Deepfakes, Chatbots, and Scams:

How AI Is Fueling Fraud and What Policymakers Must Do

NATIONAL CONSUMERS LEAGUE

Deepfakes, Chatbots, and Scams: How AI Is Fueling Fraud and What Policymakers Must Do[1]

A National Consumers League White Paper

Published: September 17, 2025

Executive Summary

Fraud in the U.S. is escalating, with reported losses reaching $12.5 billion in 2024, a 25% increase from the previous year. This spike occurred even as the number of fraud reports remained stable, highlighting that scams are becoming more effective. The highest losses were attributed to investment scams ($5.7 billion), followed by imposter scams ($2.95 billion), which were also the most frequently reported. These trends are exacerbated by the use of artificial intelligence (AI), which makes scams more realistic and believable, as noted by the FBI. The prevalence of deepfake fraud among businesses has also grown significantly, with a marked increase in both audio and video deepfake incidents. Forecasts from Forbes and Deloitte predict this trend will continue, with fraud losses driven by generative AI potentially reaching $40 billion by 2027.

While legislative efforts have begun to address this issue, they are not yet comprehensive. Currently, policies focus on data privacy, deepfakes, and election integrity. For instance, nearly 20 states have enacted data privacy laws, and several laws, including the federal TAKE IT DOWN ACT of 2025, have been introduced to criminalize deepfake pornography and require AI disclosure. However, a more robust response is needed.

This report concludes that policymakers must prioritize several key areas. First, AI systems should be built with inherent resistance to fraudulent use, and AI companies must be held accountable for any failures. Second, stronger penalties are needed for financial crimes committed with AI. Third, consumers should be empowered by providing options to opt out of AI interaction and redirect to a human representative. Finally, existing consumer protection laws, such as the Telephone Consumer Protection Act (TCPA), should be utilized to prosecute new forms of AI fraud. Ultimately, effective regulation is crucial to ensure AI serves as a beneficial tool rather than a dangerous weapon.

I. AI is Accelerating a Growing Wave of Fraud

Fraud is on the rise in the United States, with a significant increase in reported losses. According to Federal Trade Commission (FTC) data, reported losses to fraud

[1] NCL wishes to acknowledge the invaluable contributions of NCL Senior Public Policy Manager Eden Iscil and NCL intern Audrey Smith (UVA ’26) to the development of this report.

climbed to $12.5 billion in 2024, a 25% increase from the previous year.[2] The number of people who lost money to fraud also jumped, from 27% in 2023 to 38% in 2024, even though the total number of fraud reports remained stable.[3]

Investment scams accounted for the highest reported losses at $5.7 billion, a 24% increase over 2023.[4] Imposter scams were the second highest, with losses totaling $2.95 billion, and were also the most frequently reported scam category.[5] Specifically, government imposter scams saw losses increase by $171 million to a total of $789 million in 2024.[6]

The use of AI is making these scams more realistic and believable. The FBI has warned that criminals are using AI to commit fraud on a larger scale.[7] The prevalence of deepfake fraud is increasing among business leaders, with the percentage of companies experiencing an audio deepfake scam rising from 37% in 2022 to 49% in 2024.[8] Similarly, those experiencing a video deepfake scam increased from 29% to 50% during the same period.[9]

These trends are expected to continue. Forbes predicted a surge of AI-related fraud in 2025.[10] Fraud losses driven by generative AI have surged to $12.3 billion in 2023, with projections of $40 billion in losses by 2027, according to Deloitte.[11] The criminal use of AI is also growing on online chat platforms like Telegram, where messages in criminally focused channels related to AI and deepfakes for fraud increased by 644% between 2023 and 2024.[12] In an analysis conducted by Point Predictive, in 2023, there were 47,000 messages, in 2024, the number of those messages has now surpassed over 350,000, a 644% increase.[13]

---

[2] " New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024," *Federal Trade Commission*, March 10, 2025. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024#:~:text=Newly%20released%20Federal%20Trade%20Commission%20data%20show%20that,an%20increase%20in%20fraud%20reports%2C%20which%20remained%20stable.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] " Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud," *Federal Bureau of Investigation.* December 3, 2024. https://www.ic3.gov/PSA/2024/PSA241203

[8] Zaki, Adam."92% of companies have experienced financial loss due to a deepfake," *CFO,* Nov. 6, 2024. https://www.cfo.com/news/most-companies-have-experienced-financial-loss-due-to-a-deepfake-regula-report/732094/

[9] Ibid.

