Comments of Consumer Reports

In Response to the
Federal Trade Commission
Supplemental Notice of Proposed Rulemaking on Impersonation
Impersonation SNPRM, R207000

By Justin Brookman, Director of Technology Policy Grace Gedye, Policy Analyst

April 30, 2024



(1) Should the Commission amend the Impersonation Rule to include a prohibition of impersonation of individuals? Why or why not?

Yes, Consumer Reports¹ supports the Commission's proposal to include a prohibition of impersonation of individuals. Impersonation scams — including scams where the fraudster impersonates a consumer's family members and professional contacts — are prevalent, and cost consumers billions of dollars in losses per year (see *infra* Question 2a). These scams are clearly commercial — not just personal — in nature, and well within the FTC's remit. Fraud is a core consumer protection issue, and the rule falls squarely within the FTC's Section 5 authority.

Individual impersonation scams can be uniquely violating and scary, often playing on a consumer's fear that a loved one is in dire need. In one common scam, sometimes referred to as the 'Grandparent' scam, the fraudster will impersonate (or generate an impersonation of) a consumer's grandchild, child, or other family member, claiming they've been in an accident or have been arrested, and need urgent financial assistance. When Consumer Reports asked our members about individual impersonation scams, they shared stories of scammers impersonating family members and leaving them feeling "vulnerable", "shaken by the experience" and "really weirded out." (See the appendix for more on consumers' experiences with impersonation scams.)

Artificial intelligence programs capable of accurately mimicking specific voices can supercharge impersonation scams. While fraudsters don't need a particular voice to imitate a bank or government employee, replicating a family member's voice makes the 'grandparent' scam far more believable. AI voice cloning software is cheap and readily accessible. As the FTC has noted, some tools require only a brief snippet of a person's voice – potentially scraped from publicly available social media videos – to create a convincing clone. Some families have reportedly sent as much as \$15,000 after thinking they've spoken to a loved one in need, only to

¹ Founded in 1936, <u>Consumer Reports</u> (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

² Paul Schwartzman and Pranshu Verma, *Baltimore principal's racist rant was an AI fake. His colleague was arrested*, Washington Post, (April 26, 2024) https://www.washingtonpost.com/dc-md-va/2024/04/26/baltimore-ai-voice-audio-framing-principal/

and Pranshu Verma and Will Oremus, *AI voice clones mimic politicians and celebrities, reshaping reality,* Washington Post, (October 15, 2023) https://www.washingtonpost.com/technology/2023/10/13/ai-voice-cloning-deepfakes/

³ Alvaro Puig, *Scammers use AI to enhance their family emergency schemes*, Federal Trade Commission, (March 20, 2023), https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes

realize later they were conversing with a synthetic voice.⁴ Consumer Reports' members shared experiences where they received calls from people who sounded *exactly* like their family members:

- "The voice on the other end sounded just like my grandson and it said 'Gramie, I've been in an accident,'" Robert, Florida
- "I was skeptical, and told him I had heard of scams such as this. So, he said, 'I'll let Nate say a few words to you.' It sounded exactly like my Nate!! He has a rather unusual voice, so I was then almost convinced," Barbara, Indiana
- "I received a phone call from my grandson explaining that he was in a car accident at college and needed \$5,000. He sounded scared and upset and asked that I not tell his parents. So, I went to my bank to get the money and the bank teller told me it was a scam. I did not believe her as I was sure it was my grandson's voice," Anonymous, New York
- "The phone rang and a voice said, 'Hi Gramma, this is Mac. I'm in New Jersey with my friend Chris. We had an accident. I broke my nose.' I immediately knew it wasn't my grandson. He calls me Gramma Beth...and he'd have no reason to be in New Jersey. He's New York, born and bred...The voice did sound exactly like him, however, and I could easily have been duped. I hung up," Beth, New York
- "My Grandpa got a call from someone claiming to be me. Supposably, I was traveling, and my car broke down and I needed to have him send money so I could complete my travels. Grandpa said there was no doubt in his mind that I was the caller and was preparing to do as asked. Luckily, before he went through with the transaction, he reasoned that if I was in trouble and honestly needed money, he would have heard from my mom....Scary that the tools they use could imitate my voice that closely as to fool a close relative," Shawn, Minnesota
- "I received a call and heard my daughter crying hysterically! She wasn't making sense so an 'officer' took over the call. He stated I needed to come right away but would not answer my questions. Thankfully I have Life360 and looked to see where my daughter was at and it showed her at home. ... To hear my daughter's crying voice shook me for a long time!" Chris, Minnesota
- "The initial caller's voice sounded very much like my nephew's. He knew family details, pleaded with me not to call his father and promised to pay me back as soon as he got home all very convincing. I should add that I spent more than 60 years in lawenforcement and intelligence work. This scam was so carefully arranged and executed that I fell for it nevertheless," Edward, Massachusetts

