April 16, 2026

Mr. Mati Staniszewski
Co-Founder & Chief Executive Officer
ElevenLabs
169 Madison Ave
#2484
New York, NY 10016

Dear Mr. Staniszewski:

I write today to request information on ElevenLabs's efforts to prevent scammers from misusing its AI voice-generating tools. In recent years, global criminal networks have used deepfake voice programs, along with other new AI tools, to target more people with increasingly personalized and believable digital scams, fueling a booming scam industry that surpasses the global drug trade as an illicit industry.[1] Generative AI deepfakes – creating fictitious videos, voices, and documents – are "expected to rapidly increase fraud losses in the years ahead," according to Deloitte's Center for Financial Services, which predicts that these tools could enable up to $40 billion in annual fraud losses in the United States by 2027.[2] Protecting Americans from these financial losses will require collaboration between the public and private sectors, and AI companies like ElevenLabs are on the frontlines of this effort.

A 2025 study found that "[p]eople are poorly equipped to detect AI-powered voice clones" and that "AI-generated voices will soon be indistinguishable from real ones."[3] Accurate, widely available, and easy to use, AI tools can quickly create new, generic voices or clone the

---

[1] *Myanmar's Scam Empire Gets Worse, Not Better,* The Economist (May 29, 2025) (www.economist.com/asia/2025/05/29/myanmars-scam-empire-gets-worse-not-better).

[2] Deloitte's Center for Financial Services, *Generative AI is Expected to Magnify the Risk of Deepfakes and Other Fraud in Banking* (May 29, 2024) (www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html).

[3] Sarah Barrington, Emily A. Cooper, and Hany Farid, *People are Poorly Equipped to Detect AI-Powered Voice Clones,* Scientific Reports (Mar. 31, 2025) (www.nature.com/articles/s41598-025-94170-3).

voices of real people from a brief audio sample.[4] Some AI platforms also let users select from vast libraries of pre-made AI voices, saving them from having to design speakers themselves.[5] As you know, ElevenLabs offers users thousands of voices in dozens of languages.[6] In addition, technological advances now allow speakers to convert their voices into an AI voice in real time, enabling live conversations, an advancement that cybersecurity researchers described as "a key requirement for [voice phishing] attacks" in a September 2025 study.[7] The researchers further found that "the tools and infrastructure needed for real-time voice cloning are accessible to those with even limited technical and financial means."[8]

While there are legitimate uses of these tools, they are also used by foreign criminals preying on Americans – enabling these scammers to operate at "previously unthought of levels."[9] Scammers, for example, have used AI-generated voices to pose as employees of government agencies, banks, and utilities and urgently request credentials or payments from Americans.[10] On dating apps and other social media platforms, scammers also use these same kinds of voices to facilitate romance scams, a category of fraud that cost victims over $1 billion last year according to the Federal Trade Commission.[11] To appear "more believable," criminals posing as a romantic partner will "offer to talk by phone [with the victim], and they'll use AI to disguise their voice or appearance and to make it look like somebody they're not," according to an FBI special agent

---

[4] ElevenLabs, Introducing Voice Design v3 (Last updated June 25, 2025) (elevenlabs.io/blog/voice-design-v3) (accessed Apr. 6, 2026); ElevenLabs, Voice Cloning (elevenlabs.io/voice-cloning) (accessed Oct. 30, 2025); NCC Group, Pablo Alobera, Pablo López, Víctor Lasa, *Realtime AI-Supported Voice Conversion (Deepfake) and its Applications on Vishing and Social Engineering Exercises* (Sept. 30, 2025) (www.nccgroup.com/research-blog/voice-impersonation-and-deepfake-vishing-in-realtime/).

[5] ElevenLabs, Free AI Voice Generator (elevenlabs.io/ai-voice-generator) (accessed Mar. 31, 2026).

[6] *Id.*

[7] NCC Group, Pablo Alobera, Pablo López, Víctor Lasa, *Realtime AI-Supported Voice Conversion (Deepfake) and its Applications on Vishing and Social Engineering Exercises* (Sept. 30, 2025) (www.nccgroup.com/research-blog/voice-impersonation-and-deepfake-vishing-in-realtime/).

[8] *Id.*

[9] *Id.*

[10] *FCC Names Its First-Ever AI Scammer in Threat Alert*, Fox News (June 5, 2024) (www.foxnews.com/tech/fcc-names-its-first-ever-ai-scammer-threat-alert).

[11] Centre for Emerging Technology and Security, *Automating Deception: AI's Evolving Role in Romance Fraud* (Apr. 15, 2025) (cetas.turing.ac.uk/publications/automating-deception-ais-evolving-role-romance-fraud); *Federal Trade Commission Consumer Sentinel Network*, Fraud Reports (Published Aug. 15, 2025) (public.tableau.com/app/profile/federal.trade.commission/viz/shared/4WS8HTYQ6).

who investigates romance and investment scams.[12] A 2025 report found that not only do "deepfake media provide an additional layer of authenticity" for romance scammers, but they also allow these scammers to convincingly reach more people with less effort.[13] Notably, ElevenLabs offers "hundreds of high quality flirty AI voices," including "the sophisticated charmer," described on the company's website as "a charming and confident young adult female voice…with a warm, honeyed tone that's smooth and inviting."[14] Other offerings include the "velvet rogue" who has "a deep, velvety male voice … rich and resonant with a slight rasp that adds texture and masculinity."[15]

AI voice-generating technology has also facilitated new, personalized scams that use clones of trusted voices to request or authorize money or access sensitive accounts.[16] In June 2025, a New York man was sentenced to prison for his role in a high-tech, "elaborate grandparent scam" in which he stole around $20,000 from three New Hampshire families after convincing them that their loved ones were in trouble.[17] According to the *Union Leader*, "[v]ictims say the scam involved the use of artificial intelligence mimicking a loved one's voice to trick them into turning over money to bail that person out of jail."[18] One victim described how "[t]he story was presented so convincingly with my son's voice full of terror" on the deepfake call.[19] In 2024, police in Merrimack County, New Hampshire, similarly investigated dozens of reports of scam calls targeting residents in which criminals allegedly used AI to manipulate their

---

[12] *AI Making Romance Scams Harder to Spot*, KOAA News (Sept. 4, 2025) (www.koaa.com/news/local-news/ai-making-romance-scams-harder-to-spot).

[13] Centre for Emerging Technology and Security, *Automating Deception: AI's Evolving Role in Romance Fraud* (Apr. 15, 2025) (cetas.turing.ac.uk/publications/automating-deception-ais-evolving-role-romance-fraud).

[14] ElevenLabs, Flirty AI Voice Generator (elevenlabs.io/voice-library/flirty) (accessed Oct. 22, 2025).

[15] *Id.*

[16] *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (Oct. 14, 2021) (www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/); *Bronx Man Gets 4 to 8 Years for Role in 'Grandparent Scam,'* New Hampshire Union Leader (Sept. 24, 2025) (www.unionleader.com/news/courts/bronx-man-gets-4-to-8-years-for-role-in-grandparent-scam/article_58a05fcd-5edd-4d76-8dae-8ccd3937dcac.html).

[17] *Bronx Man Gets 4 to 8 Years for Role in 'Grandparent Scam,'* New Hampshire Union Leader (Sept. 24, 2025) (www.unionleader.com/news/courts/bronx-man-gets-4-to-8-years-for-role-in-grandparent-scam/article_58a05fcd-5edd-4d76-8dae-8ccd3937dcac.html).

[18] *Id.*

[19] *Id.*

voices to sound like law enforcement or the family members of victims.[20] These calls deceived at least two residents, including one who paid the scammers $5,000.[21] Voice clones have also fooled businesses with more resources at their disposal than the average American, creating what some in the AI industry have described as a "fraud crisis."[22] Cloned voices, for example, can bypass voice ID verification measures from banks or mimic company executives to authorize large payment transfers, sometimes for tens of millions of dollars.[23] In 2020, a bank manager in Hong Kong authorized $35 million in transfers after a cloned voice impersonated a client.[24] The previous year, a manager of a British energy company wired more than $240,000 to a foreign account after receiving instructions from a deepfake clone of his boss's voice.[25]

This same technology has also created alarming new avenues for political interference and disinformation. New Hampshire, for example, was the target of the "first known example of an AI-generated deepfake being deployed maliciously in an American political campaign," according to public reporting.[26] Ahead of the January 2024 presidential primary election, thousands of New Hampshire residents received a robocall from an AI-generated voice clone of

---

[20] *Merrimack County Residents Targeted by AI Phone Scams, Police Say,* WMUR (Aug. 12, 2024) (www.wmur.com/article/merrimack-county-ai-scam-call-investigate-bitcoin-croft-arrest-warrant-manipulate/61858706).

