



UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Director
Bureau of Consumer Protection

**PREPARED REMARKS FOR THE 2026 NATIONAL ADVERTISING DIVISION ANNUAL
CONFERENCE**

CHRISTOPHER MUFARRIGE*
DIRECTOR OF THE BUREAU OF CONSUMER PROTECTION

SEPTEMBER 29, 2026

* The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any individual Commissioner. I would like to thank Elisa Jillson, Hong Park, Michelle Rosenthal, and Joshua Xu for their assistance with these remarks.

I. Introduction

I am grateful for the opportunity to speak with you today about a topic of singular importance to this Administration, this Commission, and the American people: the pervasive fraud that pollutes our economy and drains the savings of hardworking Americans.

Across the country, American citizens lose tens of billions of dollars every year to scams, many of which are orchestrated by criminals abroad.¹ The Commission has long been the cop on the beat, targeting the fraudsters themselves. That work remains essential. Every successful case against a scammer is a victory for consumers, and we will continue to vigorously pursue those cases.

Importantly, where the Commission sees a pattern in a channel leveraged by scammers to reach consumers, the Commission has scrutinized that channel to ensure it is compliant with the law. The Commission has, for example, used this approach successfully in the payment process space, alleging in *Nuvei*,² *Humboldt*,³ and *Paddle*⁴ that payment processors who serviced known fraudsters had engaged in unfair practices.⁵

Digital marketplace platforms (“Platforms”),⁶ such as Facebook and Google, are many fraudsters’ channel of choice today. And some of the most pernicious scams we see on Platforms today involve government and business impersonations. In 2025, consumers reported nearly \$3.5 billion in losses due to impersonation fraud, and real losses are no doubt an order of magnitude higher.⁷ Consumers rely on government agencies and businesses to conduct their daily affairs, including to comply with the law (such as by paying tolls or obtaining a passport) and to conduct routine transactions (such as online bank transfers). Impersonation scams exploit consumers’ reasonable reliance on legitimate entities, inflicting significant harm on consumers while causing legitimate businesses to lose revenue and suffer reputational damage. The Commission’s recently announced Advance Notice of Proposed Rulemaking (“ANPR”) on Platforms that enable impersonation fraud asks whether it is time for the FTC to consider a new approach to impersonation

¹ Last year, Americans reported \$16 billion in losses to fraud. Since many Americans do not report financial losses from fraud, the FTC estimates that the true cost of fraud may be as high as \$195.9 billion.

² Press Release, FTC, *Payment Processor Nuvei Must Implement Robust Merchant Screening Practices and Pay \$4.85 Million to Settle FTC Charges that the Firm Facilitated Merchant Fraud* (Sept. 4, 2026), <https://www.ftc.gov/news-events/news/press-releases/2026/09/payment-processor-nuvei-must-implement-robust-merchant-screening-practices-pay-485-million-settle>.

³ Press Release, FTC, *FTC Takes Action Against Payment Processor Humboldt Merchant Services for Knowingly Facilitating Payment Processing for Sham Merchants* (Sept. 8, 2026), <https://www.ftc.gov/news-events/news/press-releases/2026/09/ftc-takes-action-against-payment-processor-humboldt-merchant-services-knowingly-facilitating-payment>.

⁴ Press Release, FTC, *Paddle Will Pay \$5 Million to Settle FTC Allegations of Unfair Payment-Processing Practices and Facilitation of Deceptive Tech-Support Schemes* (June 16, 2025), <https://www.ftc.gov/news-events/news/press-releases/2025/06/paddle-will-pay-5-million-settle-ftc-allegations-unfair-payment-processing-practices-facilitation>.

⁵ See, e.g., Joint Statement of Chairman Andrew N. Ferguson & Comm’r Mark R. Meador, *In re Nuvei*, No. 2223153, Fed. Trade Comm’n (Sept. 2, 2026), https://www.ftc.gov/system/files/ftc_gov/pdf/nuvei-statement-ferguson-meador.pdf [hereinafter “Joint Statement”].

⁶ 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 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.