⁴ Pranshu Verma, *They thought loved ones were calling for help. It was an AI scam*, Washington Post (March 5, 2023), https://www.washingtonpost.com/technology/2023/03/05/ai-voice-scam/

For more on consumers' experiences with impersonation scams, see the appendix.

Consumers should not be left to fend for themselves. Consumer Reports supports the Commission's inclusion of individual impersonation in the strongest of terms.

- (2) Please provide comment, including relevant data, statistics, consumer complaint information, or any other evidence, on proposed §§ 461.4 and 461.5. Regarding each provision, please include answers to the following questions:
- (a) How prevalent is the act or practice the provision seeks to address?

Imposter scams are common. In 2023, 853,935 imposter scams were reported to the FTC's Consumer Sentinel Network.⁵ Twenty one percent of those scam reports included monetary losses, which totaled \$2.7 billion in 2023.⁶ Imposter scams were the second most frequently reported category of fraud reported to the Consumer Sentinel Network in 2023, out of the 29 categories of reports that the network tracks.

Individual impersonation scams are clearly prevalent and commercially harmful. In 2023, the FBI's Internet Crime Complaint Center received 17,823 reports of confidence/romance scams, outpacing the number of government impersonation scam complaints they received.⁷ In 2022, the median loss from family or friend imposter scams was \$1,000, and the median loss from friendship and sweetheart swindles was \$2,480 according to the National Consumers League.⁸

Of particular concern—now that AI voice cloning tools are widely available—is that phone calls are still one of the most popular ways for scammers to contact consumers. In 2023, phone calls were the second most common way that fraudsters contacted consumers, based on reports to the Consumer Sentinel Network.⁹

Common stereotypes might lead one to believe that fraud primarily harms older adults, but that's not the case. Out of the consumers who reported fraud to the Consumer Sentinel Network in 2023, 44% of 20-29 year olds reported losing money, compared 25% of 70-79 year olds.¹⁰

https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf

⁵ Federal Trade Commission, *Consumer Sentinel Network Data Book 2023*, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf ⁶ ibid

⁷ Federal Bureau of Investigation, *Internet Crime Report 2023*, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

⁸ Fraud.org, a progect of the National Consumers League, Top Scams of 2022, https://nclnet.org/wp-content/uploads/2023/02/Top-Scams-of-2022-v3_Feb2023.pdf

⁹ Federal Trade Commission, Consumer Sentinel Network Data Book 2023,

¹⁰ Federal Trade Commission, *Consumer Sentinel Network Data Book 2023*, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf

Anyone can fall victim to an impersonation scam under the right circumstances, including people with professional expertise in personal finance.¹¹

(b) What is the provision's impact (including any benefits and costs), if any, on consumers, governments, and businesses, both those existing and those yet to be started?

This provision would benefit consumers by reducing scam attempts, since the rule would prompt businesses to put safeguards in place. Clarifying legal obligations and enabling the Commission to obtain penalties and seek injunctive relief are also important benefits. Without clear guidelines and effective deterrence, many bad actors will continue to conduct and facilitate AI-powered scams as they make the assessment that the benefits outweigh the risks and consequences of being caught.

Consumers cannot reasonably avoid scam attempts; simply owning a cell phone or possessing an email address makes someone vulnerable to impersonation scams. The burden should not fall on consumers alone to protect themselves from scams.

