Comments to the Federal Trade Commission
regarding the
Rule on Impersonation of Government and Businesses
R207000
89 Fed. Reg. 15,072 (Mar. 1, 2024)
Supplemental Notice of Proposed Rulemaking

submitted by
Electronic Privacy Information Center and
Consumer Action
Consumer Federation of America
National Association of Consumer Advocates
National Consumer Law Center (on behalf of its low-income clients)
National Consumers League

April 30, 2024

Grant Fergusson, Chris Frascella,
Maria Villegas Bravo, and Enid Zhou
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

I. There is substantial justification for all aspects of the proposed regulation.

A. Introduction

These comments are submitted by the following consumer and privacy advocacy organizations: **Electronic Privacy Information Center** (EPIC), **National Consumer Law Center** on behalf of its low-income clients, **Consumer Federation of America**, **National Consumers League**, **Consumer Action**, and **National Association of Consumer Advocates**. We applaud the Federal Trade Commission (FTC or Commission) for proposing enhanced tools to protect consumers from impersonation scams in this Supplemental Notice of Proposed Rulemaking (SNPRM).[1] The proposed trade regulation rule will more clearly prohibit the impersonation of not only government, businesses, or their officials, but also impersonation of real or fictitious individuals, and will provide the Commission with the critically important ability to secure redress from both the scammers responsible for defrauding Americans of billions of dollars each year and those who equip the fraudsters. This is an increasingly timely concern given the rapid growth of generative artificial intelligence tools, which can facilitate impersonation.

In section I(B) immediately below we emphasize the ample evidence in the record to support the Commission's adoption of this modification to its rule. We do not believe that there are any disputed issues of material fact to be resolved in this rulemaking. To the extent that the FTC does identify such disputed issues or conducts a hearing, the undersigned would welcome the opportunity to participate in any informal hearing to support the FTC's efforts to ensure that this rule becomes law.

In Section II, we discuss the importance of including means and instrumentalities (M&I) liability in the context of impersonation scams.

In Section III, we discuss why we support the Commission's proposed "knows or should have known" standard for M&I liability.

In Section IV, we discuss impersonation of characteristics such as affiliation or profession rather than of specific individuals.

B. There is ample evidence to support the promulgation of both proposed regulations.

The need for the FTC (and other government agencies) to seek additional methods to stop consumer losses from fraudsters impersonating individuals should be clear and, indeed, noncontroversial. As the Commission notes, "[s]ince issuance of the ANPR in December 2021, the FTC has received thousands to tens of thousands of complaints each quarter from consumers concerning romance scams or family and friend impersonations."[2] The FTC also cites to reports

[1] Federal Trade Comm'n, Trade Rule on Impersonation of Government and Businesses, Supplemental Notice of Proposed Rulemaking; Request for Public Comment, 89 Fed. Reg. 15,072 (Mar. 1, 2024), *available at* https://www.federalregister.gov/documents/2024/03/01/2024-03793/trade-regulation-rule-on-impersonation-of-government-and-businesses [hereinafter SNPRM].

[2] SNPRM at 15,076, Section V(A)(2), https://www.federalregister.gov/d/2024-03793/p-44.

from NAAG, the FBI, and AARP as further quantitative and qualitative support for the need for this modification to the agency's rule.[3] Unfortunately, there are numerous other examples, especially in the generative AI context, supporting the necessity for this rule.[4]

We also strongly support the FTC explicitly making liable those who provide the means and instrumentalities that enable fraudsters (M&I liability). This regulation is essential to provide appropriate disincentives to those that might otherwise support and facilitate impersonation scams. Providers of means and instrumentalities not only accelerate scams, oftentimes they act as gatekeepers. Romance scam campaigns would be nearly impossible to roll out at the current scale without complicit platforms like dating websites willing to look the other way.[5] Similarly, the VoIP providers who generally turn a blind eye to obviously fraudulent robocall campaigns allow scam robocalls to proliferate at scale.[6] As a matter of effective deterrence, the FTC should take the necessary steps to enable civil penalty authority via M&I liability.

---

[3] *See id.* at 15,073, Section II(A), https://www.federalregister.gov/documents/2024/03/01/2024-03793/trade-regulation-rule-on-impersonation-of-government-and-businesses#p-14; *id.* at 15,074, Section III(A), https://www.federalregister.gov/d/2024-03793/p-25.

