

The New York Times

Business/Financial Desk; SECTB

A.I. Copies Your Voice, Then Calls Up Your Bank

By Emily Flitter and Stacy Cowley
1,467 words
1 September 2023
The New York Times
NYTF
Late Edition - Final
1
English

This spring, Clive Kabatznik, an investor in Florida, called his local Bank of America representative to discuss a big money transfer he was planning to make. Then he called again.

Except the second phone call wasn't from Mr. Kabatznik. Rather, a software program had artificially generated his voice and tried to trick the banker into moving the money elsewhere.

Mr. Kabatznik and his banker were the targets of a cutting-edge scam attempt that has grabbed the attention of **cybersecurity** experts: the use of artificial intelligence to generate voice deepfakes, or vocal renditions that mimic real people's voices.

The problem is still new enough that there is no comprehensive accounting of how often it happens. But one expert whose company, Pindrop, monitors the audio traffic for many of the largest U.S. banks said he had seen a jump in its prevalence this year -- and in the sophistication of scammers' voice fraud attempts. Another large voice authentication vendor, Nuance, saw its first successful deepfake attack on a financial services client late last year.

In Mr. Kabatznik's case, the fraud was detectable. But the speed of technological development, the falling costs of generative artificial intelligence programs and the wide availability of recordings of people's voices on the internet have created the perfect conditions for voice-related A.I. scams.

Customer data like bank account details that have been stolen by hackers -- and are widely available on underground markets -- help scammers pull off these attacks. They become even easier with wealthy clients, whose public appearances, including speeches, are often widely available on the internet. Finding audio samples for everyday customers can also be as easy as conducting an online search -- say, on social media apps like TikTok and Instagram -- for the name of someone whose bank account information the scammers already have.

"There's a lot of audio content out there," said Vijay Balasubramaniyan, the chief executive and a founder of Pindrop, which reviews automatic voice-verification systems for eight of the 10 largest U.S. lenders.

Over the past decade, Pindrop has reviewed recordings of more than five billion calls coming into call centers run by the financial companies it serves. The centers handle products like bank accounts, credit cards and other services offered by big retail banks. All of the call centers receive calls from fraudsters, typically ranging from 1,000 to 10,000 a year. It's common for 20 calls to come in from fraudsters each week, Mr. Balasubramaniyan said.

So far, fake voices created by computer programs account for only "a handful" of these calls, he said -- and they've begun to happen only within the past year.

Most of the fake voice attacks that Pindrop has seen have come into credit card service call centers, where human representatives deal with customers needing help with their cards.

Mr. Balasubramaniyan played a reporter an anonymized recording of one such call that took place in March. Although a very rudimentary example -- the voice in this case sounds robotic, more like an e-reader than a person -- the call illustrates how scams could occur as A.I. makes it easier to imitate human voices.

A banker can be heard greeting the customer. Then the voice, similar to an automated one, says, "My card was declined."

"May I ask whom I have the pleasure of speaking with?" the banker replies.

"My card was declined," the voice says again.

The banker asks for the customer's name again. A silence ensues, during which the faint sound of keystrokes can be heard. According to Mr. Balasubramaniyan, the number of keystrokes correspond to the number of letters in the customer's name. The fraudster is typing words into a program that then reads them.

In this instance, the caller's synthetic speech led the employee to transfer the call to a different department and flag it as potentially fraudulent, Mr. Balasubramaniyan said.

Calls like the one he shared, which use type-to-text **technology**, are some of the easiest attacks to defend against: Call centers can use screening software to pick up technical clues that speech is machine-generated.

"Synthetic speech leaves artifacts behind, and a lot of anti-spoofing algorithms key off those artifacts," said Peter Soufleris, the chief executive of IngenID, a voice biometrics **technology** vendor.

But, as with many security measures, it's an arms race between attackers and defenders -- and one that has recently evolved. A scammer can now simply speak into a microphone or type in a prompt and have that speech very quickly translated into the target's voice.

Mr. Balasubramaniyan noted that one generative A.I. system, Microsoft's VALL-E, could create a voice deepfake that said whatever a user wished using just three seconds of sampled audio.

On "60 Minutes" in May, Rachel Tobac, a security consultant, used software to so convincingly clone the voice of Sharyn Alfonsi, one of the program's correspondents, that she fooled a "60 Minutes" employee into giving her Ms. Alfonsi's passport number.

The attack took only five minutes to put together, said Ms. Tobac, the chief executive of SocialProof Security. The tool she used became available for purchase in January.

While scary deepfake demos are a staple of security conferences, real-life attacks are still extremely rare, said Brett Beranek, the general manager of security and biometrics at Nuance, a voice **technology** vendor that Microsoft acquired in 2021. The only successful breach of a Nuance customer, in October, took the attacker more than a dozen attempts to pull off.

Mr. Beranek's biggest concern is not attacks on call centers or automated systems, like the voice biometrics systems that many banks have deployed. He worries about the scams where a caller reaches an individual directly.

"I had a conversation just earlier this week with one of our customers," he said. "They were saying, hey, Brett, it's great that we have our contact center secured -- but what if somebody just calls our C.E.O. directly on their cellphone and pretends to be somebody else?"

That's what happened in Mr. Kabatznik's case. According to the banker's description, he appeared to be trying to get her to transfer money to a new location, but the voice was repetitive, talking over her and using garbled phrases. The banker hung up.

"It was like I was talking to her, but it made no sense," Mr. Kabatznik said she had told him. (A Bank of America spokesman declined to make the banker available for an interview.)

