Voices of Uncertainty: The Social Construction of Consumer Perception in Biometric Authentication for Banking

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Drake Ferri
Spring 2025

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor
Kent Wayland, Department of Engineering and Society

Introduction

Calling one's bank no longer means speaking to a human. Increasingly, one's own voice is their password as well as their security. What once felt futuristic has quickly moved towards standard, changing how society interacts with the institutions that manage their money. In recent years, financial institutions have embraced Artificial Intelligence (AI) to enhance the speed, efficiency, and personalization of customer service. A significant development in this area is the use of voice biometric authentication, an AI-driven method that verifies customer identity using unique vocal characteristics. Banks use this technology to streamline access, eliminate passwords, and reduce the need for live customer support. These systems undoubtedly promote convenience and cost-effectiveness while aiming to maintain security, and they are rapidly becoming a core component of digital banking infrastructure.

Leveraging these same technologies, the growing advancement of voice cloning capabilities has created vulnerabilities. With only a few seconds of recorded speech, malicious actors can generate realistic, synthetic voices that may bypass voice authentication systems. This malicious potential threatens to undermine the very trust that voice biometrics aim to build. While banks move quickly to implement these systems, many consumers remain unaware of how their voice data is used, what protections are in place, or how easily these systems can be exploited. This gap between implementation and public understanding carries serious consequences. If consumers lose faith in voice-based systems, they may resist AI-powered customer service altogether, or even their banks, posing risks to adoption, institutional trust, and personal security. At stake is not just the technical reliability of these tools, but the broader relationship between automated systems in the banking industry, and public confidence in banks themselves.

This STS research investigates the role of consumer trust and awareness in the adoption of voice biometric authentication within AI-driven customer service in the banking industry. Specifically, it poses the question: How does consumer trust and awareness shape the usage of voice biometric authentication in banking customer service?

Background and Context

Voice biometric authentication has become an increasingly common feature in the digital banking landscape. Global investments in biometric technologies have grown steadily, with the voice biometrics market projected to reach $15.69 billion by 2032 (Fortune Business Insights, 2024). The technology verifies a user's identity through vocal characteristics such as pitch, cadence, and frequency, and it is often integrated into mobile apps, phone-based customer service systems, and automated assistants (Vielhauer et. al, 2017). Banks promote voice authentication as a way to improve customer convenience and reduce the friction of traditional login procedures, while aiming to maintain or enhance security. These efforts reflect broader goals within the financial industry to cut costs, scale services, and automate human-facing operations (Marr, 2020).

The adoption of voice biometrics, however, cannot be understood purely as a technical advancement. It is embedded in a larger sociotechnical system shaped by the interactions of several actors and institutions. Developers build and refine the voice recognition models that power authentication tools while banks deploy these tools and decide how and when users will interact with them. Consumers navigate the system through daily banking tasks, often without a clear understanding of how their voice data is being collected, stored, or secured (Capgemini, 2022). Regulators attempt to introduce guidelines or policies to manage the risks, although legal

frameworks often lag behind the pace of adoption. Meanwhile, malicious actors exploit the same technologies, specifically the rise of realistic voice cloning, to impersonate individuals and carry out fraud (Verma, 2023).

These components do not exist in isolation, however. Banks rely on public trust to make these systems viable while developers respond to institutional demands and consumer feedback. Consumers, in turn, base their decisions on past experiences with digital systems, as well as their perceived safety of biometric data (ABA, 2023). Fraud events force institutions to adjust their practices, and regulatory responses are often shaped by high-profile failures in the real world. This constant interaction creates a system that evolves in response to technical innovation, public reaction, and institutional pressure.

As voice cloning technology improves, the potential harms of using voice as a biometric become more visible. Unlike passwords, voiceprints cannot be changed if compromised, meanwhile a single audio sample can be enough to generate a convincing imitation, making this form of authentication vulnerable to targeted attacks. Reports of cloned voices used in scams have already emerged, including a case in which attackers used an AI-generated voice to deceive a finance worker in Hong Kong into facilitating a $25 million scam (Chen & Magramo, 2024). These events raise serious concerns about how secure voice biometrics really are, and whether current systems are equipped to handle such threats.

