AI for Financial Institutions

The Next Frontier in CX and Personalization

pindrop

TABLE OF CONTENTS

INTRODUCTION 3

APPLICATIONS OF AI 5

USING AI FOR CX AND SECURITY 7

WHAT IS YOUR AI CAPABLE OF? 16

THE TAKEAWAY: BET BIG ON AI 19

Customer Service is More Than a Buzzword.

It is the Cornerstone of an Organization's Customer Experience (CX) Strategy.

And the Contact Center Plays a Pivotal Role in This Strategy.

The challenge for modern contact center decision makers is to balance the need for outstanding CX with robust security. Artificial Intelligence (AI) holds the key to this balance. AI can provide the edge contact centers need to turn good customer experiences into great ones and to minimize the security threats across different customer touchpoints.

Banks and financial institutions in particular face this challenge more acutely. They need to protect trillions of dollars[1] entrusted to them while simultaneously searching for innovative ways to retain and attract customers.

To exacerbate this challenge, the year 2020 has brought about many changes in the way banks and financial institutions operate. Increased unemployment, government programs, incentive payouts, and loan applications have caused a spike in customer activity.

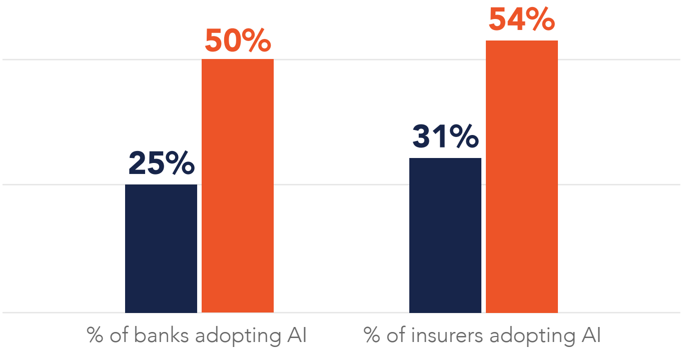
Banks have had to fundamentally alter their business practices as their customers have begun to prefer contactless methods of communication including increased self service tools and digital channels[2]. This, unfortunately, has also opened the door for fraudsters. AI is an integral piece of the puzzle that can help expedite the transition towards these self-serve customer interaction and protection models in a cost effective way.

1) F. Norrestad, Statista,Total assets of global financial institutions from 2002 to 2019, Feb 8, 2021
2) Pindrop Voice Intelligence and Security Report, 2021

AI IN BANKS TODAY

Banks and contact centers across the world are familiar with AI and are planning to expand its adoption.

GROWTH OF AI IN BANKS AND INSURANCE COMPANIES[1]



AI models are adapted in multiple ways to serve different banking environments ranging from simple rules-based process automation to more complex deep neural networks that process large and complex datasets to make probabilistic predictions.

The adoption curve of AI within the banking environment varies from function to function. Customer facing and revenue enhancing operations are the most dominant consumers of AI and their adoption of machine learning continues to gain momentum. The focus on risk management for AI has increased including applications such as fraud detection, money laundering and threat detection. Various back office and infrastructure operations use AI on a selective basis.

Banks are deploying AI for several initiatives to increase employee productivity, training and workflow optimization.

- **AI handles common queries via chatbot so that agents have more time to devote to more complex issues.**
- **AI-driven intent and emotion analysis helps agents to notice subtle signs that a customer is getting frustrated and suggest remedial actions.**
- **AI-powered tools enable better customer interaction coaching and performance improvement.**

Chart created by Pindrop based on Gartner research. Source: Gartner, Financial Services CIOs Must Focus AI Investments on 'Responsible AI' in 2021, 5 January 2021

APPLICATIONS OF AI

ROBOTIC PROCESS AUTOMATION

AI for cost effective automation of manual processes and workflows. Used for workforce optimization, back office processes, reporting

FRAUD DETECTION

AI for analyzing large and complex data sets to create probabilistic models that identify risk and predict fraudulent behavior

