meta Platforms* (Apr. 6, 2026), https://portal.ct.gov/ag/press-releases/2026-press-releases/attorney-general-tong-warns-connecticut-against-investment-scams-on-meta-platforms; N.Y. Att'y Gen., *INVESTOR ALERT: Attorney General James Warns New Yorkers of Investment Scams on Meta Platforms* (Apr. 6, 2026), https://ag.ny.gov/press-release/2026/investor-alert-attorney-general-james-warns-new-yorkers-investment-scams-meta; Sec. and Exch. Comm'n, *Social Media and Stock Tip Scams – Investor Alert* (2024), https://www.sec.gov/files/litigation/litreleases/2024/26187-investor-alert-investor.pdf; Fed. Bureau of Investigation, *Public Service Announcement*, *supra* note 36.

purchasing decisions that reflect what consumers value. In this way, economic theory explains, markets with imperfect information can harm both consumers and legitimate businesses.[41]

Impersonation scams erode both the transparency and trust required for optimal market outcomes. Through sham advertisements, impersonation scammers conceal a critical piece of information—their real identities—and exploit consumers' trust in legitimate businesses and government entities.[42] The resulting harm is not merely academic: it is a concrete market failure that leaves consumers exposed and distorts fair competition. Indeed, consumer victims lose hundreds of millions in hard-earned money to online impersonation scams each year,[43] while the legitimate businesses being

---

[41] *See, e.g.,* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. Econ., 488–500 (1970). This seminal paper demonstrates how asymmetric information can lead to a reduction in the average quality of goods and the size of the market. Imperfect information about quality can harm sellers of high-quality goods by driving them out of business.

[42] This is likely because "consumers [are] more likely to click ads appearing to come from known brands or local businesses." Consumer Fed'n of Am., *supra* note 19, at 15-16 (2026).

[43] *See* Fed. Trade Comm'n, *Fraud Reports: Subcategory Payment & Contact Method*, Tableau Public (July 28, 2026), https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts (displaying reported consumer monetary loss by contact method and fraud type, including business and government imposter frauds); Fed. Trade Comm'n, *FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025*, *supra* note 1 (reporting $3.5 billion in reported consumer monetary loss to imposter scams, regardless of contact method, in 2025). Consumer scam victims also report experiencing non-financial harms such as lost time, compromised personal information, and emotional impacts. Better Bus. Bureau, *2024 BBB Scam Tracker Risk Report*, *supra* note 25, at 9-10.

impersonated suffer lost revenue and serious reputational harm.[44] And because the marketplace does not incentivize Platforms to absorb or address the costs of the impersonation scams they further,[45] market discipline alone is insufficient to correct the problem.

Recognizing the prevalence of these pernicious impersonation scams throughout the economy, the Commission promulgated the Government and Business Impersonation Rule to curb such conduct.[46] The Rule does not, however, expressly address Platform conduct that furthers impersonation scams. In light of the foregoing record indicating that certain Platform conduct could constitute unfair or deceptive acts or practices in violation of section 5 of the FTC Act—and that such conduct is widespread—the Commission issues this Notice to solicit public comment on whether rulemaking is needed.

---

[44] *See* Horwitz & Au-Yeung, *supra* note 33 (recounting harm to legitimate businesses); Ben Rogers, *The Hidden Costs of Brand Impersonation*, Allure Security (Jan. 16, 2026), https://alluresecurity.com/blog/hidden-costs-impersonation/ (recounting reputational harms legitimate businesses suffer due to brand impersonation). Government entities also suffer both financial and reputational harm from being impersonated, as entities must divert resources to alert the public and implement consumer education, enforcement, and other measures to combat the impersonation. *See, e.g.*, Fed. Trade Comm'n, *FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025*, *supra* note 1 (recounting various FTC consumer education and enforcement efforts in response to impersonation scams, including FTC impersonations); Fed. Trade Comm'n, *Federal Trade Commission Warns of Scammers Pretending to be Agency Staff* (Mar. 19, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/03/federal-trade-commission-warns-scammers-pretending-be-agency-staff (alerting consumers about FTC impersonation scams). Government entities may also suffer financial harm to the extent impersonation scams divert money that consumers owe to government entities.

[45] *See supra* notes 22-24 and accompanying text discussing negative externalities of Platform ad-optimization tools and services.

[46] 16 CFR Part 461; *see also* 86 FR 72901, 72901-03 (Dec. 23, 2021) (providing a detailed prevalence description of government and business impersonation scams generally).

