Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	)	R207000
Impersonation NPRM	)	
	)	

COMMENTS OF NCTA – THE INTERNET AND TELEVISION ASSOCIATION

NCTA – The Internet and Television Association (NCTA)[1] respectfully submits these comments in response to the Federal Trade Commission (FTC or Commission) Notice of Proposed Rulemaking (NPRM) in the above-captioned proceeding.[2] The NPRM seeks comment on the proposed trade regulation rule to prohibit impersonation of government, businesses, or their officials.

INTRODUCTION AND SUMMARY

Impersonation scams are prevalent, persistent, and pernicious. Fraudulent imposter schemes cause significant injury to consumers and businesses nationwide, including harm to cable operators, cable program networks, and their customers. NCTA member companies continue to see widespread fraud and deception, with evolving and increasingly sophisticated and technical types of business impersonation and other impersonation scams. As described

[1] NCTA – The Internet & Television Association represents network innovators, content creators, and voice providers that connect, entertain, inform, and inspire consumers nationwide. NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving approximately 90 percent of the nation's cable television households and more than 200 cable program networks with a rich history of creating award-winning programming. The cable industry is also a leading provider of broadband service after investing more than $250 billion over the last two decades to build two-way interactive networks with fiber optic technology. NCTA's cable TV programming members increasingly stream movie and television content over those broadband services, as well as other internet and wireless-based services. Cable companies also provide state-of-the-art competitive voice service to more than 30 million customers.

[2] Trade Regulation Rule on Impersonation of Government and Businesses, 87 Fed. Reg. 62741 (Oct. 17, 2022) (to be codified at 16 C.F.R. Part 461).

more fully in NCTA's Comments on the FTC Advance Notice of Proposed Rulemaking and in Section I below, NCTA member companies dedicate significant resources to combat impersonation fraud in its many forms and work diligently to identify and stop scammers, assist law enforcement agencies, educate customers and businesses about common scams and fraud prevention, and undertake technological mitigation efforts. [3]

As discussed in Section II.A below, NCTA supports enactment of narrowly crafted FTC rules to prohibit impersonation of government and businesses, along with robust investigation and enforcement, as a meaningful tool to stop and deter such fraud and to redress victims. Section II.B cautions, however, that the proposed rule to prohibit providing the means and instrumentalities (M&I) for such impersonation scams is overbroad and could have unintended consequences. NCTA urges the FTC to clarify that liability requires both providing *deceptive* means and instrumentalities, *e.g.,* providing false or misleading claims or counterfeit items, and *actual knowledge* that the deceptive representations or goods will be used to commit impersonation violations. In this way, the FTC could hold those who intentionally enable impersonation schemes accountable in appropriate circumstances, while shielding legitimate business activities and services from potential liability. In Section II.C, NCTA also suggests that the Commission continue to consider enactment of a rule to prohibit impersonation of individuals.

I. IMPERSONATION SCAMS ARE A PERSISTENT PREVALENT FRAUD.

The FTC record in this proceeding is replete with evidence that government and business impersonation is prevalent and deceptive under Section 5 of the FTC Act. The NPRM includes

[3] NCTA, Cmt. on ANPR (Feb. 22, 2022), https://www.regulations.gov/comment/FTC-2021-0077-0169 ("NCTA's ANPR Comments").

data collectively showing millions of complaints about impersonation scams resulting in billions of dollars of consumer injury.[4]

With respect to the cable industry, NCTA's previous comments outlined schemes involving impersonation of cable operators' brands, employees, and other representatives, including payment scams and unauthorized reselling scams.[5] Our programming members also have seen fraudulent use of their company logos, brands, and characters in payment scams and other impersonation schemes such as: fake job postings used for phishing schemes; scams to sell pirated content, NFTs, or cryptocurrency; or scams to market vaping products (which suggest an effort to target underage users). Since the previous NCTA Comments, NCTA member companies also have reported a recent uptick in more sophisticated and technical scams involving impersonation of customer service representatives, often in efforts to steal service for the scammers themselves or to dupe consumers into providing payment or other sensitive personal information.