USER AUTHENTICATION

AI for enrollment and authentication of trusted users through analysis of multiple factors like voice, device, behavior, speech, risk

SPEECH ANALYTICS

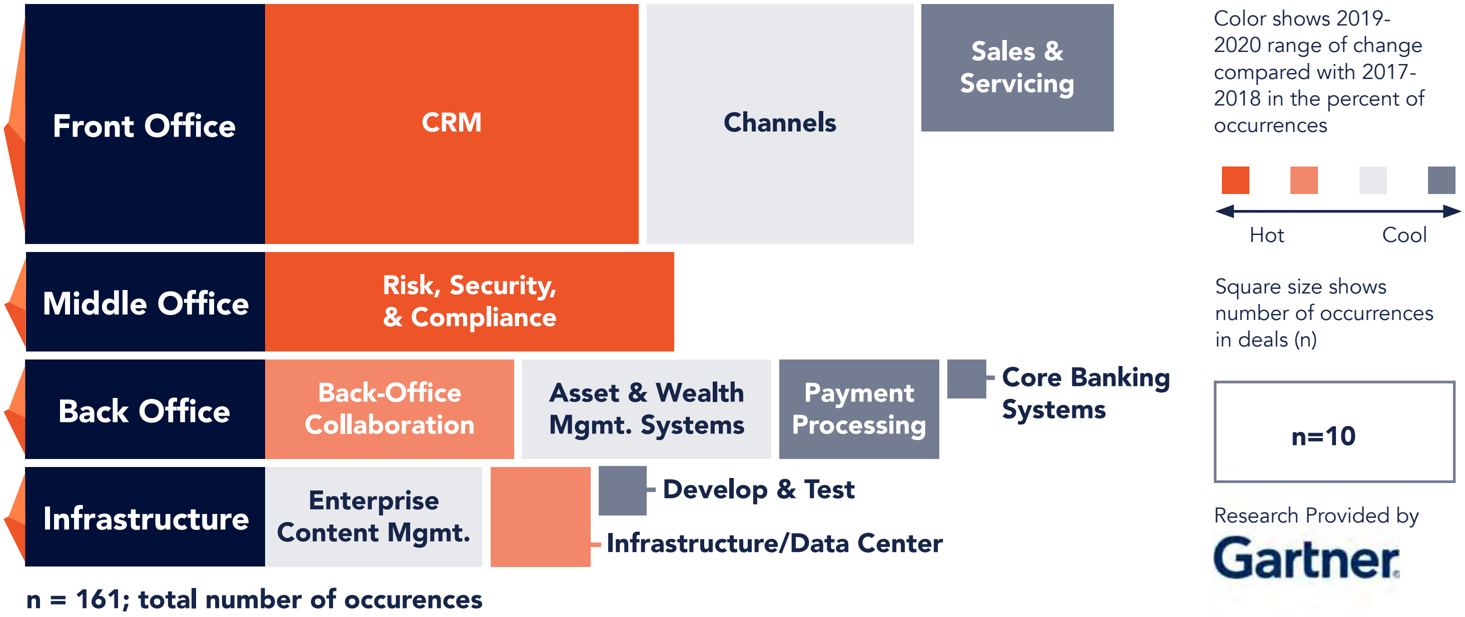
AI for advanced speech, natural language and intent recognition. Used for customer service and insights, regulatory compliance, KYC

INTELLIGENT ASSISTANTS

AI for performance of specific tasks including voice, keywords, or intent. Used for voice assisted banking, omni-channel engagement

The adoption curve of AI within the banking environment varies from function to function. Customer facing and revenue enhancing operations are the most dominant consumers of AI and their adoption of machine learning continues to gain momentum. AI has gained increased penetration in risk management functions of fraud detection, money laundering and threat detection. Various back office and infrastructure operations use AI on a selective basis.