IV. Commission's Authority to Address Platform Misconduct through Rulemaking

The Commission is well-positioned to address this growing threat of online impersonation scams by targeting Platform conduct that furthers the threat. Nearly ninety years ago, Congress amended section 5 of the FTC Act to authorize the Commission to protect consumers from "unfair or deceptive acts or practices in or affecting commerce."[47] Platform conduct falls squarely within the Commission's authority defined by long-established FTC Act jurisprudence.[48] A Platform's act or practice is deceptive where: (1) its representation, omission, or practice misleads or is likely to mislead the consumer; (2) a consumer's interpretation of the representation, omission, or practice is considered reasonable under the circumstances; and (3) the misleading representation, omission, or practice is a fact material to the consumer's choice or conduct.[49] A Platform's act or practice is "unfair" if it: (1) "causes or is likely to cause

---

[47] Wheeler-Lea Act, Pub. L. 75-447, 52 Stat. 111 (1938) (codified as amended at 15 U.S.C. 45(a)(1)).

[48] The FTC Act provides the Commission plenary authority to prevent unfair or deceptive acts or practices and only includes limited exemptions from its jurisdiction, none of which apply to Platforms. These include status-based exemptions for "banks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of Title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended, except as provided in section 406(b) of said Act." 15 U.S.C. 45(a)(2).

[49] FTC Policy Statement on Deception (Oct. 14, 1983), appended to *In re Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984); *see also FTC v. Corpay, Inc.*, 164 F.4th 807, 834 (11th Cir. 2026); *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 168 (2d Cir. 2016).

substantial injury"; (2) the injury is not "reasonably avoidable by consumers"; and (3) the injury is not "outweighed by countervailing benefits to consumers or to competition."[50]

Section 230 of the Communications Decency Act does not deprive the Commission of this authority over Platform conduct. In relevant part, section 230 states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[51] This statutory language provides Platforms an affirmative defense for liability that arises from merely hosting third-party content.[52] Beyond that, however, courts have held that section 230 immunity does not extend to all Platform conduct that

---

[50] 15 U.S.C. 45(n); FTC Policy Statement on Unfairness (Dec. 17, 1980), appended to *In re Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984); *see also Corpay*, 164 F.4th at 839-40 (confirming the three requirements for determining unfairness under section 5(n) and rejecting defendant's argument that the section contains a fourth requirement). Privity with the consumer is not necessary for section 5 to apply. *See FTC v. Five-Star Auto Club*, 97 F. Supp. 2d 502, 530 (S.D.N.Y. 2000) ("One who places into the hands of another a means of consummating a fraud or competing unfairly in violation of the Federal Trade Commission Act is himself guilty of a violation of the Act.") (citing *Regina Corp. v. FTC*, 322 F.2d 765, 768 (3d Cir. 1963)); Order Reopening and Setting Aside Order, *In re Rytr LLC*, No. C-4806 (Dec. 22, 2025) (same; identifying situations in which courts and the Commission have applied means and instrumentalities liability); *see also* Complaint, *FTC v. Amare Glob. Holdings, Inc.*, No. 2:26-cv-05900 (C.D. Cal. June 2, 2026) (alleging section 5 violations against multilevel marketing defendants, including for providing deceptive instructional and marketing materials to their brand partners).

[51] 47 U.S.C. 230(c)(1). A provider of "interactive computer service" includes search engines, *see, e.g.*, *Marshall's Locksmith Serv. Inc. v. Google, LLC*, 925 F.3d 1263, 1268 (D.C. Cir. 2019), and social media platforms, *see*, *e.g.*, *Force v. Facebook, Inc*., 934 F.3d 53, 64 (2d Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020). "Information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. 230(f)(3).

[52] "Section 230 immunity is an affirmative defense" to liability that a Platform would need to raise and prove in litigation. *U.S. v. EZ Lynk, SEZC*, 149 F.4th 190, 198 (2d Cir. 2025).

involves third-party content. For instance, the immunity does not apply to Platform conduct involving unlawful content that the Platform materially contributed to developing, even if the content includes third-party material.[53] Likewise, the Third Circuit recently held that a Platform's recommendation or curation of third-party content constitutes the Platform's own expressive conduct, which may fall outside section 230 protection.[54] More broadly, any Platform service that enhances the effectiveness of ads may fall outside the "publisher or speaker" categorization of the activity protected by

---

[53] Platforms "materially contributing" to violative content's alleged unlawfulness are considered to be developing the Platform's own content for section 230 purposes. *See Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1166 (9th Cir. 2008); *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1269 n.4 (9th Cir. 2016) ("Our sister circuits have generally adopted *Roommates.Com*'s 'material contribution' to activity test.").