Beyond security risks, the technology also introduces social and ethical concerns. Voice data is not just personal, as it carries information about a speaker's identity, accent, gender, and emotion. These features may affect how well the system recognizes different users, with the potential to introduce bias, especially if the models were trained on narrow datasets (Lyeonov et. al, 2024). Additionally, many users may not fully understand what they are opting into when they

agree to voice-based authentication, especially if the terms are hidden in lengthy privacy policies. Without transparency, users cannot make informed decisions about how their biometric data is used.

However, public perception of these concerns are not consistent throughout. Individuals with minimal digital experiences are more likely to distrust biometric systems or avoid them entirely while others may accept the technology but remain unaware of its risks. The system as a whole reflects and reinforces the need for banks to consider the full range of consumer experiences when designing and deploying voice AI.

Literature

As banks increase their reliance on artificial intelligence to automate services and verify customer identity, trust becomes a central factor in shaping adoption. In AI-driven banking interactions, especially those involving biometric data, trust is heavily influenced by transparency, perceived fairness, and individual understanding of how the technology operates. Araujo et al. (2020) argue that trust in automated decision-making depends on users believing that systems act fairly and predictably. This holds particular importance in banking, where voice biometric authentication is being used in high-stakes contexts involving financial access and sensitive personal data.

Several studies have already documented public skepticism around voice-based AI. For example, some scholars state that consumers express concern about how voice data is collected and whether it can be misused (Hasan et al. 2021). As voice recognition becomes more embedded in banking applications, these concerns are magnified by the rapid improvement of

generative AI. Other scholars further suggest this perceived risk, especially regarding deepfake voices and data security, significantly reduces consumer willingness to interact with voice-based financial services (Hasan et. al, 2023). The FBI has also warned that criminals are increasingly using voice cloning to defeat authentication systems, highlighting the growing real-world risk (FBI, 2024).

Literature on the dual nature of AI as both a tool for fraud prevention and a source of new vulnerabilities adds complexity to these discussions. Some works describe how AI strengthens security infrastructure while simultaneously expanding the surface area for attack. (Lyeonov et. al, 2024). While this duality has been explored from a systems or policy perspective, fewer studies focus on how consumers interpret these risks, or how their awareness of voice data practices shapes their behavior.

At the institutional level, scholars emphasize the need for banks to build trust alongside technological adoption (Biswas et. al, 2021). Others explore the ethical implications of AI-powered decision-making, especially where opacity makes it difficult for users to evaluate how outcomes are produced (Fares et al. 2022). Regulatory-focused work raises concerns about how speech-based technologies adhere with global data protection laws, noting that many banking deployments outpace regulatory review (Peshkova & Zlobina, 2020).

Despite these contributions, there are several gaps in the current literature. Research has yet to fully examine how voice biometric systems affect different consumer groups, particularly in relation to their understanding of how their voices are stored, processed, or potentially cloned. Some works point out that trust in AI varies significantly across demographic lines, but that little work explores how those differences play out in financial contexts (2024). Meanwhile, congressional discussions around AI ethics and human rights have begun to touch on biometric

privacy but often fail to address banking-specific systems in meaningful detail (United States Congress, 2024).

This research builds on existing literature by centering the consumer perspective in a space often shaped by institutional priorities. By examining how trust and awareness interact with the deployment of voice biometric authentication in banking, this work aims to address a gap in understanding how social context shapes the success or failure of AI technologies designed to improve efficiency and security.

Theoretical Framework

While financial institutions frame these technologies as secure and efficient, other social groups interpret their risks and implications differently. According to the Social Construction of Technology (SCOT) framework, technologies are subject to interpretive flexibility, meaning that different stakeholders assign different meanings to the same innovation based on their values, experiences, and goals (Bijker $ Pinch, 1984). Banks and developers may emphasize the innovation's ability to streamline services and reduce costs, while consumers often focus on the potential for misuse, privacy invasion, and fraud. High-profile incidents involving synthetic voice attacks have already demonstrated how easily cloned voices can be used to commit identity theft, reinforcing public skepticism (Verma, 2023).

This difference in perception can have real consequences. Many consumers are unaware that their voice can be replicated with just a few seconds of audio, and banks often fail to communicate how voice data is collected, stored, or protected. FinTech researchers Gozman, Liebenau, and Mangan argue that institutions adopting AI technologies frequently overlook the need to engage and educate users, which contributes to resistance and slows adoption (Gozman

et al, 2018). As a result, public trust becomes a key variable in determining the success or failure of voice authentication systems.

