Prepared Testimony of

Matthew F. Ferraro

Partner, Crowell & Moring LLP

Before the U.S. Senate Special Committee on Aging

Hearing on

"The AI Deception Machine: Deepfakes, Chatbots, and the New Frontier of Senior Fraud"

July 29, 2026

Chairman Scott, Ranking Member Gillibrand, and Members of the Committee:

Thank you for inviting me to testify before the Committee on this important topic. It is an honor to be before you today.

My name is Matthew F. Ferraro. I am a partner at the law firm Crowell & Moring LLP, where I counsel clients on matters at the intersection of artificial intelligence (AI), cybersecurity, and regulation. I am also a former government official. I served most recently as the Senior Counselor for Cybersecurity and Emerging Technology to the Secretary of Homeland Security from 2023 to 2025 and, earlier in my career, in the U.S. Intelligence Community. I have been writing, speaking, counseling clients, and working on government policy related to AI-generated media, or deepfakes, since 2019.[1] I am here today in my personal capacity. The views I express in this testimony are my own and do not reflect upon my current firm, my prior public or private employers, or any clients.

My testimony proceeds as follows:

- First, I describe prevalent forms of AI-related frauds, particularly those targeting seniors.
- Second, I discuss possible policy responses to these issues that legislators, including members of this Committee, may wish to pursue.
- Third, I provide steps seniors, and all of us, can take to avoid falling victim to deepfake dupes.

I conclude by noting that while new technologies married to ancient vices require responses, they should neither slake our appetite for innovation and creativity nor extinguish our faith that we can navigate the digital world with confidence.

[1] As used here a deepfake is a realistic piece of media manipulated or created by AI that is used maliciously as disinformation. *See* NINA SCHICK, DEEPFAKES: THE COMING INFOCALYPSE 8 (2020). I have drawn on one of my writings, a chapter on "Deepfake Deceptions and Responses," forthcoming in the American Bar Association's "Scams & Cybercrime Survival Guide," to inform this testimony.

I. Deepfake Dangers

To understand the scope of this issue, ask yourself: How often today have you relied upon the voice of a loved one or the image of a trusted figure before you shared something valuable with them?

Perhaps your daughter called from college this morning to ask for a few hundred dollars, and you dispatched the funds without a second thought. Maybe you experienced technical difficulties this afternoon while working from home and had a video call with your office's support technician, during which you shared your account information. Tonight, you may scroll through social media and see a doctor online touting the benefits of an herbal supplement and buy it because of their endorsement.

Now consider: What if those representations were fake—not your daughter or the office technician calling or a doctor in a commercial, but voices and images forged by AI? What if seeing and hearing were not believing?

Welcome to the world of "deepfakes." It is a world we have been living in for several years, where AI can create realistic audio, images, and videos that appear to be true-to-life but are forgeries. The technology to create such synthetic media is now advancing at a phenomenal rate. Nearly anyone can access it, often for free, and, when combined with the power of social media, deepfakes can scale nearly instantaneously. The aphorism, "a lie can travel halfway around the world while the truth is still putting on its shoes," has never been more apt.[2]

While AI-generated media can have creative uses that empower artistic expression, invigorate education, and enhance accessibility, deepfakes can supercharge scams and cyber frauds, especially those targeting senior citizens.

The figures are stark. In the first quarter of 2025 alone, financial losses from deepfake-enabled fraud exceeded $200 million, according to an industry report.[3] The consulting firm Deloitte expects that generative AI could enable fraud losses to reach $40 billion in the United States by 2027, up from $12.3 billion in 2023, a compound annual growth rate of 32%.[4]

Propelling this anticipated surge is an expected increase in scammers using deepfakes to induce, and then betray, trust. These scams pose particular dangers to the elderly. Older adults are five times more likely to lose money in a scam than younger people, according to the founder and

---

[2] *See* Niraj Chokshi, *That Wasn't Mark Twain: How a Misquotation Is Born*, N.Y. TIMES (Apr. 26, 2017), https://www.nytimes.com/2017/04/26/books/famous-misquotations.html.