[21] *Id.*

[22] Sam Altman, Remarks at the Federal Reserve's Integrated Review of the Capital Framework for Large Banks Conference in Washington, Associated Press (July 22, 2025) (www.youtube.com/watch?v=tScbQiavmpA).

[23] *Cloned Customer Voice Beats Bank Security Checks*, BBC (Nov. 28, 2024) (www.bbc.com/news/articles/c1lg3ded6j9o); *How I Broke Into a Bank Account With an AI-Generated Voice*, Vice (Feb. 23, 2023) (www.vice.com/en/article/how-i-broke-into-a-bank-account-with-an-ai-generated-voice/); Consumer Reports, *AI Voice Cloning: Do These 6 Companies Do Enough to Prevent Misuse?* (Mar. 10, 2025) (innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf); *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (Oct. 14, 2021) (www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/).

[24] *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (Oct. 14, 2021) (www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/).

[25] *An Artificial-Intelligence First: Voice-Mimicking Software Reportedly Used in a Major Theft*, The Washington Post (Sept. 4, 2019) (www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/).

[26] *A New Orleans Magician says a Democratic Operative Paid Him to Make the Fake Biden Robocall*, NBC News (Feb. 23, 2024) (www.nbcnews.com/politics/2024-election/biden-robocall-new-hampshire-strategist-rcna139760).

President Joe Biden instructing them not to vote in the upcoming election.[27] The person who executed the calls later faced criminal charges and a $6 million fine from the Federal Communications Commission. [28]

As this fraudulent activity continues, evidence suggests that technology companies could do more to prevent the misuse of their AI voice generation tools.[29] In 2024, investigative news outlet *Proof* examined eight popular AI voice cloning platforms and found few safeguards to prevent nonconsensual voice cloning: "[M]ost companies…make little or no attempt to ensure that the humans being copied have consented to the process."[30] A March 2025 Consumer Reports investigation similarly found that most of the leading AI voice cloning products had no "technical mechanism" in place to prevent users from replicating voices without permission.[31] Instead, they simply required users to self-attest that they had the right to clone a voice.[32] Moreover, the majority of the companies Consumer Reports examined did little to learn the true identities of their customers, a step that could help them track and prevent the abuse of their products.[33] Consumer Reports argued that AI voice cloning companies should adopt these two requirements, among other the safety measures, "at a bare minimum" and as a "starting point."[34]

Given the role that AI voice generation tools can play in creating scams, I seek responses to the requests below.

1. Does ElevenLabs monitor user activity and/or the content created on its platforms to detect violations of its usage policies prohibiting the use of its models for scams and fraud? If so:

---

[27] *Id.*

[28] *Political Consultant Behind Fake Biden Robocalls Faces $6 Million Fine and Criminal Charges*, Associated Press (May 23, 2024) (apnews.com/article/biden-robocalls-ai-new-hampshire-charges-fines-9e9cc63a71eb9c78b9bb0d1ec2aa6e9c).

[29] *AI Tools Make It Easy to Clone Someone's Voice Without Consent*, Proof (June 25, 2024) (www.proofnews.org/ai-tools-make-it-easy-to-clone-someones-voice-without-consent/); Consumer Reports, *AI Voice Cloning: Do These 6 Companies Do Enough to Prevent Misuse?* (Mar. 10, 2025) (innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf).

[30] *AI Tools Make It Easy to Clone Someone's Voice Without Consent*, Proof (June 25, 2024) (www.proofnews.org/ai-tools-make-it-easy-to-clone-someones-voice-without-consent/).

[31] Consumer Reports, *AI Voice Cloning: Do These 6 Companies Do Enough to Prevent Misuse?* (Mar. 10, 2025) (innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf).

[32] *Id.*

[33] *Id.*

[34] *Id.*

a. Does ElevenLabs detect, flag, and/or prohibit the creation of audio content that contains phrases commonly used in scams?
    i. If so, how often does ElevenLabs evaluate the effectiveness of its prohibitions on specific terms in preventing scams? How often does the company update its list of prohibited terms?

b. Does ElevenLabs detect, flag, and/or prohibit the creation of audio content in which a user has created a voice to misrepresent themselves as an official from a bank, government office, or other entity?

2. What actions, if any, does ElevenLabs take against users who violate its policies prohibiting the use of its models for scams and fraud?

    a. If these actions include banning users from the platform:
        i. Under what circumstances has ElevenLabs banned users for violating the company's policies prohibiting scams;
        ii. How many users has ElevenLabs banned for such violations;
        iii. How does ElevenLabs prevent these users from returning to the platform?

    b. Under what circumstances, if any, does ElevenLabs report these users to law enforcement?

3. What mechanisms does ElevenLabs maintain to verify that a speaker has consented to their voice being cloned?

    a. Does ElevenLabs require users to clone a voice from audio recorded in real time? If so, under what circumstances is this required? If not, why not?

    b. Does ElevenLabs require users to upload authentic, non-public audio of the speaker whose voice they intend to clone? Why or why not? If so:
        i. What, if any, requirements does ElevenLabs impose for such recordings? For instance, does the audio need to be of a particular length or read from a unique script?
        ii. What mechanisms does ElevenLabs maintain to ensure that any audio submitted for verification purposes is authentic?

4. Does ElevenLabs track user attempts to violate its policies prohibiting nonconsensual voice cloning? If so:

    a. How many unique users and unique attempts has ElevenLabs detected as being in violation of its policies prohibiting nonconsensual voice cloning, and what actions has it taken against the users responsible?

b. How many of these users and attempts did ElevenLabs detect *before* a nonconsensual voice clone was generated?

c. How many of these users and attempts did the company detect only *after* a nonconsensual voice clone was generated?

d. What steps, if any does the company take to adapt its measures to defend against such tactics?

5. Does ElevenLabs take specific steps to ensure that the voices of well-known individuals, such as celebrities and politicians, are not created on its platform without authorization? If so, please detail those steps. Your answer should include but not be limited to the questions below regarding the company's "no-go voices" policy of detecting and preventing users from cloning the voices of specific public figures.

    a. Does ElevenLabs track attempted violations of its prohibition on "no-go voices"? If so:
        i. How many user attempts to clone a "no-go" voice has ElevenLabs detected?
        ii. How many of those attempts did ElevenLabs thwart in real time – in other words, while the user was trying to create the prohibited voice?

    b. Does ElevenLabs monitor user activity to detect when users have succeeded in cloning a "no-go" voice despite the company's prevention efforts? If so:
        i. How many instances has ElevenLabs identified where users succeeded in cloning a "no-go" voice?
            1. In these instances, does the company track how the user circumvented the company's efforts to detect and prevent the cloning of "no-go voices"? What steps, if any, does the company then take to adapt its measures to defend against such tactics?

    c. In ElevenLabs's estimation, what is the success rate (percentage) of its real-time efforts to detect and prevent the cloning of "no go" voices?

6. What steps does ElevenLabs take to prevent the cloning of a minor's voice, which is prohibited by the company's terms of service?[35]

    a. To the extent that ElevenLabs permits users to generate synthetic "adolescent" voices using its Voice Design tools or makes children's

[35] ElevenLabs, ElevenLabs Prohibited Use Policy (elevenlabs.io/use-policy) (accessed Nov. 3, 2025).

and/or child-like voices available in its library,[36] how does the company ensure that these are not misused in harmful or exploitative ways?

7. Does ElevenLabs have a tool or mechanism in place to detect whether audio was generated by its own products? Is such a tool available to the public?

8. Does ElevenLabs watermark or otherwise signal that the content created on its platform is generated from AI? If so:

    a. Can the general public detect such a mark or otherwise verify the provenance of content generated by ElevenLabs?

    b. Can law enforcement detect such a mark or otherwise verify the provenance of content generated by ElevenLabs, and does the company provide law enforcement officials more information than the public in this regard? If so, please explain.

9. Does ElevenLabs require users to explain their reason or use case for using the company's AI voice cloning tool? If so, please describe these requirements. If not, please explain why not.

