ARTIFICIAL INTELLIGENCE AND WEAPONIZED ILLUSIONS: METHODOLOGIES FOR FEDERAL FRAUD PROSECUTIONS INVOLVING DEEPFAKES

ANDREW W. EICHNER*

Experts in the public and private sectors have vocalized concerns over the potential harms that can be inflicted when artificial intelligence (AI) is used maliciously. As AI technology increases in availability, it will become more accessible to criminal actors and allow for the emergence of new kinds of fraudulent schemes. Deepfakes are highly realistic AI-rendered depictions of individuals that criminals have already used to perpetrate fraud on an international scale. These renderings mimic third parties known to victims, allowing fraudsters to leverage the trust and familiarity of an existing relationship to perpetrate their schemes. The deepfake is used to convince the victim to send money to the fraudster under the guise of legitimacy.

This Article examines the increasing role that deepfakes play in the commission of criminal fraud schemes and suggests a methodology for federal criminal prosecutors to effectively respond to their growing threat. The Article first provides a general overview of deepfake technology: what deepfakes are, how fraudsters are using them, and how easy they are to create. It then suggests a methodology for federal prosecutors to follow when investigating and charging fraudsters that use deepfakes to perpetrate their schemes. Finally, the Author

---

* J.D., *The University of Texas School of Law*, 2012. B.A., *Boston University*, 2009. The opinions expressed in this Article in no way reflect the views of the Air National Guard, the U.S. Air Force, the Department of Defense, the Department of Justice, the Department of Veterans Affairs, or the U.S. Government. All opinions are entirely the Author's own. Additionally, all sources referenced in this Article are publicly available and are unclassified. The Author would like to thank his friends and former colleagues at the U.S. Attorney's Office for the Southern District of Mississippi, whose mentorship made him a more capable prosecutor. The Author would also like to thank his wife, family, friends, and the editors of this Article for their advice and support.

proposes an increase to the offense level of deepfake-based wire fraud under the U.S. Sentencing Guidelines based on its specific offense characteristics.

TABLE OF CONTENTS

INTRODUCTION

In March 2019, the Chief Executive Officer (CEO) of an energy company based in the United Kingdom received a phone call from his boss directing him to pay 220,000 euros to the account of a Hungarian

supplier.[1] The CEO's boss, himself the chief executive of the energy company's German parent company, "said the request was urgent, directing the executive to pay within an hour."[2] Recognizing "his boss' slight German accent and the melody of his voice on the phone," the CEO diligently complied and transferred the money as directed.[3] After completing the transaction, the CEO then received a second call from the parent company explaining that it had sent a reimbursement payment to the United Kingdom firm.[4]

Later in the day, a third call from his boss piqued the CEO's suspicion.[5] The German executive was asking for a second payment, but the promised reimbursement from earlier in the day had never arrived.[6] Additionally, the German executive appeared to be calling from an unfamiliar Austrian phone number.[7] The CEO, perceiving that something was wrong, refused to make another payment.[8] Before the first payment could be recovered, it had vanished through international wire transfers.[9] Subsequent investigation disclosed that the initial transfer "to the Hungarian bank account was subsequently moved to Mexico and distributed to other locations."[10]

A year later, "a branch manager of a Japanese company in Hong Kong received a call from a man whose voice he recognized—the director of his parent business."[11] The director advised the branch manager that "the company was about to make an acquisition, so he needed to authorize some transfers to the tune of $35 million."[12] The

---

1. Catherine Stupp, *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*, WALL ST. J., https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 [https://perma.cc/K7GT-WEDT] (last updated Aug. 30, 2019, 12:52 PM). The company's insurance firm, Euler Hermes Group SA, reported the fraud to the *Wall Street Journal* but did not name the victim companies. *Id.*
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.*
10. *Id.*
11. Thomas Brewster, *Fraudsters Cloned Company Director's Voice in $35 Million Heist, Police Find*, FORBES, https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions [https://perma.cc/K52F-5JJ2] (last updated May 2, 2023) (noting the United Arab Emirates, Dubai Public Prosecution office, is leading the investigation).
12. *Id.*

branch manager received emails from the company director and a lawyer who had been hired to coordinate the process and, "believing everything appeared legitimate, began making the transfers."[13] Before the branch manager was able to recognize something was wrong and contact authorities, the money was "transferred . . . to several bank accounts in other countries in a complex scheme involving at least 17 known and unknown defendants" and was traced through the United States.[14] Emirati authorities tracked approximately $400,000 of the stolen funds to two U.S. bank accounts.[15]

Each of these transactions was a real-world case of sophisticated fraud perpetrated by criminals using artificial intelligence (AI). In the United Kingdom example, fraudsters "used AI-based software to successfully mimic the German executive's voice by phone."[16] Because "[t]raditional cybersecurity tools designed to keep hackers off corporate networks can't spot spoofed voices," it is impossible to know whether this was the first AI-based fraud or "whether there are other incidents that have gone unreported or in which authorities didn't detect the technology in use."[17] Similarly, in the Hong Kong example, fraudsters "used 'deep voice' technology to clone the director's speech," likely making this example the second known case of "voice-shaping tools [used] to carry out a heist."[18]

The AI-conceived ruses used by these perpetrators fall into a broader category of technology that is collectively known as "deepfakes."[19] A

---

13. *Id.*; *In re* United States Pursuant to 18 U.S.C. § 3512 for Order for Commissioner's Appointment for Money Laundering Investigation at 2, No. 21-ML-00887 (D.D.C. Oct. 13, 2021), ECF No. 1 [hereinafter *In re* United States Pursuant to 18 U.S.C. § 3512].

14. *In re* United States Pursuant to 18 U.S.C. § 3512, *supra* note 13, at 2.

15. *Id.*

16. Stupp, *supra* note 1.

17. *Id.*; *see also* Jesse Damiani, *A Voice Deepfake Was Used to Scam a CEO out of $243,000*, FORBES (Sep. 3, 2019, 4:42 PM), https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000 [https://perma.cc/MZ9A-LTNP] ("It's the first *noted instance* of an artificial intelligence-generated voice deepfake used in a scam." (emphasis added)).

18. Brewster, *supra* note 11 (noting this second instance of deepfake voice fraud was a far larger heist ($35 million) than the first United Kingdom scam, which only resulted in ill-gotten gains of $240,000).

19. *See* Grace Shao, *What 'Deepfakes' Are and How They May Be Dangerous*, CNBC, https://www.cnbc.com/2019/10/14/what-is-deepfake-and-how-it-might-be-dangerous.html [https://perma.cc/DT3A-VPMZ] (last updated Jan. 17, 2020, 2:47 EST) (including fabricated images, videos, and sounds, in the category of deepfakes).

portmanteau of the terms "deep learning" and "fake,"[20] deepfakes are generally defined as "manipulated videos, or other digital representations produced by sophisticated artificial intelligence, that yield fabricated images and sounds that appear to be real."[21] The controversial technology generates heated debate at the intersection of law, politics, and national security, implicating concerns ranging from free speech, to individual privacy, to crime.[22] As one of its more nefarious purposes, deepfake technology can be used as a criminal instrument to perpetrate fraud on even the most cautious victims.[23]

Deepfake technology's potential to cause harm has been emphasized by entities in both the public and private sectors.[24]

---

20. Sophia Khatsenkova, *Audio Deepfake Scams: Criminals Are Using AI to Sound like Family and People Are Falling for It*, EURONEWS (Mar. 25, 2023, 3:09 PM), https://www.euronews.com/next/2023/03/25/audio-deepfake-scams-criminals-are-using-ai-to-sound-like-family-and-people-are-falling-fo [https://perma.cc/75GH-U23A].

21. Shao, *supra* note 19 ("Deep learning" is a form of AI "refer[ring] to arrangements of algorithms that can learn and make intelligent decisions on their own . . . . A deep-learning system can produce a persuasive counterfeit by studying photographs and videos of a target person from multiple angles, and then mimicking its behavior and speech patterns."); *see also* Dave Johnson & Alexander Johnson, *What Are Deepfakes? How Fake AI-Powered Audio and Video Warps Our Perception of Reality*, BUS. INSIDER (June 15, 2023, 10:58 AM), https://www.businessinsider.com/guides/tech/what-is-deepfake [https://perma.cc/V9E7-9ZQ7] (distinguishing deepfakes, which are created by deep learning algorithms that "teach themselves to solve problems with large sets of data and can be used to create fake content of real people" from "shallowfakes," which require more human input and are less complex than deepfakes).

22. *See* Shao, *supra* note 19; John Villasenor, *Artificial Intelligence, Deepfakes, and the Uncertain Future of Truth*, BROOKINGS INST. (Feb. 14, 2019), https://www.brookings.edu/articles/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth [https://perma.cc/B8XY-X3BZ] (suggesting that one of the tensions at play in the deepfake debate is the risk of overly broad protections "running afoul of the First Amendment and being struck down on appeal").

23. *See* Tina Brooks, Princess G., Jesse Heatley, Jeremy J., Scott Kim & Samantha M. et al., *Increasing Threat of Deepfake Identities*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf [https://perma.cc/WMD9-ZCEG] (explaining how in the past many people could easily detect digitally altered photos or audio because the technology was so rudimentary, but now, the technology has rapidly evolved and is creating far more realistic outputs than ever before).

24. *See, e.g.*, *National Security Challenges of Artificial Intelligence, Manipulated Media, and "Deepfakes", H. Permanent Select Comm. on Intel.*, 116th Cong. 2 (June 13, 2019) (statement of Rep. Adam Schiff, Chairman, H. Permanent Select Comm. on Intel.) (speaking to the American public about the potential of deepfakes to "enable

Multiple federal government agencies published warnings about the threat of deepfake scammers to the general public, including a consumer warning from the Federal Trade Commission in 2023.[25] Senator Richard Blumenthal opened a U.S. Senate hearing on AI "with a faked voice recording that was written by ChatGPT and vocalized by an audio application trained on his Senate floor speeches."[26] The AI-generated speech "outlined the reason for the hearing and warned of . . . 'technology outpac[ing] regulation,' possibly leading to misinformation and the exploitation of personal data."[27] Brad Smith, the president of technology-giant Microsoft, stated in May 2023 that his biggest concern with AI is deepfakes.[28] According to a 2022 survey of 125 cybersecurity and incident response professionals conducted by the technology company VMware, "[t]he percentage of respondents who saw malicious deepfakes used as part of an attack went up 13 percent [between 2021 and 2022,] to 66 percent" of respondents.[29]

---

malicious actors to foment chaos, division, or crisis"); Diane Bartz, *Microsoft Chief Says Deep Fakes Are Biggest AI Concern*, REUTERS (May 25, 2023, 5:01 PM), https://www.reuters.com/technology/microsoft-chief-calls-humans-rule-ai-safeguard-critical-infrastructure-2023-05-25 [https://perma.cc/J843-C86U] (describing a speech made by the President of Microsoft, Brad Smith, where he called on Washington lawmakers to regulate AI due to the risks deepfakes pose to election integrity, national security, and cybersecurity).

25. Alvaro Puig, *Consumer Alert: Scammers Use AI to Enhance Their Family Emergency Schemes*, FTC: CONSUMER ADVICE (Mar. 20, 2023), https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes [https://perma.cc/2ZQ5-ZH46] (warning consumers about a common category of scams perpetrated using AI voice cloning technology where criminals pose as family members in distress and ask for money); *accord* Brooks et al., *supra* note 23 (educating consumers about how AI-threats might arise in the commerce and national security spheres); *Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations*, FED. BUREAU OF INVESTIGATION: CYBER DIV. (Mar. 10, 2021), https://s3.documentcloud.org/documents/20514502/fbipin-3102021.pdf [https://perma.cc/PS6L-RPXQ] (alerting cybersecurity professionals and system administrators to the impending use of deepfakes and other synthetic content by foreign criminal actors).

26. Matt Berg, *Blumenthal: AI Deepfake 'One of the More Scary Moments' in Senate Hearing History*, POLITICO (May 17, 2023, 8:30 AM), https://www.politico.com/news/2023/05/17/blumenthal-ai-deepfake-recording-senate-hearing-00097349 [https://perma.cc/HQZ9-2WCJ].

27. *Id.*

28. Bartz, *supra* note 24.

29. VMWARE, GLOBAL INCIDENT RESPONSE THREAT REPORT at 3, 13 (2022), https://www.vmware.com/content/dam/learn/en/amer/fy23/pdf/1553238_Global

The federal government and private industry agree that deepfakes pose real dangers and that their potential for criminal uses must be urgently addressed.[30] While the technology is novel, federal lawmakers do not need to create new laws to counteract criminal uses of deepfakes. Deepfake fraud is perpetrated at the nexus of traditional wire fraud and aggravated identity theft. Accordingly, federal prosecutors can respond to deepfake fraud by charging violations of existing statutes prohibiting these activities.

This Article examines the increasing role that deepfakes play in the commission of criminal fraud schemes and suggests a methodology for federal criminal prosecutors to effectively respond to their growing threat. Part I provides a general overview of deepfake technology: what deepfakes are, how fraudsters are using them, and how easy they are to create. Part II suggests a methodology for federal prosecutors to follow when investigating and charging fraudsters that use deepfakes to perpetrate their schemes, focusing on the effectiveness of charging violations of wire fraud and aggravated identity theft statutes. Finally, Part III proposes an increase to the offense level of deepfake-based wire fraud under the U.S. Sentencing Guidelines based on its specific offense characteristics.

I. DEEPFAKES: AN OVERVIEW

In order to appreciate why it is important to prepare a methodology for federal prosecutions of deepfake fraud, it is important to first understand what deepfakes are, how fraudsters are using them, and the degree of technological sophistication required to create them.

_Incident_Response_Threat_Report_Weathering_The_Storm.pdf [https://perma.cc/8KEC-Z76X].

30. *See, e.g.*, Anthony Cuthbertson & Ariana Baio, *AI Congress Hearing: Sam Altman Testifies Before Congress Saying There Is 'Urgent' Need for Regulation*, INDEPENDENT (May 16, 2023, 7:39 BST), https://www.independent.co.uk/tech/sam-altman-ai-congress-live-chatgpt-openai-b2339688.html [https://perma.cc/CQ24-8AFN] (summarizing key points from the 2023 Senate Judiciary Subcommittee meeting on Privacy, Technology, and the Law, where top executives of AI companies, including OpenAI and IBM, spoke with U.S. senators about AI's potential for criminal uses, such as election fraud).