[3] *See* Carolyn Giardina, *Deepfake-Enabled Fraud Has Already Caused $200 Million in Financial Losses in 2025, New Report Finds*, VARIETY (Apr. 17, 2025, 4:29 PM), https://variety.com/2025/digital/news/deepfake-fraud-caused-200-million-losses-1236372068/ (citing report from Resemble AI, which specializes in deepfake detection).

[4] *GenAI Poses Real Threat in Deepfake Fraud*, DELOITTE (July 10, 2024), https://action.deloitte.com/insight/3993/genai-poses-real-threat-in-deepfake-fraud.

executive director of the national nonprofit Older Adults Technology Services (OATS), a part of AARP.[5] According to an AARP survey, the top digital risk for seniors is scams and fraud.[6]

Deepfake scams can take many forms; I turn next to those most relevant to seniors.[7]

A. Advertising and Investment Scams

Fraudsters often use AI to generate fake ads featuring the likenesses of celebrities or trusted professionals, luring the unsuspecting into buying products or making investments under false pretenses.

For example, a recent *New York Times* report explored the presence of hundreds of AI-generated video "doctors, healers and wellness influencers on social media touting the health benefits of supplements to American consumers. Many of these hyperrealistic looking ads promise medical miracles, and appear to be targeting older women, while making misleading health claims for a profit."[8]

In the same vein, AI-generated videos of celebrity clones have promoted Medicare, Medicaid, and tax refunds.[9] Threat actors have also used AI-generated avatars of influencers, investors, and movie stars to peddle products from cryptocurrency and dental plans to diet pills.[10]

Using deepfakes of trusted messengers to deceive victims is a broad, international phenomenon. For example, a British advertising association reported that scam ads containing famous figures, often doctored or AI-manipulated, constituted the "vast majority" of reports the government watchdog sent to online platforms in 2024.[11]

In the United States, data from the Federal Trade Commission (FTC) showed that consumers reported losing 25% more to fraud in 2024, totaling $12.5 billion, compared to the prior

---

[5] Angelica Stabile, *Aging Adults are Most Vulnerable to These Digital Risks, Experts Say*, FOX NEWS (Mar. 30, 2025), https://www.foxnews.com/health/americas-seniors-vulnerable-digital-threats-experts-warn.
[6] *Id.*
[7] While not the subject of this hearing, two other forms of deepfake-related harms merit mention: AI-generated non-consensual intimate imagery of minors and adults and AI-generated identities to secure remote employment. *See* Matthew F. Ferraro et al., *Federal and State Regulators Target AI Chatbots and Intimate Imagery*, Crowell & Moring Client Alert (Oct. 30, 2026); Scott Wise et al., *From Deepfakes to Sanctions Violations: The Rise of North Korean Remote IT Worker Schemes*, Crowell & Moring Client Alert (Sept. 22, 2025), https://www.crowell.com/en/insights/client-alerts/from-deepfakes-to-sanctions-violations-the-rise-of-north-korean-remote-it-worker-schemes
[8] Arijeta Lajka et al., *The Fake Influencers Selling Wellness on Your Feed*, N.Y. TIMES (July 21, 2026), https://www.nytimes.com/video/technology/100000011001849/ai-influencers-health-supplements-fake-ads.html.
[9] *See* Jason Koebler, *Deepfaked Celebrity Ads Promoting Medicare Scams Run Rampant on YouTube*, 404 MEDIA (Jan. 9, 2024), https://www.404media.co/joe-rogan-taylor-swift-andrew-tate-ai-deepfake-youtube-medicare-ads/.
[10] *See* Derek Kravitz, *Don't Get Caught by a Deepfake Scam*, CONSUMER REPORTS (Jan. 30, 2025), https://www.consumerreports.org/money/scams-fraud/dont-get-caught-by-a-deepfake-scam-a1121081735/; Ben Coleman, *The Impact of Deepfakes on Brand and Reputation*, REALITY DEFENDER (Aug. 7, 2024), https://www.realitydefender.com/blog/deepfakes-harm-brand-reputation.
[11] *See* Martyn Landi, *Celebrity Deepfake Scam Ads Were Most Reported to Watchdog in 2024*, PA MEDIA (Feb. 13, 2025), https://uk.finance.yahoo.com/news/celebrity-deepfake-scam-ads-were-000100107.html (citing report from Advertising Standards Authority, a self-regulatory organization of the advertising industry in the United Kingdom).