⁷ Nearly a third of consumers who reported losing money to scammers in 2025 said they were first contacted on social media platforms, with reported losses of \$2.1 billion.

fraud—one that fundamentally alters Platforms’ incentives so that they no longer benefit from the fraud they amplify.⁸

Today, I will discuss the Commission’s essential role in protecting markets from deception. I will begin by describing how the Commission has reinvigorated its fraud enforcement efforts, targeting not just bad actors directly, but also those who facilitate and benefit from fraud. I will then turn to the Commission’s consideration of a potential rule designed to realign Platform incentives, ensuring that Platforms, rather than consumers, bear the costs of deceptive impersonation ads.⁹

II. The Commission’s Proper Role Is to Reinforce Markets by Rooting Out Deception that Distorts and Undermines the Market Process

For centuries, markets have proven a boon to human existence because they promote the good of ordinary people.¹⁰ Historically, private exchange has proven a far better tool than government at allocating limited resources.¹¹ Indeed, markets, through the price system, can respond rapidly to the vagaries of consumer preferences—and coordinate dispersed knowledge—in a way that governments simply cannot.¹²

That is not to say, however, that government plays no role in markets. As John Adams famously wrote, government is instituted for the common good.¹³ Government and markets intersect where government action can facilitate and reinforce the benefits of market activity for the common good.¹⁴ For example, government plays an important role in protecting property, enforcing contracts,

⁸ Press Release, FTC, *FTC Seeks Public Comment on Whether to Update Rule on Impersonation of Government and Businesses to Address Platforms’ Role in Promoting Impersonation Scams* (Sept. 24, 2026), <https://www.ftc.gov/news-events/news/press-releases/2026/09/ftc-seeks-public-comment-whether-update-rule-impersonation-government-businesses-address-platforms>.

⁹ Andrew Ferguson & Christopher Mufarrige, *If Big Tech Doesn’t Curb Scams, They’ll Answer for It: FTC Chair*, BLOOMBERG NEWS (Sept. 28, 2026), <https://news.bloomberglaw.com/legal-exchange-insights-and-commentary/if-big-tech-doesnt-curb-scams-theyll-answer-for-it-ftc-chair>.

¹⁰ ADAM SMITH, *AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS* (Edwin Cannan ed., Univ. Chicago Press 1976) (1776). *See also* Vernon Smith, *The Two Faces of Adam Smith*, 65 S. ECON. J. 1, 3 (1998) (“Thus, Smith had but one behavioral axiom, ‘the propensity to truck, barter, and exchange one thing for another,’ where the objects of trade I will interpret to include not only goods, but also gifts, assistance, and favors out of sympathy, that is, ‘generosity, humanity, kindness, compassion, mutual friendship and esteem’ (Smith 1759; 1976, p. 38)”).

¹¹ *See* James Pethokoukis, *How the West Got Rich?*, AM. ENTER. INST. (May 23, 2016), <https://www.aei.org/economics/how-did-the-west-get-rich/> (comparing average world income two centuries ago of \$3 versus \$33 today and noting that average income in advanced economies is four times higher than the world average).

¹² *See* F.A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 527 (1945) (“It is more than a metaphor to describe the price system as a kind of machinery for registering change, or a system of telecommunications which enables individual producers to watch merely the movement of a few pointers, as an engineer might watch the hands of a few dials, in order to adjust their activities to changes of which they may never know more than is reflected in the price movement.”).

¹³ *Cf.* John Adams, Mass. Decl. of Rights, Art. VII (“Government is instituted for the common good...and not for the profit, honor, or private interest of any one man, family, or class of men.”).

¹⁴ *Cf. Oversight of the U.S. Federal Trade Commission Before the Subcomm. on Finan. Servs. & Gen. Gov’t of the H. Comm. on Approp.*, 119th Cong. 1 (2025) (statement of Andrew N. Ferguson, Chairman, Fed. Trade Comm’n) https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-Chairman-Andrew-N-Ferguson-FSGG-Testimony-05-15-2025.pdf (“No economic system in history has better promoted the common good than the American free-enterprise system. No economic system has contributed more to human flourishing. But our free-enterprise system promotes the common good of all Americans only if we protect it from anticompetitive business practices, anticompetitive

and otherwise reinforcing market activity. In many instances, markets are self-policing; the seller who disappoints the customer will be disciplined by losing sales to a competitor and suffering reputational harm.¹⁵ But market mechanisms cannot uniformly discipline deceptive sellers—particularly when product attributes are difficult to evaluate (for example, with credence goods¹⁶) or where sellers are not concerned with repeat business (e.g., one-time fraud).¹⁷