A. What Are Deepfakes and How Are They Being Used?

In late 2017, a user on the content aggregation site Reddit shared pornographic videos of celebrities, created using face-swapping technology. The username of the Redditor? Deepfakes.[31]

At its most basic level, "[a] deepfake is a fraudulent piece of content—typically audio or video—that has been manipulated or created using artificial intelligence. This content replaces a real person's voice, image, or both with similar looking and sounding artificial likenesses."[32] In addition to audio and video clips, deepfakes can take many other forms: text, images, and even real-time renderings.[33] Deepfakes are a narrower subset type of a broader category called synthetic media, generally defined as "any media which has been created or modified through the use of artificial intelligence/machine learning (AI/ML)."[34] While commercial face-swapping technology has existed since the 1990s with image editing

---

31. Meredith Somers, *Deepfakes, Explained*, MASS. INST. TECH. (July 21, 2020), https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained [https://perma.cc/UA2D-LZH9]; *see also* Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales & Javier Ortega-Garcia, *An Introduction to Digital Face Manipulation*, *in* HANDBOOK OF DIGITAL FACE MANIPULATION AND DETECTION 3, 4 (Christian Rathgeb et al. eds., 2022), https://library.oapen.org/bitstream/handle/20.500.12657/52835/978-3-030-87664-7.pdf [https://perma.cc/58ES-58XX] (recounting lore surrounding the Redditor "deepfakes").

32. *What Are Deepfakes and How Do I Spot One?*, MICROSOFT (July 18, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/deepfakes [https://perma.cc/R945-S8DG].

33. *See* Dilki Rathnayake, *Deepfakes: What They Are and Tips to Spot Them*, TRIPWIRE (Feb. 28, 2023), https://www.tripwire.com/state-of-security/deepfakes-what-they-are-and-tips-spot-them [https://perma.cc/39T2-G3KJ] (defining real-time deepfakes as audio and video clones that are generated contemporaneously, rather than pre-made); Jon Healey, *Real-Time Deepfakes Are a Dangerous New Threat. How to Protect Yourself*, L.A. TIMES (May 11, 2023, 6:42 AM), https://www.latimes.com/business/technology/story/2023-05-11/realtime-ai-deepfakes-how-to-protect-yourself [https://perma.cc/Z3MD-63RB] (explaining how real-time deepfakes enable criminals to replicate a person's voice, image, and movements in a virtual meeting); *see also* VMWARE, *supra* note 29, at 13 (describing different categories of deepfakes and the methods by which they are delivered to the victims); *cf.* Claire Moravec, *Deepfakes: When Seeing Is No Longer Believing*, SEC. MAG. (Sept. 27, 2022), https://www.securitymagazine.com/articles/98394-deepfakes-when-seeing-is-no-longer-believing [https://perma.cc/CA7N-BVZP] (discussing social media deepfakes using the recent example of "Katie Jones," who appeared online to be a Washington D.C. political player connected to a Deputy Assistant Secretary of State and a Senior Congressional Aide, but was later determined to be a social media deepfake created by a malicious actor targeting the United States).

34. Brooks et al., *supra* note 23, at 5.

software such as Adobe Photoshop, "[t]oday, the technology utilized to produce a convincing face swap involves AI."[35]

In some instances, deepfakes have been used for interesting and beneficial purposes. For instance, the news media provider Reuters worked with Synthesia, an AI startup, to synthesize presenter-led video reports from pre-recorded clips of news presenters using deepfake technology.[36] One company "train[ed] its deepfake technology . . . to create 'lost' audio of the speech [President John F. Kennedy] was due to give in Dallas on November 22, 1963, the day he was assassinated."[37] At the Massachusetts Institute of Technology, "a video shown during a lecture about deep learning . . . showed a former president welcoming students and explaining some aspects of a college course. The entire speech and video were created with deepfake technology."[38] The technology has also been used to spread positive health messaging: "[a] UK-based health charity used deepfake technology to have David Beckham delivering an anti-malaria message in nine languages."[39] In these regards, deepfakes can be used as an educational and creative tool capable of transforming art, medicine, and countless other fields.[40]

Unfortunately, the technology also has deviant and harmful uses. In addition to the types of fraud schemes highlighted in the introduction to this Article, deepfakes have allegedly been used to undermine national security and election integrity.[41] "Deepfakes are frequently

---

35. *Id.* at 9.

36. Simon Chandler, *Why Deepfakes Are a Net Positive for Humanity*, FORBES (Mar. 9, 2020, 12:33 PM), https://www.forbes.com/sites/simonchandler/2020/03/09/why-deepfakes-are-a-net-positive-for-humanity [https://perma.cc/ZPG9-HJBT].

37. *Id.*

38. *What Are Deepfakes and How Do I Spot One?*, *supra* note 32.

39. Chandler, *supra* note 36.

40. *Id.*

41. *See, e.g.*, Moravec, *supra* note 33 (recounting the story of a deepfake deployed on social media that was discovered to be the creation of foreign state-sponsored actors). Some politicians have also weaponized the existence of deepfakes to try to propagate misinformation; therefore, allegations of interference need to be viewed skeptically. *See, e.g.*, Zack Budryk, *GOP House Candidate Publishes 23-Page Report Claiming George Floyd Death Was Deepfake Video*, HILL (June 24, 2020, 7:36 PM), https://thehill.com/homenews/house/504429-gop-house-candidate-publishes-23-page-report-claiming-george-floyd-death-was [https://perma.cc/RD32-M85H]; *see also* Matteo Wong, *We Haven't Seen the Worst of Fake News*, ATLANTIC (Dec. 20, 2022), https://www.theatlantic.com/technology/archive/2022/12/deepfake-synthetic-medi

used to spread disinformation, and can be used in scams, election manipulation, social engineering attacks and other kinds of fraud."[42] In the 2023 Turkish presidential race, "Turkish President Recep Tayyip Erdogan's main political opponent accused Russia of using deepfakes and other artificial intelligence (AI)-generated material to meddle in the country's upcoming presidential election."[43] At a much more personally intrusive level, deepfakes are sometimes used to generate fake pornographic videos, creating an alarming new branch of nonconsensual pornography.[44] While "[m]ost deepfake videos are of female celebrities, . . . creators now also offer to make videos of anyone. A creator offered on Discord to make a 5-minute deepfake of a

---

a-technology-rise-disinformation/672519 [https://perma.cc/NET9-JXZC] (explaining how it is sometimes difficult to tell whether deepfakes are actually being used or whether individuals are seeking to advance or protect their own interests by blaming negative political events on the technology, "[t]he law professors Danielle Citron and Robert Chesney call this the 'liar's dividend': Awareness of synthetic media breeds skepticism of all media, which benefits liars who can brush off accusations or disparage opponents with cries of 'fake news.' Those lies then become part of the sometimes deafening noise of miscontextualized media, scientific and political disinformation, and denials by powerful figures, as well as a broader crumbling of trust in more or less everything"); Shannon Bond, *People Are Trying to Claim Real Videos Are Deepfakes. The Courts Are Not Amused*, NPR (May 8, 2023, 5:01 AM), https://www.npr.org/2023/05/08/1174132413/people-are-trying-to-claim-real-videos-are-deepfakes-the-courts-are-not-amused [https://perma.cc/6HZD-9WTY] ("[T]he unleashing of powerful generative AI to the public is also raising concerns about another phenomenon: that as the technology becomes more prevalent, it will become easier to claim that anything is fake.").

42. *What Are Deepfakes and How Do I Spot One?*, *supra* note 32.

43. Peter Aitken, *Deepfakes, Porn Tapes, Bots: How AI Has Shaped a Vital NATO Ally's Presidential Election*, FOX NEWS (May 13, 2023, 2:00 AM), https://www.foxnews.com/world/deepfakes-porn-tapes-bots-ai-shaped-vital-nato-allys-presidential-election [https://perma.cc/P6F5-BPG3].

44. "Nonconsensual pornography" has been defined as "a sexually graphic image or video of an individual distributed without the consent of the person depicted in the media." Chance Carter, *An Update on the Legal Landscape of Revenge Porn*, NAT'L ASS'N OF ATT'YS GEN. (Nov. 16, 2021), https://www.naag.org/attorney-general-journal/an-update-on-the-legal-landscape-of-revenge-porn [https://perma.cc/3RNM-HBSS] (citing Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346 (2014)). One such example of nonconsensual pornography is "[r]evenge porn . . . defined as the distribution of sexually graphic images or videos of an individual without their consent in the context of an intimate relationship." *Id.* "Nonconsensual porn can also appear as a wide variety of other content forms such as deepfakes, hidden camera photos, or upskirt photos which are not created by the victim." *Id.* (citing Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1904–28 (2019)).

'personal girl,' meaning anyone with fewer than 2 million Instagram followers, for $65."[45] The problem is pervasive: "In 2019, synthetic media expert[s] . . . set out to map out the state of deepfakes online. They found that 96% of the 14,000 deepfake videos found online were porn."[46]

Available data suggest that the use of deepfakes as a criminal tool has increased on a world-wide scale, at a seemingly exponential rate.[47] Crime data collected between 2022 and the first quarter of 2023 show that the percentage of fraud involving deepfakes "jumped from 0.2% to 2.6% in the [United States] and from 0.1% to 4.6% in Canada."[48] Simultaneously, "printed forgeries, which represented 4% [to] 5% of all fraud in 2022, dropped to 0%."[49] Similarly, the British business newspaper *Financial Times* reported "[t]he number of deepfakes used in scams in just the first three months of 2023 outstripped all of 2022 and then some, . . . with particularly high growth in Canada, the [United States], Germany and the [United Kingdom]."[50]

In VMware's 2022 *Global Incident Response Threat Report*, a majority of the 125 cybersecurity professionals surveyed identified that "deepfake attacks most often took the form of video (58 percent) rather than

---

45. Kat Tenbarge, *Found Through Google, Bought with Visa and Mastercard: Inside the Deepfake Porn Economy*, NBC NEWS (Mar. 27, 2023, 11:56 AM), https://www.nbcnews.com/tech/internet/deepfake-porn-ai-mr-deep-fake-economy-google-visa-mastercard-download-rcna75071 [https://perma.cc/FRD3-4GYT] (noting that average individuals (i.e., noncelebrities) are increasingly becoming the victims of nonconsensual deepfake pornography).

46. Emmanuelle Saliba, *Sharing Deepfake Pornography Could Soon Be Illegal in America*, ABC NEWS (June 15, 2023, 6:09 AM), https://abcnews.go.com/Politics/sharing-deepfake-pornography-illegal-america/story?id=99084399 [https://perma.cc/929H-ZKG3].

47. *See* Rathnayake, *supra* note 33 (citing recent World Economic Forum data finding "deepfake videos are increasing at an annual rate of 900%"); Alex Rolfe, *US Fraud Statistics: FAI/Deepfake Multiply at Alarming Rates*, PAYMENTS INDUS. INTEL. (May 31, 2023), https://www.paymentscardsandmobile.com/us-fraud-statistics-fai-deepfake-multiply-at-alarming-rates [https://perma.cc/56VJ-LRPL] (explaining that deepfake-related fraud "more than doubled" in the United States and Canada between 2022 and the first quarter of 2023).

48. Rolfe, *supra* note 47.

49. *Id.*

50. Mehul Srivastava, *Fears Grow of Deepfake ID Scams Following Progress Hack*, FIN. TIMES (June 28, 2023), https://www.ft.com/content/167befa0-123f-4384-a37e-c8a5b78604b2 [https://perma.cc/6ND8-D6AJ].

audio (42 percent)."[51] The potential harm of these video deepfakes is magnified by their increasing realism. While video deepfakes have historically presented imperfect renderings, the distinction between fabrication and reality is slowly diminishing.[52] Viewers distinguish between deepfakes and reality through the "uncanny valley" effect, an unsettling lifelessness in the eyes of a synthetic person.[53] However, as the technology has progressed, the uncanny valley is diminishing, allowing more viewers to be pulled into deception by deepfakes.[54] One study reported that while "people systematically overestimate their abilities to detect deepfakes," their overconfidence was misplaced and "their guesses were, for the most part, as good as flipping a coin."[55] While research shows that individuals fare better at identifying deepfakes as static images, the study found lower detection accuracy for video deepfakes.[56]

In another interesting study, scientists studied the trustworthiness of actual human faces versus deepfake faces.[57] Working under the assumption that "[f]aces provide a rich source of information, with exposure of just milliseconds sufficient to make implicit inferences about individual traits such as trustworthiness," researchers examined "whether synthetic faces activate the same judgements of trustworthiness . . . [to determine whether] a perception of

---

51. VMWARE, *supra* note 29, at 3, 13 (categorizing the most common methods of deepfake attacks—email, text messages, and social media—but noting that deepfakes are increasingly being deployed on new platforms such as third-party meeting software and other business collaboration tools).

52. *See* Healey, *supra* note 33 (explaining how "just two or three years ago," the advice for spotting fraudulent content was basic, focused on "easy-to-spot glitches, like frozen images," but now, the technology has advanced so much people are being advised to look for a suspected deepfake "blinking too much or too little, having eyebrows that don't fit the face or hair in the wrong spot, and skin that doesn't match their age").

53. Emily Willingham, *Humans Find AI-Generated Faces More Trustworthy than the Real Thing*, SCI. AM. (Feb. 14, 2022), https://www.scientificamerican.com/article/humans-find-ai-generated-faces-more-trustworthy-than-the-real-thing [https://perma.cc/N5DL-AH9U].

54. *Id.*

55. Nils C. Köbis, Barbora Doležalová & Ivan Soraperra, *Fooled Twice: People Cannot Detect Deepfakes but Think They Can*, ISCIENCE, Nov. 19, 2021, at 1, 10–11, https://www.cell.com/action/showPdf?pii=S2589-0042%2821%2901335-3 [https://perma.cc/YBF2-EZS7].

56. *Id.* at 9.