year. And of that total, $5.7 billion were lost to investment scams, more than any other category.[12] The FTC does not break down its data by investment scams using deepfakes *per se*. Still, the FTC has generally warned that fraudsters are using celebrity deepfakes for fraudulent advertising campaigns and financial scams that have triggered FTC enforcement actions.[13]

B. Deepfake Phishing Scams

The investment and advertising scams described above are a form of what I call "broadcast falsity"; AI is used to impersonate a trusted messenger, and the message is sent out widely and not tailored to a specific victim.

"Deepfake phishing scams" is a version of these activities where threat actors target individual victims through one-to-one communication.[14] In the deepfake-enabled version of phishing, a victim receives a phone call or an email, purportedly from a figure of authority, who exhorts the victim to render payment or provide sensitive information, using an AI-generated voice or video to increase the victim's trust in the veracity of the message.

A late-2024 survey in the United Kingdom by the group Hiya estimated that 26% of UK residents received a call using a deepfake voice clone over the prior 12 months, and of those, 40% reported being scammed, 35% reported losing money, and 32% had their personal information stolen. The scams were primarily financial and banking-related. In such scams, for example, a fraudster impersonates a representative of the government's tax authority and tells the victim that a criminal case has commenced or an arrest warrant has issued against the victim to induce fear and compel the victim to provide bank details, financial information, or personally identifiable information to supposedly pay the spurious debt.[15] Hiya reported Medicare scams as the most common type of fraud call in the United States. In those schemes, scammers try to obtain personal details of victims that the fraudsters can then use to bill Medicare falsely for home health services.[16] Hiya estimates that the average American fraud call victim lost $539.[17]

C. Known-Person Impersonation Scams

The frauds discussed thus far use either entirely fictious persons or impersonations of individuals rarely acquainted with specific victims. But deepfakes are also used to mimic persons the victim knows, either professionally or personally.

---

[12] Press Release, *New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024*, FED. TRADE COMM'N (Mar. 10, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.
[13] Michael Atleson, *Chatbots, Deepfakes, and Voice Clones: AI Deception for Sale*, FED. TRADE COMM'N (Mar. 20, 2023), https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale.
[14] *See* Ellen Jennings-Trace, *Deepfake Scam Calls Are Costing British Victims Hundreds Each Time - Here's How to Stay Safe*, TECH RADAR PRO (Mar. 2, 2025), https://www.techradar.com/pro/security/deepfake-scam-calls-are-costing-british-victims-hundreds-each-time.
[15] *Id.*
[16] Press Release, *AI Deepfake Fraud Calls Dominate Q4 Scams, Costing Consumers Millions*, BUSINESS WIRE (Feb. 25, 2025, 4:00 AM), https://www.businesswire.com/ws/home/20250225398435/en/AI-Deepfake-Fraud-Calls-Dominate-Q4-Scams-Costing-Consumers-Millions.
[17] *Id.*

Among the most widely publicized recent examples of this kind of fraud came to light in early 2024, when a British multinational firm reported to law enforcement that criminals had tricked an employee into attending a video call with AI-generated deepfakes of the company's chief financial officer, among others, that the employee believed were the actual people.[18] The fraudsters convinced the employee to send the equivalent of $25.6 million through fifteen transactions to complete payment for a secret project.[19]

Fraudsters have also used deepfakes to target victims for extortion by impersonating victims' family members. Sen. John Hickenlooper (D-Colo.) described in a U.S. Senate hearing in November 2024 how "scammers have cloned the voices of loved ones saying they've been kidnapped, they've been abducted, and this familiar voice is begging for ransom payments."[20]

The earliest example of this phenomenon of which I am aware occurred in February 2020, when an attorney in Pennsylvania reported that he was fooled by what he believed was an AI-enabled voice clone of his "son," who asked for $9,000 in bail money. The distraught father nearly wired the funds to someone claiming to be the son's lawyer, but he desisted only when his actual son telephoned him.[21]