[4] *See, e.g.*, Jason Koebler, *YouTube Deletes 1,000 Videos of Celebrity AI Scam Ads*, 404 Media (Jan. 25, 2024), https://www.404media.co/youtube-deletes-1-000-videos-of-celebrity-ai-scam-ads/; Charles Bethea, *The Terrifying A.I. Scam That Uses Your Loved One's Voice*, The New Yorker (Mar. 7, 2024), https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice; Daryna Antoniuk, *From AI with love: Scammers integrate ChatGPT into dating-app tool*, The Record (Oct. 5, 2023), https://therecord.media/lovegpt-romance-scam-tool-uses-chatgpt ; Godfrey Benjamin, Ripple *CEO Warns of Impersonating Deepfake Scam Videos*, CounGape (Nov. 14, 2023), https://coingape.com/ripple-ceo-warns-of-impersonating-deepfake-scam-videos/ (deepfake video of CEO used to defraud customers); Amy Bunn, *Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam*, McAfee (May 15, 2023), https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/ (one in four survey respondents experienced an AI voice cloning scam or knew someone who had). The Commission might consider companies providing GAI-related offerings presumptively on notice of fraudulent activity by virtue of how high-risk their offerings are. *See, e.g.*, EPIC, *Generating Harms: Generative AI's Impact & Paths Forward* at 3,11-12,65 (May 2023), https://epic.org/documents/generating-harms-generative-ais-impact-paths-forward/. And even apart from GAI-fueled scams, the impersonation of real or fictitious individuals is a common tactic to defraud consumers. *See, e.g.*, Fed. Commc'ns Comm'n, Love & Appiness: How to Avoid Romance Scams (updated Feb. 1, 2024), https://www.fcc.gov/love-appiness-how-avoid-romance-scams (noting fake stock photos); *Online Dating and Romance Scams*, https://www.ag.state.mn.us/Consumer/Publications/OnlineDatingRomanceScams.asp (last visited Apr. 24, 2024) (noting phony profiles); FBI, Romance Scams, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/romance-scams (last visited Apr. 24, 2024) (encouraging consumers to research the photo and profile of the would-be love interest to see if the information appears elsewhere).

[5] *See, e.g.*, Jim Axelrod, et al., *As romance scammers turn dating apps into "hunting grounds," critics look to Match Group to do more*, CBS News (Apr. 24, 2024), https://www.cbsnews.com/news/romance-scams-dating-apps-investigators-match-group/.

[6] *See generally* Margot Saunders (National Consumer Law Center) & Chris Frascella (Electronic Privacy Information Center), *Scam Robocalls: Telecom Providers Profit* at pt I(A) (June 1, 2022), *available at* https://www.nclc.org/wp-content/uploads/2022/09/Rpt_Scam_Robocalls.pdf [hereinafter "Scam Robocalls Report"].

II. The proposed means and instrumentalities (M&I) financial penalties are effective to persuade service providers to avoid facilitating these scams.

Complicit providers profit from business generated by fraudsters.[7] The threat of civil penalties imposed by a U.S. federal agency—imposed only after the fraudsters are identified and successfully prosecuted—is unlikely to deter international fraudsters themselves. The complicit enablers of fraud need a deterrent that exceeds the potential profit they will reap from turning a blind eye to the scams.

The FTC needs to change the incentive structure if the agency is going to be successful in stopping impersonation scams. Consumers suffer enormous losses from scams every year.[8] By implementing the proposed rule, the Commission would be able to seek civil penalties for violations.[9] Means and instrumentalities (M&I) liability is integral to changing this incentive structure in large part because the fraudsters themselves are generally impossible to reach—due to obfuscation tactics, operating outside the jurisdiction of U.S. agencies, being judgment proof, and in some instances being coerced into perpetrating the scams. In the case of robocalls, for instance, enforcement will only be effective if providers transmitting scam messages find liability more costly than the benefits of accepting and passing on the fraudulent call traffic. Similarly, providers that process payments should be forced to consider the financial risks of facilitating scam payments; they often have reason to suspect fraudulent activity due to repeated

---

[7] *See, e.g.*, Scam Robocalls Report at 4-5, 12-16; Press Release, FTC Sues Owner of Online Dating Service Match.com for Using Fake Love Interest Ads to Trick Consumers into Paying for a Match.com Subscription (Sept. 25, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/ftc-sues-owner-online-dating-service-matchcom-using-fake-love-interest-ads-trick-consumers-paying [hereinafter "FTC Match.com Press Release"].