57. Sophie J. Nightingale & Hany Farid, *AI-Synthesized Faces Are Indistinguishable from Real Faces and More Trustworthy*, PROC. NAT'L ACAD. SCI. USA, Feb. 14, 2022, at 1, 1.

trustworthiness could help distinguish real from synthetic faces."[58] Surprisingly, when "223 participants rated the trustworthiness of 128 faces . . . on a scale of 1 (very untrustworthy) to 7 (very trustworthy)," the average trustworthiness score for real faces was 4.48, which is noticeably less than the average trustworthiness rating of 4.82 for synthetic faces.[59] In other words, "[s]ynthetically generated faces are not just highly photorealistic, they are nearly indistinguishable from real faces and are judged more trustworthy."[60]

Not only are deepfakes becoming more effective at deceiving humans into thinking they are real, they are also becoming proficient at deceiving other machines.[61] Biometric authentication, such as using facial recognition to unlock an iPhone,[62] cannot be relied upon to identify deepfakes and prevent access to devices.[63] For example, "[i]f someone hacks a facial recognition scanner and puts a deepfake person in front of it, the system will likely open . . . . [T]hings like iris recognition could easily mistake a deepfake as the person actually grant[ing] access to the system."[64] Verification experts believe that multi-factor authentication and tools that measure "liveness"—humanlike changes such as blinks or mouth twitches—will become necessary to ensure the continued effectiveness of biometric authentication moving forward.[65]

---

58. *Id.*

59. *Id.* at 1–2 (calculating the difference in trustworthiness to be approximately 7%).

60. *Id.* at 2.

61. *See id.* at 1 (explaining that a "generator learns to synthesize increasingly more realistic faces until the discriminator is unable to distinguish it from real faces").

62. *See Face ID and Touch ID Security*, APPLE (Feb. 18, 2021), https://support.apple.com/guide/security/face-id-and-touch-id-security-sec067eb0c9e/web [https://perma.cc/5H3G-5GW8] (describing facial recognition and fingerprint sensing as forms of biometric authentication for Apple devices).

63. *See* Zac Amos, *Can Deepfakes Beat Biometric Security?*, CYBERSEC. MAG. (Apr. 24, 2023), https://cybersecurity-magazine.com/can-deepfakes-beat-biometric-security [https://perma.cc/9SE9-Z5TE] (explaining that deepfakes can trick biometric technologies by taking advantage of data and manipulating voices).

64. *Id.*

65. Hannah Murphy, *Deepfakes Make Banks Keep It Real*, FIN. TIMES (Sept. 30, 2023), https://www.ft.com/content/6ca90b12-3ee6-409c-968d-1cffe29ee973 [https://perma.cc/V3Y7-JNSM]; *see also* Joint CSI, *Contextualizing Deepfake Threats to Organizations*, U.S. DEP'T OF DEF. (2023), https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.pdf [https://perma.cc/F9NL-NJWD] ("Authentication methods are designed to be embedded at the time of capture/creation or time of edit

There is not a universal consensus yet regarding whether the existence of deepfakes will ultimately have a positive or negative impact on society.[66] What is apparent, however, is that deepfakes are becoming progressively more realistic and commonplace, which makes them especially dangerous in the hands of criminal actors.[67] Accordingly, federal prosecutors need to be prepared to meet this growing threat and must understand the best strategies to charge fraudsters who capitalize on AI technology.[68]

B. How Easy Are Deepfakes to Create?

Developments in deepfakes and similar technologies have advanced exponentially since the first deepfake was created in 2017.[69] There are multiple different underlying AI technologies that can be used to create deepfakes, such as autoencoders or generative adversarial networks ("GANs"). Autoencoders are "artificial neural network[s] trained to reconstruct input from . . . simpler representation[s]"[70] and have been responsible for many of the viral deepfakes.[71] GANs use "two

---

to bring transparency to the provenance of the media. Some examples include digital watermarking which can be used in synthetically generated media, active signals in real-time capture to verify liveness, and cryptographic asset hashing on a device." (footnotes omitted)).

66. *Compare* Rob Toews, *Deepfakes Are Going to Wreak Havoc on Society. We Are Not Prepared*, FORBES (May 25, 2020, 11:54 PM), https://www.forbes.com/sites/robtoews/2020/05/25/deepfakes-are-going-to-wreak-havoc-on-society-we-are-not-prepared [https://perma.cc/V9V2-V24K] (arguing deepfakes are a net negative for society and are growing at a fast pace with potential social and political repercussions), *with* Chandler, *supra* note 36 (arguing deepfakes are a net positive for society once people become educated on the technology's potential).

67. *See* Brooks et al., *supra* note 23, at 17–18 (explaining that criminal actors may be incentivized to attack the public on a large scale with deepfakes rather than smaller attacks that are noticed sooner by individuals).

68. *See id.* at 25 (advocating for "global collaboration between law enforcement agencies" to protect the public from deepfakes).

69. *See id.* at 6 ("Since the first deepfake in 2017, there have been many developments in deepfake and related-synthetic media technologies.").

70. U.S. GOV'T ACCOUNTABILITY OFF., DEEPFAKES 1 (2020), https://www.gao.gov/assets/gao-20-379sp.pdf [https://perma.cc/UD9A-EJFU].

71. *See* Martin Anderson, *The Future of Generative Adversarial Networks in Deepfakes*, METAPHYSIC (July 25, 2022, 11:39 AM), https://blog.metaphysic.ai/the-future-of-generative-adversarial-networks-in-deepfakes [https://perma.cc/SDR6-SVAJ] (describing autoencoders as "the architecture behind current viral deepfakes").

[machine learning] systems called neural networks [that] are trained in competition with each other."[72]

> [D]uring training, the *Generator* . . . uses random noise to attempt to recreate images similar to the training data, while the *Discriminator* . . . grades the Generator's hundreds of thousands of attempts in terms of how closely those attempts resemble the input images. Slowly, the Generator learns to recreate the source images with more fidelity, even though it never gets access to the 'real' pictures, and only improves based on how the Discriminator scores its latest attempt.[73]

"Essentially the second neural network is checking whether the image of the first network is real or fake. This way, the two neural networks train each other and become more and more realistic."[74] Simply put, the "two neural networks compete against one another, where the goal of one is to generate an image that the other will not be able to tell from its training data, and the goal of the latter is to avoid being fooled in this way."[75]

Deepfakes do not require advanced technological training or aptitude to create. In late 2019, an *Ars Technica* journalist investigating deepfakes spent $552 and used a high-powered computer to create his own deepfake video.[76] Describing himself as a deepfake neophyte, the journalist used the face of Lieutenant Commander Data (Brent Spiner) from *Star Trek: The Next Generation* to overlay Mark Zuckerberg's face in a video of the Facebook founder testifying before Congress.[77] In order to create the video, the journalist "needed a heap

---

72. KELLEY M. SAYLER & LAURIE A. HARRIS, CONG. RSCH. SERV., DEEP FAKES AND NATIONAL SECURITY 1, https://crsreports.congress.gov/product/pdf/IF/IF11333 [https://perma.cc/6UPZ-EDRR] (last updated Apr. 17, 2023).

73. Anderson, *supra* note 71. There are also alternate names for the two competing networks that are part of a GAN. *See, e.g.*, Lutz Finger, *Overview of How to Create Deepfakes—It's Scarily Simple*, FORBES (Sept. 8, 2022, 8:00 AM), https://www.forbes.com/sites/lutzfinger/2022/09/08/overview-of-how-to-create-deepfakesits-scarily-simple [https://perma.cc/ZF57-MHHF] (calling the adversarial networks the "generative neural network" and the "discriminative classifier").

74. Finger, *supra* note 73.

75. *Deepfake*, SEON, https://seon.io/resources/dictionary/deepfakes [https://perma.cc/4QMF-ZTPY].

76. *See* Timothy B. Lee, *I Created My Own Deepfake—It Took Two Weeks and Cost $552*, ARS TECHNICA (Dec. 16, 2019, 7:50 AM), https://arstechnica.com/science/2019/12/how-i-created-a-deepfake-of-mark-zuckerberg-and-star-treks-data [https://perma.cc/9YS8-59DY] (stating that creating deepfakes takes a lot of computer power to operate the neural networks).

77. *Id.*

of images of both Mark Zuckerberg and Mr. Data."[78] Even though his final product was just thirty-eight seconds long, the journalist needed nine minutes of Mr. Data and seven minutes of Mr. Zuckerberg in order to capture the "different angles, with different expressions, and in different lighting conditions" necessary to effectively create the deepfake.[79] In addition to the "$552 in cloud-computing charges," the journalist needed a computer with a powerful enough graphics processing unit ("GPU") to render the deepfake.[80] He ultimately used a "four-GPU monster . . . [with] four Nvidia T4 Tensor Core GPUs with 16GB of memory each," in addition to other high-end computing components that "largely went unused because neural network training is so GPU-heavy."[81] Overall, the deepfake took approximately two weeks to create and the AI's neural network took six days to train, notwithstanding the journalist's high-end graphics card set-up.[82] Despite these resource requirements and the video demands required to create the deepfake, the journalist found it remarkable that he could "create fairly convincing video so quickly and for so little money," noting that "there's every reason to think deepfake technology will continue to get better, faster, and cheaper in the coming years."[83]

Consistent with that prediction, the computing resource requirements for deepfakes have decreased dramatically in recent years.[84] In February 2023—less than four years after the *Ars Technica* experiment—a business professor at the University of Pennsylvania's Wharton School, Ethan Mollick, posted a deepfake video on the professional networking site LinkedIn.[85] The professor created the video "using artificial intelligence to generate his words, his voice and his moving image."[86] "With just a photograph [and] 60 seconds of audio," he was able to create the deepfake "in just a matter of minutes

78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.*
82. *Id.*
83. *Id.*
84. *See* Shannon Bond, *It Takes a Few Dollars and 8 minutes to Create a Deepfake. And That's Only the Start*, NPR (Mar. 23, 2023, 5:00 AM), https://www.npr.org/2023/03/23/1165146797/it-takes-a-few-dollars-and-8-minutes-to-create-a-deepfake-and-thats-only-the-sta [https://perma.cc/XSD9-CAXB] (explaining that anyone with a smartphone or computer can engage with deepfake technology in the present day).
85. *Id.*
86. *Id.*

by combining a few cheap AI tools."[87] Starting with ChatGPT, the professor asked the program to:

> Write a script that Ethan Mollick would say about entrepreneurship . . . Next, he turned to a tool that can clone a voice from a short audio clip . . . [where he] gave it a minute of . . . talking about some unrelated topic like cheese and then pasted the speech in and it generated the sound file. Finally, he fed that audio and a photo of himself into another AI app.[88]

In total, it took Mollick a mere eleven dollars and eight minutes to make it.[89]

As demonstrated by this short timeline of explosive technological development, while previously "[m]aking a sophisticated fake with specialized software previously could take a professional days to weeks to construct, . . . now, these fakes can be produced in a fraction of the time with limited or no technical expertise."[90] There are new and more advanced models coming out weekly that provide fraudsters with hundreds of opportunities and methods to produce visual deepfakes.[91] Given their decreasing cost and increasing accessibility and realism, federal prosecutors must be prepared to react when their investigations begin to uncover deepfakes being used to perpetrate fraud.

II. PROSECUTING DEEPFAKE FRAUD UNDER EXISTING FEDERAL CRIMINAL LAW

When compared at their fundamental level, both examples from this Article's introduction follow the same basic fact pattern: a fraudster uses an AI-generated deepfake of a third party to electronically communicate with a victim, convincing them to electronically send the fraudster or their co-conspirators money by exploiting the pre-existing relationship between that third party and victim. The remainder of this Article will examine the law as applied to this set of facts, which will be called "the model scenario."[92]

---

87. *Id.*

88. *Id.* (internal quotation marks omitted).

89. *Id.*

90. JOINT CSI, *supra* note 65, at 2.

91. Matthew Miller, *Deepfakes: Real Threat*, KPMG 9 (2023), https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/deepfakes-real-threat.pdf [https://perma.cc/4BKP-S35B].

92. *See supra* Section II.A.

Despite the seemingly sophisticated and novel means by which the crime is committed, federal prosecutions of the model scenario can still be effectively accomplished under the current criminal statutes of the U.S. Code.[93] While there are many possible charging strategies for deepfake fraud, this Part suggests the most straightforward charging methodology for federal prosecutors to follow when encountering the model scenario.[94] Specifically, the Author recommends charging wire fraud, in violation of 18 U.S.C. § 1343; and aggravated identity theft, in violation of 18 U.S.C. § 1028A.[95]

As discussed below, it is in the best interest of the federal prosecution effort to consider charging both wire fraud and aggravated identity theft where the elements of those offenses are supported by the evidence.[96] Compared to alternative statutes like money laundering or identity fraud, wire fraud is the most appropriate charge because of the simplicity of its elements and its scalability for prosecuting conspiracies.[97] It also offers appropriate sentencing options under the U.S. Sentencing Guidelines, though as discussed further in Part III of this Article, it lacks appropriate specific offense enhancements responsive to the unique facts of deepfake fraud.[98]

For the purposes of prosecuting the model scenario, wire fraud is also the most readily proven predicate offense for aggravated identity theft.[99] Aggravated identity theft provides federal prosecutors with a powerful mechanism to deter criminal conduct by carrying a mandatory consecutive two-year term of imprisonment in addition to whatever sentence the predicate offense carries.[100] Aggravated identity

---

93. *See e.g.,* 18 U.S.C. § 1028A(a)(1) (prohibiting aggravated identity theft); 18 U.S.C. § 1343 (prohibiting fraud by wire, radio, or television).

94. According to the Department of Justice's Justice Manual, federal prosecutors are expected to charge "the most serious offense that is encompassed by the defendant's conduct *and* that is likely to result in a sustainable conviction." U.S. Dep't of Just., Justice Manual § 9-27.000 (emphasis added), https://www.justice.gov/jm/jm-9-27000-principles-federal-prosecution#9-27.300 [https://perma.cc/ZZB4-RYLE] (last updated Feb. 2024). The proposed charging methodology presented in this Article aligns with that principle for the reasons discussed in this Part.

95. *See infra* Section II.A.

96. *See infra* Section II.A.

97. *See infra* Section II.A.

98. *See infra* Part III. *See generally* U.S. SENT'G GUIDELINES MANUAL § 2B1.1(b) (U.S. SENT'G COMM'N 2023) (containing no specific sentencing enhancements for deepfake fraud).

99. *See infra* Section II.B.