These scams led the Attorney General of the District of Columbia, Brian L. Schwalb, in April 2025 to issue a consumer alert warning of "a disturbing upward trend" of scammers telephoning residents, especially seniors, and impersonating with the help of AI "family members, friends, legitimate businesses, or government officials" and demanding money.[22] Schwalb warned the public of callers seeking personal financial information, asking for bail, claiming the resident's identity is being used in an international money laundering operation, claiming they owe back taxes or tolls, or promising a refund.[23]

D. Loneliness-related Scams

Fraudsters use AI-generated media to impersonate potential romantic partners as part of a swindle known as "catfishing" or "romance scams."[24] In such a fraud, threat actors often research

---

[18] *See* Kathleen Magramo, *British Engineering Giant Arup Revealed as $25 Million Deepfake Scam Victim*, CNN (May 17, 2024, 4:53 AM), https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html.

[19] *Id.*

[20] Justin Hendrix, *Transcript: US Senate Subcommittee Hearing on "Protecting Consumers from Artificial Intelligence Enabled Fraud and Scams"*, TECH POLICY PRESS (Nov. 20, 2024), https://www.techpolicy.press/transcript-us-senate-subcommittee-hearing-on-protecting-consumers-from-artificial-intelligence-enabled-fraud-and-scams/.

[21] *See* Matthew F. Ferraro, et al., *Identifying the Legal and Business Risks of Disinformation and Deepfakes: What Every Business Needs to Know*, 6 PRATT'S PRIV.& CYBERSECURITY L. REP. 142, 146 (2020) (describing incident).

[22] Press Release, *Attorney General Schwalb Issues Consumer Alert to Protect District Residents from Deepfake Telemarketing Scams*, OFFICE OF THE ATTORNEY GEN. FOR THE DISTRICT OF COLUMBIA (Apr. 18, 2025), https://oag.dc.gov/release/attorney-general-schwalb-issues-consumer-alert-3 (directing elder victims to report crimes to ElderJustice@dc.gov).

[23] *Id.*

[24] *See* Natalie Neysa Alund, *Why Do People Catfish? What are the Signs of It? Here's What You – and Your Kids – Should Know*, USA TODAY (Nov. 29, 2022, 3:27 PM), https://www.usatoday.com/story/news/nation/2022/11/29/what-is-catfishing-why-do-people-catfish/10794619002/;

potential victims by reviewing their social media and dating site profiles, contact the victim through social media, apps, or text messages, and seek to gain trust by developing an online relationship. The ploys can continue as the victim develops genuine feelings of connection and interest in the threat actor, potentially leading to the transfer of money, cryptocurrency, or gift cards. "The intimate and personal information victims often provide can then be used by the scammers for identity theft and financial account takeover schemes, among others," the U.S. Secret Service warns, "Scammers may even convert their victims into unwitting criminals by convincing them to launder and move fraudulent funds, for which the victim is then liable, both financially and potentially criminally."[25]

AI has supercharged these kinds of frauds by allowing criminals to create synthetic yet believable imagery to accompany their stories and create more convincing "catfish" online profiles, helping their victims believe they are engaged in a genuine relationship.[26] The scammers impersonate both everyday people and famous public figures to try to trick victims. These frauds can operate at an industrial scale often through fraud rings based overseas.[27]

II. Possible Public Responses

While it is for the Congress to fashion specific responses to the scams outlined above, I offer three general recommendations.

Education and Awareness. First, as a society, we should emphasize education and awareness by all digital media consumers, especially seniors. Any effective public education effort should be delivered through trusted community channels: senior centers, physicians, pharmacists, community groups, nonprofits, houses of worship and the like. Recent academic research has identified "[a]ge-inclusive digital literacy programs," along with other interventions as "crucial" to effective risk mitigation.[28]

The National Council on Aging recently told the *AP* that classes on AI at senior centers have become popular additions to efforts to enhance digital literacy.[29] The *AP* reported on successful efforts to educate seniors at a community center in the Chicago area, and the *Washington Post* described a similar ten-week course offered by Senior Planet, a nonprofit

---

Stay Safe Online: Avoid Romance Scams, U.S. SECRET SERVICE (undated), https://www.secretservice.gov/investigations/romancescams.