SCOT provides a framework to analyze how these varying perspectives shape the adoption of voice AI in banking. Interpretive flexibility highlights how consumers, developers, financial institutions, and even fraudsters co-construct the meaning and trajectory of this technology, in turn demonstrating how the system around voice biometric authentication in banking continues to evolve in response to emerging risks and public concerns.

Methods

To address the research question of consumer trust and risk awareness regarding voice biometric authentication in banking customer service, I needed to collect evidence from both institutional and public perspectives. This included how financial institutions frame voice authentication as a secure and convenient technology, how consumers perceive and understand these claims, and how real-world incidents and regulatory responses shape the broader context. I also needed examples that illustrate moments when the system either functions as intended or fails, particularly in cases of fraud or public concern, in order to trace how trust and awareness are negotiated over time.

I gathered evidence from four key areas. First, to understand consumer perspectives, I included survey data and industry reports that assess public attitudes toward biometric technologies in banking. Sources such as consumer reports and banking biometrics studies provided insight into consumer trust levels and preferences. Second, I examined how financial institutions and developers frame voice biometrics by analyzing promotional content, blog posts,

and onboarding language from vendors and institutions. These sources reveal how the technology is presented as secure, efficient, and user-friendly.

Next, to identify system vulnerabilities, I incorporated high-profile fraud cases and investigative journalism that document the use of AI-generated voice in financial scams. News reports and articles helped contextualize how voice cloning challenges the assumed security of these systems. Finally, I consulted public discussions of regulation and oversight, including U.S. Government discussions and inquiries as well as policy commentary, in order to assess the role of regulation and institutional accountability.

To analyze the evidence, I organized sources according to the stakeholder group they represented, consumers, banks and developers, regulators, and malicious actors, using the SCOT framework to examine how each group assigns meaning to voice biometric authentication. In particular, I focused on how the technology's role, risks, and value shift across perspectives. To do this, I compared institutional claims of security and convenience with consumer trust concerns and publicized fraud incidents, identifying tensions and disagreements in expectations. This approach allowed me to trace how voice AI adoption is shaped by ongoing negotiations between trust, risk, and social context within the banking sector.

Results

Consumers interacting with voice biometric authentication in banking often express trust in the system, with this confidence largely stemming from the perceived security and convenience of biometrics, as well as trust in the banking institutions offering these services, rather than a detailed understanding of the underlying technology. According to a 2024 survey by Aware, banks were ranked as the most trusted institutions to manage biometric data, with voice

recognition rated positively as long as it was associated with a well-known financial provider (Aware, 2024). Consumers interacting with voice biometric authentication in banking reported their trust was largely due to the perception that biometrics are more secure and convenient than traditional passwords, even though many do not fully understand the underlying technology (Lee, 2017). A 2023 Digital Banking Report by Entrust Cybersecurity Institute further revealed that 72% of respondents were comfortable with banks using biometric technology in their procedures. Throughout these cases, most consumers surveyed were unfamiliar with how the system worked or what the long-term risks of voice data storage might be. Instead of viewing voice biometrics as a complex security tool, users tended to see it as a convenient extension of a brand they already trusted.

This finding is reinforced by earlier studies that show a strong preference for biometrics over traditional passwords in mobile banking environments. In a 2017 report by EyeVerify, 82% of users described voice authentication as faster and more secure than passwords (Lee, 2017). Notably, very few respondents acknowledged the fact that, unlike a password, a voiceprint cannot be changed once compromised. Consumers appeared to equate biometric features with infallibility, often assuming that if a system is presented as modern and efficient, it must also be secure.

Much of this perception appears to be shaped by the way financial institutions and technology providers present voice biometrics. Marketing materials from Illuma, a company that specializes in voice authentication and fraud prevention, describe voice authentication as passive, frictionless, and inherently secure, emphasizing its ability to streamline customer service without requiring PINs, passwords, or repeated logins (Illuma, 2025a). These materials highlight speed and convenience, with unclear references to potential fraud and accuracy issues through

voice cloning. In the case of Illuma, instances of deepfakes and fraud are acknowledged, but are followed by reasons to trust the services rather than being scared off by these previous instances (Illuma, 2025b). In other cases, such as with Chase Bank's description of their voice AI usage, consumers are introduced to the technology as something that is "easier, faster, and more secure" (Chase, 2025). While the technology used throughout these banks may indeed be more secure, there is often little evidence to support such a statement outside of the appeals to credibility. However, the framing of these institutions strongly influences user assumptions, presenting voice biometrics as a closed, reliable system.