100. *See infra* Section II.B; 18 U.S.C. § 1028A(a)(1).

theft charges offer a powerful incentive for defendants to cooperate because that two-year term of imprisonment can only be reduced upon motion from the prosecution based on a defendant's substantial assistance.[101] As discussed further in Section II.B, this encourages defendants to cooperate with the prosecution, which is mutually advantageous to both parties.[102]

A. Wire Fraud: 18 U.S.C. § 1343

If a federal prosecutor encounters the model scenario, the case should be charged as a violation of 18 U.S.C. § 1343, the traditional wire fraud statute. In relevant part, the statute provides:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.[103]

1. Proving wire fraud

To demonstrate wire fraud, prosecutors must prove the following elements beyond a reasonable doubt: (1) the defendant knowingly devised or intended to devise any scheme to defraud; (2) the scheme to defraud employed false material representations, pretenses, or promises; (3) the defendant transmitted or caused to be transmitted by way of wire, radio, or television communications, in interstate or foreign commerce, any writing, sign, signal, picture, or sound for the purpose of executing such scheme; and (4) the defendant acted with a specific intent to defraud.[104]

---

101. *See* 18 U.S.C. § 3553(e).

102. *See infra* Section II.B.

103. 18 U.S.C. § 1343.

104. This is a modified version of the Fifth Circuit's Pattern Jury Instruction for wire fraud. *See* 2.57 WIRE FRAUD: MONEY/ PROPERTY OR HONEST SERVICES 18 U.S.C. § 1343 [18 U.S.C. § 1346], *in* COMM. ON PATTERN JURY INSTRUCTIONS, DIST. JUDGES ASS'N FIFTH CIR., PATTERN JURY INSTRUCTIONS (CRIMINAL CASES) 263 (2019) [hereinafter PATTERN JURY INSTRUCTION 2.57], https://www.lb5.uscourts.gov/juryinstructions/fifth/crim2019.pdf [https://perma.cc/A6WZ-Z66A]. There can be some variation in the wording or construction of elements between circuits. *See, e.g.*, 15.35 WIRE FRAUD (18 U.S.C.

The first, second, and fourth elements of wire fraud are easily satisfied when prosecuting the model scenario. A scheme to defraud, as required by the first element, "means any plan, pattern, or course of action intended to deprive another of money or property or bring about some financial gain to the person engaged in the scheme."[105] A representation, pretense, or promise employed in a scheme to fraud, as required in the second element, "is 'false' if it is known to be untrue or is made with reckless indifference as to its truth or falsity" and it "is 'material' if it has a natural tendency to influence, or is capable of influencing, the decision of the person or entity to which it is addressed."[106] The use of a deepfake to instigate the transfer of funds is itself the scheme to defraud, constituting a "course of action intended to deprive another of money."[107] Additionally, the deepfake itself satisfies the requirement of being a false material representation. The deepfake is a false representation created by AI and very particularly selected to manipulate the victim that is being used to materially influence the decision-making of the victim.[108] In other words, the victim relies on the illusion of legitimacy created by the deepfake.[109]

The specific intent of the fraudster, as required by the fourth element, is clearly discernable by circumstantial evidence. "A 'specific intent to defraud' means a conscious, knowing intent to deceive or cheat someone."[110] Direct evidence of intent, such as a confession, is

---

§ 1343), *in* NINTH CIRCUIT JURY INSTRUCTIONS COMM., MANUAL OF MODEL CRIMINAL JURY INSTRUCTIONS FOR THE DISTRICT COURTS OF THE NINTH CIRCUIT 361 (2022 ed.), https://www.ce9.uscourts.gov/jury-instructions/sites/default/files/WPD/Criminal_Instructions_2023_08.pdf [https://perma.cc/Y5N7-GWHM] (last updated Aug. 2023) (listing the elements of wire fraud as (1) the defendant knowingly participated in, devised, or intended to devise a scheme or plan to defraud, or a scheme or plan for obtaining money or property by means of false or fraudulent pretenses, representations, promises, or omitted facts; (2) the statements made or facts omitted as part of the scheme were material; (3) the defendant acted with the intent to defraud; and (4) the defendant used, or caused to be used, an interstate or foreign wire communication to carry out or attempt to carry out an essential part of the scheme).

105. PATTERN JURY INSTRUCTION 2.57, *supra* note 104, at 263.
106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.*
110. *Id.*

not necessary to successfully prosecute the model scenario.[111] "Direct evidence of an intent to defraud is rare; a specific intent to defraud may be shown, however, by circumstantial evidence and inferences drawn from the scheme itself that show that the scheme was reasonably calculated to deceive individuals of ordinary prudence and comprehension."[112] The model scenario provides ample circumstantial evidence showing the fraudster's intent. The deepfake is uniquely created to target a particular victim, which is apparent because it is designed to mimic a known third party affiliated with the victim.[113] The deepfake, which is controlled by the fraudster or their affiliates, specifically directs the transfer of funds, so it is apparent the fraudster is attempting to deceive the victim into causing the wire transmission.[114]

The potentially more complicated component of the offense is its third element: that the defendant transmitted or caused to be transmitted by way of wire, radio, or television communications, in interstate or foreign commerce, any writing, sign, signal, picture, or sound for the purpose of executing such scheme.[115] Proving this element involves satisfying three sub-requirements: first, that the transmission moved by wire, radio, or television communication;

---

111. *See e.g.,* United States v. Sloan, 492 F.3d 884, 890–91 (7th Cir. 2007) (finding that there was sufficient evidence of a scheme to defraud through the defendant's half-truths in his advertisements and not listing his own name to the registration).

112. *Id.* at 891 (citing United States v. Stephens, 421 F.3d 503, 509 (7th Cir. 2005)); *see also* United States v. Vance, 956 F.3d 846, 855 (6th Cir. 2020) ("[G]iven the general nature of fraud crimes, direct evidence of a defendant's fraudulent intent is typically not available; therefore, this court allows specific intent to defraud [to] be established by circumstantial evidence and by inferences drawn from examining the scheme itself which demonstrate that the scheme was reasonably calculated [by the defendant] to deceive persons of ordinary prudence and comprehension." (internal quotation marks omitted) (quoting United States v. Winkle, 477 F.3d 407, 413 (6th Cir. 2007))); United States v. Rogers, 321 F.3d 1226, 1230 (9th Cir. 2003) ("It is settled law that intent to defraud may be established by circumstantial evidence." (citing United States v. Plache, 913 F.2d 1375, 1381 (9th Cir. 1990))).

113. *See* PATTERN JURY INSTRUCTION 2.57, *supra* note 104, at 263–64 ("What must be proved beyond a reasonable doubt is that the defendant knowingly devised or intended to devise a scheme . . . ."); s*ee, e.g.*, Johnson & Johnson, *supra* note 21 (discussing how deepfakes are created "with the end goal of portraying something that didn't actually occur in reality").

114. *See* PATTERN JURY INSTRUCTION 2.57, *supra* note 104, at 264 (explaining that to establish wire fraud, you must show that the use of the communications through interstate commerce was related to the scheme).

115. *Id.* at 263.

second, that the transmission moved in either interstate or foreign commerce; and third, that the transmission was a writing, sign, signal, picture, or sound that furthers the fraudulent scheme.[116] It is not required that the fraudster intend the use of a particular wire; knowledge that the use of wires will follow in the ordinary course of business or are reasonably foreseeable is sufficient.[117] Furthermore:

> It is also not necessary that the government prove that the material transmitted by wire [radio] [television] communications was itself false or fraudulent, or that the use of the interstate [foreign] wire communications facilities was intended as the specific or exclusive means of accomplishing the alleged fraud. What must be proved beyond a reasonable doubt is that the use of the interstate [foreign] wire communications facilities was closely related to the scheme because the defendant either wired something or caused it to be wired in interstate [foreign] commerce in an attempt to execute or carry out the scheme.[118]

There are at least two different methodologies a federal prosecutor may follow to satisfy this element: they may focus on the transmission of the deepfake or the transmission of victim's money. Between these two options, focusing on the money transmission is likely the more effective strategy.

---

116. *Id.*

117. *See, e.g.*, United States v. Mullins, 613 F.3d 1273, 1280 (10th Cir. 2010) ("To sustain her convictions [for wire fraud], the evidence need not go so far as to prove she 'specifically intend[ed] for use of this or that wire,' but it must at least show that Ms. Mullins did 'an act with knowledge that the use of the wires will follow in the ordinary course of business, or where such use can reasonably be foreseen, even though not actually intended.'" (alteration in original) (quoting United States v. Wittig, 575 F.3d 1085, 1099 (10th Cir. 2009))); United States v. Jinian, 725 F.3d 954, 960 (9th Cir. 2013) ("One 'causes' use of . . . wire communications where such use can reasonably be foreseen, even though not specifically intended." (alteration in original) (quoting United States v. Cusino, 694 F.2d 185, 188 (9th Cir. 1982))).

118. PATTERN JURY INSTRUCTION 2.57, *supra* note 104, at 264 (alterations in original); *see also Jinian*, 725 F.3d at 960 ("A wire communication is 'in furtherance' of a fraudulent scheme if it is 'incident to the execution of the scheme,' meaning that it 'need not be an essential element of the scheme, just a "step in the plot."'" (internal citations omitted) (quoting United States v. Lo, 231 F.3d 471, 478 (9th Cir. 2020); and then quoting United States v. Garlick, 240 F.3d 789, 795 (9th Cir. 2001))); United States v. Ford, 603 F.2d 1043, 1047 (2d Cir. 1979) (internal citations omitted) ("To prove that interstate wire facilities were used in furtherance of a fraudulent scheme the government must show not that the wire transmission was an essential element, but simply that it was for the purpose of executing the scheme." (internal citations omitted)).

First, a federal prosecutor may try to argue that the transmission of the deepfake to communicate with the victim satisfies the third element.[119] Despite the wide variety of deepfakes, they can all be described either as a writing, sign, signal, picture, or sound.[120] Because the fraud inevitably occurs through the perpetrator's use of some type of remote communication—by phone call, video conference, or some similar type of exchange—the deepfake is also necessarily transmitted by some kind of wire.[121] The potential difficulty of this prosecution strategy ultimately falls along the jurisdictional component of the element: that the transmission moved in either interstate or foreign commerce.[122] Multiple federal courts of appeals have held that the prosecution must demonstrate that the communication actually crossed a state border to support a conviction.[123] In other words, "[t]he use of the internet alone is insufficient to establish the required interstate nexus."[124]

Because of technologies such as virtual private networks ("VPNs"), it can often be difficult for investigators to track the exact origin of a cyberfraudster's activity. "A VPN . . . allows internet users to browse the web while keeping their identities and locations hidden."[125] While

---

119. *See* PATTERN JURY INSTRUCTION 2.57, *supra* note 104, at 263 (stating that the third element of wire fraud requires showing that there was some sort of transmission of a writing, sign, signal, picture, or sound by wire in interstate commerce to satisfy 18 U.S.C. § 1343).

120. *See supra* Section II.A.

121. *See* PATTERN JURY INSTRUCTION 2.57, *supra* note 104, at 263 (requiring transmission "by way of wire"); *Deepfake*, *supra* note 75 (describing that fraud through deepfakes is achieved by impersonating individuals on live video or phone calls through a generated video, image, or audio).

122. PATTERN JURY INSTRUCTION 2.57, *supra* note 104, at 263.

123. *See, e.g.*, United States v. Kieffer, 681 F.3d 1143, 1153 (10th Cir. 2012) ("[W]e recognize[] that § 1343's '"in commerce" terminology has been repeatedly held to require that communications actually cross state lines to support a conviction.'"(quoting United States v. Schaefer, 501 F.3d 1197, 1202 (10th Cir. 2007)); United States v. Biyiklioglu, 652 F. App'x 274, 280 (5th Cir. 2016) (per curiam) (unpublished opinion) ("A conviction under § 1343 'requires that the wire communication cross state lines.'" (quoting *Ayres*, 845 F.2d at 1366)).

124. *Biyiklioglu*, 652 F. App'x at 280 (citing *Kieffer*, 681 F.3d at 1155) ("'[O]ne individual's use of the internet, "standing alone," does not establish an interstate transmission . . . because the origin and host servers, whether one and the same or separate, might be located in the same state as the computer used to access the website.'" (quoting *Kieffer*, 681 F.3d at 1155)).

125. Laurens Cerulus, *Police Take Down VPN Service Used by Cybercriminals*, POLITICO (Jan. 18, 2022, 11:00 AM), https://www.politico.eu/article/police-germany-take-down-vpn-cybercriminals [https://perma.cc/BZQ9-Y7N2].

VPNs can improve cybersecurity for normal users, they can also camouflage cyberfraudsters.[126] Using VPNs, criminals can "connect to a server in a different country and spoof [their] location[,] . . . hiding [their] true IP address behind the IP address of a VPN server" and obscuring their true location.[127] As a result, investigators may find it difficult to identify the geographic location where the fraudster is initiating their attack, which could complicate a prosecution following this strategy.[128]

Federal prosecutors can avoid this complicated issue by instead focusing on the wire transmission of money rather than on the transmission of the deepfake itself. The model scenario inevitably creates at least one easily identified wire transfer: the transmission of funds from the victim's bank account to a bank account identified by the fraudster.[129] As noted above, the third element of wire fraud can be satisfied using wires that "the defendant . . . caused to be transmitted" and it is sufficient that the wire transmission is reasonably foreseeable as a byproduct of the fraudulent scheme.[130] Because the natural consequence of the defendant's scheme is to foreseeably cause a victim to wire transmit the money, this is an acceptable wire to satisfy the element's jurisdictional requirement. Interviews with employees of

---

126. *Id.* (reporting on a coordinated multinational effort to take down servers for VPNLab.net, described by Europol as "a popular choice for cybercriminals, who could use its services to carry on committing their crimes without fear of detection by authorities" (internal quotations omitted)).

127. Max Eddy & Chris Stobing, *Why You Need a VPN, and How to Choose the Right One*, PC MAG., https://www.pcmag.com/how-to/what-is-a-vpn-and-why-you-need-one [https://perma.cc/KE2L-4FC4] (last updated Dec. 27, 2023).

128. If the location of the VPN server being used by the fraudster is discernable and it is located across state or international lines from the victim, federal prosecutors may also argue that the wire transmission between the VPN server and the victim's location satisfies the third element of wire fraud.

129. *See generally* PATTERN JURY INSTRUCTION 2.57, *supra* note 104, at 264–65 (discussing intent and the usage of a wire in a scheme to defraud).