10. Does ElevenLabs enter into contractual agreements with its customers that designate which party holds liability if the company's product is misused? If so, please describe the nature of these agreements.

Sincerely,

Margaret Wood Hassan
Ranking Member
U.S. Congress Joint Economic Committee

cc: David Schweikert
Chairman, Joint Economic Committee

Eric Schmitt
Vice Chairman, Joint Economic Committee

[36] ElevenLabs, Voice Design (elevenlabs.io/docs/product-guides/voices/voice-design) (accessed Nov. 3, 2025); ElevenLabs, School Boy AI Voice Generator (elevenlabs.io/voice-library/school-boy) (accessed Nov. 3, 2025).

April 16, 2026

Mr. Tom Lee
Co-Founder & Chief Executive Officer
Lovo AI
SkyDeck
2150 Shattuck Ave
Penthouse, Suite 1300
Berkeley, CA 94704

Dear Mr. Lee:

I write today to request information on LOVO's efforts to prevent scammers from misusing its AI voice-generating tools. In recent years, global criminal networks have used deepfake voice programs, along with other new AI tools, to target more people with increasingly personalized and believable digital scams, fueling a booming scam industry that surpasses the global drug trade as an illicit industry.[1] Generative AI deepfakes – creating fictitious videos, voices, and documents – are "expected to rapidly increase fraud losses in the years ahead," according to Deloitte's Center for Financial Services, which predicts that these tools could enable up to $40 billion in annual fraud losses in the United States by 2027.[2] Protecting Americans from these financial losses will require collaboration between the public and private sectors, and AI companies like LOVO are on the frontlines of this effort.

A 2025 study found that "[p]eople are poorly equipped to detect AI-powered voice clones" and that "AI-generated voices will soon be indistinguishable from real ones."[3] Accurate, widely available, and easy to use, AI tools can quickly create new, generic voices or clone the

---

[1] *Myanmar's Scam Empire Gets Worse, Not Better,* The Economist (May 29, 2025) (www.economist.com/asia/2025/05/29/myanmars-scam-empire-gets-worse-not-better).

[2] Deloitte's Center for Financial Services, *Generative AI is Expected to Magnify the Risk of Deepfakes and Other Fraud in Banking* (May 29, 2024) (www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html).

[3] Sarah Barrington, Emily A. Cooper, and Hany Farid, *People are Poorly Equipped to Detect AI-Powered Voice Clones,* Scientific Reports (Mar. 31, 2025) (www.nature.com/articles/s41598-025-94170-3).

voices of real people from a brief audio sample.[4] Some AI platforms also let users select from vast libraries of pre-made AI voices, saving them from having to design speakers themselves.[5] As you know, LOVO offers users more than 500 voices in 100 languages.[6] In addition, technological advances now allow speakers to convert their voices into an AI voice in real time, enabling live conversations, an advancement that cybersecurity researchers described as "a key requirement for [voice phishing] attacks" in a September 2025 study.[7] The researchers further found that "the tools and infrastructure needed for real-time voice cloning are accessible to those with even limited technical and financial means."[8]

While there are legitimate uses of these tools, they are also used by foreign criminals preying on Americans – enabling these scammers to operate at "previously unthought of levels."[9] Scammers, for example, have used AI-generated voices to pose as employees of government agencies, banks, and utilities and urgently request credentials or payments from Americans.[10] On dating apps and other social media platforms, scammers also use these same kinds of voices to facilitate romance scams, a category of fraud that cost victims over $1 billion last year according to the Federal Trade Commission.[11] To appear "more believable," criminals posing as a romantic partner will "offer to talk by phone [with the victim], and they'll use AI to disguise their voice or appearance and to make it look like somebody they're not," according to an FBI special agent who investigates romance and investment scams.[12] A 2025 report found that not only do "deepfake media provide an additional layer of authenticity" for romance scammers, but they

---

[4] LOVO, Home Page (lovo.ai/) (accessed Jan. 20, 2026); LOVO, *AI Voice Cloning for Creators & Professionals* (lovo.ai/custom-voice) (accessed Jan. 20, 2026).

[5] LOVO, Home Page (lovo.ai/) (accessed Jan. 20, 2026).

[6] *Id.*

[7] NCC Group, Pablo Alobera, Pablo López, Víctor Lasa, *Realtime AI-Supported Voice Conversion (Deepfake) and its Applications on Vishing and Social Engineering Exercises* (Sept. 30, 2025) (www.nccgroup.com/research-blog/voice-impersonation-and-deepfake-vishing-in-realtime/).

[8] *Id.*

[9] *Id.*

[10] *FCC Names Its First-Ever AI Scammer in Threat Alert*, Fox News (June 5, 2024) (www.foxnews.com/tech/fcc-names-its-first-ever-ai-scammer-threat-alert).

[11] Centre for Emerging Technology and Security, *Automating Deception: AI's Evolving Role in Romance Fraud* (Apr. 15, 2025) (cetas.turing.ac.uk/publications/automating-deception-ais-evolving-role-romance-fraud); *Federal Trade Commission Consumer Sentinel Network*, Fraud Reports (Published Aug. 15, 2025) (public.tableau.com/app/profile/federal.trade.commission/viz/shared/4WS8HTYQ6).

[12] *AI Making Romance Scams Harder to Spot*, KOAA News (Sept. 4, 2025) (www.koaa.com/news/local-news/ai-making-romance-scams-harder-to-spot).

also allow these scammers to convincingly reach more people with less effort.[13] LOVO offers voice characteristics that romance scammers could potentially misuse, including options for "flirty" or "intimate" speakers.[14]

AI voice-generating technology has also facilitated new, personalized scams that use clones of trusted voices to request or authorize money or access sensitive accounts.[15] In June 2025, a New York man was sentenced to prison for his role in a high-tech, "elaborate grandparent scam" in which he stole around $20,000 from three New Hampshire families after convincing them that their loved ones were in trouble.[16] According to the *Union Leader*, "[v]ictims say the scam involved the use of artificial intelligence mimicking a loved one's voice to trick them into turning over money to bail that person out of jail."[17] One victim described how "[t]he story was presented so convincingly with my son's voice full of terror" on the deepfake call.[18] In 2024, police in Merrimack County, New Hampshire, similarly investigated dozens of reports of scam calls targeting residents in which criminals allegedly used AI to manipulate their voices to sound like law enforcement or the family members of victims.[19] These calls deceived at least two residents, including one who paid the scammers $5,000.[20] Voice clones have also fooled businesses with more resources at their disposal than the average American, creating what

---

[13] Centre for Emerging Technology and Security, *Automating Deception: AI's Evolving Role in Romance Fraud* (Apr. 15, 2025) (cetas.turing.ac.uk/publications/automating-deception-ais-evolving-role-romance-fraud).

[14] LOVO, *What Emotions can LOVO Express?* (2024) (help.lovo.ai/hc/en-us/articles/21885080508185-What-emotions-can-LOVO-express).

[15] *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (Oct. 14, 2021) (www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/); *Bronx Man Gets 4 to 8 Years for Role in 'Grandparent Scam,'* New Hampshire Union Leader (Sept. 24, 2025) (www.unionleader.com/news/courts/bronx-man-gets-4-to-8-years-for-role-in-grandparent-scam/article_58a05fcd-5edd-4d76-8dae-8ccd3937dcac.html).

[16] *Bronx Man Gets 4 to 8 Years for Role in 'Grandparent Scam,'* New Hampshire Union Leader (Sept. 24, 2025) (www.unionleader.com/news/courts/bronx-man-gets-4-to-8-years-for-role-in-grandparent-scam/article_58a05fcd-5edd-4d76-8dae-8ccd3937dcac.html).

[17] *Id.*

[18] *Id.*

[19] *Merrimack County Residents Targeted by AI Phone Scams, Police Say,* WMUR (Aug. 12, 2024) (www.wmur.com/article/merrimack-county-ai-scam-call-investigate-bitcoin-croft-arrest-warrant-manipulate/61858706).