[8] For the third year in a row, the FTC received more than 90,000 annual reports of imposter scams related to friends/family-based or to romance-based frauds. *See* FTC, *Consumer Sentinel Network: Data Book 2023* at 87 (Feb. 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf. The FTC estimates based on reports it has received that these two types of impersonation scams alone cost consumers more than $536MM in 2023, *see* FTC Consumer Sentinel Network, Fraud Reports by Subcategory Payment & Contact Info (published Feb. 8, 2024) (Rank by Total Losses, quarters 1 through 4 checked for 2023, indicating $536.4M in total losses from romance scams). This is more than double the $188MM in consumer losses reported in 2019, *see id.* (Rank by Total Losses, quarters 1 through 4 checked for 2019, indicating $156.8M in total losses from romance scams and $31.2M in total losses from friends/family impersonation scams). These are longstanding scams that have gotten pronouncedly worse over the past 15 years; the FTC has published reports on romance impostor scams since at least as early as its 2012 consumer data book, in which it reported approximately 5 reports for 2010. *See* FTC, *Consumer Sentinel Network: Data Book 2012* at 82 (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/consumer-sentinel-network-data-book-january/sentinel-cy2012.pdf. The FTC has published data on friend/family impostor scams since at least as early as its 2010 consumer data book, in which it reported approximately 2 complaints for 2008. *See* FTC, *Consumer Sentinel Network: Data Book 2010* at 78 (Mar. 2011), https://www.ftc.gov/sites/default/files/documents/reports_annual/sentinel-cy-2010/sentinel-cy2010.pdf.

[9] *See, e.g.*, SNPRM at 15,076, Section V(A)(1), https://www.federalregister.gov/d/2024-03793/p-42 (discussing the implications of the Supreme Court decision in *AMG*).

complaints and attempts to recoup payments by victims.[10] Other commenters have highlighted similar examples.[11] Complicit providers are in the best position to protect consumers because they act as gatekeepers between the fraudster and the success of their scam. These providers should not be able to profit from failing to protect consumers, and in fact should be strongly deterred from turning a blind eye to scams.

Scammers are generally effective at being hard to track, making enforcement difficult. For example, fraudulent robocall providers typically work through multiple intermediary providers to make call tracing more difficult for law enforcement.[12] In Vermont's case against TCAVoIP, the Vermont Attorney General noted that many illegal robocall campaigns come from foreign sources, passing through smaller voice service providers, then larger voice service providers, then the terminating carrier (the phone subscriber's phone company).[13] Downstream providers are often unable to penetrate this shell game and prevent the scam calls from reaching the fraudster's intended prey: consumers.[14] The obfuscations offered by complicit providers should be punished, as the proposed rule would allow.[15]

U.S. authorities encounter jurisdictional obstacles when seeking to take action against scammers operating outside the country. The Federal Communications Commission (FCC) has lamented that "[u]nfortunately, in the case of foreign-originated calls, we face substantial difficulties in enforcing such an obligation on the foreign originating provider."[16] Transmissions of scam calls between providers may start in foreign countries or within the U.S., but intermediary providers are often used to cross in and out of the U.S. to deliberately obfuscate the identity of the