[54] *Anderson v. TikTok, Inc.*, 116 F.4th 180, 184 (3d Cir. 2024). While a number of circuits have held that section 230 protects a Platform's recommendation or curation of third-party content, many of these cases follow precedent that predate the Supreme Court's decision in *Moody v. NetChoice, LLC*, 603 U.S. 707 (2024). *See, e.g.*, *Force.,* 934 F.3d 53; *Jones v. Dirty World Ent. Recordings LLC*, 755 F.3d 398 (6th Cir. 2014); *Klayman v. Zuckerberg*, 753 F.3d 1354 (D.C. Cir. 2014). In *Moody*, the Court held that a Platform's "presenting a curated compilation of speech originally created by others" constitutes the Platform's own "expressive conduct" for First Amendment purposes. 603 U.S. at 728. The Court has yet to address the section 230 implications of *Moody*, but the Third Circuit held that *Moody* excludes Platform curation/recommendation activities from section 230 immunity, and two Justices have indicated a willingness to take the same approach. *See Anderson*, 116 F.4th at 184 ("Given the Supreme Court's observations that platforms engage in protected first-party speech under the First Amendment when they curate compilations of others' content via their expressive algorithms, id. at 2409, it follows that doing so amounts to first-party speech under § 230, too."); *Doe Through Roe v. Snap, Inc.*, 144 S. Ct. 2493, 2494 (2024) (proposing the Court consider the implications of *Moody* for narrowing section 230 immunity) (Thomas, J., joined by Gorsuch, J., dissenting from denial of cert.); *but see Computer & Commc'ns Indus. Ass'n v. Paxton*, No. 24-50721, 2026 WL 2130729, at *14 (5th Cir. July 24, 2026) ("The argument that we must choose between [*Moody* and circuit precedent on section 230] presents a false choice."); *Doe 1 v. Meta Platforms, Inc.*, 174 F.4th 1159, 1168-69 (9th Cir. 2026) (following circuit precedent immunizing algorithmic recommendations, and without discussion, declining to apply *Moody* to section 230).

section 230.[55] In any event, whether a particular type of Platform conduct falls outside section 230 immunity involves a fact-intensive inquiry, and the Commission has posed specific questions below to solicit information relevant to making that determination. To the extent Platform conduct falls outside section 230 and is unfair or deceptive, the Commission may exercise its authority to protect consumers from such conduct.

The Commission's authority includes not only the power to pursue enforcement actions against Platforms engaged in unfair or deceptive acts or practices but also the power to promulgate rules that define with specificity the violative acts and practices.

---

[55] The statutory text of section 230 does not appear to support the expansive reading of "publisher or speaker" activity that some courts have given in an effort to advance their understanding of Congress's policy choice. *See, e.g.*, *Universal Commc'n Sys., Inc. v. Lycos, Inc.*, 478 F.3d 413, 418 (1st Cir. 2007) (noting courts "have generally interpreted Section 230 immunity broadly, so as to effectuate Congress's policy choice") (internal quotes removed); *see also Snap, Inc.*, 144 S. Ct. at 2493 (Thomas, J., joined by Gorsuch, J., dissenting from denial of cert.) ("Notwithstanding the statute's narrow focus, lower courts have interpreted § 230 to 'confer sweeping immunity' for a platform's own actions."). Its language appears to limit immunity to a platform's passive hosting of third-party content. *See* Brief for the United States as Amicus Curiae, 2022 WL 17650509, at *13-20. Moreover, a growing body of cases suggests a shift in section 230 jurisprudence to limit "publisher or speaker" immunity to reflect this strict construction of the statutory text. *See, e.g.*, *Doe v. Snap, Inc.*, 88 F.4th 1069 (5th Cir. 2023) (stating section 230 does not immunize design defect claims against platform) (Elrod, J., joined by Smith, Willett, Duncan, Engelhardt, Oldham, Wilson, Js., dissenting from denial of rehearing *en banc*); *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1094 (9th Cir. 2021) (holding section 230 does not bar claim based on Snapchat design); *Gonzalez v. Google LLC*, 2 F.4th 871, 913 & 922 (9th Cir. 2021) (stating section 230 does not immunize platform conduct to amplify and develop third-party content) (Berzon, J., concurring; Gould, J., concurring in part); *Force*, 934 F.3d at 76 (stating section 230 does not immunize platform recommendations of third-party content) (Katzmann, C.J., concurring); *FTC v. LeadClick Media*, 838 F.3d at 176 (2d Cir. 2016) (holding that a claim based on provider's involvement in editing third-party's deceptive content is "not derived from… status as a publisher or speaker"); *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1204-05 (10th Cir. 2009) (stating section 230 does not immunize provider against liability "for its conduct rather than for the content of the information it was offering") (Tymkovitch, J., concurring).

This rulemaking authority includes the power to promulgate regulatory "requirements prescribed for the purpose of preventing" the violative acts and practices.[56] The Commission has already exercised its rulemaking authority to promulgate the Impersonation Rule. The Commission now solicits public comment on whether it should exercise that authority again to enhance the Rule, or to promulgate some other measure, to combat the impersonation fraud proliferating on social media, search engines, and other digital marketplace platforms.