Markets can function and self-correct only when participants can rely on truthful information. Fraud and deception erode trust, harming not just individual consumers but the competitive process itself. This is where government—and specifically, the Commission—plays a critical role. By targeting fraud and deception that distorts or supplants the market process, the Commission safeguards the conditions under which competitive markets can flourish. Protecting consumers from deception is therefore not merely about preventing individual losses; it preserves the integrity of the marketplace itself, for the benefit of all Americans.

III. The Commission Has Reinvigorated the Fraud Program

To this end, Chairman Ferguson has reinvigorated the Commission’s fraud program. This Commission has brought numerous actions against fraudsters, including obtaining \$90 million from the ringleaders of the IM Mastery Academy business venture scam.¹⁸ In another major fraud action, the Commission secured \$145 million in settlements with Assurance IQ, LLC and MediaAlpha, Inc., resolving allegations that the companies engaged in unlawful conduct by deceptively telemarketing short-term medical, limited benefit indemnity, and bundled supplemental health products while misrepresenting these plans as comprehensive ACA-compliant insurance, causing consumers to purchase coverage that lacked the essential benefits they were promised.¹⁹

A. Actions Targeting Impersonation Fraud

A key focus of our fraud work is combating government and business impersonation fraud, in which a bad actor pretends to be a real government entity or a legitimate bank, hotel, or other business. Consumers report impersonation fraud more than any other type of fraud. To address the concerns consumers raise, the Commission is vigorously enforcing the Impersonation Rule and other applicable laws. For example, in an action last October against American Tax Services, the FTC obtained nearly \$10 million from scammers that allegedly impersonated the IRS to sell their purported

consolidation, and fraud. Without vigorous enforcement of our competition and consumer-protection laws, our free-enterprise system would benefit only the wealthy and the corrupt.”)

¹⁵ Benjamin Klein & Keith Leffler, *The Role of Market Forces in Assuring Contractual Performance*, 89 J. POL. ECON. 615 (1981); see also Oliver Williamson, *Credible Commitments: Using Hostages to Support Exchange*, 73 AM. ECON. REV. 519 (1983).

¹⁶ “With a credence good, consumers are never sure about the extent of the good they actually need. Therefore, sellers act as experts determining the customers’ requirements. This information asymmetry between buyers and sellers obviously creates strong incentives for sellers to cheat on services.” Winand Emons, *Credence Goods and Fraudulent Experts*, 28 RAND J. ECON. 107 (1997); see Michael R. Darby & Edi Karni, *Free Competition and the Optimal Amount of Fraud*, 16 J.L. & ECON. 67 (1973).

¹⁷ See C. Shapiro, *Consumer Information, Product Quality, and Seller Reputation*, 13 BELL J. ECON. 20 (1982).

¹⁸ Press Release, FTC, *Lead Defendants in the IM Mastery Academy MLM Scheme to Turn Over Tens of Millions of Dollars in Assets to Settle FTC Charges* (May 13, 2026), <https://www.ftc.gov/news-events/news/press-releases/2026/05/lead-defendants-im-mastery-academy-mlm-scheme-turn-over-tens-millions-dollars-assets-settle-ftc>.

¹⁹ Press Release, FTC, *Assurance IQ and MediaAlpha to Pay a Total of \$145 Million to Settle FTC Charges That They Misled Consumers Seeking Health Insurance* (Aug. 7, 2025), <https://www.ftc.gov/news-events/news/press-releases/2025/08/assurance-iq-mediaalpha-pay-total-145-million-settle-ftc-charges-they-misled-consumers-seeking>.

tax-relief services.²⁰ These scammers targeted older consumers in selling fictitious add-on services, often for tens of thousands of dollars at a time, until the FTC put a stop to their scam.

