United States Senate
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
WASHINGTON, DC 20510–6075

May 4, 2023

Mr. Brian Moynihan
Chief Executive Officer
Bank of America
100 North Tryon Street
Charlotte, North Carolina 28255

Dear Mr. Moynihan:

We write to request information regarding your financial institution's use of voice authentication tools. In recent years, financial institutions have promoted voice authentication as a secure tool that makes customer authentication faster and safer. Customers have used voice authentication tools to gain access to their accounts. According to news reports, however, voice authentication may not be foolproof, and they highlight several concerns.[1]

In February, *Vice*[2] detailed how artificial intelligence (AI) generated voice clips can be used to fool financial institutions' voice authentication tools—potentially allowing fraudsters to gain access to accounts. To show the vulnerabilities associated with voice authentication systems, the journalist used a free voice creation service to generate the sound clips needed to easily access a bank account. The AI-generated voice clip fooled the bank's fraud detection system. This was not a one-off. Most recently, on April 28th, the *Wall Street Journal* explained how their reporter used the same voice creation service to fool her bank's credit card voice authentication system.[3] In these two instances, reporters generated their own voice clips. Worryingly, the prevalence of video clips publicly available on Instagram, TikTok, and YouTube have made it easier than ever for bad actors to replicate the voices of other people.[4]

Fraudsters, however, do not need AI-generated tools to trick voice authentication systems. In 2017, a BBC reporter's twin brother successfully mimicked the reporter's voice and fooled a bank's voice authentication system.[5] Despite these breaches, financial institutions continue to market voice authentication as safe and reliable without identifying the risks customers should consider before opting into this service.

---

[1] Vice, *How I Broke Into a Bank Account With an AI-Generated Voice* (February 23, 2023); Cybernews, *How AI voice cloning threatens the security of banking systems* (March 9, 2023); The Guardian, *AI can fool voice recognition used to verify identity by Centrelink and Australian tax office* (March 16, 2023); Wall Street Journal, *I Cloned Myself With AI. She Fooled My Bank and My Family.* (April 28th, 2023)
[2] Vice, *How I Broke Into a Bank Account With an AI-Generated Voice* (February 23, 2023)
[3] Wall Street Journal, *I Cloned Myself With AI. She Fooled My Bank and My Family.* (April 28th, 2023)
[4] CBS News, *Cybercriminals are using AI voice cloning tools to dupe victims* (March 21, 2023)
[5] BBC, *BBC fools HSBC voice recognition security system* (May 19, 2017)

We seek to better understand what measures financial institutions are taking to ensure the security of the voice authentication tools and the steps they are taking to ensure strong data privacy for voice data. Like a fingerprint, face ID, or retinal scan, voice data is among the most intimate types of data that can be collected about a person. Consumers deserve to understand how their voice data is being collected, stored, used, and retained.

In light of the significant risks raised by this technology, we request that you provide responses to the following questions by May 18, 2023:

1. Describe your financial institution's use of voice authentication services for account access purposes. In addition, please provide the following information:

    a. The date your financial institution first began offering this service.

    b. A detailed description of the type of information a customer is able to access once the voice authentication step is cleared.

    c. Are your voice authentication tools proprietary, or are you using third-party tools? If you are using third-party tools, state which tools and which companies provide the tools.

2. Describe how frequently voice authentication tools are assessed and reviewed to ensure they continue to provide a high level of security and privacy in the face of technological advances and emerging threats. Please also describe how your institution is addressing the specific threat of AI to the security of your voice authentication tools.

3. Does your institution use or has it used in the past voice data collected from customers to train or test your voice authentication tools?

4. Describe how your institution responds to breaches of accounts due to flaws in or workarounds of your voice authentication tools.

5. Describe how your institution safeguards consumer/customer voice data. In responding to this question, please provide the following information:

    a. If your institution transmits consumer and/or customer voice data to any third party in order to provide voice authentication services, and if so, which third parties.

    b. The frequency to which your institution collects and stores voice data from customers.

    c. Where customer voice data is stored. Please include details regarding if customer voice data is stored or processed by a foreign company, or stored overseas.

    d. How your institution disposes of hardware that was used to store voice data.

e. How your institution treats customer voice data at the conclusion of their financial relationship with the institution.

Thank you for your prompt attention to this matter. Should you have any questions, please contact Committee staff at (202) 224-7391.

Sincerely,

Sherrod Brown
Chairman