[20] *Id.*

some in the AI industry have described as a "fraud crisis."[21] Cloned voices, for example, can bypass voice ID verification measures from banks or mimic company executives to authorize large payment transfers, sometimes for tens of millions of dollars.[22] In 2020, a bank manager in Hong Kong authorized $35 million in transfers after a cloned voice impersonated a client.[23] The previous year, a manager of a British energy company wired more than $240,000 to a foreign account after receiving instructions from a deepfake clone of his boss's voice.[24]

This same technology has also created alarming new avenues for political interference and disinformation. New Hampshire, for example, was the target of the "first known example of an AI-generated deepfake being deployed maliciously in an American political campaign," according to public reporting.[25] Ahead of the January 2024 presidential primary election, thousands of New Hampshire residents received a robocall from an AI-generated voice clone of President Joe Biden instructing them not to vote in the upcoming election.[26] The person who executed the calls later faced criminal charges and a $6 million fine from the Federal Communications Commission. [27]

---

[21] Sam Altman, Remarks at the Federal Reserve's Integrated Review of the Capital Framework for Large Banks Conference in Washington, Associated Press (July 22, 2025) (www.youtube.com/watch?v=tScbQiavmpA).

[22] *Cloned Customer Voice Beats Bank Security Checks*, BBC (Nov. 28, 2024) (www.bbc.com/news/articles/c1lg3ded6j9o); *How I Broke Into a Bank Account With an AI-Generated Voice*, Vice (Feb. 23, 2023) (www.vice.com/en/article/how-i-broke-into-a-bank-account-with-an-ai-generated-voice/); Consumer Reports, *AI Voice Cloning: Do These 6 Companies Do Enough to Prevent Misuse?* (Mar. 10, 2025) (innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf); *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (Oct. 14, 2021) (www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/).

[23] *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (Oct. 14, 2021) (www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/).

[24] *An Artificial-Intelligence First: Voice-Mimicking Software Reportedly Used in a Major Theft*, The Washington Post (Sept. 4, 2019) (www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/).

[25] *A New Orleans Magician says a Democratic Operative Paid Him to Make the Fake Biden Robocall*, NBC News (Feb. 23, 2024) (www.nbcnews.com/politics/2024-election/biden-robocall-new-hampshire-strategist-rcna139760).

[26] *Id.*

[27] *Political Consultant Behind Fake Biden Robocalls Faces $6 Million Fine and Criminal Charges*, Associated Press (May 23, 2024) (apnews.com/article/biden-robocalls-ai-new-hampshire-charges-fines-9e9cc63a71eb9c78b9bb0d1ec2aa6e9c).

As this fraudulent activity continues, evidence suggests that technology companies could do more to prevent the misuse of their AI voice generation tools.[28] In 2024, investigative news outlet *Proof* examined eight popular AI voice cloning platforms and found few safeguards to prevent nonconsensual voice cloning: "[M]ost companies…make little or no attempt to ensure that the humans being copied have consented to the process."[29] A March 2025 Consumer Reports investigation similarly found that most of the leading AI voice cloning products had no "technical mechanism" in place to prevent users from replicating voices without permission.[30] Instead, they simply required users to self-attest that they had the right to clone a voice.[31] Moreover, the majority of the companies Consumer Reports examined did little to learn the true identities of their customers, a step that could help them track and prevent the abuse of their products.[32] Consumer Reports argued that AI voice cloning companies should adopt these two requirements, among other the safety measures, "at a bare minimum" and as a "starting point."[33]

Given the role that AI voice generation tools can play in creating scams, I seek responses to the requests below.

1. Does LOVO monitor user activity and/or the content created on its platforms to detect violations of its usage policies prohibiting the use of its models for unlawful activity? If so:

    a. Is any such monitoring designed to identify scam activity specifically?

    b. Does LOVO detect, flag, and/or prohibit the creation of audio content that contains phrases commonly used in scams?
        i. If so, how often does LOVO evaluate the effectiveness of its prohibitions on specific terms in preventing scams? How often does the company update its list of prohibited terms?

[28] *AI Tools Make It Easy to Clone Someone's Voice Without Consent*, Proof (June 25, 2024) (www.proofnews.org/ai-tools-make-it-easy-to-clone-someones-voice-without-consent/); Consumer Reports, *AI Voice Cloning: Do These 6 Companies Do Enough to Prevent Misuse?* (Mar. 10, 2025) (innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf).

[29] *AI Tools Make It Easy to Clone Someone's Voice Without Consent*, Proof (June 25, 2024) (www.proofnews.org/ai-tools-make-it-easy-to-clone-someones-voice-without-consent/).

[30] Consumer Reports, *AI Voice Cloning: Do These 6 Companies Do Enough to Prevent Misuse?* (Mar. 10, 2025) (innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf).

[31] *Id.*

[32] *Id.*

[33] *Id.*

c. Does LOVO detect, flag, and/or prohibit the creation of audio content in which a user has created a voice to misrepresent themselves as an official from a bank, government office, or other entity?

2. What actions, if any, does LOVO take against users who violate its policies prohibiting the use of its models for unlawful scam and fraud activity?

    a. If these actions include banning users from the platform:
        i. Under what circumstances has LOVO banned users for violating the company's policies prohibiting scams;
        ii. How many users has LOVO banned for such violations;
        iii. How does LOVO prevent these users from returning to the platform?

    b. Under what circumstances, if any, does LOVO report these users to law enforcement?

3. What mechanisms does LOVO maintain to verify that a speaker has consented to their voice being cloned?

    a. Does LOVO require users to clone a voice from audio recorded in real time? If so, under what circumstances is this required? If not, why not?

    b. Does LOVO require users to upload authentic, non-public audio of the speaker whose voice they intend to clone? Why or why not? If so:
        i. What, if any, requirements does LOVO impose for such recordings? For instance, does the audio need to be of a particular length or read from a unique script?
        ii. What mechanisms does LOVO maintain to ensure that any audio submitted for verification purposes is authentic?

4. Does LOVO track user attempts to violate its policies prohibiting nonconsensual voice cloning? If so:

    a. How many unique users and unique attempts has LOVO detected as being in violation of its policies prohibiting nonconsensual voice cloning, and what actions has it taken against the users responsible?

    b. How many of these users and attempts did LOVO detect *before* a nonconsensual voice clone was generated?

    c. How many of these users and attempts did the company detect only *after* a nonconsensual voice clone was generated?

d. What steps, if any, does the company take to adapt its measures to defend against such tactics?

5. Does LOVO take specific steps to ensure that the voices of public figures, such as celebrities and politicians, are not created on its platform without authorization? If so, please detail those steps.

    a. Does LOVO monitor for instances in which users attempt to clone the voice of a public figure without authorization? If so:
        i. How many user attempts to clone a public figure's voice without authorization has LOVO detected?
        ii. How many of those attempts did LOVO thwart in real time – in other words, while the user was trying to create the unauthorized voice?

    b. Does LOVO monitor user activity to detect when users have succeeded in cloning a public figure's voice without authorization despite the company's prevention efforts? If so:
        i. How many instances of users successfully cloning a public figure's voice without authorization has LOVO detected?
        ii. In these instances, does the company track how the user circumvented the company's efforts to detect and prevent the unauthorized cloning of a public figure's voice? What steps, if any, does the company then take to adapt its measures to defend against such tactics?

    c. In LOVO's estimation, what is the success rate (percentage) of its real-time efforts to detect and prevent the unauthorized cloning of voices belonging to public figures?

6. Does LOVO permit the cloning of a minor's voice? If not, what steps does the company take to prevent such activity? If so, what steps does the company take to ensure that these cloned voices are not misused in harmful or exploitive ways?

    a. To the extent that LOVO permits users to generate synthetic children's voices or makes such voices available in its library, how does the company ensure that these are not misused in harmful or exploitative ways?

7. Does LOVO have a tool or mechanism in place to detect whether audio was generated by its own products? Is such a tool available to the public?

8. Does LOVO watermark or otherwise signal that the content created on its platform is generated from AI? If so:

a. Can the general public detect such a mark or otherwise verify the provenance of content generated by LOVO?

b. Can law enforcement detect such a mark or otherwise verify the provenance of content generated by LOVO, and does the company provide law enforcement officials more information than the public in this regard? If so, please explain.

9. Does LOVO require users to explain their reason or use case for using the company's AI voice cloning tool? If so, please describe these requirements. If not, please explain why not.

10. Does LOVO enter into contractual agreements with its customers that designate which party holds liability if the company's product is misused? If so, please describe the nature of these agreements.