In April, the FTC filed suit against Innovative Partners for allegedly impersonating the government and large insurance companies to deceive consumers into buying health care plans that did not provide the comprehensive coverage that defendants advertised.²¹ Many consumers came across this deceptive scheme while researching online for health insurance options. Consumers attempting to find healthcare.gov or the website for their state's insurance marketplace or Medicaid agency on Google Search wound up on advertising and marketing websites run by lead-generation companies. These companies allegedly used deceptive online ads, including search ads that included government-related URLs and names to mislead consumers.

We have also taken action against companies that operate deceptive lead-generation websites. Last year, we sued MediaAlpha for allegedly impersonating the government by placing deceptive search text ads on search engines, like Google.²² Consumers who searched for government-related health care terms or state-run marketplaces were deceptively directed to MediaAlpha's lead-generation websites that continued the deception by using names, URLs, references, terms, and images that deceptively implied a government affiliation.

B. Actions Targeting Those Who Facilitate or Contribute to Fraud

The Commission is aggressively pursuing these bad actors. And our work yields results. In 2025, the FTC obtained over \$1.8 billion in redress for consumers affected by deceptive or unfair business practices.²³

Unfortunately, that impressive statistic is dwarfed by the sheer amount of fraud overall. In light of the pervasiveness of fraud, it can be more efficient to direct law enforcement resources upstream—to the companies that enable fraudsters to use American infrastructure to perpetrate their fraud. For example, earlier this month, the Commission announced an action against Nuvei, settling allegations that the payment processor opened and maintained payment processing accounts for merchants that it knew or should have known were engaged in deception.²⁴ According to the complaint, Nuvei processed over \$30 million for the Reimage tech support scam, despite knowing that Reimage was funneling money from American consumers to foreign scammers. Under the terms of the settlement, the defendants are required to pay \$4.85 million for consumer refunds and must stop processing payments for tech support telemarketers.

²⁰ Press Release, FTC, *State of Nevada Sue to Stop Tax Debt Relief Scammers from Falsely Impersonating the Government, Making False Claims and Threats to Consumers* (Oct. 17, 2025), <https://www.ftc.gov/news-events/news/press-releases/2025/10/ftc-nevada-sue-tax-debt-relief-scammers-falsely-impersonating-government>.

²¹ Press Release, FTC, *FTC Sues to Stop Deceptive Health Care Scheme* (Apr. 22, 2026), <https://www.ftc.gov/news-events/news/press-releases/2026/04/ftc-sues-stop-deceptive-health-care-scheme>.

²² *MediaAlpha* Press Release, *supra* note 19.

²³ FTC, *Congressional Budget Justification Fiscal Year 2027* (Apr. 3, 2026), available at https://www.ftc.gov/system/files/ftc_gov/pdf/ftc-fy-2027-congressional-budget-justification.pdf. (The Commission's ability to obtain redress is limited by its legal authority under the FTC Act. The Supreme Court held in *AMG Capital Management v. FTC* that the Commission cannot seek equitable monetary relief under Section 13(b) of the FTC Act. 593 U.S. 67 (2021)).

²⁴ Nuvei Press Release, *supra* note 2.

When the Commission announced *Nuvei*, Chairman Ferguson and Commissioner Meador issued a joint statement explaining that the Commission will take action against payment processors who know, should know, or consciously avoid knowing that they are enabling fraudsters to scam American consumers. The joint statement distinguished liability where there is knowledge of the wrongdoing from “the good-faith payment processor working to grant small businesses, startups, and other risk-taking enterprises access to America’s consumers.”²⁵

Processing payment for fraudsters is lucrative. However, when payments companies process fraud, they do not bear meaningful responsibility for the enormous social cost that results when consumers are victimized by the fraudsters whose payments the processor handles. These costs represent negative externalities—costs that are not borne by the parties best positioned to reduce them—in this case, the processors.²⁶ The result is that processors seeking to maximize their payment-processing revenues have insufficient financial disincentive to refrain from doing business with known bad actors.²⁷ In other words, processors internalize the revenue but externalize the risk.