Within the context of AI-based fraud, this provision would benefit businesses that provide tools to detect AI-generated content, by increasing the demand for quality products. The increased demand for AI and fraud detection services would also likely cause new businesses to form.

Yet another benefit to businesses would be regulatory clarity. Companies developing generative AI products are keenly aware they can be misused. Recently, OpenAI revealed it had developed a voice cloning product, but had not released it publicly, due to concerns over misuse. ¹² It appears Microsoft has also developed an AI voice cloning tool, VALL-E, but has not released it publicly so far. ¹³ In a paper about the tool, Microsoft researchers acknowledged the potential for impersonation: "Since VALL-E could synthesize speech that maintains speaker identity, it may carry potential risks in misuse of the model, such as spoofing voice identification or impersonating a specific speaker." ¹⁴ OpenAI, Microsoft, and other businesses working on generative AI products – including companies that have yet to be formed – would benefit from rules that clarify their responsibility and liability.

¹¹ Charlotte Cowels, *The Day I Put \$50,000 in a Shoe Box and Handed it to a Stranger*, The Cut, (February 15, 2024), https://www.thecut.com/article/amazon-scam-call-ftc-arrest-warrants.html

¹² Unsigned blog post from OpenAI, *Navigating the Challenges and Opportunities of Synthetic Voice*, (March 29, 2024) https://openai.com/blog/navigating-the-challenges-and-opportunities-of-synthetic-voices

¹³ Benj Edwards, *Microsoft's new AI can simulate anyone's voice with 3 seconds of audio*, Ars Technica, (January 9, 2023) https://arstechnica.com/information-technology/2023/01/microsofts-new-ai-can-simulate-anyones-voice-with-3-seconds-of-audio/

¹⁴ Chengyi Wang et. al, *Neural Codec Language Models are Zero-Shot Text to Speech Synthesizers*, (Janruary 5, 2023) https://arxiv.org/pdf/2301.02111

Companies that do not currently have reasonable safeguards in place to prevent their products and services from being used for scams may incur costs setting up those safeguards. However, the benefits to consumers outweigh these costs.

(c) What alternative proposals should the Commission consider?

Consumer Reports does not have alternative proposals for the Commission to consider. The proposal is proportionate and urgently needed.

However, we would encourage the Commission to consider issuing best practices for specific industries and products that are known to be used in impersonation fraud. That could be helpful to companies who want to ensure they comply with the rule. For example, the Commission could suggest that AI voice cloning companies put mechanisms in place that would make it difficult to make a synthetic copy of someone's voice without their consent.

(3) Does the Rule, if amended as proposed by the SNPRM, contain a collection of information?

(4) Would the Rule, if amended as proposed by the SNPRM, have a significant economic impact on a substantial number of small entities? If so, how could it be modified to avoid a significant economic impact on a substantial number of small entities?

Many entities that would be impacted by the proposed rule are large corporations, such as large telecom and technology companies, and large financial institutions. Looking at AI voice cloning technology specifically, there are not a lot of companies that make voice cloning services publicly available that could be used for deception and fraud. As mentioned above, some larger companies, such as Microsoft and OpenAI, have developed AI voice cloning tools, and then decided not to release them publicly. ¹⁵¹⁶

The cost of putting safeguards in place to prevent products from being used for fraud is a reasonable cost of doing business.

(5) The SNPRM proposes including in the amended Impersonation Rule a two-part prohibition against impersonation of individuals in § 461.4. Is this prohibition clear and understandable? Is it ambiguous in any way? How if at all should it be improved?

¹⁵ Unsigned blog post from OpenAI, *Navigating the Challenges and Opportunities of Synthetic Voice*, (March 29, 2024) https://openai.com/blog/navigating-the-challenges-and-opportunities-of-synthetic-voices

¹⁶ Benj Edwards, *OpenAI holds back wide release of voice-cloning tech due to misuse concerns*, Ars Technica, (March 29, 2024) https://arstechnica.com/information-technology/2024/03/openai-holds-back-wide-release-of-voice-cloning-tech-due-to-misuse-concerns/

Yes, this is clear.