V. Anticipated Benefits of Rulemaking

The Commission anticipates multiple benefits from using rulemaking to address growing concern about impersonation fraud on Platforms. First, rulemaking would provide the Commission a powerful enforcement tool to address Platform-optimized impersonation scams by targeting the market failure generating such conduct. As explained above, misaligned Platform incentives appear to drive the proliferation of impersonation scam ads. A rule could realign those incentives by subjecting Platforms to court-imposed monetary sanctions for their involvement in furthering those ads. Such a rule would effectively impose the social costs of Platform-optimized impersonation scams on the Platforms that are likely in the best position to reduce them.[57]

Second, rulemaking would enable the Commission to craft rule requirements that build on the existing scaffolding of legally mandated and voluntary measures that

---

[56] 15 U.S.C. 57a(a)(1)(B).
[57] *See* H. Beales, *et al.*, *The Efficient Regulation of Consumer Information*, 24 J.L. & Econ., 491-539 (1981) for an overview of government interventions in response to market failures. The paper argues that intervention is often warranted in cases where injury is substantial.

Platforms have already implemented. While these existing measures lack the scope and rigor to adequately address the conduct at issue, they provide monitoring, takedown, and other processes that the Commission could harness in crafting an appropriate rule. For instance, section 3 of the TAKE IT DOWN ACT requires Platforms to establish a process for individuals to request the removal of offensive posted material but only if it qualifies as a non-consensual intimate visual depiction (e.g., "revenge porn").[58] Section 512 of the Digital Millennium Copyright Act requires internet service providers, including Platforms, to implement a process for copyright owners to request the removal of infringing *copyrighted* material but not infringing *trademarked* material typically used in impersonation scams.[59] The INFORM Consumers Act ("INFORM Act") requires Platforms to verify third-party sellers and provide consumers a way to report suspicious conduct relating to these sellers, including impersonation scams—but only if the sellers are deemed "high volume third party sellers" and only if the Platform qualifies as an "online marketplace."[60] Moreover, the INFORM Act does not require online marketplaces to investigate reported cases of suspicious sellers or terminate services for confirmed cases.

In addition to these measures prescribed by law, many Platforms highlight their adoption of some voluntary measures aimed at reducing fraudulent ads in their

---

[58] 47 U.S.C. 223a.
[59] 17 U.S.C. 512. Section 512 addresses safe harbor requirements, including the process to request removal of infringing material, for "infringement of copyright" only.
[60] 15 U.S.C. 45f.

ecosystem.[61] However, the type and quality of such measures vary across Platforms, and the Platforms could even degrade or scrap these voluntary measures altogether if the current media scrutiny lessens and impersonation scams remain profitable. Moreover, the studies and articles discussed above explain why these voluntary measures are inadequate at curbing widescale impersonation scams on Platforms.[62]

These existing legally mandated and voluntary measures, while inadequate for combatting impersonation scams, nonetheless provide the Commission with a starting point. Platforms are already engaged in some practices that could prevent their current amplification of impersonation scams. Rulemaking would allow the Commission to tailor rule requirements that build on these existing efforts and thereby minimize unnecessary compliance costs for Platforms.

Third, a rule that targets this core market failure would enable the Commission to maximize its law enforcement efforts. Enforcement actions are time- and resource-intensive. Rather than expend the Commission's efforts only on investigating and litigating a limited number of impersonation scams at a time, a rule would potentially prevent or mitigate substantially more impersonation scams by addressing the Platform

---

[61] *See, e.g.*, Kaitlyn Huamani, *AI Is A Gold Mine for Spammers and Scammers, but Google Is Using It as a Tool to Fight Back*, Associated Press (Apr. 16, 2026), https://apnews.com/article/google-ads-safety-report-ai-scams-defense-06d9ef869958555884989e8ec25974be; Asim BN, *Meta Removes 134 Million Scam Ads and Disrupts 12 Million Accounts to Combat Online Scams*, Digital Information World (Dec. 4, 2025), https://www.digitalinformationworld.com/2025/12/meta-removes-134-million-scam-ads-and.html. According to these articles, Google attempts to use AI to screen potential scam ads before they run, while Meta attempts to identify and remove scam ads after they are posted.

[62] *See supra* Section III.

conduct that optimizes or otherwise contributes to the scams. By defining, with specificity, the Platform conduct that is unfair or deceptive, the rule would give Platforms the guidance they need to refrain from problematic practices that further impersonation scams, while also allowing the Commission to pursue enforcement actions against Platforms based on the defined conduct itself, without the need to demonstrate that the defined conduct is unfair or deceptive. The result is a framework that both prevents and mitigates a universe of impersonation scams by addressing the underlying Platform practices that drive them.

Finally, a rule would provide the Commission a more efficient means to recover money under section 19 for consumers injured by the prohibited Platform conduct.[63] More specifically, a rule would enable the Commission to seek court-ordered consumer redress in one Federal district court action brought under section 19(a)(1), rather than the longer, less efficient, two-step process for obtaining redress under section 19(a)(2).[64]

---

[63] Since 2021, when the Supreme Court held that section 13(b) of the FTC Act (15 U.S.C. 53(b)) did not authorize equitable monetary relief, section 19 (15 U.S.C. 57b) is the only statutory authorization for the Commission to obtain monetary relief to redress consumers harmed by unfair or deceptive acts or practices. *See AMG Cap. Mgmt., LLC v. FTC*, 593 U.S. 67, 81-82 (2021).