Consumers deserve a payment system that is competitive, transparent, and fortified against fraud. When payment processors undermine trust in the payment system and fail to take the appropriate compliance measures, Commission action is necessary to restore trust in the market. That is what we have done over the past eighteen months. And that is exactly what we will continue to do.

IV. The Commission Is Exploring a Proposed Rule That May Correct Platform Incentives and Force Platforms to Internalize the Cost of Fraud that Consumers Currently Bear

The Commission’s enforcement action against Nuvei—and a similar recent action against payment processor Humboldt Merchant Services²⁸—illustrate how law enforcement can correct an externality problem. As our investigations showed, Nuvei profited from processing transactions for tech support scammers while shifting the resulting fraud costs onto consumers and the broader U.S. payments system. The monetary relief and due-diligence obligations in the Commission’s order force Nuvei to internalize the cost imposed by fraudsters. Moreover, the order compels Nuvei to bear the costs associated with fraudulent merchants and adopt efficient, economically grounded screening and monitoring measures, ensuring that Nuvei internalizes the harm it helps create rather than externalizing it to the public.

²⁵ Joint Statement, *supra* note 5, at 6.

²⁶ 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). These types of externalities—and corresponding costs—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).

²⁷ Cf. 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.”).

²⁸ *Humboldt* Press Release, *supra* note 3.

The same economic logic animates the Commission’s ANPR on digital platforms. Today, Platforms earn substantial revenue by optimizing advertising—including ads placed by impersonators and scammers—while the resulting harm is borne entirely by consumers, who absorb the financial losses and marketplace distortions. In effect, Platforms internalize the profits but externalize the costs of fraud. The ANPR therefore asks whether rulemaking should correct this incentive misalignment by requiring Platforms, like payment processors, to internalize the social costs of the deception their systems materially facilitate. It further seeks comment on whether platforms should be subject to enforceable obligations that make fraud prevention a cost-effective, built-in component of their business models, rather than an optional or reputational consideration.

Platforms have become essential—indeed, an unavoidable—infrastructure for American consumers. But Platforms have increasingly become fertile ground for impersonation scams, driven in large part by ad-optimization practices. For instance, reports indicate that scammers are using Meta’s powerful ad-optimization and targeting tools to deliver Medicare-impersonation ads to older Americans, precisely the group most vulnerable to, and disproportionately harmed by, such schemes.²⁹ Fraudsters are also using these tools to impersonate popular consumer brands—for example, impersonating McCormick Spice with fake “giveaway” ads on Meta platforms that redirect consumers to fraudulent websites.³⁰

Fraudsters are also leveraging Google’s massive infrastructure,³¹ which accounts for about 90% of all search traffic.³² Indeed, fraudsters are purchasing high-ranking sponsored placements on

²⁹ 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*, at 18-19, 22-25 (2025), https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf (“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).

³⁰ 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.”).

³¹ See, e.g., *FTC v. Simple Health Plans LLC, et al.*, No. 18-cv-62593 (S.D. Fla. Feb. 7, 2024) (granting \$195 million judgment against company that used Google to deceptively advertise health insurance); *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 et al. v. Grubhub, Inc.*, No. 1:24-cv-12923 (N.D. Ill. Aug. 25, 2025) (obtaining settlement against a company that used Google ads to make unsubstantiated earnings claims); *FTC v. Daxo, Inc., et al.*, No. 2:24-cv-00569 (W.D. Wash. Apr. 25, 2024) (alleging that a company made itself appear to be an official bill payment site for a third party using search engine ads, including through Google); *FTC v. Click4Support, LLC, et al.*, No. 2:15-cv-05777 (E.D. Pa. Feb. 7, 2016) (obtaining settlement against a company that used Google ads to pose as a tech support company to gain control over consumers’ computers and defraud them); *FTC v. Elite IT Partners, Inc., et al.*, No. 2:19-cv-00125 (D. Utah Dec. 9, 2019) (similar); *FTC v. Mercury Marketing, LLC, et al.*, No. 1:25-cv-02021 (D. Md. Jun. 24, 2025) (alleging that a company used Google ads to impersonate substance abuse disorder treatment clinics).

³² *United States v. Google LLC*, No. 1:20-cv-03010 (D.D.C. Sept. 2, 2025).