Meanwhile, not all companies in the voice biometrics space present the technology in the same way. iProov, a firm that specializes in various forms of biometric identity verification, warns that voice authentication should not be used for onboarding or other high-risk processes, arguing that it lacks the robustness required to stand alone in such situations (iProov, 2023). This contrast suggests that even among developers and institutions, the role and reliability of voice authentication are not fully agreed upon. Technologies are often assumed to be settled once deployed, but in reality, their function and limitations are actively contested as different actors in the system assign different meanings and levels of trust to the same tool (Johnson, 2005). For consumers, encountering inconsistent messages like these can generate confusion and uncertainty, especially when the technology has already been presented as secure and frictionless.

Tensions such as these are further amplified by real-world incidents in which voice authentication systems have failed. In a 2023 investigation by VICE, a journalist demonstrated that a synthetic voice, created using a short audio clip, could successfully bypass a UK bank's biometric security system and access a user's account (Cox, 2023). This case received

widespread attention and marked a shift in how the local public began to perceive voice AI (Cox, 2023). What was previously viewed as a reliable safeguard became, in the eyes of many, a vulnerability. Similarly, in 2025, Reuters reported that criminals had used a cloned voice to impersonate Italy's Minister of Defense, Guido Crosetto, and defraud a former owner of a soccer club, Inter Milan, out of nearly one million euros (Amante, 2025). In this case, the criminals created a deepfake of Crosetto's voice to request financial assistance for kidnapped Italian journalists in the Middle East. In this case, someone who was uneducated on the risks of voice AI and deep fake creation was taken advantage of. Stories like these extend beyond bringing flaws to the forefront, as they reshape how society interprets the technology and its usage.

As public concerns around voice cloning and biometric fraud grew, federal regulators began to take a more direct approach. In 2023, the U.S. Senate Banking Committee initiated inquiries into the use of voice authentication systems at major U.S. banks, including Bank of America. In a letter to the bank's CEO, the Committee cited recent reports of AI-generated voices being used to bypass authentication and requested information about the bank's security protocols, voice data storage practices, and how risks are communicated to consumers (U.S. Senate Banking Committee, 2023). This inquiry did not result in formal regulation but served as an institutional acknowledgment that the risks associated with voice biometrics are significant and growing. If consumers remain unaware of how vulnerable these systems can be, or additionally what happens to their data, then their trust may be based on assumption rather than informed consent.

At the regulatory level, efforts to manage the risks posed by deepfakes remain limited. The United States Senate Committee on AI and Human Rights has addressed the broader implications of generative AI, but has yet to offer specific guidance tailored to biometric voice

authentication in financial systems (United States Senate, 2024). Some scholars have described this regulatory gap as a central challenge in ensuring the safe application of AI tools in finance (Lyeonov et. al, 2024). In the absence of formal guidelines, institutions are left to define their own standards, while consumers may be uncertain about their rights and protections. Across the globe, similar conversations have emerged. In India, rising biometric-related cybercrime prompted calls by regulatory bodies for stronger regulation and clearer consumer protections (Tripathi, 2025). Responses such as these have added another layer to the public narrative, shifting voice biometrics from a space of innovation into one of scrutiny.

Discussion

These findings show that in its current state, consumer trust in voice biometric authentication is largely shaped by how institutions present the technology, rather than by users' understanding of how it works. This trust, while widespread, rests on the authority of banks along with the promise of convenience, with less of an emphasis on informed engagement with the risks. As a result, consumers adopt voice authentication systems assuming they are secure, without questioning how their data is collected, stored, or protected.

Institutional framing plays a central role in reinforcing this assumption. By emphasizing ease of use and leaving out clear discussion of vulnerabilities, banks encourage users to view the technology as safe by default. This narrative discourages deep thinking and positions the technology as a background feature rather than a system requiring consent or oversight. For many consumers, voice biometrics are not evaluated on their merits, but accepted as part of a broader institutional brand.