[64] *See* 15 U.S.C. 57b(a)(1) and (2). When the Commission has reason to believe that a rule has been violated, the Commission can commence a Federal court action to ask a Federal judge to determine liability and, if proven, require violators to provide redress. *See* 15 U.S.C. 57b(a)(1), (b). Without a rule, the path to court-ordered redress is longer. The Commission must first conduct an administrative proceeding to determine whether the respondent engaged in unfair or deceptive acts or practices in violation of section 5(a) of the FTC Act. If the Commission finds that the respondent did so, the Commission issues a cease-and-desist order, which might not become final until after the resolution of any resulting appeal to a Federal court of appeals. Then, to obtain redress, the Commission must initiate a second action in Federal district court, in which it must prove that the violator engaged in objectively fraudulent or dishonest conduct in order to obtain court-ordered redress. *See* 15 U.S.C. 57b(a)(2), (b).

VI. Objectives, Regulatory Alternatives, and Request for Comments

For the foregoing reasons, the Commission seeks comments on whether it should commence a rulemaking proceeding to amend the Rule, or to adopt some other measure, to address unfair or deceptive practices by Platforms that further government and business impersonation scams through their ad-optimization tools and services. While the materials cited above and in the prior proceeding promulgating the Rule indicate the pervasiveness of such practices,[65] the Commission now solicits additional public comment to supplement that record and ensure its rulemaking adequately responds to concerns from consumers, industry, and other stakeholders.

Specifically, the Commission seeks information on Platforms' business operations and financial incentives relating to advertising and advertising optimization; how those operations and incentives intersect with impersonation scams advertised on those Platforms; whether Platforms are engaged in unfair or deceptive acts or practices in furthering impersonation scams through their advertising-optimization tools and services (e.g., content creation, audience targeting); and whether any of these acts or practices are prevalent in the U.S. economy. The Commission also seeks information regarding ways to address these acts or practices, including amending the Impersonation Rule, promulgating a new rule, or implementing alternatives to regulation. Potential alternatives to regulation could include educating consumers and businesses on avoiding

---

[65] *See supra* Section III; 86 FR 72901 (Dec. 23, 2021); 87 FR 62741 (Oct. 17, 2022); 89 FR 15017 (Mar. 1, 2024); 89 FR 15072 (Mar. 1, 2024).

impersonation scams on Platforms or implementing measures to encourage voluntary industry-wide efforts aimed at combatting impersonation scams.

In responding to the questions below, the Commission invites the public to submit any market studies, economic data, or other empirical evidence. The Commission reminds commenters that, while it reviews all submissions, comments may be more persuasive when substantiated with evidence, particularly economic data.

A. Questions About the Marketplace for Advertising on Platforms

1. How many Platforms allow users to post advertisements on their platform(s)? How many Platforms offer advertising-optimization tools/services, such as audience targeting or advertisement content creation services?[66]

2. What are the names of the Platforms identified in response to Question A.1, and for each, what are the gross annual revenues generated from advertising and advertising-optimization tools/services, respectively? Which of these Platforms, if any, are small businesses?[67]

3. Do Platforms generate revenue from providing advertising and/or

---

[66] For instance, audience targeting services include such services as target audience profiling, as well as targeting based on demographics, employment background, location, interests, user activity, and shopping history. Advertisement content creation services include such services as ad copy creation, image and video generation, ad enhancements, and product listing creation or enhancement.

[67] Please use the U.S. Small Business Administration's ("SBA") standards for defining "small business" to answer any questions regarding small businesses in Section VI. *See Size Standards, https://www.sba.gov/federal-contracting/contracting-guide/size-standards.* SBA defines "small business" by NAICS code based on either employment levels or annual receipts. To the extent any questions regarding small businesses in Section VI implicate any other "small entities"— small governmental jurisdictions or small nonprofit organizations as defined by section 601 of the Regulatory Flexibility Act (5 U.S.C. 601-612)—please provide information for those "small entities."

advertising-optimization tools/services for deceptive ads? If so, what financial incentives, if any, do Platforms have to prevent the use of their digital platforms and advertising-optimization tools/services for deceptive ads?

4. What kinds of businesses advertise on Platforms or use Platform advertising-optimization tools/services?

a. Which industries, if any, have the types of businesses that do not advertise on Platforms or use these tools/services? Why do businesses in these industries not advertise on Platforms or use these tools/services?

b. What percentage of ads on Platforms advertise small businesses? What percentage of these ads utilize Platform advertising-optimization tools and services?