130. *Id.* at 263 (alteration omitted); *see also* United States v. Mullins, 613 F.3d 1273, 1280 (10th Cir. 2010) (quoting *Wittig*, 575 F.3d at 1099) (stating evidence does not need to prove specific intent, just that person acted with knowledge); Pereira v. United States, 347 U.S. 1, 8–9 (1954) ("Knowledge that the use of the mails will follow in the ordinary course of business, or where such use can reasonably be foreseen, even though not actually intended, then he 'causes' the mails to be used."); United States v. Jinian, 725 F.3d 954, 960 (9th Cir. 2013) ("'One 'causes' use of . . . wire communications where such use can reasonably be foreseen, even though not specifically intended.'" (quoting United States v. Cusino, 694 F.2d 185, 188 (9th Cir. 1982))).

the transferring and receiving financial institutions will reveal how the money moves during wire transmissions and will help federal prosecutors demonstrate a clear interstate (or international) wire transmission.[131]

Furthermore, if the victim's bank uses the Automated Clearing House ("ACH") network to facilitate wire transfers, it may be even easier for investigators to identify the path of a wire transmission. "An ACH is an electronic fund transfer made between banks and credit unions across what is called the Automated Clearing House network. ACH is used for all kinds of fund transfer transactions . . . ."[132] ACH transfers "may be used to transfer funds to individuals or businesses in the United States or abroad."[133] There are two only ACH operators—the Federal Reserve and The Clearing House—meaning all ACH transfers necessarily involve transmission through locations controlled by one of these two operators.[134] Because the ACH network is only located in a limited number of states,[135] identifying both the original location of the victim's wire transmission and the clearing house that processed the transmission of funds may provide a clear interstate wire to satisfy the third element.

2. Scalability of wire fraud for prosecuting conspiracies

In addition to being the most straightforward charge for federal prosecutions of deepfake fraudsters, wire fraud is also easily scalable to prosecute a conspiracy if the evidence identifies a network of co-conspirators. 18 U.S.C. § 1349 provides: "Any person who attempts or

---

131. *See also* JEAN-PIERRE BRUN, LARISSA GRAY, CLIVE SCOTT, KEVIN M. STEPHENSON, STOLEN ASSET RECOVERY INITIATIVE, THE WORLD BANK ASSET RECOVERY HANDBOOK: A GUIDE FOR PRACTITIONERS 19–20 (2011), https://www.unodc.org/documents/corruption/Publications/StAR/StAR_Publication_-_Asset_Recovery_Handbook.pdf [https://perma.cc/K4KR-9GBC] (explaining that money laundering legislation requires financial institutions to file reports regarding suspicious activity).

132. *What is an ACH?*, CFBP, https://www.consumerfinance.gov/ask-cfpb/what-is-an-ach-en-1065 [https://perma.cc/C73S-BHW4] (last reviewed Aug. 27, 2020).

133. *Can I Use the Automated Clearing House (ACH) Network to Transfer Funds Abroad?*, CFBP, https://www.consumerfinance.gov/ask-cfpb/can-i-use-the-automated-clearing-house-ach-network-to-transfer-funds-abroad-en-1165 [https://perma.cc/R77T-Y47Y] (last reviewed Jan. 8, 2024).

134. *How ACH Payments Work*, NACHA, https://www.nacha.org/content/how-ach-payments-work [https://perma.cc/6TX5-HH8K].

135. *The Twelve Federal Reserve Districts*, BD. OF GOVERNORS OF THE FED. RSRV. SYS., https://www.federalreserve.gov/aboutthefed/federal-reserve-system.htm [https://perma.cc/5RZM-YQLB] (last updated Apr. 24, 2017).

conspires to commit any offense under [Chapter 63 of Title 18 of the U.S. Code] shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy."[136] "To be convicted of conspiracy under § 1349, the jury must find: (1) two or more persons agreed to commit fraud; (2) the defendant knew the unlawful purpose of the agreement; and (3) the defendant joined the agreement with the intent to further the unlawful purpose."[137] By charging conspiracies where appropriate, federal prosecutors can potentially leverage co-conspirators as cooperators, helping to facilitate the destruction of an entire fraud network while also potentially gaining cooperating defendants who are willing to provide valuable insight into the strategies used by fraudsters on the cutting edge of deepfake technology.[138]

3. Sentencing wire fraud

Federal sentencing principles require federal judges to consider the U.S. Sentencing Guidelines ("Sentencing Guidelines") when determining an appropriate sentence for a defendant.[139] To put it simply, under the Sentencing Guidelines, to determine the sentencing range applicable to a defendant, federal judges determine the offense level of a crime under a particular Sentencing Guideline section, consider any appropriate adjustments to the offense level, identify the defendant's Criminal History Category, and then filter that

136. 18 U.S.C. § 1349.

137. United States v. Beacham, 774 F.3d 267, 272 (5th Cir. 2014) (citing United States v. Grant, 683 F.3d 639, 643 (5th Cir. 2012)); *see also* United States v. Rogers, 769 F.3d 372, 377 (6th Cir. 2014) (explaining that to sustain a conviction under 18 U.S.C. § 1349, in addition to proving wire fraud, "the government also was required to establish beyond a reasonable doubt that 'two or more persons conspired, or agreed, to commit the crime of [wire fraud]' and 'that the defendant knowingly and voluntarily joined the conspiracy'" (alteration in the original) (quoting SIXTH CIRCUIT PATTERN JURY INSTRUCTION 3.01A)).

138. *See infra* note 186 and accompanying text.

139. Federal judges must consider the U.S. Sentencing Guidelines when determining a sentence, but they are not bound by them. *See* 18 U.S.C. § 3553(a)(4) ("The court, in determining the particular sentence to be imposed, shall consider . . . the kinds of sentence and sentencing range established for . . . the applicable category of offense committed by the applicable category of defendant as set forth in the guidelines . . . issued by the Sentencing Commission . . . ."); *see also* United States v. Booker, 543 U.S. 220, 245 (2005) (holding that the U.S. Sentencing Guidelines are advisory, not mandatory).

information through a table that yields a sentencing range.[140] The offense levels range from one to forty-three, and the Criminal History Categories range from one to six.[141] The lowest range of imprisonment is zero to six months, while the highest is life imprisonment.[142]

Appendix A of the Sentencing Guidelines, which "specifies the offense guideline section(s) . . . applicable to the statute of conviction," provides that 18 U.S.C. § 1343 is referenced to Sentencing Guidelines section 2B1.1.[143] Because wire fraud carries a statutory maximum penalty of twenty years imprisonment, its base offense level under the Sentencing Guidelines is seven.[144] While this base offense level is low, the specific offense characteristics of wire fraud can dramatically increase the offense level.[145] Among other factors, the amount of loss, the number of victims, and the degree of harm caused to those victims can all result in increases in the offense level.[146] If, as in the Hong Kong example discussed in the introduction, a loss equaled approximately $35,000,000, the Sentencing Guidelines would apply a twenty-two level increase, bringing the offense level to twenty-nine before considering any other adjustments.[147] For a first time offender, this would increase the imprisonment range from zero to six months up to eighty-seven to 108 months.[148]

Federal prosecutors should argue that the use of deepfakes to perpetrate the fraudulent scheme constitutes sophisticated means, which yields an additional two-level enhancement under the

---

140. *See* U.S. SENT'G COMM'N, AN OVERVIEW OF THE FEDERAL SENTENCING GUIDELINES 3, https://www.ussc.gov/sites/default/files/pdf/about/overview/Overview_Federal_Sentencing_Guidelines.pdf [https://perma.cc/F8PA-7HWF]; U.S. SENT'G GUIDELINES MANUAL, *supra* note 98, ch. 5, pt. A (sentencing table).

141. U.S. SENT'G GUIDELINES MANUAL, *supra* note 98, ch. 5, pt. A (sentencing table).

142. *Id.*

143. *Id.* app. A.

144. 18 U.S.C. § 1343 (statutory maximum penalty); U.S. SENT'G GUIDELINES MANUAL, *supra* note 98, § 2B1.1(a)(1).

145. U.S. SENT'G GUIDELINES MANUAL, *supra* note 98, § 2B1.1(a)(1). For the rules regarding determination of loss under § 2B1.1, see *id.* § 2B1.1(b)(3).

146. *Id.* § 2B1.1(b)(1)–(2). In fiscal year 2022, the median loss for offenses involving theft, property destruction, and fraud was $160,737. U.S. SENT'G COMM'N, QUICK FACTS THEFT, PROPERTY DESTRUCTION, AND FRAUD OFFENSES FISCAL YEAR 2022 1 (2023), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Theft_Property_Destruction_Fraud_FY22.pdf [https://perma.cc/7YNE-HL4H]. "12.9% involved loss amounts of $6,500 or less . . . [and] 17.5% involved loss amounts greater than $1.5 million." *Id.*

147. U.S. SENT'G GUIDELINES MANUAL, *supra* note 98, § 2B1.1(b)(1)(L).

148. *Id.* ch. 5, pt. A (sentencing table).

Sentencing Guidelines.[149] A fraud includes sophisticated means when it involves "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense."[150] The prosecution should appropriately argue that the crime involves complex and intricate offense conduct because the model scenario involves stealing the means of identification of a real person in order to trick the victim and then filtering those means of identification through artificial intelligence to create a deepfake.[151]

While section 2B1.1 does contain substantial enhancements based on the amount of loss sustained through the fraud, it offers limited enhancements specifically targeted to punish the unique offense characteristics of identity theft that are intrinsically intertwined with deepfake-based wire fraud. This problem, and a proposed solution to it, are discussed further in Part III.[152]

B. Aggravated Identity Theft: 18 U.S.C. § 1028A

In addition to wire fraud, federal prosecutors encountering the model scenario should consider charging the fraudsters with aggravated identity theft, in violation of 18 U.S.C. § 1028A. Pursuant to § 1028A(a)(1), "[w]hoever, during and in relation to any felony violation enumerated in [§ 1028A(c)], knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years."[153]

> The term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—
>
> (A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
>
> (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

149. *Id.* § 2B1.1(b)(10)(C) ("If . . . the offense otherwise involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means, increase by 2 levels. If the resulting offense level is less than level 12, increase to level 12.").

150. *Id.* § 2B1.1 cmt. 9(B).

151. *Id.*

152. *See infra* Part III.

153. 18 U.S.C. § 1028A(a)(1).

> (C) unique electronic identification number, address, or routing code; or
>
> (D) telecommunication identifying information or access device (as defined in [18 U.S.C. § 1029(e)]).[154]

Included among the enumerated predicate offenses in § 1028A(c) are all crimes contained in Chapter 63 of Title 18, including both wire fraud and conspiracy to commit wire fraud.[155] Accordingly, either of these crimes can be charged in conjunction with aggravated identity theft.

1. Proving aggravated identity theft

In order to prove aggravated identity theft, federal prosecutors must demonstrate that: (1) the defendant knowingly transferred, possessed, or used a means of identification of another person; (2) that the defendant did so without lawful authority; (3) that the defendant transferred, possessed, or used the means of identification of another person during and in relation to the qualifying predicate offense as enumerated in 18 U.S.C. § 1028A(c); and (4) that the defendant knew that the means of identification in fact belonged to another real person, living or dead.[156] The knowledge element can be proven with

---

154. 18 U.S.C. § 1028(d)(7). 18 U.S.C. § 1028(d) instructs that its definitions apply to both 18 U.S.C. § 1028 and 18 U.S.C. § 1028A.

155. 18 U.S.C. § 1028A(c)(5).

156. This is a modified version of the Fifth Circuit's Pattern Jury Instruction (2019) for aggravated identity theft. *Compare* PATTERN JURY INSTRUCTION 2.48C, AGGRAVATED IDENTITY THEFT 18 U.S.C. § 1028A(A)(1), *in* COMM. ON PATTERN JURY INSTRUCTIONS, DIST. JUDGES ASS'N FIFTH CIR., PATTERN JURY INSTRUCTIONS (CRIMINAL CASES) 238 (2019) [hereinafter PATTERN JURY INSTRUCTION 2.48C], https://www.lb5.uscourts.gov/juryinstructions/fifth/crim2019.pdf [https://perma.cc/3LDZ-JHPN], *with* MODEL JURY INSTRUCTION 15.9, FRAUD IN CONNECTION WITH IDENTIFICATION DOCUMENTS—AGGRAVATED IDENTITY THEFT (18 U.S.C. § 1028A), *in* NINTH CIRCUIT JURY INSTRUCTIONS COMM., MANUAL OF MODEL CRIMINAL JURY INSTRUCTION FOR THE DISTRICT COURTS OF THE NINTH CIRCUIT 309 (2022 ed., rev. Mar. 2023) [hereinafter PATTERN JURY INSTRUCTION 15.9], https://www.ce9.uscourts.gov/jury-instructions/sites/default/files/WPD/Criminal_Instructions_2022_3.pdf [https://perma.cc/9CTY-6ZSN] (where the elements of aggravated identity theft are summarized as (1) the defendant knowingly transferred, possessed, or used without legal authority a means of identification of another person or a false identification document; (2) that the defendant knew that the means of identification belonged to a real person; and (3) the defendant did so during and in relation to qualifying predicate offense as enumerated in 18 U.S.C. § 1028A(c)). *See also* Flores-Figueroa v. United States, 556 U.S. 646, 647 (2009) (where the Supreme Court clarified that the prosecution must "show that the defendant *knew* that the 'means of identification' he or she unlawfully transferred, possessed, or used, in fact, belonged to 'another person'").

either direct or circumstantial evidence.[157]

Under the model scenario, most of the elements of aggravated identity theft are necessarily met during the commission of the fraudulent scheme.[158] The fraudster uses the unique biometric data of a real person—their voice—to create a deepfake that can convince the victim to wire transfer the funds.[159] The person in this type of fraud is necessarily real because the existing relationship between the victim and that person is essential to the effectiveness of the deceit.[160] The offender's knowledge of the fact that the means of identification belongs to a real person is demonstrated circumstantially—the fraudster or their associate picked a very particular person to mimic in order to leverage the trust of the preexisting relationship.[161] The only element that may require additional evidence is that the defendant used the means of identification without lawful authority, which could easily be resolved through the testimony of the individual whose biometric data was misused.[162]

---

157. *See* United States v. Valerio, 676 F.3d 237, 244 (1st Cir. 2012) (holding in a section 1028A case, the court noted "when a crime has a knowledge element, 'it is well-established that knowledge may be proven by circumstantial evidence alone; indeed, it frequently cannot be proven in any other way'" (quoting United States v. Agosto-Vega, 617 F.3d 541, 549 (1st Cir. 2010))); United States v. Doe, 842 F.3d 1117, 1120 (9th Cir. 2016) ("While direct evidence of the knowledge element is often presented in § 1028A prosecutions, this Court has recognized that the element can be proven by circumstantial evidence." (citing United States v. Miranda-Lopez, 532 F.3d 1034, 1040 (9th Cir. 2008))); United States v. Doe, 661 F.3d 550, 561–62 (11th Cir. 2011) (discussing multiple Eleventh Circuit cases where aggravated identity theft convictions were affirmed based on circumstantial evidence of the defendant's knowledge (citing United States v. Holmes, 595 F.3d 1255 (11th Cir. 2010); and then citing United States v. Gomez-Castro, 605 F.3d 1245 (11th Cir. 2010))).