Sincerely,

Margaret Wood Hassan
Ranking Member
U.S. Congress Joint Economic Committee

cc: David Schweikert
Chairman, Joint Economic Committee

Eric Schmitt
Vice Chairman, Joint Economic Committee

April 16, 2026

Mr. Cliff Weitzman
Chief Executive Officer & Founder
Speechify
7901 4th Street N
Suite 6193
St. Petersburg, FL 33702

Dear Mr. Weitzman:

I write today to request information on Speechify's efforts to prevent scammers from misusing its AI voice-generating tools. In recent years, global criminal networks have used deepfake voice programs, along with other new AI tools, to target more people with increasingly personalized and believable digital scams, fueling a booming scam industry that surpasses the global drug trade as an illicit industry.[1] Generative AI deepfakes – creating fictitious videos, voices, and documents – are "expected to rapidly increase fraud losses in the years ahead," according to Deloitte's Center for Financial Services, which predicts that these tools could enable up to $40 billion in annual fraud losses in the United States by 2027.[2] Protecting Americans from these financial losses will require collaboration between the public and private sectors, and AI companies like Speechify are on the frontlines of this effort.

A 2025 study found that "[p]eople are poorly equipped to detect AI-powered voice clones" and that "AI-generated voices will soon be indistinguishable from real ones."[3] Accurate, widely available, and easy to use, AI tools can quickly create new, generic voices or clone the

---

[1] *Myanmar's Scam Empire Gets Worse, Not Better,* The Economist (May 29, 2025) (www.economist.com/asia/2025/05/29/myanmars-scam-empire-gets-worse-not-better).

[2] Deloitte's Center for Financial Services, *Generative AI is Expected to Magnify the Risk of Deepfakes and Other Fraud in Banking* (May 29, 2024) (www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html).

[3] Sarah Barrington, Emily A. Cooper, and Hany Farid, *People are Poorly Equipped to Detect AI-Powered Voice Clones,* Scientific Reports (Mar. 31, 2025) (www.nature.com/articles/s41598-025-94170-3).

voices of real people from a brief audio sample.[4] Some AI platforms also let users select from vast libraries of pre-made AI voices, saving them from having to design speakers themselves.[5] As you know, Speechify offers more than 1,000 voices in over 60 languages.[6] In addition, technological advances now allow speakers to convert their voices into an AI voice in real time, enabling live conversations, an advancement that cybersecurity researchers described as "a key requirement for [voice phishing] attacks" in a September 2025 study.[7] The researchers further found that "the tools and infrastructure needed for real-time voice cloning are accessible to those with even limited technical and financial means."[8]

While there are legitimate uses of these tools, they are also used by foreign criminals preying on Americans – enabling these scammers to operate at "previously unthought of levels."[9] Scammers, for example, have used AI-generated voices to pose as employees of government agencies, banks, and utilities and urgently request credentials or payments from Americans.[10] On dating apps and other social media platforms, scammers also use these same kinds of voices to facilitate romance scams, a category of fraud that cost victims over $1 billion last year according to the Federal Trade Commission.[11] To appear "more believable," criminals posing as a romantic partner will "offer to talk by phone [with the victim], and they'll use AI to disguise their voice or

---

[4] Speechify, *AI Voice Cloning: Clone Your Voice Instantly* (speechify.com/voice-cloning/) (accessed Feb. 11, 2026); Speechify, *Speechify, Text to Speech & Voice AI* (speechify.com/?srsltid=AfmBOorYuso0uazvTBhagabfDjVV4bvMfZrcXVrSfFe0dSPq_dQnQOXE) (accessed Feb. 25, 2026).

[5] Speechify, *AI Voice Cloning: Clone Your Voice Instantly* (speechify.com/voice-cloning/) (accessed Feb. 11, 2026); Speechify, *Speechify, Text to Speech & Voice AI* (speechify.com/?srsltid=AfmBOorYuso0uazvTBhagabfDjVV4bvMfZrcXVrSfFe0dSPq_dQnQOXE) (accessed Feb. 25, 2026).

[6] Speechify, *Speechify, Text to Speech & Voice AI* (speechify.com/?srsltid=AfmBOorYuso0uazvTBhagabfDjVV4bvMfZrcXVrSfFe0dSPq_dQnQOXE) (accessed Feb. 25, 2026).

[7] NCC Group, Pablo Alobera, Pablo López, Víctor Lasa, *Realtime AI-Supported Voice Conversion (Deepfake) and its Applications on Vishing and Social Engineering Exercises* (Sept. 30, 2025) (www.nccgroup.com/research-blog/voice-impersonation-and-deepfake-vishing-in-realtime/).

[8] *Id.*

[9] *Id.*

[10] *FCC Names Its First-Ever AI Scammer in Threat Alert*, Fox News (June 5, 2024) (www.foxnews.com/tech/fcc-names-its-first-ever-ai-scammer-threat-alert).

[11] Centre for Emerging Technology and Security, *Automating Deception: AI's Evolving Role in Romance Fraud* (Apr. 15, 2025) (cetas.turing.ac.uk/publications/automating-deception-ais-evolving-role-romance-fraud); *Federal Trade Commission Consumer Sentinel Network*, Fraud Reports (Published Aug. 15, 2025) (public.tableau.com/app/profile/federal.trade.commission/viz/shared/4WS8HTYQ6).

appearance and to make it look like somebody they're not," according to an FBI special agent who investigates romance and investment scams.[12] A 2025 report found that not only do "deepfake media provide an additional layer of authenticity" for romance scammers, but they also allow these scammers to convincingly reach more people with less effort.[13] Notably, Speechify's website gives users tips on designing custom voices, some of which have characteristics that romance scammers could potentially misuse.[14] For example, Speechify noted that "[a] female voice can be described as breathy, suggesting an air of softness or sensuality. A throaty or husky voice adds a layer of complexity and allure." [15] The website also stated, "[b]reathy voices suggest an undertone of intimacy," while "[a] throaty voice carries a deep, intimate, and possibly attractive way to describe a voice."[16]

AI voice-generating technology has also facilitated new, personalized scams that use clones of trusted voices to request or authorize money or access sensitive accounts.[17] In June 2025, a New York man was sentenced to prison for his role in a high-tech, "elaborate grandparent scam" in which he stole around $20,000 from three New Hampshire families after convincing them that their loved ones were in trouble.[18] According to the *Union Leader*, "[v]ictims say the scam involved the use of artificial intelligence mimicking a loved one's voice to trick them into turning over money to bail that person out of jail."[19] One victim described how "[t]he story was presented so convincingly with my son's voice full of terror" on the deepfake call.[20] In 2024, police in Merrimack County, New Hampshire, similarly investigated dozens of

---

[12] *AI Making Romance Scams Harder to Spot*, KOAA News (Sept. 4, 2025) (www.koaa.com/news/local-news/ai-making-romance-scams-harder-to-spot).

[13] Centre for Emerging Technology and Security, *Automating Deception: AI's Evolving Role in Romance Fraud* (Apr. 15, 2025) (cetas.turing.ac.uk/publications/automating-deception-ais-evolving-role-romance-fraud).

[14] Speechify, *How to Describe a Voice in Great Detail* (June 14, 2023) (speechify.com/blog/how-to-describe-voice/).

[15] *Id.*

[16] *Id.*

[17] *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (Oct. 14, 2021) (www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/); *Bronx Man Gets 4 to 8 Years for Role in 'Grandparent Scam,'* New Hampshire Union Leader (Sept. 24, 2025) (www.unionleader.com/news/courts/bronx-man-gets-4-to-8-years-for-role-in-grandparent-scam/article_58a05fcd-5edd-4d76-8dae-8ccd3937dcac.html).

[18] *Bronx Man Gets 4 to 8 Years for Role in 'Grandparent Scam,'* New Hampshire Union Leader (Sept. 24, 2025) (www.unionleader.com/news/courts/bronx-man-gets-4-to-8-years-for-role-in-grandparent-scam/article_58a05fcd-5edd-4d76-8dae-8ccd3937dcac.html).