B. Questions About the Role of Platforms in Advertising Optimization

1. What advertising-optimization tools/services does each Platform identified in response to Question A.2 provide its advertisers?

a. How does each tool/service work? What capabilities or functions does each type of tool/service provide advertisers?

b. To what extent does each tool/service create, develop, or modify the content (including images) of the advertisement? What specific actions does the tool/service perform to create, develop, or modify the content of the advertisement?

c. To what extent does each tool/service control the delivery of the advertisement, including when, where, and to whom the advertisement is displayed? What specific actions does the tool/service take to control the delivery of the advertisement?

d. To what extent does each tool/service optimize the advertisement in ways other than those referenced in Questions B.1.b and B.1.c? What specific action(s) does the tool/service perform?

e. For each tool/service, what percentage of businesses advertising on the Platform utilize the tool/service? What percentage of businesses utilizing the service are small businesses?

2. What measures does each Platform identified in response to Question A.2 employ to prevent the use of their advertising-optimization tools/services for deceptive advertising involving government or business impersonation ("Impersonation Ads")?

a. Does the Platform verify the advertiser's identity prior to providing access to its tools/services? If so, how? What criteria, factors, and/or metrics does the Platform use to perform the verification?

b. Does the Platform perform any steps other than verifying the advertiser's identity to determine whether to provide access to its tools/services? If so, what and how? For instance, does the Platform evaluate the advertiser's website for signs that the advertiser is engaged in Impersonation Ads? What criteria, factors, and/or metrics does the Platform use to determine whether to provide access to its tools/services?

c. Does the Platform restrict the use of trademarks, tradenames, or other names or symbols identifying government or business entities unaffiliated with the advertiser, when optimizing the content or delivery of advertisements? If so, how? What criteria, factors, and/or metrics does the Platform use to determine whether to restrict the use of particular trademarks, tradenames, or other identifying names or symbols?

d. Does the Platform screen or monitor advertisements to determine whether they are Impersonation Ads? If so, how? What criteria, factors, and/or metrics does the Platform use to determine whether an advertisement is an Impersonation Ad?

e. Does the Platform take any steps to remediate Impersonation Ads that have already been posted and/or optimized? If so, what steps? What criteria, factors, and/or metrics does the Platform use to determine which steps to take to remediate the posted and/or optimized Impersonation Ad?

f. Does the Platform take any steps to discipline advertisers who have engaged in Impersonation Ads? If so, what steps? What criteria, factors, and/or metrics does the Platform use to determine whether to discipline the advertiser and which disciplinary steps to take?

g. Does revenue or any other benefit that the Platform derives from posting, or from providing tools/services for optimizing, Impersonation Ads play a role in the Platform's setting or use of the criteria, factors, and/or metrics referenced in response to Questions B.2.a through B.2.f above? If so, how?

C. Questions About the Prevalence of Unfair or Deceptive Acts or Practices ("UDAP") by Platforms That Further Impersonation Ads

1. Which of the Platform practices identified in response to Questions B.1

and B.2 do you consider unfair or deceptive in furthering Impersonation Ads (hereinafter, "Platform UDAPs")?

a. Specifically for Platform advertising-optimization tools/services that tailor the ad content or delivery to the consumer,[68] do Platforms either actively encourage or fail to take reasonable steps to prevent the use of such tools/services for Impersonation Ads? If so, how?

b. To what extent do Platform advertising-optimization tools/services that tailor the ad content or delivery to search queries using government or business names constitute a Platform UDAP?

c. Do any of these Platform UDAPs further other types of deceptive advertising, apart from Impersonation Ads? If so, which Platform UDAPs, and how?

d. Are there any limitations on the types of deceptive ads that each of these Platform UDAPs can further? If so, please identify and explain those limitations.

2. Do non-advertising posts on Platforms contribute to impersonation fraud (e.g., sham LinkedIn or Facebook profiles used to bolster the credibility of an impersonation scam conducted via text or phone)? If so, how?

a. What Platform UDAPs enable the use of non-advertising posts for

[68] For instance, Platform tools/services may tailor third-party ad content to appeal to a particular consumer, or target the delivery of the ad to a particular consumer, based on the consumer's profile (e.g., demographic information) or the consumer's online activity (e.g., specific search terms entered by the consumer).

impersonation fraud?

b. Do Platforms either actively encourage, or fail to take reasonable steps to prevent, the use of non-advertising posts for impersonation fraud? If so, how?

c. Do Platforms generate revenue from non-advertising posts? If so, how?

3. How do the Platform UDAPs identified in response to Questions C.1 and C.2 impact:

a. Competition among Platforms?

b. Competition among businesses advertising on Platforms?

4. Do the Platform UDAPs identified in response to Questions C.1 and C.2 impact small businesses differently than other businesses? If so, how?

5. Do the Platform UDAPs identified in response to Questions C.1 and C.2 have any benefits for businesses or consumers? If so, what are these benefits?