158. *See infra* Section II.C.2.

159. *See* Elvira Carrero, *Voice Deepfake: Is It Possible to Detect a Fake Voice?*, MOBBEEL, https://www.mobbeel.com/en/blog/voice-deepfake [https://perma.cc/V6ZL-B3UC] (describing how a deepfake is trained with the voice recordings of a person to generate a synthetic voice that emulated it).

160. *See, e.g.*, Tanushree Saxena, *Deepfake Voice Scam: Emerging Threat*, CYBERPEACE (Apr. 20, 2023), https://www.cyberpeace.org/resources/blogs/deepfake-voice-scam-emerging-threat [https://perma.cc/8R8P-WF46].

161. *See id.* (explaining that by impersonating a familiar relationship, the fraudster raises the likelihood the victim will fall for the hoax).

162. *See id.* (listing the ways a defendant could use the voice recording to scam others).

2. Recent Supreme Court jurisprudence does not undermine the viability of charging aggravated identity theft for the model scenario

The viability of this charge for prosecuting the model scenario is not undermined by the Supreme Court's recent jurisprudence limiting the applicability of aggravated identity theft. In its June 2023 opinion in *Dubin v. United States*,[163] the Supreme Court examined whether aggravated identity theft was an appropriate charge where the use of a means of identification was an ancillary feature of the fraudulent scheme.[164] Dubin was charged and convicted for healthcare fraud, in violation of 18 U.S.C. § 1347; specifically, for creating falsehoods in Medicaid billing that inflated the amount of reimbursement received.[165] In addition to this charge, Dubin was convicted of aggravated identity theft under 18 U.S.C. § 1028A(a)(1), based on the theory that his fraudulent billing submissions to Medicaid included the real patient's Medicaid reimbursement numbers, thereby constituting use of a means of identification in furtherance of the fraudulent scheme.[166] While the district court expressed doubt that the scenario amounted to aggravated identity theft, it denied the defendant's post-trial challenge to the conviction on precedential grounds.[167] The Fifth Circuit affirmed the conviction.[168] Noting that "[m]any lower courts have . . . [followed] more restrained readings of the aggravated identity theft statute," the Supreme Court granted certiorari to resolve the conflict.[169]

The Court explained that the case turns on two elements of aggravated identity theft: the *use* of a means of identification *in relation to* the fraud.[170]

> The Government reads the terms broadly and in isolation. On the Government's view, "[a] defendant uses a means of identification 'in relation to' a predicate offense if the use of that means of identification 'facilitates or furthers' the predicate offense in some way. As to "uses," the Government seems just to mean "employ[s]" in any sense. Section 1028A(a)(1) would thus apply automatically any time a name or other means of identification

163. 599 U.S. 110 (2023).
164. *Id.* at 114.
165. *Id.* at 115.
166. *Id.*
167. *Id.*
168. *Id.*
169. *Id.* at 116.
170. *Id.* at 116–17.

> happens to be part of the payment or billing method used in the commission of a long list of predicate offenses . . . .
>
> Petitioner, in response, offers a more targeted reading. For petitioner, using a means of identification in relation to a predicate offense requires "a genuine nexus to the predicate offense." On this reading, the means of identification is at the crux of what makes the predicate offense criminal, rather than merely an ancillary feature of a payment method. When the underlying crime involves fraud of deceit, as many of § 1028A's predicates do, this entails using a means of identification specifically in a fraudulent or deceitful manner.[171]

After considering the language of the statute and the Court's prior jurisprudence,[172] the Court determined that "[t]aken together, from text to context, from content to common sense, § 1028A(a)(1) is not amenable to the Government's attempt to push the statutory envelope."[173] The Court held "[a] defendant 'uses' another person's means of identification 'in relation to' a predicate offense when this use is at the crux of what makes the conduct criminal," clarifying that "being at the crux of the criminality requires more than a causal relationship."[174] Specifically, "with fraud or deceit crimes like the one in [*Dubin*], the means of identification specifically must be used in a manner that is fraudulent or deceptive. Such fraud or deceit going to identity can often be succinctly summarized as going to 'who' is involved."[175]

Charging aggravated identity theft in response to the model scenario satisfies the Court's new interpretation of the statute. As described above, aggravated identity theft in the model scenario is intrinsically intertwined with wire fraud.[176] The use of a means of identification of a real person—the deepfake—is a necessary component of the fraudulent scheme because it is the mechanism that causes the victim to wire transfer funds.[177] In other words, the deepfake is not an ancillary component of the fraudulent scheme. Instead, it sits "at the crux of what makes the conduct criminal" and is "specifically . . . used

171. *Id.* at 117 (internal citations omitted).
172. *Id.* at 116–31.
173. *Id.* at 131.
174. *Id.* at 131.
175. *Id.* at 131–32.
176. *See supra* notes 165–75 and accompanying text.
177. *Dubin*, 599 U.S. at 131; *see* Saxena, *supra* note 160 (highlighting the role trust based on the voice plays in the scheme).

in a manner that is fraudulent or deceptive."[178] Accordingly, aggravated identity theft is still an appropriate charge under the model scenario.[179]

3. Sentencing aggravated identity theft

For sentencing purposes, aggravated identity theft is a powerful charge for prosecutors. A conviction under the statute mandates a two-year term of imprisonment which must run consecutive to any other term of imprisonment imposed by the sentencing court.[180] Courts are also explicitly prohibited from reducing the defendant's other terms of imprisonment for convictions under other statutes to try to mitigate the mandatory minimum imprisonment requirements imposed for aggravated identity theft.[181] The U.S. Sentencing Guidelines similarly explain that "[s]ection 1028A . . . provides a mandatory term of imprisonment"[182] and that "the guideline sentence is the term of imprisonment required by statute."[183] The Guidelines further note that "Chapters Three (Adjustments) and Four (Criminal History and Criminal Livelihood) shall not apply to that count of conviction."[184]

---

178. *Id.* at 131–32.

179. *Id.* at 131 (holding that the "petitioner did not use the patient's means of identification in relation to a predicate offense within the meaning of § 1028A(a)(1)").

180. 18 U.S.C. §§ 1028A(a)(1), (b)(2). However, "a term of imprisonment imposed on a person for a violation of [18 U.S.C. § 1028A] may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of [18 U.S.C. § 1028A] . . . ." 18 U.S.C. § 1028A(b)(4). "Thus, section 1028A allows but does not require that multiple counts of conviction be served consecutively, or 'stacked' with one another." U.S. SENT'G COMM'N, MANDATORY MINIMUM PENALTIES FOR IDENTITY THEFT OFFENSES IN THE FEDERAL CRIMINAL JUSTICE SYSTEM 8 (2018), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2018/20180924_ID-Theft-Mand-Min.pdf [https://perma.cc/MDA9-KVZH]; U.S. SENT'G GUIDELINES MANUAL *supra* note 98, § 2B1.6 cmt. n.1(A).

181. 18 U.S.C. § 1028A(b)(3) ("[I]n determining any term of imprisonment to be imposed for the felony during which the means of identification was transferred, possessed, or used, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section . . . .").

182. U.S. SENT'G GUIDELINES MANUAL *supra* note 98, § 2B1.6 cmt. n.1(A).

183. *Id.* § 2B1.6(a).

184. *Id.* This mandate is especially significant because the highest category of offenders convicted of aggravated identity theft have little or no prior criminal history (Criminal History Category I). *See* U.S. SENT'G COMM'N, QUICK FACTS SECTION 1028A

The only mechanism which allows the court to sentence below the mandatory minimum two-year term of imprisonment for aggravated identity theft is a motion by the prosecution for substantial assistance pursuant to 18 U.S.C. § 3553(e).[185] Defendants that seek to benefit from a substantial assistance motion by the prosecution may be inclined to proffer or cooperate with the prosecution team, which can provide numerous benefits to the government.[186] This type of assistance can potentially identify other confederates or co-conspirators working with the defendant.[187] The defendant may also be willing to explain how they created or accessed the deepfake, assisting prosecutors and investigators by providing them with additional insight into how criminals are using artificial intelligence and deepfake technology.[188]

AGGRAVATED IDENTITY THEFT OFFENSES FISCAL YEAR 2022 1 (2023), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Aggravated_Identity_Theft_FY22.pdf [https://perma.cc/NTQ6-TF73] (48.6% of offenders convicted under 18 U.S.C. § 1028A had little or no criminal history category, while the next closest category of offenders were in Criminal History Category 3 (16.4%)).

185. 18 U.S.C. § 3553(e) ("Upon motion of the Government, the court shall have the authority to impose a sentence below a level established by statute as a minimum sentence so as to reflect a defendant's substantial assistance in the investigation or prosecution of another person who has committed an offense."); *see also* U.S. SENT'G GUIDELINES MANUAL, *supra* note 98, § 5K1.1 (policy statement on substantial assistance); MANDATORY MINIMUM PENALTIES FOR FEDERAL IDENTITY THEFT OFFENSES, *supra* note 180, at 10 ("Offenders may receive relief from the aggravated identity theft mandatory minimum penalty if the prosecution files a motion based on the defendant's 'substantial assistance' pursuant to 18 U.S.C. § 3553(e). When such motion is filed, section 3553(e) authorizes the court to impose a sentence below the mandatory minimum penalty." (footnote omitted)).

186. Communication between the defendant and the prosecution can occur during a proffer (where the defendant does not have to agree to become a full cooperator but can still provide information advantageous to the government) or it could result from a full cooperation agreement with the prosecution. Both types of communication are covered by written agreements between the prosecution and the defendant. For an example of a proffer, see Ben Protess, Alan Feuer & Maggie Haberman, *Giuliani Sat for Voluntary Interview in Jan. 6 Investigation*, N.Y. TIMES (June 28, 2023), https://www.nytimes.com/2023/06/28/us/politics/giuliani-jan-6-investigation.html [https://perma.cc/PW3N-GBX9].

187. *See* Max Soni, *What Is a Proffer Agreement?*, SPODEK L. GRP., https://www.federallawyers.com/criminal-defense/what-is-a-proffer-agreement [https://perma.cc/735G-GQWK] (last updated Mar. 21, 2024) (explaining that with a proffer agreement there is incentive for a defendant to identify others involved).

188. *See id.* (discussing how providing substantial cooperation is one of the only ways to reduce a sentence).

Moreover, the advantages of substantial assistance inure to the benefit of both parties, not just the prosecution. According to data published by the U.S. Sentencing Commission, substantial assistance motions created significant downward departures for aggravated identity theft defendants during fiscal year 2022.[189] For the defendants who were only convicted of a violation of aggravated identity theft, the average sentence reduction for a substantial assistance departure was 67.4%, turning a mandatory twenty-four month term of imprisonment into just below eight months of confinement.[190] Similarly, the defendants who were convicted of aggravated identity theft and at least one other offense benefitted from a sentenced reduction of 59.8% for substantial assistance.[191] Given that the average sentence for offenders convicted of both § 1028A and another offense was fifty months, this resulted in an almost thirty (30) month average reduction in the sentence.[192]

C. A Brief Commentary on Other Charging Methodologies: Why Money Laundering and Identity Fraud Are Not Preferred to Wire Fraud and Aggravated Identity Theft

While the charging methodology proposed in this Article is the easiest way to charge a case with facts analogous to the model scenario, it is not the only way to charge such a case. Under the right circumstances, prosecutors may consider additional charges. For example, a federal prosecutor may consider charging a money laundering offense, in violation of 18 U.S.C. §§ 1956 or 1957; or fraud and related activity in connection with identification documents, authentication features, and information, in violation of 18 U.S.C. § 1028 ("identity fraud").[193] These charges could be brought in

189. QUICK FACTS SECTION 1028A AGGRAVATED IDENTITY THEFT OFFENSES FISCAL YEAR 2022, *supra* note 184, at 2.

190. *Id.*

191. *Id.* Twenty-four months reduced by 67.4% calculates to 7.824 months of imprisonment, meaning an average reduction in sentence of just over sixteen months.

192. *Id.* at 1–2. Fifty months reduced by 59.8% calculates to 20.1 months of imprisonment, meaning an average reduction in sentence of just under thirty months.

193. To distinguish aggravated identity theft (18 U.S.C. § 1028A) and avoid confusion, the Author refers to the different charges in 18 U.S.C. § 1028 collectively as "identity fraud." In fact, 18 U.S.C. § 1028(a) contains eight different types of identity theft and identity fraud charges. When discussing identity fraud, the Author is generally referring to 18 U.S.C. § 1028(a)(7) because, as discussed below, it is the only provision of 18 U.S.C. § 1028 which could reasonably be charged when prosecuting the model scenario. *See infra* Section II.C.2.

conjunction with, or independent of, the offenses suggested above in Sections II.A and II.B.