[19] *Id.*

[20] *Id.*

reports of scam calls targeting residents in which criminals allegedly used AI to manipulate their voices to sound like law enforcement or the family members of victims.[21] These calls deceived at least two residents, including one who paid the scammers $5,000.[22] Voice clones have also fooled businesses with more resources at their disposal than the average American, creating what some in the AI industry have described as a "fraud crisis."[23] Cloned voices, for example, can bypass voice ID verification measures from banks or mimic company executives to authorize large payment transfers, sometimes for tens of millions of dollars.[24] In 2020, a bank manager in Hong Kong authorized $35 million in transfers after a cloned voice impersonated a client.[25] The previous year, a manager of a British energy company wired more than $240,000 to a foreign account after receiving instructions from a deepfake clone of his boss's voice.[26]

This same technology has also created alarming new avenues for political interference and disinformation. New Hampshire, for example, was the target of the "first known example of an AI-generated deepfake being deployed maliciously in an American political campaign," according to public reporting.[27] Ahead of the January 2024 presidential primary election, thousands of New Hampshire residents received a robocall from an AI-generated voice clone of

---

[21] *Merrimack County Residents Targeted by AI Phone Scams, Police Say,* WMUR (Aug. 12, 2024) (www.wmur.com/article/merrimack-county-ai-scam-call-investigate-bitcoin-croft-arrest-warrant-manipulate/61858706).

[22] *Id.*

[23] Sam Altman, Remarks at the Federal Reserve's Integrated Review of the Capital Framework for Large Banks Conference in Washington, Associated Press (July 22, 2025) (www.youtube.com/watch?v=tScbQiavmpA).

[24] *Cloned Customer Voice Beats Bank Security Checks*, BBC (Nov. 28, 2024) (www.bbc.com/news/articles/c1lg3ded6j9o); *How I Broke Into a Bank Account With an AI-Generated Voice*, Vice (Feb. 23, 2023) (www.vice.com/en/article/how-i-broke-into-a-bank-account-with-an-ai-generated-voice/); Consumer Reports, *AI Voice Cloning: Do These 6 Companies Do Enough to Prevent Misuse?* (Mar. 10, 2025) (innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf); *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (Oct. 14, 2021) (www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/).

[25] *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (Oct. 14, 2021) (www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/).

[26] *An Artificial-Intelligence First: Voice-Mimicking Software Reportedly Used in a Major Theft*, The Washington Post (Sept. 4, 2019) (www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/).

[27] *A New Orleans Magician says a Democratic Operative Paid Him to Make the Fake Biden Robocall*, NBC News (Feb. 23, 2024) (www.nbcnews.com/politics/2024-election/biden-robocall-new-hampshire-strategist-rcna139760).

President Joe Biden instructing them not to vote in the upcoming election.[28] The person who executed the calls later faced criminal charges and a $6 million fine from the Federal Communications Commission. [29]

As this fraudulent activity continues, evidence suggests that technology companies could do more to prevent the misuse of their AI voice generation tools.[30] In 2024, investigative news outlet *Proof* examined eight popular AI voice cloning platforms and found few safeguards to prevent nonconsensual voice cloning: "[M]ost companies…make little or no attempt to ensure that the humans being copied have consented to the process."[31] A March 2025 Consumer Reports investigation similarly found that most of the leading AI voice cloning products had no "technical mechanism" in place to prevent users from replicating voices without permission.[32] Instead, they simply required users to self-attest that they had the right to clone a voice.[33] Moreover, the majority of the companies Consumer Reports examined did little to learn the true identities of their customers, a step that could help them track and prevent the abuse of their products.[34] Consumer Reports argued that AI voice cloning companies should adopt these two requirements, among other the safety measures, "at a bare minimum" and as a "starting point."[35]

Given the role that AI voice generation tools can play in creating scams, I seek responses to the requests below.

1. Does Speechify monitor user activity and/or the content created on its platforms to detect violations of its usage policies prohibiting the use of its models for fraudulent activity? If so:

    a. Is any such monitoring designed to identify scam activity specifically?

---

[28] *Id.*

[29] *Political Consultant Behind Fake Biden Robocalls Faces $6 Million Fine and Criminal Charges*, Associated Press (May 23, 2024) (apnews.com/article/biden-robocalls-ai-new-hampshire-charges-fines-9e9cc63a71eb9c78b9bb0d1ec2aa6e9c).

[30] *AI Tools Make It Easy to Clone Someone's Voice Without Consent*, Proof (June 25, 2024) (www.proofnews.org/ai-tools-make-it-easy-to-clone-someones-voice-without-consent/); Consumer Reports, *AI Voice Cloning: Do These 6 Companies Do Enough to Prevent Misuse?* (Mar. 10, 2025) (innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf).

[31] *AI Tools Make It Easy to Clone Someone's Voice Without Consent*, Proof (June 25, 2024) (www.proofnews.org/ai-tools-make-it-easy-to-clone-someones-voice-without-consent/).

[32] Consumer Reports, *AI Voice Cloning: Do These 6 Companies Do Enough to Prevent Misuse?* (Mar. 10, 2025) (innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf).

[33] *Id.*

[34] *Id.*

[35] *Id.*

b. Does Speechify detect, flag, and/or prohibit the creation of audio content that contains phrases commonly used in scams?
    i. If so, how often does Speechify evaluate the effectiveness of its prohibitions on specific terms in preventing scams? How often does the company update its list of prohibited terms?

c. Does Speechify detect, flag, and/or prohibit the creation of audio content in which a user has created a voice to misrepresent themselves as an official from a bank, government office, or other entity?

2. What actions, if any, does Speechify take against users who violate its policies prohibiting the use of its models for fraud?

    a. If these actions include banning users from the platform:
        i. Under what circumstances has Speechify banned users for violating the company's policies prohibiting scams;
        ii. How many users has Speechify banned for such violations;
        iii. How does Speechify prevent these users from returning to the platform?

    b. Under what circumstances, if any, does Speechify report these users to law enforcement?

3. What mechanisms does Speechify maintain to verify that a speaker has consented to their voice being cloned?

    a. Does Speechify require users to clone a voice from audio recorded in real time? If so, under what circumstances is this required? If not, why not?

    b. Does Speechify require users to upload authentic, non-public audio of the speaker whose voice they intend to clone? Why or why not? If so:
        i. What, if any, requirements does Speechify impose for such recordings? For instance, does the audio need to be of a particular length or read from a unique script?
        ii. What mechanisms does Speechify maintain to ensure that any audio submitted for verification purposes is authentic?

4. Does Speechify track user attempts to violate its policies prohibiting nonconsensual voice cloning? If so:

    a. How many unique users and unique attempts has Speechify detected as being in violation of its policies prohibiting nonconsensual voice cloning, and what actions has it taken against the users responsible?

b. How many of these users and attempts did Speechify detect *before* a nonconsensual voice clone was generated?

c. How many of these users and attempts did the company detect only *after* a nonconsensual voice clone was generated?

d. What steps, if any, does the company take to adapt its measures to defend against such tactics?

5. Does Speechify take specific steps to ensure that the voices of public figures, such as celebrities and politicians, are not created on its platform without authorization? If so, please detail those steps.

    a. Does Speechify monitor for instances in which users attempt to clone the voice of a public figure without authorization? If so:
        i. How many user attempts to clone a public figure's voice without authorization has Speechify detected?
        ii. How many of those attempts did Speechify thwart in real time – in other words, while the user was trying to create the unauthorized voice?

    b. Does Speechify monitor user activity to detect when users have succeeded in cloning a public figure's voice without authorization despite the company's prevention efforts? If so:
        i. How many instances of users successfully cloning a public figure's voice without authorization has Speechify detected?
        ii. In these instances, does the company track how the user circumvented the company's efforts to detect and prevent the unauthorized cloning of a public figure's voice? What steps, if any, does the company then take to adapt its measures to defend against such tactics?

    c. In Speechify's estimation, what is the success rate (percentage) of its real-time efforts to detect and prevent the unauthorized cloning of voices belonging to public figures?

6. Does Speechify permit the cloning of a minor's voice? If not, what steps does the company take to prevent such activity? If so, what steps does the company take to ensure that these cloned voices are not misused in harmful or exploitive ways?

    a. To the extent that Speechify permits users to generate synthetic children's voices or makes such voices available in its library, how does the company ensure that these are not misused in harmful or exploitative ways?

7. Does Speechify have a tool or mechanism in place to detect whether audio was generated by its own products? Is such a tool available to the public?

8. Does Speechify watermark or otherwise signal that the content created on its platform is generated from AI? If so:

    a. Can the general public detect such a mark or otherwise verify the provenance of content generated by Speechify?

    b. Can law enforcement detect such a mark or otherwise verify the provenance of content generated by Speechify, and does the company provide law enforcement officials more information than the public in this regard? If so, please explain.

9. Does Speechify require users to explain their reason or use case for using the company's AI voice cloning tool? If so, please describe these requirements. If not, please explain why not.

10. Does Speechify enter into contractual agreements with its customers that designate which party holds liability if the company's product is misused? If so, please describe the nature of these agreements.