[10] McKenna, Frank. "5 AI Scams Set To Surge In 2025: What You Need To Know," *Forbes*, Dec 16, 2024. https://www.forbes.com/sites/frankmckenna/2024/12/16/5-ai-scams-set-to-surge-in-2025-what-you-need-to-know/

[11] Lalchand et. al. "Generative AI is expected to magnify the risk of deepfakes and other fraud in banking," *Deloitte Center for Financial Services*, May 29, 2024. https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html

[12] Ibid.

[13] Ibid.

Without proper regulation, AI has the potential to cause significant harm to consumers and dominate the fraud landscape. The following sections discuss current legislative efforts and outline priorities for future policy.

II. Key Areas of Policymaker Focus

Privacy Laws

The lack of comprehensive federal data privacy laws leaves consumers vulnerable to fraud, as scammers can more easily access personal information. AI exacerbates this problem by using personal data to create realistic-looking and sounding scams. While there is no federal bill, nearly 20 states have enacted their own omnibus data privacy bills.[14] These laws typically give consumers the right to opt out of the collection and sale of their personal information. Some states are tightening these laws, such as Utah, which now allows people to correct inaccurate information[15] and Oregon, which prohibits the sale of precise location data and children's data. [16]

A comprehensive federal data privacy law is a necessary next step to create a uniform standard for companies and ensure consistent protection for all consumers, regardless of their state of residence.

Deepfakes

Deepfakes are AI-edited images, videos, or audio that have been used for both entertainment and unethical purposes, including impersonation scams and non-consensual pornography. This type of media has been used to create fake images and videos of well-known national leaders and celebrities. Some of these are solely meant for entertainment, but many deepfakes are used for unethical purposes. For example, in January of 2024, a sexually explicit deepfake image of Taylor Swift circulated online, inciting anger and skepticism among fans.[17] Scarlett Johansson also spoke out earlier this year, warning about

[14] "US state-by-state AI legislation snapshot," *BCLP.* https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html

[15] " Utah Amends Consumer Privacy Law to Add Correction Rights and Enacts Data Sharing Requirements for Social Media Companies," *Westlaw Today*, March 31, 2025. https://today.westlaw.com/Document/Ia07a7b050be611f082a5ae4bb4582a09/View/FullText.html?transitionType=Default&contextData=(sc.Default)&firstPage=true

[16] Mollod, Jonathan. "Oregon Strengthens Geolocation Data Privacy and Children's Personal Data Protections, Adding to Compliance for Data Brokers and Others," *National Law Review*, July 22, 2025. https://natlawreview.com/article/oregon-strengthens-geolocation-data-privacy-and-childrens-personal-data-protections

[17] "Taylor Swift deepfakes spread online, sparking outrage," *CBS News*, January 26, 2024. https://www.cbsnews.com/news/taylor-swift-deepfakes-online-outrage-artificial-intelligence/

misuse of AI, after a deepfake video falsely portrayed her and other Jewish celebrities sending a message of protest to Kanye West.[18]

These examples and many more sparked the first attempts at deepfake regulation in 2023. Leaving deepfake material unregulated can lead to fraudulent behavior of all kinds, including impersonation scams and distribution of non-consensual deepfake pornographic material. NCL reviewed almost 20 enacted, proposed, and failed laws at the federal and state level that aim to address deepfakes and impersonation. These efforts mainly fall under the categories of regulating and criminalizing the making and use of deepfake porn, as well as regulating the impersonation of any individual without a disclosure that AI was used, whether it is being used for entertainment or otherwise.[19]

The TAKE IT DOWN ACT of 2025 is the first federal law that addresses deepfake pornography.[20] The Act criminalizes deepfake pornography, requires online platforms to remove content within 48 hours of notice, and creates penalties for those who create and distribute this content.[21] This bill is a good first start, but preventative work should also be done to limit deepfake creation and distribution in the first place.