This Article does not focus on money laundering or identity fraud as a charging strategy and therefore does not provide the same detailed analysis of the elements of those offenses. Nonetheless, it is important to explain why charges like money laundering and identity fraud are not preferred over charging wire fraud and aggravated identity theft.[194] As discussed below, both of these charges are harder to prove than wire fraud and do not offer benefits or tools to the prosecution commensurate with that added difficulty.[195]

Additionally, as a statutory matter, federal prosecutors cannot charge aggravated identity theft with the relevant money laundering or identity fraud statutes that would be appropriate to charge in prosecuting the model scenario.[196] The inability to charge aggravated identity theft is independently sufficient justification to charge wire fraud over alternatives that cannot satisfy § 1028A's predicate requirements.[197]

---

194. Beyond money laundering and identity fraud, there are of course other criminal charges that could be considered in relation to the model scenario. However, many of these other charges are even less compelling alternatives. For example, if a prosecution team discovers a conspiracy perpetrating the deepfake fraud, the federal prosecutor could simply present a charge alleging a violation of 18 U.S.C. § 371 to the grand jury, alleging a general conspiracy rather than charging a wire fraud conspiracy in violation of 18 U.S.C. § 1349. The maximum term of imprisonment for general conspiracy is only five years, 18 U.S.C. § 371, compared to wire fraud conspiracy's twenty years, reducing the defendant's punitive exposure while offering the government no benefit, *id.* § 1343. Charging this type of offense when a more serious provable offense exists also contradicts charging principles of the Justice Manual. *See* U.S. Dep't of Just., Just. Manual § 9-27.300 (2024) [hereinafter Justice Manual], https://www.justice.gov/jm/jm-9-27000-principles-federal-prosecution [https://perma.cc/JMW8-2PPY] ("[P]rosecutors should consider whether the consequences of those charges for sentencing would yield a result that is proportional to the seriousness of the defendant's conduct, and whether the charge achieves such purposes of the criminal law as punishment, protection of the public, specific and general deterrence, and rehabilitation."). However, this may not be the scenario if offering the charge with a lower statutory maximum is an incentive to an early cooperator to plead guilty, when the value of the assistance justifies the benefit of a reduced statutory maximum. *See* Justice Manual, *supra* note 194, § 9-27.400 (relating to plea agreements generally); *id.* § 9-27.430 (selecting plea agreement charges).

195. *See infra* Section II.C.1.

196. *See* 18 U.S.C. § 1028A(c) (listing the predicate offenses for aggravated identity theft, which do not include any of the money laundering statutes and specifically excludes 18 U.S.C. § 1028(a)(7)).

197. *See id.* (listing the predicate offenses for aggravated identity theft).

1. Money laundering: 18 U.S.C. §§ 1956 and 1957

"The Federal statutes proscribing money laundering were enacted in 1986 with the passage of the Money Laundering Control Act, codified at 18 U.S.C. §§ 1956 and 1957."[198] Money laundering under § 1956 "outlaws four kinds of laundering—promotional, concealment, structuring, and tax evasion—committed or attempted under one or more of three jurisdictional conditions (i.e., laundering involving certain financial transactions, laundering involving international transfers, and stings)."[199] "The majority of Section 1956's crimes are related in one way or another to the commission or purported commission of at least one of a list of predicate offenses," more commonly known as specified unlawful activities.[200] While § 1956 "does not make simply spending or depositing tainted money a separate crime," 18 U.S.C. § 1957 does.[201] Section 1957 penalizes the knowing engagement or attempted engagement in a monetary transaction in criminally derived property of a value greater than $10,000 when derived from a specified unlawful activity.[202] Money laundering's conspiracy statute, 18 U.S.C. § 1956(h), covers conspiracies that violate either (or both) of §§ 1956 and 1957, making money laundering scalable to effectively prosecute entire organizations of criminals, similar to wire fraud.[203]

Criminal money laundering charges present unique opportunities for asset forfeiture.[204] "The effective use of both criminal and civil asset

198. Justice Manual, *supra* note 194, § 9-105.100.

199. CHARLES DOYLE, CONG. RSCH. SERV., MONEY LAUNDERING: AN ABRIDGED OVERVIEW OF 18 U.S.C. § 1956 AND RELATED FEDERAL CRIMINAL LAW 1 (Nov. 2017), https://crsreports.congress.gov/product/pdf/RS/RS22401/11 [https://perma.cc/RY3N-V724].

200. *Id. See generally* 18 U.S.C. § 1956(c)(7) (defining specified unlawful activity).

201. DOYLE, *supra* note 199, at 2.

202. 18 U.S.C. § 1957.

203. *See* 18 U.S.C. § 1956(h) ("Any person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy."); *id.* § 1349 (prescribing a wire fraud conspiracy offense by "[a]ny person who attempts or conspires to commit any offense under this chapter").

204. The Department of Justice's Asset Forfeiture Program has four primary goals:

> 1. To punish and deter criminal activity by depriving criminals of property used in or acquired through illegal activities.
>
> 2. To promote and enhance cooperation among federal, state, local, tribal, and foreign law enforcement agencies.

forfeiture is an essential component of the Department of Justice's efforts to combat the most sophisticated criminal actors and organizations—including terrorist financiers, cyber criminals, fraudsters, human traffickers, and transnational drug cartels."[205] Pursuant to 18 U.S.C. § 982(a)(1), "[t]he court, in imposing sentence on a person convicted of an offense in violation of [18 U.S.C. §§] 1956, 1957, or 1960 . . . , shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property."[206] In certain money laundering cases, this has been interpreted to extend to include the forfeiture of commingled funds or property acquired using commingled funds—in other words, the forfeiture of legitimate funds when they have been mixed with illicit laundered funds to facilitate the criminal scheme.[207] Asset forfeiture mechanisms for wire fraud are comparably limited, generally permitting collection of proceeds only.[208]

---

3. To recover assets that may be used to compensate victims when authorized under federal law.

4. To ensure the [Asset Forfeiture] Program is administered professionally, lawfully, and in a manner consistent with sound public policy.

U.S. DEP'T OF JUST., ATT'Y GEN. GUIDELINES ON THE ASSET FORFEITURE PROGRAM 1 (2018), https://www.justice.gov/media/983596/dl [https://perma.cc/ED9S-QVYX]. "To achieve these goals the Department of Justice should use asset forfeiture to the fullest extent possible to investigate, identify, seize, and forfeit the assets of criminals and their organizations while ensuring that due process rights of all property owners are protected." *Id.*

205. *Id.*

206. 18 U.S.C. § 982(a)(1).

207. *See, e.g.*, United States v. Puche, 350 F.3d 1137, 1153 (11th Cir. 2003) ("Forfeiture of commingled funds, however, is proper when the government demonstrates that the defendant pooled the funds to facilitate or 'disguise' his illegal scheme." (quoting United States v. Bornfield, 145 F.3d 1123, 1135 (10th Cir. 1998))); United States v. McGauley, 279 F.3d 62, 76–77 (1st Cir. 2002) (affirming forfeiture of commingled funds following a money laundering conviction (citing *Bornfield*, 145 F.3d at 1135; United States v. Tencer, 107 F.3d 1120, 1135 (5th Cir. 1997); and then citing United States v. Baker, 227 F.3d 955, 970 n.4 (7th Cir. 2000))).

208. 18 U.S.C. § 982(a)(2) ("The court, in imposing sentence on a person convicted of a violation of, or a conspiracy to violate . . . [18 U.S.C. § 1343], . . . affecting a financial institution, . . . shall order that the person forfeit to the United States any property constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of such violation."); *see also id.* § 982(a)(3)(F) (providing an additional criminal asset forfeiture provision for wire fraud convictions involving the sale of assets acquired or held by the Federal Deposit Insurance Corporation or the National Credit Union Administration); *id.* § 982(a)(4) ("With

Additionally, when wire fraud is the predicate specified unlawful activity for money laundering, the offense level for money laundering under the U.S. Sentencing Guidelines may be higher than wire fraud.[209] Under the Sentencing Guidelines, the base offense level for money laundering will either be:

> (1) The offense level for the underlying offense from which the laundered funds were derived, if (A) the defendant committed the underlying offense (or would be accountable for the underlying offense under subsection (a)(1)(A) of [U.S. Sentencing Guideline] § 1B1.3 (Relevant Conduct); and (B) the offense level for that offense can be determined; or
>
> (2) 8 plus the number of offense levels from the table in § 2B1.1 (Theft, Property Destruction, and Fraud) corresponding to the value of the laundered funds, otherwise.[210]

Specific offense characteristics yield additional offense levels. For example, the defendant's level will automatically increase by one-level if they are convicted under § 1957; or two-levels if they are convicted under § 1956.[211] Additionally, as with asset forfeiture, commingled funds may play a role in sentencing a money laundering defendant, potentially resulting in a higher offense level.[212] Sentencing data from fiscal year 2022 published by the Sentencing Commission also shows

---

respect to an offense listed in [18 U.S.C. § 982(a)(3)] committed for the purpose of executing or attempting to execute any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent statements, pretenses, representations, or promises, the gross receipts of such an offense shall include any property, real or personal, tangible or intangible, which is obtained, directly or indirectly, as a result of such offense."); *id.* § 982(a)(8) (differentiating specialized forfeiture provisions for wire fraud involving telemarketing).

209. U.S. SENT'G GUIDELINES MANUAL, *supra* note 98, § 2S1.1(a).

210. *Id.*

211. *Id.* § 2S1.1(b)(2). Defendants convicted under 18 U.S.C. § 1956 may also receive a two-level enhancement if the offense involved sophisticated laundering, meaning "complex or intricate offense conduct pertaining to the execution or concealment of the 18 U.S.C. § 1956 offense." *Id.* § 2S1.1(b)(3), § 2S1.1 cmt. 5(A).

212. *See id.* § 2S1.1 cmt. 3(B) (explaining that if sentencing under section 2S1.1(a)(2), "[i]n a case in which a transaction, financial transaction, monetary transaction, transportation, transfer, or transmission results in the commingling of legitimately derived funds with criminally derived funds, the value of the laundered funds, for purposes of subsection (a)(2), is the amount of the criminally derived funds, not the total amount of the commingled funds, if the defendant provides sufficient information to determine the amount of criminally derived funds without unduly complicating or prolonging the sentencing process. *If the amount of the criminally derived funds is difficult or impracticable to determine, the value of the laundered funds, for purposes of subsection (a)(2), is the total amount of the commingled funds.*" (emphasis added)).

that money laundering sentences are generally higher.[213] For theft, property destruction, and fraud defendants, the average sentence was twenty-three months.[214] For defendants convicted of aggravated identity theft and another offense, the average sentence was fifty months.[215] For money laundering offenders, the average sentence was seventy-one months.[216]

While money laundering can be a very effective charge for these reasons, there are several factors that make it more complicated than wire fraud and therefore not preferable as the primary charge when prosecuting the model scenario. First, as noted above, money laundering requires the prosecution to prove connection to a specified unlawful activity.[217] Because wire fraud is the most identifiable specified unlawful activity in the model scenario,[218] the prosecution would still need to demonstrate the wire fraud scheme anyways to meet their burden when proving money laundering. This means that proving money laundering requires proving wire fraud plus the

213. U.S. SENT'G COMM'N, QUICK FACTS MONEY LAUNDERING OFFENSES FISCAL YEAR 2022 1–2 (2023), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Money_Laundering_FY22.pdf [https://perma.cc/7HD8-7239] (charting the average sentencing increase since 2018).

214. QUICK FACTS THEFT, PROPERTY DESTRUCTION, AND FRAUD OFFENSES FISCAL YEAR 2022, *supra* note 146, at 1.

215. QUICK FACTS SECTION 1028A AGGRAVATED IDENTITY THEFT OFFENSES FISCAL YEAR 2022, *supra* note 184, at 1.

216. QUICK FACTS MONEY LAUNDERING OFFENSES FISCAL YEAR 2022, *supra* note 213, at 1. This data contains a sentencing average for all money laundering sentences under U.S. Sentencing Guidelines section 2S1.1. *Id.* at 1 n.1. Therefore, the sentencing average does not just include money laundering where fraud is the specified unlawful activity; it also includes sentences where, for example, "laundered funds were proceeds of an offense involving a controlled substance, violence, weapons, national security, or the sexual exploitation of a minor." *Id.* at 1. Additionally, "30.0% [of money laundering offenders] were convicted of an offense carrying a mandatory minimum penalty" but it is unclear which statutory provision demanded that mandatory minimum. *Id.* Because the sentencing data between fraud, aggravated identity theft, and money laundering do not strictly compare fraud across the three categories, the comparison between these sets of data is imperfect but nonetheless illustrative of the fact that money laundering convictions generally yield higher sentences.

217. 18 U.S.C. § 1956.

218. *See id.* § 1956(c)(7)(A) (specified unlawful activities include "any act or activity constituting an offense listed in section 1961(1) of this title except an act which is indictable under subchapter II of chapter 53 of title 31"); *id.* § 1961(1)(B) (including wire fraud in violation of 18 U.S.C. § 1343).

subsequent laundering activity, increasing the burden on the prosecution by creating additional evidentiary requirements.[219]

Additionally, depending on the exact nature of the money laundering scheme, the Department of Justice may require individual U.S. Attorneys' Offices to seek higher organizational levels of approval before the case can be presented to a grand jury.[220] Seeking higher approval to pursue money laundering charges helps ensure that the statute is properly charged and that unfamiliar prosecutors are equipped to handle the complexity of the case. However, additional levels of review also slow the speed of the prosecution effort. The fraudster can now continue their criminal activity for a longer time. Unless special circumstances apply, wire fraud prosecutions do not require these same higher levels of approval.[221]

The requirement to prove a specified unlawful activity when charging money laundering yields a double-edged sword: while it provides the prosecution opportunities for powerful asset forfeiture and sentencing enhancements, it also complicates their case-in-chief. The Department of Justice's approval requirements for certain types of money laundering charges also create additional hurdles before pursuing a money laundering prosecution.[222] Because of these considerations and the fact that a federal prosecutor cannot charge aggravated identity theft in this charging methodology, money laundering is not a preferred charge to wire fraud when prosecuting the model scenario.[223]

---

219. *See supra* notes 217–18 and accompanying text.

220. *See, e.g.*, Justice Manual, *supra* note 194, § 9-105.300 (describing approval requirements for money laundering cases).

221. The U.S. Attorney is generally authorized to initiate prosecutions and "has plenary authority with regard to federal criminal matters" within their district. *See id.* § 9-2.001; *id.* § 9-2.030 (detailing how the United States Attorney can initiate prosecution). For examples of some of the special circumstances requiring higher organizational levels of approval within the Department of Justice see *id.* § 9-2.400 (providing a prior approvals chart).

222. *See id.* § 9-105.300 (prescribing prior authorization from the Department of Justice's Criminal or Tax Division when prosecuting extraterritorial, tax evasion, attorneys' fees, and financial institution money laundering cases).

223. *See, e.g.*, *id.* § 9-105.330 (requiring U.S. Attorneys' Offices to consult with the Department of Justice's Criminal Division when the "specified unlawful activity" under a § 1956 money laundering charge "consists primarily of one or more financial or fraud offenses").