6. Congress authorized the Commission to propose a rule defining unfair or deceptive acts or practices with specificity when the Commission "has reason to believe that the unfair or deceptive acts or practices which are the subject of the proposed rulemaking are prevalent."[69] A determination about prevalence can be made either on the basis of previous Commission cease-and-desist orders regarding such acts or practices, or when the Commission has "any other information" that "indicates a widespread pattern of unfair or deceptive acts or

[69] 15 U.S.C. 57a(b)(3).

practices."[70] For each Platform UDAP identified in your response to Questions C.1 and C.2, please answer the following:

a. What information or data indicates that the Platform UDAP is prevalent or is not prevalent?

b. How frequently do consumers encounter Impersonation Ads furthered by the Platform UDAP?

c. How many consumers have encountered Impersonation Ads furthered by the Platform UDAP?

d. What proportion of consumers have encountered Impersonation Ads furthered by the Platform UDAP?

e. What is the consumer harm caused by Impersonation Ads furthered by the Platform UDAP? Consumer harm can include monetary losses as well as wasted time (e.g., time spent initiating chargebacks, seeking refunds, or resolving identity fraud).

7. Do you expect future developments in the Platform marketplace to change any of your responses to the above questions? If so, how?

D. Questions About Regulations and Regulatory Alternatives to Address Unfair or Deceptive Acts or Practices by Platforms

1. Is there a need for new regulations to prevent Platform UDAPs? Why or why not?

a. If new regulations are needed, should the Impersonation Rule be

[70] *Id.*

amended, or should a new rule or rules be created? Should the new regulations prohibit Platform conduct that further deceptive advertising other than those involving impersonation scams? Why or why not?

b. Should the Commission consider alternatives to new regulation, such as the publication of additional consumer and business education? If so, what are these alternatives, and how effectively would they prevent Platform UDAPs?

c. What are the benefits and costs to consumers and businesses under your proposed approach compared to the other options, whether issuing a new rule(s), amending the existing Rule, or implementing an alternative to new regulation?

2. In certain industries, companies cooperate to combat abuses in the marketplace. For instance, banks and payment processors use the MATCH database to identify merchants that pose a high risk to the payment system.[71] What barriers, if any, do Platforms face in working together as an industry to combat impersonation scams?

a. To what extent do Platforms share information with each other regarding confirmed or suspected impersonation scams and/or related scam advertisers? Would additional information sharing within the industry assist Platforms in combatting impersonation scams? What

[71] MATCH stands for Member Alert to Control High-Risk Merchants. Mastercard maintains the database. *See MATCH Pro*, Mastercard.com, https://developer.mastercard.com/match/documentation/.

prevents such additional information sharing?

b. What steps could the Commission take to lower or remove these barriers to the Platforms working together to more effectively combat impersonation scams?

E. Questions About Specific Rule Provisions

The Commission may consider a range of measures in proposing any new or amended regulations to address prevalent Platform UDAPs. For instance, the Commission may tailor the previously proposed means-and-instrumentalities provision by requiring Platforms to evaluate advertisements prior to posting, and by prohibiting Platforms from providing advertising optimization services to those engaged in Impersonation Ads. The Commission also may require Platforms to take affirmative steps to address Impersonation Ads that are posted, including: implementing a program to detect suspected Impersonation Ads; providing consumers a clear and conspicuously placed tool to report suspected Impersonation Ads; investigating suspected Impersonation Ads; removing confirmed Impersonation Ads; discontinuing advertising optimization services for confirmed Impersonation Ads; and taking appropriate disciplinary action against the offending advertiser. Instead of serving as affirmative requirements, these measures may form the basis of a safe harbor provision by which Platforms' compliance could provide a defense to liability under any new regulations. In addition, the Commission may consider ancillary measures, such as requiring Platforms to maintain records documenting their compliance, to facilitate enforcement of the new or amended rule. The following questions solicit comments on these and other potential regulatory measures.

1. What regulatory requirements, if any, would be helpful for mitigating Platform UDAPs that are prevalent in the marketplace? What regulatory requirements would not be helpful? For each requirement (helpful or unhelpful), please provide the following information:

a. What benefit would the requirement provide, including time and money saved, for consumers?

b. What benefit would the requirement provide for legitimate businesses advertising on Platforms and for the Platforms themselves?

c. What costs would the requirement impose on consumers?

d. What costs would the requirement impose on Platforms and on legitimate businesses advertising on Platforms? For each discrete requirement, describe each component of such costs, including costs to read and understand the rule, costs to update procedures and train personnel on compliance, costs to revise web pages and apps for compliance, costs for record keeping, and any other compliance costs, and state whether said costs would be imposed on Platforms, legitimate businesses, or both. If Platforms were to pass along the costs imposed on them to others, please state to what extent and to whom (e.g., small business advertisers, consumers).