(6) For purposes of prohibiting impersonation of individuals, should the Commission define "individual" to mean "a person, entity, or party, whether real or fictitious, other than those that constitute a business or government under this part"? Is this definition clear and understandable? Is it ambiguous in any way? How if at all should it be improved?

Yes, the definition is clear and understandable.

(7) The SNPRM proposes including in the amended Impersonation Rule a two-part prohibition in § 461.5 against providing goods or services with knowledge or reason to know that those goods or services will be used to (a) materially and falsely pose as, directly or by implication, a government entity or officer thereof, a business or officer thereof, or an individual, in or affecting commerce as commerce is defined in the Federal Trade Commission Act (15 U.S.C. 44); or (b) materially misrepresent, directly or by implication, affiliation with, including endorsement or sponsorship by, a government entity or officer thereof, a business or officer thereof, or an individual, in or affecting commerce as commerce is defined in the Federal Trade Commission Act (15 U.S.C. 44). Should the Rule be revised to contain this prohibition against providing goods or services with knowledge or reason to know that those goods or services will be used to unlawfully impersonate a government, business, or individual? Why or why not? Is the standard "know or have reason to know," which reflects current law, sufficiently clear and understandable? Is it ambiguous in any way? How, if at all, should it be improved?

In general, companies should take reasonable steps to prevent consumer harms that could arise from the use of their platforms, products and services. This is consistent with nineteen years of FTC holdings that companies have data security obligations to protect consumers from malicious behavior by third-party actors.¹⁷

The Commission has derived this important principle from its Section 5 unfairness authority, which holds that companies are prohibited from engaging in behavior that (1) causes consumers significant injury that is (2) not reasonably avoidable by consumers and (3) is not offset by countervailing benefits to consumers or competition. In the data security context, the Commission has reasoned that failure to take reasonable remedial actions in response to external threats can cause consumers unavoidable injury that is not outweighed by lower costs or other benefits.

¹⁷ See Press Release, BJ's Wholesale Club Settles FTC Charges, (Jun. 16, 2005), Fed. Trade Comm'n., https://www.ftc.gov/news-events/news/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges; Press Release, DSW Inc. Settles FTC Charges, (Dec. 1, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/12/dsw-inc-settles-ftc-charges.

Even outside of the data security context, the FTC has used its authority to take action against platforms that fail to address fraudulent practices conducted by third-parties by taking reasonable interventions. ¹⁸ The Commission should similarly hold that companies have a duty to take reasonable actions to prevent the use of their services or products for impersonation scams.

"Know or have reason to know" is sufficiently clear as a standard of knowledge, but the proposed language leaves a bit of ambiguity over how far companies are expected to go if they have reason to know their product or service will be used as the "means or instrumentalities" for an impersonation scam.

Internet service providers certainly know that scams are conducted via their service. Telecom companies know that fraudsters use phones and cellular networks to take advantage of people. What, exactly, should they do?

Consumer Reports proposes a reasonableness standard: Companies that know or have reason to know they are providing the means and instrumentalities for impersonation scams must take reasonable measures to protect consumers. A component of the reasonableness standard should be countervailing consumer benefits. For the company's anti-scam measures to be 'reasonable', the benefits to consumers of each of those measures should outweigh the benefits to consumers of *not* taking such actions. Put differently, companies should marshal all the strategies at their disposal to prevent their tools from being used for fraud – including not offering a certain products in the first place – up and until the drawbacks to consumers of those strategies overcome the benefit of fraud reduction. A reasonableness standard would also align with the Commission's prior communications on deepfakes and voice cloning tools. ¹⁹ Without a reasonableness standard, companies could pursue fraud detection strategies that are overly invasive, or are harmful to consumers in other ways that may outweigh the benefit of scam reduction.