Some member companies also report sophisticated schemes to compromise customers' home networks, route traffic through residential IP addresses, and essentially impersonate residential broadband subscribers online for a variety of illegal purposes, including piracy and online fraud. This type of "RES IP" scam can harm consumers and put them at risk of liability for the fraudulent activity conducted under the guise of their residential IP address. All these impersonation scams can damage company brands, interfere with customer relationships, and result in financial losses to consumers and businesses.

---

[4] NPRM, 87 Fed. Reg. at 62748-49; *see also* FTC Press Release, New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021 (Feb. 22, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0 (stating that more than $2.3 billion of consumer losses reported last year were due to imposter scams, nearly double the $1.2 billion amount reported in 2020).

[5] NCTA's ANPR Comments at 3.

NCTA member companies have undertaken significant efforts to reduce these scams' prevalence. Our member companies work with law enforcement to identify the fraudsters, file civil complaints against bad actors when they can be found, undertake security mitigation efforts, and provide a plethora of consumer and business education. For example, NCTA member companies host dozens of webpages devoted to educating both consumers and businesses about common scams including phishing, fake emails, and caller ID spoofing,[6] and alerting consumers about impersonation scams involving their brands.[7]

II. NCTA SUPPORTS ENACTMENT OF NARROWLY CRAFTED RULES TO PROHIBIT IMPERSONATION FRAUD, *PROVIDED* THAT ANY LIABILITY FOR "MEANS AND INSTRUMENTALITIES" IS CAREFULLY TAILORED.

A. The Commission Should Enact Targeted Rules to Prohibit Government and Business Impersonation.

NCTA supports enactment of narrowly tailored rules prohibiting impersonation of government and businesses – along with rigorous enforcement – as means to penalize bad actors and deter fraudulent conduct. NCTA recognizes that a recent U.S. Supreme Court decision[8] has significantly hampered the FTC's ability to seek efficient and effective relief in enforcement actions against impersonation fraud without a related rule violation. The FTC's proposed impersonation rules would make it "unlawful to falsely pose as or to misrepresent, directly or by implication, affiliation with, including endorsement or sponsorship by" a government entity or officer (proposed 16 C.F.R. § 461.2) or a business or officer thereof (proposed 16 C.F.R. § 461.3). These one-sentence rules prohibiting government and business impersonation, modeled

[6] *E.g.,* https://www.spectrum.net/support/internet/protecting-against-online-and-phone-scams; https://www.spectrum.net/support/voice/caller-id-spoofing; https://www.xfinity.com/support/articles/phishing-scams.
[7] *E.g.,* https://internetsecurity.xfinity.com/help/alerts; https://www.cox.com/residential/support/about-fake-cox-emails.html#:t; https://www.paramount.com/recruiting-fraud-statement.
[8] *AMG Capital Mgmt., LLC v. FTC*, 141 S. Ct. 1341 (2021).

on language in the FTC's Telemarketing Sales Rule (TSR),[9] would expand the FTC's remedies, enabling it to obtain civil penalties and consumer redress for rule violations.[10]

B. The Commission Should Clarify That Any Liability for Providing the Means and Instrumentalities for Impersonation Fraud Requires Actual Knowledge.

NCTA cautions the Commission that an overly broad rule prohibiting provision of the means and instrumentalities for impersonation scams would have unintended consequences of interfering or deterring legitimate commercial activities, and compound the harm caused by fraudsters to consumers and small, medium and large businesses. Clarifying that liability stems from actual knowledge that the means and instrumentalities provided are for impersonation fraud would strike the right balance of empowering the FTC's enforcement efforts and protecting legitimate businesses and consumers.

If the FTC decides to enact a rule to prohibit providing the means and instrumentalities for impersonation fraud, the rule should be carefully scoped. Specifically, it should bar only the means and instrumentalities that are inherently misleading (such as deceptive claims or counterfeit goods) and penalize the provider only when it has actual knowledge that the means and instrumentalities will be used in impersonation violations. This clarification would permit

---

[9] 16 C.F.R. § 310.3(a)(2)(vii).