[10] *See, e.g.*, Press Release, NCL applauds decisive action by CFPB against fraudulent payments processor (Jan. 19, 2022), https://nclnet.org/cfpb_brightspeed/ (payment processor continued to serve scammers despite being aware of nearly 1,000 consumer complaints against their clients); Comments of NCLC, et al., to NACHA – The Electronic Payments Association at 2-3(Oct. 9, 2015), https://www.consumer-action.org/downloads/coalition/CommentsonNACHA.pdf (providing examples of how third party senders enable fraud).
[11] *See, e.g.*, SNPRM at 15,073, Section II(B), https://www.federalregister.gov/d/2024-03793/p-17 (NAAG comments on marketing companies, call centers, etc.); id. at 15,073-74, Section II(B), https://www.federalregister.gov/d/2024-03793/p-18 (Apple comments on gift card gray markets).
[12] *See* Scam Robocalls Report at 13-14 (citing to Complaint, State of Vermont v. Bohnett, Case No. 5:22-cv-00069 (D. Vt. Mar. 18,2022)).
[13] Complaint, State of Vermont v. Bohnett, Case No. 5:22-cv-00069 at ¶ 34 (D. Vt. Mar. 18,2022)).
[14] *See* Scam Robocalls Report at 36-37, endnotes 77-80.
[15] *See, e.g.*, SNPRM at 15,077, Section V(A)(3), https://www.federalregister.gov/d/2024-03793/p-46.
[16] Fed. Commc'ns Comm'n, Sixth Report and Order in CG Dkt. No. 17-59, Fifth Report and Order in WC Dkt. No. 17-97 at ¶ 99 (Rel. May 20, 2022), https://docs.fcc.gov/public/attachments/FCC-22-37A1.pdf.

originating provider.[17] These scams may also part of larger, international criminal syndicates that require concerted effort to address at the international scale.[18]

Fraudsters may shuffle and hide assets, making it difficult to obtain any meaningful monetary judgment against them, rendering them "judgment proof." The FTC itself sees this from time to time when it has to suspend its own monetary judgements due to the bad actor's inability to pay.[19] This not only reduces the deterrent power of a financial penalty but also makes it difficult to make consumers whole again.

In some instances, the individuals executing impersonation scams may themselves be victims of crime, such as human trafficking. Pig butchering is a type of fraud where the scammers target victims by gaining their trust, convincing victims to invest or transfer real money to fake accounts or platforms, then cutting contact. This is often coupled with romance scams as a way to gain trust. These scams have been linked to several criminal syndicates in Southeast Asia that engage in human trafficking to "staff" their fraudulent enterprises. Often times, the scammers directly communicating with the victims on a daily basis are themselves victims of human trafficking and subject to brutal, inhumane conditions.[20] The mastermind behind this kind of

---

[17] *See* Scam Robocalls Report at 36, endnote 74; *see also* NCLC et al., Letter to FTC re: FTC Collaboration Act of 2021 Study at 20 (Aug. 14, 2023), https://www.nclc.org/wp-content/uploads/2023/08/FTC_AG-Fraud-Collaboration-consumer-comments-8-14-23-final3-Lauren-Saunders.pdf (discussing international dimension of bank wire transfer fraud); Press Release, FTC, Law Enforcers Nationwide Announce Enforcement Sweep to Stem the Tide of Illegal Telemarketing Calls to U.S. Consumers (Jul. 19, 2023), available at https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-law-enforcers-nationwide-announce-enforcement-sweep-stem-tide-illegal-telemarketing-calls-us [hereinafter "Telemarketing Sweep Press Release"].

[18] *See e.g.*, Press Release, U.S. Law Enforcement Disrupts Networks Used to Transfer Fraud Proceeds, Taking Over 4,000 Actions in Fifth Campaign (May 22, 2023), https://www.justice.gov/opa/pr/us-law-enforcement-disrupts-networks-used-transfer-fraud-proceeds-taking-over-4000-actions (noting global effort to address money mules); Europol, *Money muling*, https://www.europol.europa.eu/crime-areas/forgery-of-money-and-means-of-payment/money-muling (last visited Apr. 24, 2024) (noting EU-wide effort).

[19] *See, e.g.*, Press Release, FTC Action Leads to Permanent Ban for Scammers Who Charged Students Seeking Debt Relief with Junk Fees (Feb. 6, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-action-leads-permanent-ban-scammers-who-charged-students-seeking-debt-relief-junk-fees ("monetary judgment of $7.4 million, which is largely suspended due to an inability to pay"). *But see* Press Release, FTC Takes Action to Ban Payment Processor From Debt Relief Processing (Nov. 8, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/11/ftc-takes-action-ban-payment-processor-debt-relief-processing (suspending monetary judgment due to inability to pay).