Google 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 the imposter’s—and in some cases malicious—websites.³³ Search-engine impersonation is a popular method for travel and banking impersonation schemes, which steer consumers running a search for specific hotels or banks—say, for example, “Hilton hotel in Portsmouth” or “Bank of America”—to an imposter site.³⁴ To the extent that Meta or Google or any Platform is working with advertisers to create and enhance these deceptive ads,³⁵ they could be materially contributing to the deceptiveness of impersonation ads in violation of Section 5 of the FTC Act.³⁶

Of course, ad-optimization itself is not a problem. Ad-optimization brings enormous benefits to legitimate businesses disseminating non-deceptive ads as well as benefits to consumers whose search costs are lessened by access to truthful advertising.³⁷ Through ad-optimization, legitimate businesses can capture the attention of consumers most likely to be interested in their products and services and maximize the appeal of those offerings. But a real problem arises when ad-optimization enhances deception—that is, when a Platform materially contributes to deception by creating, emphasizing, or combining misleading ad content.

Platforms’ advertising practices cannot be understood without first examining the economic incentives that govern multi-sided markets, *i.e.*, markets in which a single intermediary simultaneously serves distinct user groups and sets the terms on which they interact. In the case of ad-supported Platforms, the business model hinges on connecting consumers on one side with advertisers on the other, and the Platform’s financial rewards rise with the volume and engagement of ads it delivers. This intermediary structure creates a powerful incentive to optimize all paid advertisements, irrespective of whether the ads originate from legitimate businesses or from impersonators and scammers.

³³ See N.J. Cybersecurity & Comm’n’s 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”).

³⁴ See, e.g., 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); *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>.

³⁵ See, e.g., Seth Kugel, *The Click That Cost \$11,000 and Other Travel Pitfalls*, N.Y. Times, Apr. 17, 2026, https://www.nytimes.com/2026/04/09/travel/travel-scams-airlines-hotels.html?eafs_enabled=false.

³⁶ *Cf. FTC v. LeadClick Media, LLC*, 838 F.3d 158 (2d Cir. 2016) (defendant that “materially contribut[ed]” to deception not entitled to immunity under Section 230).

³⁷ See George Stigler, *The Economics of Information*, 69 J. POL. ECON. 213, 220–24 (1961).

Platforms earn revenue each time an optimized ad is clicked, giving them a simple, powerful incentive: maximize ad impressions, clicks, and engagement. But the economic consequences of this incentive structure are fundamentally asymmetric. Platforms internalize the advertising revenue while externalizing the costs of fraud, leaving consumers to absorb the losses when optimized scam ads mislead, defraud, or divert them. This is a textbook negative externality. Impersonation scams proliferate because the market fails to impose the social costs of the harm on the actor best positioned to prevent it. In economic terms, the Platform internalizes the gains but externalizes the risks, meaning the “price” it effectively pays for distributing and optimizing deceptive ads is artificially low. And when markets underprice harmful conduct, we get more of it: here, an overproduction and amplification of impersonation scams.

The Platforms can fix this problem. Platforms control the design of their ad-optimization systems. They decide how ads are screened, ranked, recombined, and delivered. And they can adjust these practices at relatively low cost compared to consumers or legitimate businesses, who bear the consequences of fraud but cannot efficiently prevent it.³⁸

Although Platforms may have some reputational incentive to limit fraud, that incentive is weakened substantially when a Platform possesses significant market power. In a competitive market, consumers dissatisfied with deceptive ads can discipline firms by “voting with their feet.” That feedback both reduces the likelihood of fraud and incentivizes firms to invest in efficient levels of fraud prevention. But when a dominant Platform enjoys significant market power, switching becomes impractical for consumers due to lock-in, network effects, and a lack of realistic alternatives. In other words, consumers’ ability to protect themselves is diminished.