e. To what extent could Platforms comply with the requirement by scaling processes Platforms currently use to comply with the Digital Millennium Copyright Act, TAKE IT DOWN Act, INFORM Act, and any other law or voluntary effort to identify and/or remove problematic online content? What impact would such scaling have on the costs to comply with the requirement?

f. What modifications, if any, should the Commission make to the requirement to reduce the costs imposed on legitimate businesses advertising on Platforms, particularly small businesses?

g. Should the requirement be limited to advertisers of certain types of products and services? If so, why and which types of products and services?

h. Would the requirement interfere with a Platform's provision of services to legitimate businesses not engaged in deceptive advertising?

   i. If so, what kinds of Platform services and how?

   ii. How can the Commission modify the requirement to accommodate Platform services to legitimate businesses not engaged in deceptive advertising?

i. Would the requirement discourage Platforms from innovating their services or tools, particularly with respect to services or tools incorporating the use of artificial intelligence?

   i. If so, what kinds of Platform services and how?

   ii. How can the Commission modify the requirement to avoid discouraging Platform innovation?

j. Does the requirement overlap or conflict with existing Federal, State, or local laws or regulations?

   i. If so, what laws or regulations, and how?

ii. Should any Rule amendment address such overlaps or conflicts? If so, why, and how? If not, why not?

k. To what extent does the requirement address Platform UDAPs that materially contribute to the development of impersonation-specific ad content?

l. To what extent does the requirement address Platform UDAPs that provide audience targeting for impersonation fraud ads?

m. To what extent does the requirement address Platform UDAPs that enhance the effectiveness of impersonation fraud ads, other than through developing impersonation-specific ad content and audience targeting?

n. Should the requirement trigger liability only if the Platform has some level of knowledge of, or participation in, the Impersonation Ad? If so, what level of knowledge or participation should trigger liability?

o. Does the requirement help prevent other kinds of deceptive advertising that do not involve impersonation? If so, what kind of deceptive advertising, and how?

2. Specifically for Platform advertising-optimization tools/services that tailor the ad content or delivery to the consumer, what requirements would be a cost-effective way to prevent the use of such tools/services for deceptive advertising?

3. Would requiring Platforms to verify the identity of the advertiser before providing advertising-optimization tools/services be a cost-effective way to help mitigate Platform UDAPs? Why or why not? Which specific verification requirements would be helpful?

4. Would requiring Platforms to screen and/or monitor for Impersonation Ads be a cost-effective way to help mitigate Platform UDAPs? Why or why not? Which specific monitoring requirements would be helpful?

5. Would requiring Platforms to investigate and/or take other steps to respond to complaints identifying suspected Impersonation Ads be a cost-effective way to help prevent Platform UDAPs? Why or why not? Which specific requirements would be helpful?

   a. What types of complaints (e.g., consumer complaints, competitor complaints, complaints from those being impersonated), and what volume of complaints (by individuals, small businesses, or others) should trigger a duty for Platforms to investigate a suspected Impersonation Ad?

   b. What steps should Platforms take to investigate and confirm a suspected Impersonation Ad?

   c. Should Platforms be required to respond to complaints by taking down confirmed Impersonation Ads? If so, how much time do Platforms need to take down the confirmed Impersonation Ads?

   d. Should Platforms be required to respond to complaints by terminating advertising-optimization tools/services for the confirmed Impersonation Ads? If so, how much time do Platforms need to terminate such services?

F. Miscellaneous

1. For each of your responses to the questions above, please answer the following:

a. What timeframe(s) does your response cover?

b. Do you expect your response to change significantly in the next few years? If so, how and why?

c. What evidence supports your response?

VII. Comment Submissions

You can file a comment online or on paper. For the FTC to consider your comment, we must receive it on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. Write "16 CFR Part 461—Impersonation Rule, Matter No. R207000" on your comment. Your comment—including your name and your State—will be placed on the public record of this proceeding, including, to the extent practicable, on the *https://www.regulations.gov* website.

We encourage you to submit comments through the *https://www.regulations.gov* website. Postal mail addressed to the Commission will be subject to delay because of heightened security screening. If you prefer to file your comment on paper, write "16 CFR Part 461—Impersonation Rule, Matter No. R207000" on your comment and on the envelope, and send it via overnight service to: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Mail Stop H-144 (Annex P), Washington, DC 20580.

Because your comment will be placed on the publicly accessible website at www.regulations.gov, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other State identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential"—as provided by section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)—including competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c), 16 CFR 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted publicly at *www.regulations.gov*, we cannot redact or remove your comment from that website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *https://www.ftc.gov/site-information/privacy-policy*.

VIII. Regulatory Review

E.O. 12866 states that agencies should assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, and distributive impacts). E.O. 14215 requires all executive branch departments and agencies to submit all their proposed and final significant regulatory actions to the Office of Management and Budget (OMB) for review. OMB determined that this ANPRM is a significant regulatory action under E.O. 12866.

By direction of the Commission.

April J. Tabor,

Secretary.