Sincerely,

Margaret Wood Hassan
Ranking Member
U.S. Congress Joint Economic Committee

cc: David Schweikert
Chairman, Joint Economic Committee

Eric Schmitt
Vice Chairman, Joint Economic Committee

April 16, 2026

Mr. Sabba Keynejad
Co-Founder & Chief Executive Officer
VEED
17-18 Clere Street
Shoreditch, London EC2A 4LJ

Dear Mr. Keynejad:

I write today to request information on VEED's efforts to prevent scammers from misusing its AI voice-generating tools. In recent years, global criminal networks have used deepfake voice programs, along with other new AI tools, to target more people with increasingly personalized and believable digital scams, fueling a booming scam industry that surpasses the global drug trade as an illicit industry.[1] Generative AI deepfakes – creating fictitious videos, voices, and documents – are "expected to rapidly increase fraud losses in the years ahead," according to Deloitte's Center for Financial Services, which predicts that these tools could enable up to $40 billion in annual fraud losses in the United States by 2027.[2] Protecting Americans from these financial losses will require collaboration between the public and private sectors, and AI companies like VEED are on the frontlines of this effort.

A 2025 study found that "[p]eople are poorly equipped to detect AI-powered voice clones" and that "AI-generated voices will soon be indistinguishable from real ones."[3] Accurate, widely available, and easy to use, AI tools can quickly create new, generic voices or clone the

---

[1] *Myanmar's Scam Empire Gets Worse, Not Better,* The Economist (May 29, 2025) (www.economist.com/asia/2025/05/29/myanmars-scam-empire-gets-worse-not-better).

[2] Deloitte's Center for Financial Services, *Generative AI is Expected to Magnify the Risk of Deepfakes and Other Fraud in Banking* (May 29, 2024) (www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html).

[3] Sarah Barrington, Emily A. Cooper, and Hany Farid, *People are Poorly Equipped to Detect AI-Powered Voice Clones,* Scientific Reports (Mar. 31, 2025) (www.nature.com/articles/s41598-025-94170-3).

voices of real people from a brief audio sample.[4] Some AI platforms also let users select from vast libraries of pre-made AI voices, saving them from having to design speakers themselves.[5] VEED, for instance, offers more than 35 voices that can speak dozens of languages.[6] In addition, technological advances now allow speakers to convert their voices into an AI voice in real time, enabling live conversations, an advancement that cybersecurity researchers described as "a key requirement for [voice phishing] attacks" in a September 2025 study.[7] The researchers further found that "the tools and infrastructure needed for real-time voice cloning are accessible to those with even limited technical and financial means."[8]

While there are legitimate uses of these tools, they are also used by foreign criminals preying on Americans – enabling these scammers to operate at "previously unthought of levels."[9] Scammers, for example, have used AI-generated voices to pose as employees of government agencies, banks, and utilities and urgently request credentials or payments from Americans.[10] On dating apps and other social media platforms, scammers also use these same kinds of voices to facilitate romance scams, a category of fraud that cost victims over $1 billion last year according to the Federal Trade Commission.[11] To appear "more believable," criminals posing as a romantic partner will "offer to talk by phone [with the victim], and they'll use AI to disguise their voice or

[4] VEED, *AI Voice Cloning* (www.veed.io/tools/ai-voice-cloning) (accessed Feb.17, 2026); VEED, *Voicemaker* (www.veed.io/tools/voice-over-generator/voicemaker) (accessed Feb.17, 2026); VEED, *VEED vs. ElevenLabs 2026: Which AI Voice Tool Is Right for You?* (www.veed.io/learn/veed-vs-elevenlabs) (Accessed Feb. 26, 2026).

[5] VEED, *AI Voice Cloning* (www.veed.io/tools/ai-voice-cloning) (accessed Feb.17, 2026); VEED, *Voicemaker* (www.veed.io/tools/voice-over-generator/voicemaker) (accessed Feb.17, 2026); VEED, *VEED vs. ElevenLabs 2026: Which AI Voice Tool Is Right for You?* (www.veed.io/learn/veed-vs-elevenlabs) (Accessed Feb. 26, 2026).

[6] VEED, *VEED vs. ElevenLabs 2026: Which AI Voice Tool Is Right for You?* (www.veed.io/learn/veed-vs-elevenlabs) (Accessed Feb. 26, 2026).

[7] NCC Group, Pablo Alobera, Pablo López, Víctor Lasa, *Realtime AI-Supported Voice Conversion (Deepfake) and its Applications on Vishing and Social Engineering Exercises* (Sept. 30, 2025) (www.nccgroup.com/research-blog/voice-impersonation-and-deepfake-vishing-in-realtime/).

[8] *Id.*

[9] *Id.*

[10] *FCC Names Its First-Ever AI Scammer in Threat Alert*, Fox News (June 5, 2024) (www.foxnews.com/tech/fcc-names-its-first-ever-ai-scammer-threat-alert).

[11] Centre for Emerging Technology and Security, *Automating Deception: AI's Evolving Role in Romance Fraud* (Apr. 15, 2025) (cetas.turing.ac.uk/publications/automating-deception-ais-evolving-role-romance-fraud); *Federal Trade Commission Consumer Sentinel Network*, Fraud Reports (Published Aug. 15, 2025) (public.tableau.com/app/profile/federal.trade.commission/viz/shared/4WS8HTYQ6).

appearance and to make it look like somebody they're not," according to an FBI special agent who investigates romance and investment scams.[12] A 2025 report found that not only do "deepfake media provide an additional layer of authenticity" for romance scammers, but they also allow these scammers to convincingly reach more people with less effort.[13]

AI voice-generating technology has also facilitated new, personalized scams that use clones of trusted voices to request or authorize money or access sensitive accounts.[14] In June 2025, a New York man was sentenced to prison for his role in a high-tech, "elaborate grandparent scam" in which he stole around $20,000 from three New Hampshire families after convincing them that their loved ones were in trouble.[15] According to the *Union Leader*, "[v]ictims say the scam involved the use of artificial intelligence mimicking a loved one's voice to trick them into turning over money to bail that person out of jail."[16] One victim described how "[t]he story was presented so convincingly with my son's voice full of terror" on the deepfake call.[17] In 2024, police in Merrimack County, New Hampshire, similarly investigated dozens of reports of scam calls targeting residents in which criminals allegedly used AI to manipulate their voices to sound like law enforcement or the family members of victims.[18] These calls deceived at least two residents, including one who paid the scammers $5,000.[19] Voice clones have also fooled businesses with more resources at their disposal than the average American, creating what

---

[12] *AI Making Romance Scams Harder to Spot*, KOAA News (Sept. 4, 2025) (www.koaa.com/news/local-news/ai-making-romance-scams-harder-to-spot).

[13] Centre for Emerging Technology and Security, *Automating Deception: AI's Evolving Role in Romance Fraud* (Apr. 15, 2025) (cetas.turing.ac.uk/publications/automating-deception-ais-evolving-role-romance-fraud).

[14] *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (Oct. 14, 2021) (www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/); *Bronx Man Gets 4 to 8 Years for Role in 'Grandparent Scam,'* New Hampshire Union Leader (Sept. 24, 2025) (www.unionleader.com/news/courts/bronx-man-gets-4-to-8-years-for-role-in-grandparent-scam/article_58a05fcd-5edd-4d76-8dae-8ccd3937dcac.html).

[15] *Bronx Man Gets 4 to 8 Years for Role in 'Grandparent Scam,'* New Hampshire Union Leader (Sept. 24, 2025) (www.unionleader.com/news/courts/bronx-man-gets-4-to-8-years-for-role-in-grandparent-scam/article_58a05fcd-5edd-4d76-8dae-8ccd3937dcac.html).

[16] *Id.*

[17] *Id.*

[18] *Merrimack County Residents Targeted by AI Phone Scams, Police Say,* WMUR (Aug. 12, 2024) (www.wmur.com/article/merrimack-county-ai-scam-call-investigate-bitcoin-croft-arrest-warrant-manipulate/61858706).