As the Commission increasingly takes on consumer protection cases against Platforms with market power—and even monopoly power—we must confront the reality that Platforms may not face sufficient incentives to prevent fraud, and that their market power exacerbates the resulting externality. In competitive markets, reputational harm and consumer choice operate as natural constraints on deceptive conduct. Consumers respond to quality deterioration through exit—opting for the services of a competitor. That threat of exit itself is a powerful deterrent. But the market’s ability to discipline breaks down when a Platform enjoys monopoly power or something close to it. While consumers may communicate their dissatisfaction (such as by sending complaints or seeking refunds), exit is not a realistic option due to the lack of competition.³⁹ As a result, deception by a monopolist (or a firm with significant market power) becomes both harder to detect and harder to avoid.⁴⁰ Indeed, this dynamic has direct implications for how we think about the Commission’s dual

³⁸ STEVEN SHAVELL, *ECONOMIC ANALYSIS OF ACCIDENT LAW* (1987).

³⁹ Cf. ALBERT O. HIRSCHMAN, *EXIT, VOICE, AND LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES*, Harv. Univ. Press (1970).

⁴⁰ When applying traditional black letter law deception principles, the presence of significant market power—and, in particular, monopoly power—presents a novel fact pattern. Under Section 5 of the FTC Act and state UDAP statutes, a representation, omission, or practice is material if it is likely to affect a consumer’s choice or conduct regarding a product or service. But when a firm possesses monopoly power—and deploys deception to preserve that power—the conventional tools for assessing materiality may be unreliable. Market signals that normally reveal whether a deceptive practice mattered to consumers (such as cross-price elasticity or switching behavior) are fundamentally distorted by the

consumer protection and competition missions—and why, in cases involving Platforms with market power, both missions must remain top of mind.

The ANPR will explore these issues and what, if any, measures Platforms are capable of taking to prevent fraud. Think for a moment about the measures Platforms could take to prevent the optimization of impersonation ads. They could verify identities, screen advertiser accounts, detect repeat offenders, flag mismatches between an ad and the entity it purports to represent, and disable optimization services for suspicious accounts before an ad ever reaches a consumer. None of these measures require evaluating whether the ad’s substantive claims about a product are true. They simply require confirming that advertisers are who they say they are—a basic safeguard every major Platform is capable of performing.

And that is precisely why impersonation ads are the clearest, most tractable category of fraud. Unlike other forms of deception that might demand complex, time-intensive assessments of efficacy or performance, identifying impersonation rarely requires deep expertise or lengthy review. A Platform does not need to adjudicate whether a supplement works or whether an investment strategy is sound. It only needs to check whether the ad is coming from the genuine business or agency it claims to be. That is a low-cost, low-burden verification.

This is the logic behind the Commission’s potential rule. The ANPR does not ask whether Platforms should prevent *all* fraud. It does not ask whether they should police the entire universe of advertising claims. What it asks is far narrower: whether their systems should prevent impersonation scams, the very type of scam most amenable to simple preventative tools.

absence of competition. One result here is courts may risk drawing inappropriate inferences from consumer behavior that appears non-responsive only because the monopolist has eliminated meaningful alternatives. While Section 5 jurisprudence recognizes presumptions of materiality for express and intentionally implied claims, the presumption can be rebutted. When a firm with durable market power engages in deception, the resulting patterns of consumer switching, or lack thereof, will often differ from those observed in competitive markets. In other words, courts will likely be presented with consumer switching dynamics that do not replicate typical markets. Economists have long cautioned against evaluating consumer behavior against a distorted baseline. *See, e.g.,* George W. Stocking & Willard F. Mueller, *The Cellophane Case and the New Competition*, 45 Am. Econ. Rev. 29 (1955).

A potential solution to this problem can be drawn from the D.C. Circuit’s reasoning in *United States v. Microsoft Corp.*, 253 F.3d 34 (D.C. Cir. 2001). In *Microsoft*, the government challenged exclusionary conduct aimed at “nascent” competitive threats—conduct whose but-for market consequences could not be confidently reconstructed. Recognizing this epistemic problem, the court declined to require precise proof of how the market would have evolved absent the challenged conduct. Instead, it adopted a more flexible monopoly causation standard, holding that causation may be inferred where the conduct “reasonably appears capable of making a significant contribution to maintaining monopoly power.” *Microsoft*, 253 F.3d at 79. This same logic has implications for materiality analysis in deception cases involving dominant Platforms. When a firm possesses significant market power, traditional economic evidence about how consumers would have behaved “but for” the deception may be inherently difficult to determine because consumers’ choices are shaped by lock-in, network effects, and limited competitive alternatives. In such settings, the question should not be whether plaintiffs can precisely quantify the but-for world, but whether the deception was *reasonably capable* of affecting consumer decision-making under real-world market conditions. Arguably, just as *Microsoft* recognizes a relaxed causation standard where monopoly power and nascent competition make the but-for world unknowable, deception law should not require courts to reconstruct the hypothetical choices of consumers who lacked meaningful competitive options in the first place.