After two more calls like that came through in quick succession, the banker reported the matter to Bank of America's security team, Mr. Kabatznik said. Concerned about the security of Mr. Kabatznik's account, she stopped responding to his calls and emails -- even the ones that were coming from the real Mr. Kabatznik. It took about 10 days for the two of them to re-establish a connection, when Mr. Kabatznik arranged to visit her at her office.

"We regularly train our team to identify and recognize scams and help our clients avoid them," said William Halldin, a Bank of America spokesman. He said he could not comment on specific customers or their experiences.

Though the attacks are getting more sophisticated, they stem from a basic **cybersecurity** threat that has been around for decades: a data breach that reveals the personal information of bank customers. From 2020 to 2022, bits of personal data on more than 300 million people fell into the hands of hackers, leading to $8.8 billion in losses, according to the Federal Trade Commission.

Once they've harvested a batch of numbers, hackers sift through the information and match it to real people. Those who steal the information are almost never the same people who end up with it. Instead, the thieves put it up for sale. Specialists can use any one of a handful of easily accessible programs to spoof target customers' phone numbers -- which is what likely happened in Mr. Kabatznik's case.

Recordings of his voice are easy to find. On the internet there are videos of him speaking at a conference and participating in a fund-raiser.

"I think it's pretty scary," Mr. Kabatznik said. "The problem is, I don't know what you do about it. Do you just go underground and disappear?"

Audio produced by Tally Abecassis.

Audio produced by Tally Abecassis.

Vijay Balasubramaniyan leads Pindrop, a voice-verification tech company. He said voice deepfakes so far account for only "a handful" of fraudulent calls. (PHOTOGRAPH BY DUSTIN CHAMBERS FOR THE NEW YORK TIMES) (B5) This article appeared in print on page B1, B5.

Document NYTF000020230901ej9100032

THE WALL STREET JOURNAL.

Merrill Lynch Penalized

By Mengqi Sun
267 words
12 July 2023
The Wall Street Journal
J
B2
English

Broker-dealer Merrill Lynch has agreed to pay a total of $12 million in fines to regulators for failing to file about 1,500 suspicious-activity reports over more than a decade.

Under U.S. **anti**-**money**-**laundering** rules, broker-dealers like Merrill Lynch are required to file suspicious-activity reports to the Financial Crimes Enforcement Network on transactions above $5,000 when they might signal criminal activities, such as tax evasion, to assist U.S. government agencies in detecting and preventing money laundering.

Merrill Lynch's parent company, which was implementing the broker-dealer's **anti**-**money**-**laundering** program following Bank of America's acquisition of Merrill during the 2008-09 financial crisis, used a $25,000 threshold, instead of the $5,000 one, for reporting SARs between 2009 and late 2019, the Securities and Exchange Commission said Tuesday.

Merrill agreed to pay $6 million to settle the SEC charges.

In a parallel enforcement action, the Financial Industry Regulatory Authority, the brokerage industry's self-regulator, fined Merrill an additional $6 million for longstanding **anti**-**money**-**laundering** program failures, the regulator said Tuesday. Finra alleged Merrill failed to apply the right threshold for SARs reporting for more than 10 years and failed to file nearly 1,500 SARs to regulators.

"Following an internal review, we reported this matter to regulators and have enhanced our process and training regarding these filings," a spokeswoman for Merrill Lynch said in an email.

Broker-dealers' compliance with filing SARs has been one of the top priorities for examinations by the SEC and Finra in recent years.

Document J000000020230712ej7c0001t

Search Summary

Text	(technology OR "AI" OR fintech OR "digital banking" OR "cloud computing" OR blockchain OR cybersecurity OR "machine learning" OR "data analytics" OR "big data" OR "predictive analytics" OR "cloud migration" OR "edge computing" OR "5G banking" OR "API banking" OR "open banking" OR "data governance" OR "data monetization" OR "digital transformation" OR "quantum computing" OR "AI-driven banking" OR "AI in compliance" OR "AI-powered fraud detection" OR "AI in customer service" OR "AI in investment banking" OR "conversational AI" OR "generative AI" OR "robo-advisors" OR "natural language processing" OR "algorithmic trading" OR "automated risk assessment" OR "AI regulatory challenges" OR "embedded finance" OR neobanks OR "Banking as a Service" OR "BaaS" OR regtech OR suptech OR "decentralized finance" OR DeFi OR "cryptocurrency adoption" OR "Central Bank Digital Currencies" OR CBDCs OR tokenization OR "real-time payments" OR "Buy Now Pay Later" OR BNPL OR "cyber resilience" OR "Zero Trust security" OR "identity verification" OR "fraud detection" OR "insider threats" OR "AI-driven cybersecurity" OR "financial data breaches" OR "data privacy laws" OR GDPR OR CCPA OR "operational risk management" OR "regulatory compliance technology" OR KYC OR "Know Your Customer" OR AML OR "Anti-Money Laundering" OR "hyper-personalization in banking" OR "customer-centric banking" OR "omnichannel banking" OR "digital wallets" OR "contactless payments" OR "voice banking" OR "biometric authentication" OR "wearable banking" OR "banking UX/UI innovations" OR "financial inclusion technology")
Date	07/01/2023 to 09/30/2023

Source	The New York Times Or The Wall Street Journal Or The Economist Or Forbes
Author	All Authors
Company	Bank of America Corporation
Subject	All Subjects
Industry	All Industries
Region	All Regions
Language	English
Results Found	2
Timestamp	7 March 2025 4:39 AM GMT