AI ADOPTION BY FUNCTIONAL AREA



Research Provided by Gartner

Source: Gartner, Artificial Intelligence Heat Map for Banking and Investment Services, 2021, 22 January 2021

WHY IS AI SO IMPORTANT FOR BANKS?

It cannot be overstated how critical CX is for banks, both from a revenue growth and customer churn perspective.

1% Improvement in CX could increase revenue by

$110M ↑

While only

18%

of customers will continue association with a brand after it has dissapointed them.

For banks and their contact center decision makers, the challenge is to consistently outperform these CX expectations while building and maintaining a healthy brand differentiation over competition. On the flip side, security and risk professionals need to ensure that these interactions are secure and trustworthy and do not expose the organization to data breaches and fraud risks. AI has proven to be an asset in this regard. AI has not only helped banks save money through automation of processes but has also fundamentally improved customer service which has resulted in new, previously unrealized opportunities such as omni-channel customer experience and service personalization.

According to Gartner Research[3], the three top business drivers for buying AI are

Improving Customer Service/Experience

Reducing Costs

Improving Risk Management

1) Forrester Research - "How Customer Experience Drives Business Growth, 2020"
2) Forrester Research - "Transform The Contact Center For Customer Service Excellence, 2021"
3) Gartner, Artificial Intelligence Heat Map for Banking and Investment Services, 2021, 22 January 2021

How can banks use AI to achieve better CX?

There are three important questions to answer in order to have a successful AI strategy

What specific outcomes do banks want to achieve with AI?

What are the technology, process and business considerations towards implementing and operationalizing AI?

What are the best practices for long term success?

SPECIFIC OUTCOMES

AI for Better CX

During and after the pandemic, consumers have increasingly started to rely on phone and online channels for service. Pindrop Research[1] has found an increase in call volumes as well as in call durations as customers have sought to reduce physical touchpoints. The transition to digital interactions has not been a zero sum game either. The total volume of interactions, be it through phone channel or online means has increased, which means banks now have to connect the dots between various channels as part of an asynchronous customer journey. Personalizing this customer experience journey and authenticating the customers quickly and in a protected fashion are two of the more significant challenges facing banks today.

Reduced Athentication Time

Industry experts advise that a vital ingredient of superior CX is how quickly the agent can answer the caller's specific question. Time spent identifying the caller without getting closer to resolution chips away at the CX. By validating the incoming Caller ID / phone number based on machine learning models, banks can improve this process. These validated callers can be authorized to perform low risk activities in the IVR and self serve channels (balance inquiry, service status check) without subjecting them to extensive authentication and ID&V processes. The speed of authentication results in higher customer satisfaction and lower ID&V costs. Recent case study[2] at a large North American telecom provider demonstrated a reduction of 25 seconds in average call handle time and growth in customer satisfaction due to 75% incoming call verification rate and 2% increase in IVR call containment.

Enrollment Protection

With a combination of high scale machine learning and deep neural networks, banks can fine tune the accuracy of authentication processes to ensure a high level of confidence in their authenticated customers. The key is to check the level of risk during authentication. AI models trained with risk engines and advanced risk modeling can predict with a degree of certainty that the call or user can be safely enrolled for the purposes of future authentication. Thus banks can continue to trust their authenticated customers while reducing reliance on expensive knowledge based or multiple step authentication processes. Pindrop studies have shown that enrollment protection can reduce the likelihood of enrolling a fraudster by over 600% compared to traditional KBAs[3].

1) Pindrop - *"Voice Intelligence and Security Report, 2021"*
2) Aite - *"Next Caller Improves Customer Service in Contact Centers via Spoofing Detection, 2020"*
2) *Pindrop Research Labs*

Multi-Factor Authentication

Banks today face a complex and ever-evolving security landscape. Threats could come in various forms - synthetic voices, spoofed caller IDs, social engineering. Relying solely on a single form of authentication, be it traditional KBAs, OTP or identity checks, leaves the organization vulnerable to threats from other unforeseen vectors. To avoid this and to ensure that only the genuine customers are authenticated, banks need to leverage multiple factors (voice, behavior, carrier signature, caller ID, device intelligence) to authenticate users. AI plays a crucial role in combining valuable intelligence from multiple sources into an easily digestible authentication and risk score that can be used confidently for smooth customer experience.