This dynamic becomes unstable when public failures or contradictory messages challenge the dominant narrative. As soon as users encounter news of deep fake fraud or hear conflicting guidance from different providers, their confidence begins to shift. These moments create uncertainty, not only about the technology's reliability, but about how much they were ever told in the first place. The lack of a consistent message from industry actors makes it difficult for users to know whether they should trust the banking system at all.

While some consumers respond to this uncertainty by becoming more cautious, the lack of regulatory standards increases the clarity issues within the system. Without clear protections or consistent communication, banking institutions set their own policies and consumers are left to navigate an increasingly complex landscape with limited guidance. This weakens the basis for trust and creates uneven experiences, where awareness and skepticism develop only in reaction to failures.

Voice biometric authentication, as a result, remains socially unsettled in the context of banking. It is not only a technical tool, but a system defined by interpretation, contested meaning, and shifting expectations. Whether it succeeds in gaining lasting trust will depend less on its advertised efficiency and more on how institutions engage with consumer concerns, communicate risks, and respond to growing public awareness.

Conclusion

This voice usage in banking reveals how technologies are adopted not just through innovation, but through the narratives that shape public trust. As institutions continue to implement these systems, the gap between technical capacity and user understanding raises important questions about responsibility and informed consent. The stakes extend beyond fraud

prevention or customer experience, reflecting the broader challenge of regulating AI tools that evolve faster than public awareness or policy can keep up.

Looking ahead, this tension will only grow as generative technologies become more accessible and more convincing. Institutions will need to move beyond surface-level certainties and invest in clear communication, meaningful user education, and shared standards. At the same time, researchers and policymakers must work to better understand how trust is built and broken in automated systems. As consumers become more educated on the technologies, a heavier emphasis will be placed on how institutions engage with consumer concerns, communicate risks, and respond to growing public awareness. The success of voice authentication will depend not just on whether it works, but on whether people believe in the systems that use it, and whether those systems deserve that belief.

References

American Bankers Association. (2023, November 3). Consumer survey: Digital banking experience 2023. https://www.aba.com/about-us/press-room/press-releases/consumer-survey-digital-banking-experience-2023

Araujo, T., Helberger, N., & Kruikemeier, S. (2020). In AI we trust? perceptions about automated decision-making by artificial intelligence. *AI & Society, 35*(3), 611-623.

Aware. (2024, October 15). *New consumer report from Aware reveals widespread trust in biometrics*. https://www.aware.com/press-releases/new-consumer-report-from-aware-reveals-widespread-trust-in-biometrics/

Bijker, W. E, & Pinch, T. F. (1984). The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. Social Studies of Science, 14(3), 399–441.

Biswas, S., Carson, B., Chung, V., Singh, S., & Thomas, R. (2021). Building the AI Bank of the Future. *Global Banking Practice, May 2021* https://www.mckinsey.com/~/media/mckinsey/industries/financial services/our insights/building the ai bank of the future/building-the-ai-bank-of-the-future.pdf

Capgemini. (2022). *World Retail Banking Report 2022*. https://www.capgemini.com/wp-content/uploads/2022/05/2022_04_21_World-Retail-Banking-Report_2022-1.pd

Chase. 2025. *Voice ID*. https://www.chase.com/personal/voice-biometrics

Cox, J. (2023, February 23). *How I broke into a bank account with an AI-generated voice*. VICE. https://www.vice.com/en/article/how-i-broke-into-a-bank-account-with-an-ai-generated-voice

Fares, O. H., Butt, I., & Lee, S. H. M. (2022). Utilization of artificial intelligence in the banking sector: a systematic literature review. *Journal of Financial Services Marketing*, 1–18. Advance online publication. https://doi.org/10.1057/s41264-022-00176-7

Federal Bureau of Investigation. (2024, December 3). *Criminals use generative artificial intelligence to facilitate financial fraud*. FBI Internet Crime Complaint Center. https://www.ic3.gov/PSA/2024/PSA241203

Fortune Business Insights. (2025). *Voice biometrics market size, share & trends*. https://www.fortunebusinessinsights.com/industry-reports/voice-biometric-solutions-market-100509

Fortune Business Insights. (2024). *Voice biometrics market size, share & trends*. https://www.fortunebusinessinsights.com/industry-reports/voice-biometric-solutions-market-100509

Gozman, D., Liebenau, J., & Mangan, J. (2018, January 1). The Innovation Mechanisms of Fintech Start-Ups: Insights from SWIFT's Innotribe Competition. *Journal of Management Information Systems*, 35(1), 145 - 179. Retrieved from https://doi.org/10.1080/07421222.2018.1440768

Hasan, R., Rahman, M., & Shams, R. (2021). Consumer trust and perceived risk for voice-controlled artificial intelligence: The case of Siri, Journal of Business Research, Volume 131, Pages 591-597, https://doi.org/10.1016/j.jbusres.2020.12.012.