[10] We also encourage Commission efforts to restore access to "Whois" data about domain name owners, including continued advocacy before Congress and ICANN, to help combat impersonation fraud. Whois data about domain name registrants has become harder to access because of a misinterpretation of the European Union's General Data Protection Regulation. The NPRM states that the proposed rules prohibiting impersonation would cover, among other things, creating a website impersonating a business. NPRM, 87 Fed. Reg. at 62746-47. The FTC has long emphasized that Whois data is a critical tool for investigation and enforcement against fraudulent websites. *See, e.g., Prepared Statement of the Federal Trade Commission Before the Internet Corporation for Assigned Names and Numbers Meeting Concerning Whois Databases* (June 26, 2006) https://www.ftc.gov/system/files/documents/public_statements/417701/p035302whoisdatabases.pdf; *Prepared Statement of the Federal Trade Commission on the Integrity and Accuracy of the "WHOIS" Database, Hearing Before the Subcomm. on Courts, the Internet, & Intellectual Property of the H. Comm. on the Judiciary*, 107th Cong. (May 22, 2002), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-whois-datebase/whois.pdf.

the Commission to target bad actors without stifling legitimate business activity. Honest businesses should not be subject to potential liability if, without their knowledge and intentional support, their non-deceptive business identities, networks, logos, marketing materials, or other products or services are misused by impostors. In those situations, small businesses may be victims of impersonation fraud themselves; an overly broad FTC rule would compound the harm caused by bad actors.

The impersonation scam rules proposed in the NPRM include a short, one-sentence M&I prohibition in proposed Section 461.4: "It is unlawful to provide the means and instrumentalities for a violation of § 461.2 and § 461.3." The proposed rule would thereby seemingly impose direct liability for the providers – even if they have no idea that their products or services are being used to engage in a deceptive impersonation scheme.

The NPRM notes that FTC case law describes a form of liability for a party who, despite not having direct contact with injured consumers, "passes on a *false or misleading* representation *with knowledge or reason to expect* that consumers may possibly be deceived as a result."[11] The NPRM, however, does not include any further discussion of the deceptive nature of the instrumentalities or the knowledge required to hold a party liable for providing the means and instrumentalities for impersonation fraud, nor are these elements incorporated in the proposed rule. This leaves open the possibility that parties could be subject to enforcement actions for their unwitting or tangential provision of legitimate goods or services to impostors, including if they are the victims of scams. For example, taking the proposed rule on its face, a broadband provider

[11] *Shell Oil Co.*, 128 F.T.C. 749 (1999) (emphasis added) (cited in NPRM, note 131 & accompanying text); *see also* Jessica Rich, *The FTC's Proposed Impersonation Scam Rule – Not as Straightforward as it Looks* (Nov. 21, 2022) https://www.adlawaccess.com/2022/11/articles/the-ftcs-proposed-impersonation-scam-rule-not-as-straightforward-as-it-looks/ (former Director of the FTC Bureau of Consumer Protection discusses the need to clarify a knowledge standard for means and instrumentalities violations in the final impersonation rule, stating that M&I cases often (but not always) include evidence of knowledge, with entities charged with deliberately furnishing deceptive claims or materials).

could be liable simply for providing internet service to a customer, without any knowledge that the customer is using the service to perpetrate impersonation fraud.