[20] *See, e.g.*, Cezary Podkul, *What's a Pig Butchering Scam? Here's How to Avoid Falling Victim to One*, ProPublica (Sept. 19, 2022), https://www.propublica.org/article/whats-a-pig-butchering-scam-heres-how-to-avoid-falling-victim-to-one; Cezary Podkul, Cindy Liu, *Human Trafficking's Newest Abuse: Forcing Victims Into Cyberscamming*, Propublica (Sept. 13, 2022), https://www.propublica.org/article/human-traffickers-force-victims-into-cyberscamming. *See also* Sophos, *Criminals Leverage "As-a-Service" Business Model with Sha Zhu Pan Kits,* Globally Expanding Cryptocurrency Fraud (Feb. 2, 2024), https://www.sophos.com/en-us/press/press-releases/2024/02/criminals-leverage-service-business-model-sha-zhu-pan-kits-globally (giving voluntary bad actors toolkits to implement a pig butchering scheme). This added layer of deception also increases the difficulty in tracing the scam as well as getting proper jurisdiction over foreign actors.

criminal operation is unlikely to be deterred by the threat of monetary fines if they are engaging in human trafficking. Their victims who have been coerced into perpetrating the fraud are also unlikely to be deterred by monetary fines, as they are effectively committing crimes under duress. In these schemes, deterrence must apply somewhere else if it is to be effective.

The FTC already investigates and engages in enforcement actions in this space, but amending the rule to explicitly include means and instrumentalities liability will go far to reduce complicity in fraudulent schemes by allowing the Commission to pursue civil penalties in addition to injunctive relief. As finding the individual scammers is difficult, and recovering money from them is nearly impossible, government enforcement has pursued complicit service providers.[21] For example, in 2019, the FTC filed a complaint and sought civil penalties against Match Group, the operator of popular dating website Match.com, for unfairly exposing consumers to the risk of fraud.[22] The complaint alleges, among several unfair and deceptive trade practices, that Match.com used messages from accounts already flagged as fraudulent to entice free users to pay for services from Match.com.[23] The same flagged accounts were blocked from communicating with users who were already paying for services on the dating website.[24] Between the filing of the complaint and the case's later resolution on different grounds, though, the Supreme Court overturned decades of precedent by restricting the Commission's ability to recover restitution and other equitable monetary relief.[25] By creating means and instrumentalities liability in this rule, and thereby unlocking civil penalties, the Commission can ensure that it can pursue perpetrators who enable and accelerate fraudulent impersonation schemes with the strongest deterrent tools in its arsenal.

III. We support the Commission's proposed "knows or should have known" standard for M&I liability as a financial incentive.

The FTC has long established, and courts have long upheld, the FTC's ability to seek redress under Section 5 not only from those who directly defraud consumers but also from companies that knew or should have known that they were providing means and instrumentalities to enable

---

[21] *See, e.g.*, Telemarketing Sweep Press Release; Notice of Apparent Liability for Forfeiture, In re Sumco Panama et al., EB-TCD-21-00031913 at ¶ 31 (Dec. 23, 2022), https://docs.fcc.gov/public/attachments/FCC-22-99A1.pdf (noting that only two out of nearly a dozen participants in an auto warranty scam responded to FCC subpoenas).

[22] *See, e.g.*, Complaint, FTC v. Match Group, Inc., Case No. 3:19-cv-02281 (N.D. Tx. Sept. 25, 2019), https://www.ftc.gov/system/files/documents/cases/match_-_complaint.pdf [hereinafter "Match.com Complaint"]; FTC Match.com Press Release.

[23] *See* FTC Match.com Complaint at ¶¶ 34-35, 64.

[24] *See id.*

[25] *See* SNPRM at 15,076, Section V(A)(1), https://www.federalregister.gov/documents/2024/03/01/2024-03793/trade-regulation-rule-on-impersonation-of-government-and-businesses#p-42; Press Release, FTC Proposes New Protections to Combat AI Impersonation of Individuals (Feb. 15, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals (noting the importance of a trade regulation rule to improve the agency's ability to require defendants to return money to injured consumers). The Commission may be able to obtain consumer redress (such as restitution) under Section 19(a)(2) after the conclusion of an administrative process resulting in a final cease and desist order, and under Section 19(a)(1) after the violation of a rule (such as this impersonation rule).

such fraud, if the resulting consumer injury was a predictable consequence of the company's actions.[26] This counsels in favor of a "knows or should have known" standard for means and instrumentalities (M&I) liability under the FTC's Section 5 authority.