Some of the knowledge standards proposed by industry groups in comments for the proposal regarding impersonation of businesses and government entities are patently insufficient. An "actual knowledge" standard, which was proposed by NCTA, would incentivize companies to essentially put their heads in the sand. Companies that wish to avoid liability could choose not to gather any information that would reveal that their products or services are being used for fraud. NCTA also proposed that liability only apply when "inherently deceptive means and instrumentalities" are provided. That standard would be far too narrow. There are lots of products and services that are used for legal, legitimate ends, and are also used for fraud, such as

¹⁸ See press release, *Court Orders Permanent Halt to Illegal Qchex Check Processing Operation*, Federal Trade Commission, (February 9, 2009) https://www.ftc.gov/news-events/news/press-releases/2009/02/court-orders-permanent-halt-illegal-qchex-check-processing-operation-court-finds-qchex-unfair

¹⁹ Michael Atleson, *Chatbots, deepfakes, and voice clones: AI deception for sale*, Federal Trade Commission Business Blog, (March 20, 2023), https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale

money transfer services. Those products are not inherently deceptive, but companies should still have to take reasonable steps to protect consumers.

Voice of the Net, another industry group, suggested that the "liability standard should be based on knowledge and the lack of action to prevent fraudulent activity." This is also too narrow, because companies may take actions that do not meaningfully reduce the likelihood of fraud, such as including in their terms of service agreements that their products should not be used to violate the law. Not all actions are equal, and companies should not be able to avoid liability for doing the bare minimum.

Appendix: Consumer experiences related to individual impersonation scams, from Consumer Reports' members

"The man on the phone said he was a Sheriff and had my grandson in custody. He had made the mistake of riding with buddies who were carrying pot. He, personally, had none on him, but he was an accomplice. Nate was a teacher, so it didn't fit him, but...who knows who one might ride with! I was skeptical, and told him I had heard of scams such as this. So he said, "I'll let Nate say a few words to you." It sounded exactly like my Nate!! He has a rather unusual voice, so I was then almost convinced. He did only say about 5 words. Then the other man came back on. He asked for a few thousand dollars to let him get off free. I said, "I do not have that kind of money". But he kept prodding me. Finally, he said "you must NOT tell his mother; he is afraid of her finding out." And I thought Now this is too weird. I'm not that stupid. So, I hung up and called her, and she called Nate where he was teaching, to satisfy me. She never did buy it even for a second, but I wasn't sure. Both got a laugh out of it, but I was really weirded out. THAT VOICE WAS NATE'S." – Barbara, Indiana

"I received a phone call from my grandson explaining that he was in a car accident at college and needed \$5,000. He sounded scared and upset and asked that I not tell his parents. So, I went to my bank to get the money and the bank teller told me it was a scam. I did not believe her as I was sure it was my grandson's voice. The bank teller insisted that I call my daughter to check on my grandson. So, I did. My daughter said that her son, my grandson, was fine and she texted him. Within a few minutes, my grandson called me on my cellphone while I was at the bank. He told me it was not him who had called asking for money. He explained that he was not in a car accident and did not need money. I had a hard time believing that I was almost a victim of this scam." – **Anonymous, New York**

"The phone rang and a voice said, 'Hi Gramma, this is Mac. I'm in New Jersey with my friend Chris. We had an accident. I broke my nose.' I immediately knew it wasn't my grandson. He calls me Gramma Beth, kind of all run together, and he'd have no reason to be in New Jersey. He's New York, born and bred, although I have lived in New Jersey. The voice did sound exactly like him, however, and I could easily have been duped. I hung up." – **Beth, New York**

"My Grandpa got a call from someone claiming to be me. Supposably, I was traveling, and my car broke down and I needed to have him send money so I could complete my travels. Grandpa said there was no doubt in his mind that I was the caller and was preparing to do as asked. Luckily, before he went through with the transaction, he reasoned that if I was in trouble and

honestly needed money, he would have heard from my mom. He chose not to be at his phone when they called back as he was not sure he could have said no to his grandson. Scary that the tools they use could imitate my voice that closely as to fool a close relative." – **Shawn,**