A knowledge standard for M&I liability would address the harms of impersonation fraud without exposing unwitting businesses or consumers to unnecessary liability or risk. It is also supported by the record. Notably, the bipartisan National Association of Attorneys General (NAAG), which is uniquely experienced in enforcement actions against impersonation scams, stated that "[i]mpersonators often use other companies' products and services to execute their scams," citing a list of companies, services, and platforms used to reach consumers.[12] NAAG opined that a company could be held responsible under the proposed impersonation rule when it "provides substantial assistance or support to impersonators *and knows* or should have known that their products or services are being used in a fraudulent impersonation scheme."[13] NAAG explains:

> To be clear, businesses are often victims themselves, and often are partners with regulators in investigations of imposter schemes. But, when a business makes an intentional decision to substantially support or to willfully ignore an imposter scheme that does harm consumers, they should be held accountable for their part in that harm.[14]

Accordingly, if the Commission enacts a rule imposing M&I liability, that liability should be predicated on actual knowledge that deceptive means and instrumentalities provided to another will be used to commit impersonation fraud. For example, language could be added to the proposed rule to clarify: "It is unlawful to provide the deceptive means and instrumentalities

---

[12] NAAG, Cmt. on ANPR at 8 (Feb. 22, 2022), https://www.regulations.gov/comment/FTC-2021-0077-0152.

[13] *Id.* at 10 (emphasis added) (citing cases in other consumer fraud contexts to illustrate standards that could be applied when there is sufficient evidence of culpability in contributing to fraudulent impersonation schemes).

[14] *Id.* at 11; s*ee also* USTelecom Cmt. on ANPR at 4 (Feb. 22, 2022), https://www.regulations.gov/comment/FTC-2021-0077-0160 ("Should the Commission move forward with impersonation rules, it should make clear that liability for providing the means and instrumentalities of impersonation fraud requires proof of knowledge of such fraud or conscious avoidance of it, consistent with FTC precedent and TSR and Section 5 jurisprudence.").

for a violation of § 461.2 and § 461.3 to a person when the provider knows that the person is engaged in an act or practice that violates §§ 461.2 and 461.3 of this Rule."

An express requirement of deception and actual knowledge is crucial for imposition of M&I liability. Without specifying such a standard, an M&I rule could have the perverse effect of quashing the provision of legitimate business products and services and deterring companies' well-meaning efforts to monitor and investigate potential impersonation fraud, for fear that any general awareness gained could be used to impose potential liability against them.[15]

C. The Commission Could Consider Further Rules to Prohibit Impersonation of Individuals.

The NPRM asks whether the proposed rule should be expanded to address the impersonation of individuals, such as the impersonation of romantic partners or grandparents in scams seeking monetary payment or contribution.[16] A new rule to prohibit impersonating individuals – including through unauthorized use of an individual's online credentials, accounts, IP addresses, and digital networks – is worth further consideration. As noted above, NCTA member companies have seen an increase in sophisticated "RES IP" scams to impersonate customers online and route traffic through their home networks and residential IP addresses. A further rulemaking proceeding could also be useful to develop a deeper record of various types of individual impersonation scams in interstate commerce.

---

[15] *See id.* at 3-4 ("This knowledge element is critical, because it protects those whose involvement in the illegal activity was purely incidental. Without it, an innocent entity whose ordinary course of work brought it – unknowingly – into contact with a bad actor could find itself facing enforcement and liability.").

[16] Expanding the proposed rule to prohibit impersonation of individuals would not (and should not) cover portrayals ("impersonations") of individuals in television or film content. As the Commission explained in the NPRM, the impersonation rule would not prohibit impersonation in artistic or recreational costumery or impersonation in connection with political or other non-commercial speech, because the misrepresentation must be "material" and "in or affecting commerce." The proposed impersonation rule "sweeps no more broadly than the existing prohibition against unfair and deceptive practices in Section 5 of the FTC Act." NPRM, 87 Fed. Reg. at 62747.

CONCLUSION

NCTA and its member companies appreciate the FTC's work to monitor and investigate government and business impersonation scams, to hold bad actors accountable, and to redress victims. As discussed above, we support the FTC's efforts to strengthen its tools to combat and deter this fraud, including narrowly crafted new rules designed to subject bad actors to liability and civil penalties, while protecting legitimate business activity. We stand ready to assist the FTC with its enforcement and educational efforts.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Joni Lupovitz
NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W., Suite 100
Washington, DC 20001-1431
(202) 222-2445

December 16, 2022