We support the FTC's application of a "knows or should have known" standard for means and instrumentalities (M&I) liability for companies whose products or services are used to facilitate impersonation scams. As we have seen with scam robocalls, discussed above, it is often nearly impossible to protect consumers by stopping the scammers themselves; it has generally been more effective and efficient to create financial incentives to discourage the voice service providers from being complicit or complacent in transmitting scam robocall traffic.[27] As FCC Commissioner Geoffrey Starks noted in 2021: "illegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it."[28]

Similarly in the impersonation scam context, the Commission should create financial incentives to discourage complicity and complacency among providers of products or services that could be used to facilitate impersonation scams. Actual knowledge alone is not an appropriate standard, as a company should have a strong financial incentive to investigate suspicious activity prior to

---

[26] *See, e.g.*, FTC v. Neovi, No. 09-55093 at 8748, at *5 (9th Cir. 2010), https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100615neoviopinion.pdf ("Courts have long held that consumers are injured for purposes of the [FTC] Act not solely through the machinations of those with ill intentions, but also through the actions of those whose practices facilitate, or contribute to, ill intentioned schemes if the injury was a predictable consequence of those actions."). There have also been relevant FTC actions not yet ruled on by a court that put businesses on notice that they can be held liable for this misconduct, *see e.g.* Amended Compl, FTC v. Walmart, 1:22-cv-03372 at ¶¶ 34, 37, 47, 48, 53-54, 93, 97, 102-03, 110, 111, 167 (N.D. Ill. June 03,2023), https://www.ftc.gov/system/files/ftc_gov/pdf/x220026walmartfiledamendedcomplaint.pdf (discussing awareness of fraud, obligations, and failure to detect and prevent fraud as a Section 5 violation); Compl., FTC v. MoneyGram International Inc., 1:09-cv-06576 at ¶¶ 38, 47, 76, 83 (N.D. Ill. Oct. 19, 2009), https://www.ftc.gov/sites/default/files/documents/cases/2009/10/091020moneygramcmpt.pdf (noting fraud reports, failure to mitigate fraud, and related Section 5 violations); Press Release, MoneyGram to Pay $18 Million to Settle FTC Charges That it Allowed its Money Transfer System to be Used for Fraud (Oct. 20, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/10/moneygram-pay-18-million-settle-ftc-charges-it-allowed-its-money-transfer-system-be-used-fraud ("The FTC's complaint alleges that MoneyGram ignored warnings from law enforcement officials and even its own employees that widespread fraud was being conducted over its network, claiming that proposals to deal with the problem were too costly and were not the company's responsibility.").

[27] *See, e.g.*, Telemarketing Sweep Press Release; Scam Robocalls Report; Press Release, 50 Attorneys General form a bipartisan task force to combat robocalling (Aug. 2, 2022), https://ncdoj.gov/attorney-general-josh-stein-leads-new-nationwide-anti-robocall-litigation-task-force/ ("I'm proud to create this nationwide task force to hold companies accountable when they turn a blind eye to the robocallers they're letting on to their networks so they can make more money."); Complaint and Demand for Jury Trial, State of Arizona ex rel. Mayes, et al. v. Michael D. Lansky, LLC, dba Avid Telecom, et al., Case No. 4:23-cv-00233 at ¶¶ 109-11, 298, 301-04 (D. Az. May 23, 2023) (noting VoIP provider had to be aware that it was trafficking in illegal robocalls due to publicly cited violations against its upstream providers and due to direct reports from downstream providers, yet the provider continued to transmit illegal calls).

[28] *In re* Call Authentication Trust Anchor, Further Notice of Proposed Rulemaking, WC Docket No. 17-97 (Sept. 30, 2021) (Statement of Comm'r Geoffrey Starks).

obtaining actual knowledge that its offerings are being used to perpetrate fraud. As such, where a provider fails to take action to prevent scams despite having received notice, or despite having access to data from which that provider should have detected fraudulent behavior, or despite having some other reason to suspect that their offerings have been used to facilitate scams, that failure to act should result in liability. The FTC has stated that penalties for rules violations can be helpful to deter misconduct.[29] This is the kind of financial incentive that will promote consumer protection and will discourage complicity and complacency regarding fraud.