Minnesota

"I had a phone call from someone that impersonated my brother's voice saying that he was in trouble and that he needed money immediately which I found very disturbing because the phone hung up. The call also said his name but apparently it wasn't his direct phone line. This type of technology can be dangerous in so many ways and is so unnecessary. We can remain to live how we have been without it. I think that in some instances the government may need this technology but I think normal society needs to be without reach of this." – **Mandy, Texas**

"I received a call and heard my daughter crying hysterically! She wasn't making sense so an 'officer' took over the call. He stated I needed to come right away but would not answer my questions. Thankfully I have Life360 and looked to see where my daughter was at and it showed her at home. I hung up on the fake officer and called my daughter who assured me she was safe at home! I called the police and reported the call and they said it was a trafficking tactic! To hear my daughter's crying voice shook me for a long time!" – **Chris, Minnesota**

"Got a call on a Saturday morning from what I thought was my brother's son. Told me he had been in an automobile accident, and the police were holding him saying he was at fault. Woman driving other car was injured and in hospital. Nephew lives in Wisconsin but said he had been at a wedding in New York City and had started to drive home when the accident occurred. He needed \$500 to post bail and get out of jail. Told me a lawyer would be calling me with instructions on how to send the money. Within the hour, the lawyer called and told me to buy a money transfer card at a big box store near me and send it to the big box store's branch in New Jersey. I tried to call my brother to find out what he knew of the situation, but he didn't answer his phone.

After several unsuccessful tries to reach him, I went to the big box store and bought a gift certificate to send to New Jersey. The big box clerk tried to dissuade me from sending the money after she established that I did not know the person to whom I was preparing to send it. I told her to go ahead and send the money anyway. I left the store and tried phoning my brother once again from its parking lot. This time I had luck. He told me his son was still in Wisconsin and had not gone to any wedding in New York. I went back into the store and asked the clerk if the money had been sent. She said no. I said I would like it back and she gave it to me.

The initial caller's voice sounded very much like my nephew's. He knew family details, pleaded with me not to call his father and promised to pay me back as soon as he got home - all very convincing.

I should add that I spent more than 60 years in law-enforcement and intelligence work. This scam was so carefully arranged and executed that I fell for it nevertheless. It was only dumb luck that I got back into the big box store in time to cancel the funds transfer. I returned again later, and gave the clerk a bottle of wine and my heartfelt thanks." – **Edward, Massachusetts**

"About a week after my grandson returned to college to start his final semester of college this past January, I received a phone call from a number I didn't recognize. My husband had just been in the hospital and we were expecting a call from a doctor which is the only reason I answered the phone. The voice on the other end sounded just like my grandson and it said "Gramie, I've been in an accident". The voice sounded just like my grandson but I knew he would have been in class at that time and the phone number on caller ID was not my grandson's cell number. I paused for a few seconds because the caller knew the name (Gramie) that my grandson calls me but my instincts told me this was a fake caller. I responded "No, this isn't my grandson, you're a scammer. Why don't you go out and get an honest job". I then hung up the phone, immediately texted my grandson and daughter. My daughter had just texted with her son (my grandson) and knew he was fine. My grandson texted me back quickly and said that he was indeed in class and was not in an accident." – **Robert, Florida**

"The caller began by asking how I was; then proceeded to tell me that he was my grandson and was having a bad day. The story was that he had been in an auto accident while driving someone else's car and had been arrested (the reason for that was unclear). He said he had been examined for minor injuries and now needed bail money: \$6500! I didn't really recognize the voice, but kept talking to him because I have four grandsons and I'm only confident that I can recognize two of them over the phone. I promptly told the caller that I don't have that much cash readily accessible; I added that I would need to talk with Grandpa about this. I became more suspicious when "my grandson" gave me "his lawyer's" phone number as a person to get back to. Then he asked me not to call his "parents" because he wanted to "tell them in person about what had happened." I then was certain that this was not my grandson. I proceeded to read him the riot act about how we don't do things that way in our family, etc. Whoever he was, he got an earful. (I was concerned enough that I did verify with my daughters that none of my grandsons had been in an auto accident. I really was shaken by the experience; but having some acting experience helped me to channel my anxiety into my verbal abuse of the caller.)" — Victoria, Nebraska