2. Identity fraud: 18 U.S.C. § 1028

Like money laundering, identity fraud in violation of 18 U.S.C. § 1028, may also be a viable charge for federal prosecutors to consider, but it is not preferred to wire fraud.[224] Identity fraud offers none of the unique asset forfeiture or sentencing advantages of money laundering and has a lower statutory maximum term of imprisonment than wire fraud. It also places additional evidentiary burdens on the prosecution.[225]

The methodology for a deepfake-based identity fraud prosecution under the model scenario would require charging a violation of 18 U.S.C. § 1028(a)(7), as it is the only provision of § 1028 that applies to the model scenario.[226] This statute provides:

> Whoever . . . knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law . . . shall be punished as provided in [18 U.S.C. § 1028(b)].[227]

The term "means of identification" has the same meaning between identity fraud and aggravated identity theft and therefore includes "any . . . unique biometric data, such as a fingerprint, voice print, retina or iris image, or other unique physical representation."[228] As with aggravated identity theft, because the deepfake captures the unique biometric data of a real person (for example, their voice), the deepfake rendering is a means of identification.[229]

---

224. 18 U.S.C. § 1028.

225. *See infra* note 230 and accompanying text.

226. 18 U.S.C. §§ 1028(a)(7) and (a)(8) are the only provisions of the statute that criminalize misuses of a means of identification. *See generally* 18 U.S.C. § 1028 (criminalizing fraud and related activity with identification documents). If there is evidence that the offenders are trafficking in means of identification (in other words, facts different than the model scenario but plausible as part of a deepfake fraud conspiracy), the offenders could also be charged under 18 U.S.C. § 1028(a)(8). For purposes of this statute, trafficking means "to transport, transfer, or otherwise dispose of, to another, as consideration for anything of value; or . . . to make or obtain control of with intent to so transport, transfer, or otherwise dispose of." *Id.* § 1028(d)(12).

227. *Id.* § 1028(a)(7).

228. *Id.* § 1028(d)(7)(B).

229. *Id.* (detailing the forms of biometric data used for identification); *id.* § 1028A (listing predicate felony violations that qualify for an aggravated identity theft charge including § 1028).

As demonstrated by the statutory language, the conviction for identity fraud under § 1028(a)(7) requires the prosecution to establish the connection to a predicate offense.[230] Because the means of identification is being used to trick the victim into wire transmitting funds, the natural predicate for identity fraud in the model scenario is wire fraud.[231] Accordingly, the prosecution needs to demonstrate the wire fraud scheme anyway if it intends to meet its burden for identity fraud. In this sense, identity fraud places the same type of additional evidentiary burden on the prosecution team as money laundering.[232] However, unlike money laundering, identity fraud does not carry any of the unique asset forfeiture or sentencing benefits that could potentially justify charging the offense.[233] Additionally, not only does identity fraud lack the sweeping asset forfeiture powers of money laundering, it also carries fewer forfeiture provisions than wire fraud.[234]

Additionally, the maximum punitive exposure for a violation of § 1028(a)(7) is only fifteen years imprisonment, compared to twenty years imprisonment for wire fraud and money laundering.[235] The lower

---

230. *See, e.g.*, United States v. Auernheimer, 748 F.3d 525, 535 (3d Cir. 2014) ("The two essential conduct elements under § 1028(a)(7) are transfer, possession, or use, and doing so in connection with a federal crime or state felony."); United States v. Mink, 9 F.4th 590, 602 (8th Cir. 2021) ("[T]o prove the charged § 1028(a)(7) violation in Mink's case, the government was required to show that Mink used the means of identification 'with the intent to commit, or to aid or abet, or in connection with' a felony. The grand jury charged Mink with the predicate felony of being a felon in possession of a firearm in violation of 18 U.S.C. § 922(g)(1). Accordingly, § 1028(a)(7) has 'two distinct conduct elements': (1) the transfer, possession, or use of a means of identification of another person; and (2) as relevant to Mink's case, that he was a felon in possession of a firearm.").

231. 18 U.S.C. § 1028A.

232. *See* 18 U.S.C. § 1028A(a)(1) (requiring the prosecution to meet their burden in a wire fraud charge in order to find aggravated identity theft so long as the first felony is established).

233. *See supra* note 208 and accompanying text.

234. *See generally* 18 U.S.C. § 982(a). While the asset forfeiture provisions in 18 U.S.C. § 982(a)(2) and (8) provide asset forfeiture mechanisms for both wire fraud and identity fraud, the additional asset forfeiture provisions in 18 U.S.C. § 982(a)(3) and (4) apply to convictions for wire fraud but not identity fraud. *Id.*

235. *See id.* § 1028(b)(1)(D) (stating that maximum imprisonment is fifteen years for "an offense under [18 U.S.C. § 1028(a)(7)] . . . that involves the transfer, possession, or use of 1 or more means of identification if, as a result of the offense, any individual committing the offense obtains anything of value aggregating $1,000 or more during any 1-year period."); *id.* § 1028(b)(2)(B) (enumerating that any other violation of 18 U.S.C. § 1028(a)(7) has a statutory maximum of five years imprisonment); *id.* § 1343

statutory maximum term of imprisonment for identity fraud also impacts its base offense level at sentencing. Both wire fraud and identity fraud reference the same provision of the U.S. Sentencing Guidelines: section 2B1.1.[236] Because the statutory maximum term of imprisonment is less than twenty years, the base offense level for identity fraud is only six, compared to wire fraud's base offense level of seven.[237] At the higher offense levels, a single offense level can translate to months or even years of imprisonment.[238]

Charging identity fraud is an even more disadvantageous alternative to wire fraud than money laundering. While money laundering charges at least offer unique asset forfeiture and sentencing tools, identity fraud offers neither.[239] In fact, it reduces the punitive exposure available compared to wire fraud and causes an inherent reduction in the offense level calculation under the Sentencing Guidelines.[240] These considerations, coupled with the fact that § 1028(a)(7) is statutorily barred as a predicate for aggravated identity theft, demonstrate that identity fraud is also not a preferred charge over wire fraud for prosecuting the model scenario.[241]

III. A PROPOSAL FOR AMENDING THE U.S. SENTENCING GUIDELINES TO RESPOND TO THE GROWING THREAT OF DEEPFAKE FRAUD

Title 18 U.S.C. § 3553(a) establishes the factors to be considered by a sentencing court when imposing a sentence.[242] Among other factors, the court is obligated to consider:

> (1) the nature and circumstances of the offense and the history and characteristics of the defendant;
>
> (2) the need for the sentence imposed—
>
> (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
>
> (B) to afford adequate deterrence to criminal conduct;

(penalizing wire fraud with a statutory maximum of twenty years imprisonment); *id.* § 1956(a) (penalty for money laundering is a statutory maximum of twenty years imprisonment).

236. U.S. SENT'G GUIDELINES MANUAL, *supra* note 98, app. A.

237. *Id.* § 2B1.1(a).

238. *See id.* ch. 5, pt. A (sentencing table).

239. *See supra* note 234 and accompanying text.

240. *See generally id.* § 2B1.1(2) (listing means to increase sentencing for identity theft without listing asset forfeiture considerations).

241. 18 U.S.C. § 1028A(c)(4).

242. *See generally id.* § 3553(a).

> (C) to protect the public from further crimes of the defendant; and
>
> (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner; [and]
>
> (3) the kinds of sentences available.[243]

The court is also required to consider the kinds of sentences and the sentencing range established for the defendant under the U.S. Sentencing Guidelines and relevant policy statements issued by the U.S. Sentencing Commission.[244]

A critical component of the nature of deepfake fraud is the use of a stolen identity in order to perpetrate the fraudulent scheme.[245] Unfortunately, the identity theft enhancements under Sentencing Guidelines section 2B1.1 do not apply to wire fraud sentencing under the facts of the model scenario. Under section 2B1.1(b)(11):

> If the offense involved (A) the possession or use of any (i) device-making equipment, or (ii) authentication feature; (B) the production or trafficking of any (i) unauthorized access device or counterfeit access device, or (ii) authentication feature; or (C)(i) the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification, or (ii) the possession of 5 or more means of identification that unlawfully were produced from, or obtained by the use of, another means of identification, increase by 2 levels. If the resulting offense level is less than level 12, increase to level 12.[246]

In other words, for the enhancement to apply, either: (1) the unauthorized means of identification must be used to obtain another means of identification; or (2) the crime involved the possession of five or more means of identification that themselves were produced from or obtained by the use of another means of identification.[247] Neither of these fact patterns fit the model scenario and, accordingly, there is no applicable sentencing enhancement for the identity theft component of the deepfake fraud. Federal prosecutors are left to argue only for a sophisticated means enhancement: that the deepfake's use is indicative of the complex or intricate offense conduct

---

243. *Id.* § 3553(a)(1)–(3).
244. *Id.* § 3553(a)(4)–(5).
245. *See supra* Sections II.A–B.
246. U.S. SENT'G GUIDELINES MANUAL, *supra* note 98, § 2B1.1(b)(11).
247. *Id.* § 2B1.1(b)(11)(C).

characterizing the fraudulent scheme.[248] Because the current version of section 2B1.1 does not account for the identity theft aspects of deepfake fraud, it fails to accurately capture the "nature and circumstances of the offense" and provides no greater deterrence for a perpetrator of deepfake fraud than a perpetrator of general wire fraud.[249]

There are multiple ways section 2B1.1 could be amended to better respond to the specific offense characteristics of deepfake fraud in the model scenario.[250] Section 2B1.1(b)(11)(C) could be altered to add a third scenario tracking the language of aggravated identity theft, such as: "If the offense involved . . . (C)(iii) the transfer, possession, or use, without lawful authority, of a means of identification of another person, . . . increase by 2 levels." This language addition would incorporate the penalty for the identity theft component of the deepfake wire fraud scheme into the existing identity theft provision of the Sentencing Guideline. To ensure consistency with the definition of "means of identification" in the statute, Application Note 10(A) should also be amended to reference and incorporate the statutory definition.[251]

Alternatively, rather than tying the enhancement to one of the existing subsections, section 2B1.1(b) could be amended to include an entirely new subsection that exclusively identifies the use of a means of identification of another person as a specific offense characteristic with its own offense level increase. This would give policymakers the flexibility to establish an offense level enhancement directly proportional to the severity of the deepfake fraud threat. Such a section could read: "If the offense involved the transfer, possession, or

248. *Id.* § 2B1.1 cmt. 9(B).

249. 18 U.S.C. § 3553(a)(1), (a)(2)(B).

250. The U.S. Sentencing Commission is responsible for amending the U.S. Sentencing Guidelines. "Generally, the Commission promulgates guidelines on an annual basis." U.S. SENT'G COMM'N, SENTENCING RESOURCES GUIDE 5, https://www.ussc.gov/sites/default/files/pdf/about/overview/USSC-Resources-Guide.pdf [https://perma.cc/H45N-DDY6]. There have been years when the Commission did not have a quorum and its functions were limited. *See* Debra Cassens Weiss, *Sotomayor and Barrett Flag Sentencing Commission's Longtime Lack of Quorum*, ABA J. (Jan. 11, 2022, 1:30 PM), https://www.abajournal.com/news/article/barrett-and-sotomayor-flag-sentencing-commissions-longtime-lack-of-a-quorum [https://perma.cc/7L79-2QYP] (noting how the U.S. Sentencing Commission has felt recent criticism from Supreme Court justices because it has not held a quorum for three years).

251. *See* U.S. SENT'G GUIDELINES MANUAL, *supra* note 98, § 2B1.1 cmt. 10 ("Means of identification" is undefined).

use, without lawful authority, of a means of identification of another person, increased by 4 levels. If the resulting offense level is less than level 20, increase to level 20."[252] Using offense level increases and minimums like these, the new penalty for deepfake fraud would result in strong deterrence for fraudsters inclined to use deepfakes to perpetrate their fraud.

Additionally, crime data from the U.S. Sentencing Commission suggest that an increased term of imprisonment may decrease recidivism, further justifying an increase in offense level for deepfake fraud. "Recidivism 'refers to a person's relapse into criminal behavior, often after the person receives sanctions or undergoes intervention for a previous crime.'"[253] A 2022 Sentencing Commission report examining recidivism trends for federal offenders shows that a minimal decline in recidivism begins around thirty-six months of incarceration, while a statistically significant decrease in recidivism occurs beginning at sixty months of incarceration.[254] The data also show that lower terms of imprisonment actually have the opposite effect, with offenders who received less than twenty-four months up to thirty-six months of imprisonment actually showing a seven percent increase in the likelihood of re-offending.[255] In other words, "offenders serving longer sentences had a lower likelihood of recidivism and took longer to recidivate."[256] Therefore, a longer term of incarceration for deepfake fraud may both deter first-time offenders as well as stop convicts from re-offending.

As currently written, the Sentencing Guidelines do not properly enhance the criminal sentences based on the unique offense characteristics of deepfake fraud. Given the threat posed to society by criminal actors using deepfakes to accomplish their fraudulent schemes, lawmakers should consider amending the Sentencing

252. As with the first proposed modification to section 2B1.1, the words "means of identification" would also need to be added to the definitions contained in the Application Notes.

253. U.S. SENT'G COMM'N, LENGTH OF INCARCERATION AND RECIDIVISM 1, 6 (2022), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2022/20220621_Recidivsm-SentLength.pdf [https://perma.cc/RE5F-65YN] (quoting *Recidivism*, U.S. DEP'T OF JUST.: NAT'L INST. OF JUST., https://nij.ojp.gov/topics/corrections/recidivism [https://perma.cc/3XE8-CBCR]).

254. *Id.* at 19.

255. *Id.*

256. *Id.*

Guidelines in accordance with one of the above recommendations to more effectively deter and punish deepfake fraudsters.

CONCLUSION

Deepfake fraud has the possibility to affect every stratum of American society, from the targeting of particular individuals, to multinational organizations, to state governments, to the federal government. Government organizations and the private sector alike have already sounded the alarm regarding the threat of deepfakes, with some heralding the technology as one of the greatest potential criminal threats stemming from society's progress with artificial intelligence.[257] As the technology continues to improve in quality and decrease in cost, the accessibility of deepfakes to criminals will only increase and their potential harm will grow.

Federal prosecutors must be prepared to respond to this threat with a functional prosecution methodology. Rather than hoping for legislative change that provides new criminal statutes to react to the threat, prosecutors should focus their charging methodology on existing federal criminal laws, allowing them to be proactive and prepared. While some changes to the U.S. Sentencing Guidelines could permit more substantial penalties to better deter criminals, existing wire fraud and aggravated identity theft statutes already provide an effective framework for charging, convicting, and sentencing fraudsters using deepfakes.

257. *See supra* notes 25–30 and accompanying text.