We also urge the Commission to consider how it might mitigate any friction created by Section 230-based legal challenges to its rule, however meritless those challenges may be.[30] The Commission should communicate clearly to companies that if any provision of its rule is found unenforceable against one or more entities, it remains enforceable in all other respects and against all other entities covered by the rule, implementing a rule amendment if the Commission feels that is necessary. Although Section 230 has a narrow scope,[31] some courts have regrettably misconstrued Section 230 as creating a broad grant of immunity for platforms and even stretched the notion of what constitutes a platform.[32] As such, the FTC should emphasize that each provision of its impersonation rule remains in effect against other entities even if a provision may be stayed or be determined to be invalid against one or more entities. We note in particular that creators of generative AI tools are unlikely to enjoy Section 230 immunity when the tool materially contributes to the violative content.[33] More broadly, Section 230 does not protect a company from claims that target its own obligations not to cause harm.[34] We again point to court-recognized obligations companies have to prevent predictable consumer harm;[35] this

---

[29] *See, e.g.*, Fed. Trade Comm'n, Notices of Penalty Offenses, https://www.ftc.gov/enforcement/penalty-offenses (last visited Apr. 24, 2024) ("Civil penalties can help the Commission deter conduct that harms consumers. Because they can exceed what a wrongdoer earned through their misconduct, penalties send a clear message that preying on consumers will not be profitable.").

[30] *See, e.g.*, U.S. v. Stratics Networks Inc., No. 23-CV-0313-BAS-KSC, 2024 WL 966380 (S.D. Cal. Mar. 6, 2024); EPIC, NetChoice v. Bonta, EPIC.org, https://epic.org/documents/netchoice-v-bonta/ (last visited Apr. 24, 2024).

[31] *See, e.g.*, EPIC, In re: Casino-Style Games Litigation, EPIC.org, https://epic.org/documents/in-re-casino-style-games-litigation/ (last visited Apr. 24, 2024); Statement of Commissioner Rebecca Kelly Slaughter Regarding the Presentation on the Telemarketing Sales Rule Amendments as Prepared for Delivery, Fed. Trade Comm'n Open Meeting (Mar. 21, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/March24OCMTSRStatementSlaughterFinal_0.pdf ("I won't unpack all the deficiencies in the court's application of 230's liability shield right now but I'm confident the court got it wrong here. When companies actively facilitate—and profit from—lawbreaking, we have to be able to hold them to account and at the very least we should have the opportunity to prove our case in court.").

[32] *See, e.g.*, Stratics *supra* note 30; Br. of Amicus Curiae Electronic Privacy Information Center in Support of Neither Party, Gonzalez v. Google, No. 21-1333 at Section II (9th Cir. Dec. 7, 2022), *available at* https://epic.org/documents/gonzalez-v-google/; Carrie Goldberg, *Winning Through Losing*, Americanbar.org (Dec. 18, 2020), https://www.americanbar.org/groups/diversity/women/publications/perspectives/2021/december/winning-through-losing/ (discussing Herrick v. Grindr case).

[33] *See, e.g.*, EPIC, *Generating Harms: Generative AI's Impact & Paths Forward* at 20-22 (May 2023), https://epic.org/documents/generating-harms-generative-ais-impact-paths-forward/.

[34] *See id.* at 19-20.

[35] *See, e.g.*, Neovi *supra* note 26.

suggests that Section 230 should not apply in nearly any instance of M&I liability under a "knows or should have known" standard.

IV. The Commission should clarify that its proposed prohibition on individual impersonation covers impersonation of both specific individuals *and* affiliations, to unlock immediate civil penalty authority for such deceptive misconduct.

Fraudsters need not impersonate a specific individual, real or fictitious, to effectively defraud consumers. While most impersonation scams rely on impersonations of specific individuals or entities, others may instead rely on fraudulent assertions of affiliation or expertise. For example, many recovery scams—scams targeting recent victims of fraud—tend to rely on victims' deference to authoritative or trustworthy types of individuals: lawyers, fraud investigators, consumer advocates, and so forth.[36] A successful recovery scammer need not impersonate a specific individual so long as she fraudulently borrows the social trust and expertise of a chosen profession or affiliation that the victim trusts or seeks to support.[37] In certain circumstances, fraudsters may even succeed while using their real names; the deception stems not from any personal identity but instead from an affiliation. While this would clearly constitute a deceptive act or practice, codifying it under an impersonation rule will make it easier for the FTC to seek civil penalties.