Companies that create AI should ensure that their AI is resistant to efforts to use it for impersonation scams. Much work remains for legislators to address how to define consensual creation and distribution of deepfake material, disclosures that AI has been used to generate said material, and require swift penalties for individuals who have manufactured and distributed these deepfakes.

Elections

Regulations on AI-generated material related to elections were introduced just before the 2024 election season. Legislators became increasingly concerned about how AI deepfakes, ads, and other synthetic election materials could impact the public's opinions and voting decisions. A notable example is a February 2024 audio deepfake of former President Joe Biden, urging people to refrain from voting in the New Hampshire primary.[22]

Other examples, such as an AI-generated image of President Donald Trump and convicted sex trafficker Jeffrey Epstein with a young girl that went viral on X.[23] Falsified

---

[18] Glynn, Paul. "Scarlett Johansson warns of 'AI misuse' after fake Kanye video," *BBC*, February 13, 2025. https://www.bbc.com/news/articles/c0qwkdlxgxno

[19] "US state-by-state AI legislation snapshot," *BCLP.* https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html

[20] United States, Congress, Senate, TAKE IT DOWN Act. Congress.gov, 2025. S.146, 119th Congress, https://www.congress.gov/bill/119th-congress/senate-bill/146/text/ih

[21] Ibid.

[22] Swenson, Ali; Weissert, Will. "New Hampshire investigating fake Biden robocall meant to discourage voters ahead of primary," *AP News*, January 22, 2024. https://apnews.com/article/new-hampshire-primary-biden-ai-deepfake-robocall-f3469ceb6dd613079092287994663db5

[23] McCreary, Joedy. "Image of Donald Trump, Jeffrey Epstein on private jet is AI generated," *USA Today*, January 12, 2024. https://www.usatoday.com/story/news/factcheck/2024/01/12/ai-donald-trump-jeffrey-epstein-jet-fact-check/72202337007/

information, as well as impersonation of election candidates and official endorsements, cause the public to be confused and base their voting decisions on the wrong information. Reckless and nefarious use of AI in elections can lead to heightened electoral fraud and harm voters nationwide.

NCL reviewed nearly 30 enacted, proposed, and failed laws at the federal and state levels that address AI use in elections. Most laws fall under the categories of election-related deepfakes, AI used in election ads, AI defrauding people out of their right to vote, and distributing AI-generated media for a certain window of time prior to an election.[24]

The threat of AI to election integrity is likely to continue to grow. Policymakers should continue to advocate for laws addressing anti-democratic uses of AI. Priority should be given to bills that require the release of accurate information about candidates and elections. Transparency in the form of a disclosure is a good thing, but transparency is not enough without the remedy of correct information being just as widely available.

AI and Fraud

Consumer protection agencies have increasingly warned about the ability fraudsters will soon have to make their scams even more believable using AI. Fraud has exploded in the United States over just the past few years, and the ability of criminals to augment existing impersonation techniques, make it easier than ever to create ever-more realistic-looking emails.

U.S. legislators have recognized the ways that AI has the potential to explicitly carry out fraudulent activities and defraud millions of consumers. While no laws that directly address fraud have yet been enacted, efforts have been made to restrict AI's ability to scam and defraud consumers. Notable examples include S. 1993, sponsored by Sen. Josh Hawley and cosponsored by Sen. Richard Blumenthal in 2023.[25] This bill would have removed Sec. 230 immunity for AI-related fraud. Section 230 is part of the Communications Act of 1934 and gives online platforms federal immunity with respect to user-generated content. S. 1993 would have taken that immunity away when AI-generated content is involved in fraud online.[26]

Another example is H.R. 10125, sponsored by Rep. Ted Lieu. This bill would increase penalties for the commission of financial crimes using artificial intelligence.[27] Once again, this holds AI platforms accountable for the harm they produce and incentivizes them to prioritize fraud resistance in their models. NCL's review identified fewer than ten bills at