By focusing on impersonation scams, the ANPR targets the harm that Platforms can reduce most efficiently. It focuses on the kind of fraud where the least-cost avoider is unmistakable. And it underscores that, while Platforms may have complex, revenue-driven incentives in many areas, preventing the optimization of impersonation scams is not a heavy lift. Nor would the potential rule impede any legitimate, pro-competitive benefit of the Platform. Indeed, taking steps to prevent, detect, and remove impersonation fraud is a basic responsibility for any Platform whose architecture shapes what millions of consumers see.

This is where the Commission’s potential rulemaking could serve the public. Our ANPR solicits public comment on whether to expand the existing Impersonation Rule to cover such practices. A rule here has the potential to correct the misaligned Platform incentives driving the proliferation of impersonation scams online. A potential rule could correct misaligned incentives by, first, defining the specific problematic Platform practices as unfair or deceptive, and second, exposing those practices to the threat of a streamlined enforcement action for monetary relief.

Of course, in order for the Commission to potentially craft an effective rule, it would need relevant information to shape the rulemaking—information about how Platforms operate their ad-optimization businesses, the extent to which each ad-optimization practice furthers impersonation scams, how widespread these practices are, and what steps Platforms are already taking to stop these practices. The Commission would also need information on what kinds of requirements are cost-effective and helpful for preventing the optimization of impersonation ads.

At this early stage, the Commission is considering all types of potential rule requirements. For example, in a potential rule, the Commission may require Platforms to evaluate advertisements for impersonation and prohibit Platforms from providing ad-optimization services to those engaged in impersonation scams. Potential rule requirements could obligate Platforms to take affirmative steps to address impersonation ads that have already been posted, including: implementing a program to detect suspected impersonation ads; providing consumers a clearly and conspicuously placed tool to report suspected impersonation ads; investigating suspected impersonation ads; removing confirmed impersonation ads through a process similar to that in the Take It Down Act, which requires covered Platforms to establish a process for victims to request the removal of non-consensual intimate images;⁴¹ discontinuing ad-optimization services for confirmed impersonation ads; and taking appropriate disciplinary action against the offending advertiser. Instead of serving as affirmative requirements, these potential measures could form the basis of a safe harbor provision under which Platforms’ compliance could provide a defense to liability under any new regulations governing ad-optimization practices. In addition, a potential rulemaking could consider ancillary measures, such as potentially requiring Platforms to maintain records documenting their compliance, in order to facilitate enforcement of the new or amended rule.

Accordingly, the publication of the ANPR will begin a public comment period when industry, consumers, and other stakeholders will have the opportunity to shape a potential rulemaking by providing the Commission with information relevant to these issues.⁴² After considering the comments, the Commission may then publish a specific rule proposal in a Notice of Proposed

⁴¹ FTC, *Complying With the Take It Down Act* (May 2026), <https://www.ftc.gov/business-guidance/resources/complying-take-it-down-act>.

⁴² 15 U.S.C. § 57a(b)(2)(A).

Rulemaking, if it has reason to believe that the Platform practices at issue are prevalent.⁴³ Following another round of public comments on the proposed rule language, the Commission may then publish a final rule along with a Statement of Basis and Purpose to explain the rule's rationale.⁴⁴

I encourage every one of you to engage in this potential rulemaking process and submit your insights, concerns, and other comments to inform the Commission as it considers potential regulatory measures to address Platform ad-optimization practices.

* * * * *

Thank you for the opportunity to speak today. I look forward to your questions.

⁴³ *Id.* § 57a(b)(3).

⁴⁴ *Id.* § 57a(d).