The proliferation of consumer-facing AI chatbots and other generative AI tools dramatically increases the likelihood of consumer scams tied to this type of fraud. Many generative AI tools use models built on data scraped from publicly available websites, including social media sites and online forums rife with misinformation and fraud.[38] When companies scrape these sites for data, they rarely filter the content they receive before training and testing their models. As a result, many generative AI tools are trained on—and may parrot back—information connected to

[36] *See Refund and Recovery Scams*, FTC Consumer Advice (Dec. 2023), https://consumer.ftc.gov/articles/refund-and-recovery-scams; Damian Chmiel, *Hundreds of Polish FX and Crypto Traders Lose Millions in "Fool Me Twice" Fraud Scheme*, Finance Magnates (Nov. 23, 2023), https://www.financemagnates.com/forex/hundreds-of-polish-fx-and-crypto-traders-lose-millions-in-fool-me-twice-fraud-scheme/.

[37] *See, e.g.*, Press Release, FTC and States Combat Fraudulent Charities That Falsely Claim to Help Veterans and Servicemembers (July 19, 2018), https://www.ftc.gov/news-events/news/press-releases/2018/07/ftc-states-combat-fraudulent-charities-falsely-claim-help-veterans-servicemembers; Uncle Sham? FTC challenges company's Made in USA and military claims (Dec. 6, 2023), https://www.ftc.gov/business-guidance/blog/2023/12/uncle-sham-ftc-challenges-companys-made-usa-military-claims.

[38] *See* Emma Fletcher, *Social Media: A Golden Goose for Scammers*, FTC Data Spotlight (Oct. 6, 2023), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers; Thomas Claburn, *How to Spot OpenAI's Crawler Bot and Stop it Slurping Sites for Training Data*, Register (Aug. 8, 2023), https://www.theregister.com/2023/08/08/openai_scraping_software/; Sara Morrison, *The Tricky Truth About How Generative AI Uses Your Data*, Vox (July 27, 2023), https://www.vox.com/technology/2023/7/27/23808499/ai-openai-google-meta-data-privacy-nope.

fraud schemes.[39] For example, an accountant's AI chatbot may present findings that *appear* convincingly crafted by lawyers or financial advisers, even when the findings are false, misleading, or otherwise harmful to consumers. This phenomenon goes beyond the intentional training and use of generative AI to defraud consumers as well;[40] even well-intended AI chatbots on legitimate websites may share false, deceptive, or otherwise harmful information labeled as trusted advice from lawyers, doctors, or other trusted professions. Here, as above, consumers are deceived not by the impersonation of any specific individual, but by the perceived authority of a trusted affiliation or profession.

To effectively capture the nuance of impersonated affiliation, the Commission should amend its proposed § 461.4, "Impersonation of Individuals Prohibited," to cover unlawful conduct by persons who misrepresent that they are or are affiliated with an individual *or type of individuals* (a profession like doctor or membership like veteran). Without this clarification, the Commission risks creating a small, but growing, loophole in its approach to impersonation scams.

V. Conclusion

We congratulate and thank the Commission for its important progress in protecting Americans from imposter scams.

Respectfully submitted, this the 30th day of April 2024, by:

Chris Frascella
Counsel

Maria Villégas Bravo
Law Fellow

Grant Fergusson
Equal Justice Works Fellow

Enid Zhou
Senior Counsel

Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

[39] *See* Sara Fischer, *Exclusive: GPT-4 Readily Spouts Misinformation, Study Finds*, Axios (Mar. 21, 2023), https://www.axios.com/2023/03/21/gpt4-misinformation-newsguard-study; Emily M. Bender et al., *On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?*, Proc. 2021 ACM Conf. on Fairness, Accountability, & Transparency 610, 615–618 (2021).

[40] *See, e.g.*, Oli Buckley & Jason R.C. Nurse, *Cybercriminals Are Creating Their Own AI Chatbots to Support Hacking and Scam Users*, Conversation (Feb. 8, 2024), https://theconversation.com/cybercriminals-are-creating-their-own-ai-chatbots-to-support-hacking-and-scam-users-222643.