[24] "US state-by-state AI legislation snapshot," *BCLP.* https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html
[25] "Hawley, Blumenthal Introduce Bipartisan Legislation to Protect Consumers and Deny AI Companies Section 230 Immunity," *Office of Josh Hawley*, June 14, 2023. https://www.hawley.senate.gov/hawley-blumenthal-introduce-bipartisan-legislation-protect-consumers-and-deny-ai-companies-section/
[26] Ibid.
[27] United States, Congress, House, AI Fraud Deterrence Act. Congress.gov, 2024. H.R.10125, 118th Congress, https://www.congress.gov/bill/118th-congress/house-bill/10125/text/ih

the federal and state levels that directly address AI's potential to increase fraud. Absent such regulations, consumers will depend on AI model developers to voluntarily ensure that their AI systems are resistant to scammers' attempts to use it to defraud consumers.

Chatbots

Consumer advocacy organizations have warned about the potential for chatbot scams to explode once AI increases the believability of interactions. Currently, no federal efforts have been made to address this, but approximately 10 enacted, proposed, or failed state laws address deceptive chatbot usage. Most of these laws require a clear disclosure that a user is interacting with an AI chatbot.[28]

While transparency is important, it is often not enough. Consumers should also have the option to opt out of interacting with AI or be redirected to a human representative. Consumers should also have the option not only to know they are engaging with AI, but also to opt out of interactions with AI if they wish, or to be redirected to an actual human with whom they can communicate. A proposed bill in Minnesota, SF1886 of 2025, offers this solution by requiring that consumers be given the option to interact with a human if they are dissatisfied with their chatbot experience.[29]

NTIA Safeguards

The National Telecommunications and Information Administration (NTIA) has taken a first step toward national AI regulation with safeguards focused on accountability and safe implementation. These safeguards include requiring companies to evaluate AI mechanisms and ensuring that entities receiving federal grants are implementing sound internal AI system assurances. Since the NTIA took these steps, other states have created laws that regulate the development and deployment of AI systems.[30]

Another would ensure that entities contracting with the federal government or receiving federal grants are enacting sound internal AI system assurances. Overall, these examples show that NTIA is focused on accountability and safe implementation of AI that is trained to resist fraud before being introduced to the public. Since those steps were taken by the NTIA, other states have followed suit, creating laws that regulate the development and deployment of AI systems.

Additional Safeguards

---

[28] "US state-by-state AI legislation snapshot," *BCLP.* https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html

[29] Minnesota, Legislature, 2025. SF1886, 94th Legislature, https://www.revisor.mn.gov/bills/text.php?number=SF1886&version=latest&session_year=2025&session_number=0

[30] " AI Accountability Policy Report," *National Telecommunications and Information Administration*, March 27, 2024. https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report

While few statutes specifically address the threat of AI and fraud, existing laws may be applied in novel ways. For example, the Telephone Consumer Protection Act (TCPA) of 1991 regulates telemarketing calls, including the use of automated dialing systems and prerecorded messages, to protect consumer privacy.[31] While TCPA may not be specifically directed toward AI, it could be used to prosecute robocalls that use AI to emulate a human being.

Because current AI legislation is rapidly developing and changing, it is crucial to be aware of all the laws in the consumer protection toolkit, so that even if there is not a regulation on a certain AI behavior, fraud caused by the AI mechanism can still be addressed.

III. Conclusion

As Kara Swisher has said, "AI can be a weapon, but it's a tool".[32] The key distinction lies in effective regulation that protects consumers. While current efforts are steps in the right direction, much more protection is needed to prevent AI from making it easier to defraud consumers.

Resistance to fraudulent behavior must be built into AI systems before they are released to the public, and AI companies must be held accountable for any failures to do so. Transparency is a good priority, but it must be paired with consumer agency, giving individuals the option to choose a secure alternative if they wish. Emphasizing these priorities is essential if we are committed to AI being a safe and useful tool, rather than a dangerous weapon.

[31] United States, Congress, Senate, Telephone Consumer Protection Act of 1991. Congress.gov, 1991. S.1462, 102nd Congress, https://www.congress.gov/bill/102nd-congress/senate-bill/1462

[32] "Tech journalist and podcast host Kara Swisher talks about AI," *PBS*, October 19, 2023. https://www.pbs.org/video/tech-journalist-and-podcast-host-kara-swisher-a8uakk/