[25] *See Stay Safe Online*.

[26] *See* Paul Raffile, *A Digital Pandemic: Uncovering the Role of 'Yahoo Boys' in the Surge of Social Media-Enabled Financial Sextortion Targeting Minors*, NETWORK CONTAGION RESEARCH INSTITUTE (Jan. 2024), at 19-20, https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf.

[27] *See* Glenn Chapman, *Scammers Using AI To Dupe The Lonely Looking For Love*, BARRONS (Feb. 12, 2025, 10:07 AM), https://www.barrons.com/news/scammers-using-ai-to-dupe-the-lonely-looking-for-love-e1f6bb2c,

[28] Ansh Mittal, *Navigating the Digital Mirage: The Impact of Deepfakes and AI on Older Adults' Ability to Discern Authentic Content*, 7 INT'L J. FOR MULTIDISCIPLINARY RES. 1, 12 (2025) https://www.ijfmr.com/papers/2025/5/59035.pdf.

[29] Dan Merica, *Classes Across the Country Help Seniors Interact with a World Altered by AI*, AP (Aug. 13, 2024), https://apnews.com/article/seniors-artificial-intelligence-deepfake-education-classes-bc30958c273af7c79bfe77d321617738.

affiliated with AARP, to teach seniors in Maryland about AI-generated images and the risks of AI scams and deepfakes.[30]

We can also draw lessons from international exemplars, such as Finland, which has integrated media literacy and AI-media spotting training into its education programs for both young and old.[31]

Coordination. Many government agencies at both the state and federal level are alive to the dangers of deepfakes, even though there is no national law on this topic. (There are a number of state laws that address deepfake harms and frauds.) In the absence of tailor-made deepfake laws, regulators have relied on existing laws to support investigations and enforcement. The adage applies: if it is illegal without AI, it is illegal with AI. For example, in April 2024, the FTC implemented a rule that prohibits the impersonation of a business or government entity, providing the FTC with stronger enforcement tools to investigate fraudsters.[32] The FTC has proposed amending that rule to extend such protections to the impersonation of specific people.[33] The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) has also alerted financial institutions that the abuse of deepfake media and Generative AI may contribute to fraud and cybercrime, both of which are part of FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism National Priorities.[34] Greater coordination across the federal and state levels could promote efficiency and valuable knowledge sharing among policymakers, law enforcement, and industry.

Technology. While the surest defender against deepfake dupes lies between our ears, technology has a role to play, too. These technologies include tools to detect AI-generated content after the fact and provenance technology, which tags with metadata (sometimes called "content credentials") media as either generated by AI or captured by a human, such that it is difficult to alter the media after-the-fact without leaving evidence of manipulation.[35] Efforts to broaden the embrace of both of these technologies could help American seniors tell facts from fakes.

---

[30] Likewise, I had the privilege of presenting a webinar on deepfakes in October 2020 to Encore Learning, a nonprofit organization based in Arlington, Virginia that provides courses to people over 50. My lecture was arranged by two leaders of Encore Learning, lifelong public servants, and family friends of many decades, the late Barb Spangler and the late Steve Spangler.

[31] *After Decades of Teaching Media Literacy, Finland Equips Students with Skills to Spot AI Deepfakes*, EURONEWS (May 1, 2026), https://www.euronews.com/next/2026/01/05/after-decades-of-teaching-media-literacy-finland-equips-students-with-skills-to-spot-ai-de.

[32] Press Release, *FTC Announces Impersonation Rule Goes into Effect Today*, FED. TRADE COMM'N (Apr. 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-impersonation-rule-goes-effect-today.

[33] Press Release, *FTC Proposes New Protections to Combat AI Impersonation of Individuals*, FED. TRADE COMM'N (Feb. 15, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals.

[34] *FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions*, FINCEN (Nov. 13, 2024), at 2, https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf.