[19] *Id.*

some in the AI industry have described as a "fraud crisis."[20] Cloned voices, for example, can bypass voice ID verification measures from banks or mimic company executives to authorize large payment transfers, sometimes for tens of millions of dollars.[21] In 2020, a bank manager in Hong Kong authorized $35 million in transfers after a cloned voice impersonated a client.[22] The previous year, a manager of a British energy company wired more than $240,000 to a foreign account after receiving instructions from a deepfake clone of his boss's voice.[23]

This same technology has also created alarming new avenues for political interference and disinformation. New Hampshire, for example, was the target of the "first known example of an AI-generated deepfake being deployed maliciously in an American political campaign," according to public reporting.[24] Ahead of the January 2024 presidential primary election, thousands of New Hampshire residents received a robocall from an AI-generated voice clone of President Joe Biden instructing them not to vote in the upcoming election.[25] The person who executed the calls later faced criminal charges and a $6 million fine from the Federal Communications Commission. [26]

---

[20] Sam Altman, Remarks at the Federal Reserve's Integrated Review of the Capital Framework for Large Banks Conference in Washington, Associated Press (July 22, 2025) (www.youtube.com/watch?v=tScbQiavmpA).

[21] *Cloned Customer Voice Beats Bank Security Checks*, BBC (Nov. 28, 2024) (www.bbc.com/news/articles/c1lg3ded6j9o); *How I Broke Into a Bank Account With an AI-Generated Voice*, Vice (Feb. 23, 2023) (www.vice.com/en/article/how-i-broke-into-a-bank-account-with-an-ai-generated-voice/); Consumer Reports, *AI Voice Cloning: Do These 6 Companies Do Enough to Prevent Misuse?* (Mar. 10, 2025) (innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf); *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (Oct. 14, 2021) (www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/).

[22] *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (Oct. 14, 2021) (www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/).

[23] *An Artificial-Intelligence First: Voice-Mimicking Software Reportedly Used in a Major Theft*, The Washington Post (Sept. 4, 2019) (www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/).

[24] *A New Orleans Magician says a Democratic Operative Paid Him to Make the Fake Biden Robocall*, NBC News (Feb. 23, 2024) (www.nbcnews.com/politics/2024-election/biden-robocall-new-hampshire-strategist-rcna139760).

[25] *Id.*

[26] *Political Consultant Behind Fake Biden Robocalls Faces $6 Million Fine and Criminal Charges*, Associated Press (May 23, 2024) (apnews.com/article/biden-robocalls-ai-new-hampshire-charges-fines-9e9cc63a71eb9c78b9bb0d1ec2aa6e9c).

As this fraudulent activity continues, evidence suggests that technology companies could do more to prevent the misuse of their AI voice generation tools.[27] In 2024, investigative news outlet *Proof* examined eight popular AI voice cloning platforms and found few safeguards to prevent nonconsensual voice cloning: "[M]ost companies…make little or no attempt to ensure that the humans being copied have consented to the process."[28] A March 2025 Consumer Reports investigation similarly found that most of the leading AI voice cloning products had no "technical mechanism" in place to prevent users from replicating voices without permission.[29] Instead, they simply required users to self-attest that they had the right to clone a voice.[30] Moreover, the majority of the companies Consumer Reports examined did little to learn the true identities of their customers, a step that could help them track and prevent the abuse of their products.[31] Consumer Reports argued that AI voice cloning companies should adopt these two requirements, among other the safety measures, "at a bare minimum" and as a "starting point."[32]

Given the role that AI voice generation tools can play in creating scams, I seek responses to the requests below.

1. Does VEED monitor user activity and/or the content created on its platforms to detect violations of its usage policies prohibiting the use of its models for fraudulent activity? If so:

    a. Is any such monitoring designed to identify scam activity specifically?

    b. Does VEED detect, flag, and/or prohibit the creation of audio content that contains phrases commonly used in scams?
        i. If so, how often does VEED evaluate the effectiveness of its prohibitions on specific terms in preventing scams? How often does the company update its list of prohibited terms?

---

[27] *AI Tools Make It Easy to Clone Someone's Voice Without Consent*, Proof (June 25, 2024) (www.proofnews.org/ai-tools-make-it-easy-to-clone-someones-voice-without-consent/); Consumer Reports, *AI Voice Cloning: Do These 6 Companies Do Enough to Prevent Misuse?* (Mar. 10, 2025) (innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf).

[28] *AI Tools Make It Easy to Clone Someone's Voice Without Consent*, Proof (June 25, 2024) (www.proofnews.org/ai-tools-make-it-easy-to-clone-someones-voice-without-consent/).

[29] Consumer Reports, *AI Voice Cloning: Do These 6 Companies Do Enough to Prevent Misuse?* (Mar. 10, 2025) (innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf).

[30] *Id.*

[31] *Id.*

[32] *Id.*

c. Does VEED detect, flag, and/or prohibit the creation of audio content in which a user has created a voice to misrepresent themselves as an official from a bank, government office, or other entity?

2. What actions, if any, does VEED take against users who violate its policies prohibiting the use of its models for fraud?

    a. If these actions include banning users from the platform:
        i. Under what circumstances has VEED banned users for violating the company's policies prohibiting scams;
        ii. How many users has VEED banned for such violations;
        iii. How does VEED prevent these users from returning to the platform?

    b. Under what circumstances, if any, does VEED report these users to law enforcement?

3. What mechanisms does VEED maintain to verify that a speaker has consented to their voice being cloned?

    a. Does VEED require users to clone a voice from audio recorded in real time? If so, under what circumstances is this required? If not, why not?

    b. Does VEED require users to upload authentic, non-public audio of the speaker whose voice they intend to clone? Why or why not? If so:
        i. What, if any, requirements does VEED impose for such recordings? For instance, does the audio need to be of a particular length or read from a unique script?
        ii. What mechanisms does VEED maintain to ensure that any audio submitted for verification purposes is authentic?

4. Does VEED track user attempts to violate its policies prohibiting nonconsensual voice cloning? If so:

    a. How many unique users and unique attempts has VEED detected as being in violation of its policies prohibiting nonconsensual voice cloning, and what actions has it taken against the users responsible?

    b. How many of these users and attempts did VEED detect *before* a nonconsensual voice clone was generated?

    c. How many of these users and attempts did the company detect only *after* a nonconsensual voice clone was generated?

d. What steps, if any, does the company take to adapt its measures to defend against such tactics?

5. Does VEED take specific steps to ensure that the voices of public figures, such as celebrities and politicians, are not created on its platform without authorization? If so, please detail those steps.

    a. Does VEED monitor for instances in which users attempt to clone the voice of a public figure without authorization? If so:
        i. How many user attempts to clone a public figure's voice without authorization has VEED detected?
        ii. How many of those attempts did VEED thwart in real time – in other words, while the user was trying to create the unauthorized voice?

    b. Does VEED monitor user activity to detect when users have succeeded in cloning a public figure's voice without authorization despite the company's prevention efforts? If so:
        i. How many instances of users successfully cloning a public figure's voice without authorization has VEED detected?
        ii. In these instances, does the company track how the user circumvented the company's efforts to detect and prevent the unauthorized cloning of a public figure's voice? What steps, if any, does the company then take to adapt its measures to defend against such tactics?

    c. In VEED's estimation, what is the success rate (percentage) of its real-time efforts to detect and prevent the unauthorized cloning of voices belonging to public figures?

6. Does VEED permit the cloning of a minor's voice? If not, what steps does the company take to prevent such activity? If so, what steps does the company take to ensure that these cloned voices are not misused in harmful or exploitive ways?

    a. To the extent that VEED permits users to generate synthetic children's voices or makes such voices available in its library, how does the company ensure that these are not misused in harmful or exploitative ways?

7. Does VEED have a tool or mechanism in place to detect whether audio was generated by its own products? Is such a tool available to the public?

8. Does VEED watermark or otherwise signal that the content created on its platform is generated from AI? If so:

a. Can the general public detect such a mark or otherwise verify the provenance of content generated by VEED?

b. Can law enforcement detect such a mark or otherwise verify the provenance of content generated by VEED, and does the company provide law enforcement officials more information than the public in this regard? If so, please explain.

9. Does VEED require users to explain their reason or use case for using the company's AI voice cloning tool? If so, please describe these requirements. If not, please explain why not.

10. Does VEED enter into contractual agreements with its customers that designate which party holds liability if the company's product is misused? If so, please describe the nature of these agreements.

Sincerely,

Maggie Hassan

_____

Margaret Wood Hassan
Ranking Member
U.S. Congress Joint Economic Committee

cc: David Schweikert
Chairman, Joint Economic Committee

Eric Schmitt
Vice Chairman, Joint Economic Committee