Hasan, S., Godhuli, E. R., Rahman, M. S., & Mamun, M. A. A. (2023). The adoption of conversational assistants in the banking industry: is the perceived risk a moderator?. *Heliyon*, *9*(9), e20220. https://doi.org/10.1016/j.heliyon.2023.e20220

Illuma. 2025. *Can AI "Deepfake" software impersonate a voice well enough to hack an account?* https://illuma.cx/can-ai-deepfake-software-impersonate-a-voice-well-enough-to-hack-an-account/

Illuma. 2025. *Your quick guide to voice biometrics in banking*. https://illuma.cx/voice-biometrics-banking/

iProov. (2023, August 15). *Voice biometrics for private banking and wealth management: A false sense of security?* https://www.iproov.com/blog/voice-biometrics-false-security

Johnson, D. (2005). Social construction of technology. In C. Mitcham (Ed.), Encyclopedia of Science, Technology, and Ethics (Vol. 4, pp. 1791–1795). Macmillan Reference.

Lee, J. (2017, May 4). *EyeVerify study finds consumers trust biometrics for mobile banking and payments*. Biometric Update. https://www.biometricupdate.com/201705/eyeverify-study-finds-consumers-trust-biometrics-for-mobile-banking-and-payments

Lyeonov, S., Draskovic, V., Kubaščikova, Z., & Fenyves, V. (2024). Artificial Intelligence and Machine Learning in Combating Illegal Financial Operations: Bibliometric Analysis. *Human Technology*, *20*(2), 325–360. https://doi.org/10.14254/1795-6889.2024.20-2.5

Marr, B., Ebook Central - Academic Complete, Ebook Central - College Complete, & O'Reilly Online Learning: Academic/Public Library Edition (2019). *Artificial Intelligence in Practice: How 50 Successful Companies Used Artificial Intelligence to Solve Problems*. Hoboken: Wiley.

Narang, Ashima & Vashisht, Priyanka & Bhaskar, Shalini. (2024). Artificial Intelligence in Banking and Finance. International Journal of Innovative Research in Computer Science and Technology. 12. 130-134. doi: 10.55524/ijircst.2024.12.2.23.

Peshkova, G. Y., & Zlobina, O. V. (2020). Digital Transformation Of Banking With Speech Technologies. In I. V. Kovalev, A. A. Voroshilova, G. Herwig, U. Umbetov, A. S.

Budagov, & Y. Y. Bocharova (Eds.), Economic and Social Trends for Sustainability of Modern Society (ICEST 2020), vol 90. European Proceedings of Social and Behavioural Sciences (pp. 294-303). European Publisher.https://doi.org/10.15405/epsbs.2020.10.03.34

Tripathi, A. (2025, January 7). *Biometric frauds in banks: Generative AI new weapon*. Times of India. https://timesofindia.indiatimes.com/blogs/techtonic/biometric-frauds-in-banks-generative-ai-new-weapon/

United States Congress Senate Committee on the Judiciary Subcommittee on Human Rights and the Law, & United States Congress Senate (2024). Artificial Intelligence and Human Rights: Hearing Before the Subcommittee on Human Rights and the Law of the Committee on the Judiciary, United States Senate, One Hundred Eighteenth Congress, First Session, June 13, 2023. Washington: U.S. Government Publishing Office.

United States Senate Committee on Banking, Housing, and Urban Affairs. (2023, May 4). *Letter to Bank of America regarding voice authentication systems*. https://www.banking.senate.gov/imo/media/doc/bank_of_america_voice_authentication_letter2.pdf

Verma, P. (2023, April 24). *AI-generated voices are being used to trick people and steal*. *The Washington Post*. https://www.washingtonpost.com/technology/interactive/2023/ai-voice-generators/

Vielhauer, C., & Knovel, A., S. E. (2017). *User-centric Privacy and Security in Biometrics*. London, United Kingdom: The Institution of Engineering and Technology.