SESSION ID: AFD-W01

Look Who’s Talking: How Fraudsters Steal Voices and Make Billions

Vijay A. Balasubramaniyan
Co-Founder & CEO
Pindrop
@pindrop
MARKET FORCES ALTERING STRATEGIES

Multigenerational Customers
Different preferences
Different use of technology
Different expectation on CX

Voice as a Channel
More usage of Voice
Creation of new voice devices
Phone channel is still most preferred

CX Becomes Strategic
– Business will compete on CX over product and price
– CX will start to impact revenue and loyalty
– Customers will churn based on 3 or fewer poor experiences
SERVING FIVE GENERATIONS OF CUSTOMERS

- Calls - 48%, Email - 24%
- 57% of baby boomers and Gen Z prefer calls
- 55% believe calls solve problem quickest
VOICE IS PERSUASIVE

70% Have used a voice assistant

40% Have tried voice commerce

49% refers phone channel
CUSTOMER EXPERIENCE IS STRATEGIC

1. Now Strategic Imperative
2. Causes Churn Quickly
3. 20% Revenue Impact
4. Personalization vs. Speed
FRAUD CONTINUES TO ESCALATE AND EVOLVE

- Phone Fraud is Increasing
- Data breaches fuel Account takeover
- Synthetic Identity becomes the fastest growing financial crime in the US
- Deepfake audio and video starting to impact enterprises
- ....and on and on
Web & Mobile
Multiple layers of security between client’s device and browser to on premise equipment.

Call Center
Anti-fraud and authentication reliant on what callers know (single factor detection).
COST OF VOICE FRAUD TODAY

- **Fraud Loss**: $14B Annual loss caused by fraud
- **Reputation Risk**: 41% Consumers blame the brand for fraud happening
- **High Operations Cost**: $1M Annual expense from 1 second
- **Poor Customer Experience**: 30% of callers unable to authenticate due to KBA
The Rise of Deepfake Content

AI-Manipulated Audio & Video

Deepfakes first entered the public eye late 2017, when an anonymous Redditor under the name "deepfakes" began uploading videos of celebrities into adult content using a tool to insert faces into footage frame by frame.

Today, advances in artificial intelligence and neural networks can produce audio and visuals with quality that begins to rival that of human perception.
The Federal Trade Commission thinks a 5 billion dollar fine is going to stop us from violating people's privacy. Suckers.
ATTACKS - THREAT TO THE PRIVATE SECTOR

August 30th, 2019: Criminals used AI-based software to impersonate a chief executive’s voice and demand a fraudulent transfer of €220,000 ($243,000). The CEO of a U.K.-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm’s German parent company, who asked him to send the funds to a Hungarian supplier.

July 19th, 2019: BBC reported on three successful audio attacks on private companies. In each, a company's "CEO" called a senior financial officer to request an urgent money transfer. Millions of dollars were stolen from each company, whose names were not revealed.

June 11th, 2019: A fake video of Mark Zuckerberg giving a sinister speech about the power of Facebook has been posted to Instagram. The company previously said it would not remove this type of video.
FAKE PRESIDENT FRAUD

Someone purporting to be a senior officer of the company, typically the COO, CFO or Chief Executive

Win the confidence of the target

Publicly Available Data

- Company Website
- Social Media

Private Data (Intranet)

- Data Breach
- Physical Access
- Email Compromise
- Audio (e.g. meetings)

Someone in the accounts department with responsibility for making payments
HUMAN VS. MACHINE SURVEY

57% Detection Accuracy
CURRENT SOLUTIONS: SYNTHETIC SPEECH DETECTION

Speech Synthesis from Lyrebird

Detection of Wavenet and Tacotron 2

Custom Speech Synthesis Engine

Trained on various voice spoofing attacks including most recent Deepfake attacks

Among Top performing systems at ASVspoof 2019
NEW BINARY CLASSIFIER FOR SYTHETIC SPEECH