[35] *See generally* Mounir Ibrahim & Ashish Jaiman, Opinion, *To Defend Democracy, We Must Protect Truth Online*, THE HILL (Apr. 25, 2021, 5:00 PM), https://thehill.com/opinion/cybersecurity/550191-to-defend-democracy-we-must-protect-truth-online (describing provenance technology); Press Release, *Technology and Media Entities Join Forces to Create Standards Group Aimed at Building Trust in Online Content*, C2PA (Feb. 22, 2021), https://c2pa.org/post/c2pa_initial_pr/.

III. Tips and Tricks to Avoid Deepfake Scams

Irrespective of larger public efforts, seniors—and us all—can take steps today to protect ourselves and our loved ones against deepfake scams. Consider these best practices:

a. Prepare Proactively

- For emergencies, create a secret word or phrase with loved ones or close professional colleagues to verify their identity (choose something a deepfake impersonator would not know). If you receive a call from someone claiming to be that person, asserting that they are in distress or require funds, ask them for the pass phrase.

- Don't overshare online, including of videos and photos of yourself.

- Consider setting your social media profiles to private.

- Do not place inordinate trust in doctors or celebrities peddling investments or products that sound too good to be true. They almost always are

- Use strong passwords for online accounts, enable multi-factor authentication, and regularly update operating systems and antivirus software. (This is good cyber hygiene irrespective of deepfake-related risks.)

- Teach children and young adults in your life about the dangers of online exploitation and abuse. Point them to the U.S. Department of Homeland Security's Know 2 Protect Campaign (https://www.dhs.gov/know2protect) for more information.

b. Stay Skeptical

- If you do not know someone in real life, never transfer or receive money or cryptocurrency to or from them; buy gift cards for them; open bank accounts with or for them; start businesses on their behalf; or share personal information with them.

- Be cautious if someone you don't know is messaging you from an unfamiliar phone number or social media account.

- Double-check calls or emails that claim to be from a bank, delivery company, or government agency. If a bank, delivery service, or government agency is contacting you, visit their verified website or call their official phone number to address the issue. Be aware: Government agencies will rarely send messages to your phone about taxes or fees. Distrust all such messages and verify them through established channels.

c. Watch and Listen Carefully

- Be on the lookout for subtle imperfections in images and videos you view online or on video conferences, such as distorted hands or feet, blurry backgrounds, mismatching earrings, inaccurate shadows, watermarks, delays in responses and lags in the image's movement, or inconsistencies around the eyes and mouth and between the image and the voice.

- If you receive a phone call that purports to be from a trusted source asking you to do something suspicious, listen closely to the tone, intonation, and word choice for hints of AI manipulation. When in doubt, hang up.

d. Report Readily

- If you believe you have been the victim of a deepfake in any manner, notify all involved financial institutions and law enforcement, including the FBI's Internet Crime Complaint Center (http://www.ic3.gov) for financial fraud and the U.S. Secret Service (https://www.secretservice.gov/contact/field-offices) for romance scams.

IV. Conclusion

With so many deepfake scams and cons circulating, it may be challenging to believe that you can trust anything. In a world where no media seems real and anything is possible, skepticism can lead to cynicism and even nihilism.

But such a reaction is unnecessary. Greater education, coordination, and developments in deepfake detection and provenance technology, coupled with the straightforward steps outlined here, can help seniors (and us all) make sense of deepfakes, avoid their most pernicious uses, and navigate the digital world with "fortitude and buoyancy."[36]

In sum, we should be skeptical of the videos, audio, and imagery we encounter through our screens. We should look for markers of legitimacy in the media and its context. We should quiz ourselves: Do we know this person? What is the nature of this conversation or this request? Does this endorsement sound too good to be true? We should also trust our instincts, pause before taking any major step, and consult with our family and friends. For it is not through our devices but in our real lives where our most important relationships of confidence, understanding, and trust are formed, nurtured, and sustained.

#

[36] I owe this cheerful phrase, used in a different context, to WINSTON S. CHURCHILL, THE SECOND WORLD WAR: THE HINGE OF FATE 54 (1950).