More Self-Serve Capability

AI driven authentication can encourage banks to trust their customers and the protection of their authentication process, which in turn can divert their customer interactions to cost effective self-serve formats such as the IVR, apps, online portals. Pindrop sees approximately 3-5% increase in IVR call containment across financial institutions due to machine learning and multifactor authentication process.

User Personalization

An important benefit of AI is that it gives banks an ability to leverage multiple data sources to identify the risk level associated with each interaction. Combining low risk level with knowledge of past behaviors and preferences, the banks can provide a more personalized self-serve menu to those users which could contribute to enhanced CX.

Agent Satisfaction & Productivity

Due to the COVID-19 pandemic banks have had to reorganize their call center operations. A recent Forrester Consulting study commissioned by Pindrop[1] found that 66% of financial institutions had to shift half or more agents to remote operations and would continue to do so in the near future. These changes along with increased call volumes and call durations have put a strain on call center agent workflows. AI driven authentication processes can reduce call handle times and help route call flows better resulting in improved agent productivity.

AI plays a crucial role in combining valuable intelligence from multiple sources into an easily digestible authentication and risk score that can be used confidently for smooth customer experience.

[1] *Forrester Opportunity Snapshot - "Reducing IVR Fraud Through Advanced Account Risk Capabilities, 2020", a commissioned study conducted by Forrester Consulting on behalf of Pindrop*

SPECIFIC OUTCOMES

AI for Better Protection

Banks have to continuously upgrade their security arsenal to help stop an ever expanding network of sophisticated fraudsters. In addition they need to be proactive in protecting against data breaches, detecting security threats and protect against money laundering. These challenges are further complicated by the exposure to risk from various channels across different locations. However while strengthening their defenses to fight fraud, banks can not lose the sight of customer experience. They still need to ensure that the barriers they are erecting to keep fraudsters at bay, do not end up obstructing and alienating their genuine customers. In other words, balancing nimble CX with robust protection is a balancing act. AI is a crucial lever that can help address this balance. According to Gartner, "improving risk management" is one of the top three business drivers for AI[1]. Banks could improve their AI strategy with the following outcomes:

Smarter Fraud Detection

Traditional fraud detection approaches require a high degree of effort, sifting through a multitude of cases and wasted time and resources that could be better utilized serving customers and growing revenue. Customer service agents get tasked with figuring out whether a caller is fraudulent; a task which they are neither suited for nor required to do. AI helps solve these problems. Machine learning and DNN based models are trained on vast and varied datasets that could identify high risk activities which could lead to fraud. These models are continuously trained based on actual fraud feedback to further increase their prediction accuracy. Over time AI trained models turn out more accurate predictions of fraud which means banks can get better at prioritizing high risk call populations vs low risk ones based on exposure levels. This can enable banks to redirect maximum effort to the highest risk/ high exposure activities, thus maximizing not only effectiveness at stopping fraud but also to free up organization capacity towards revenue generating activities.

Improved Effectiveness of Fraud Investigators

Banks with large and sophisticated fraud investigation teams can benefit immensely from using AI fraud detection tools. Pindrop research[2] shows that a large majority of calls are either genuine or present only moderate risk. Most fraud is concentrated within a few high risk calls limited to 2% of the call volume; the proverbial "needle in the haystack". AI predictive models can help find the needle which helps to focus the fraud team's effort and time for maximum impact.

1) Gartner, Artificial Intelligence Heat Map for Banking and Investment Services, 2021, 22 January 2021
2) Pindrop - "Voice Intelligence and Security Report, 2021"

Unburdened CSRs

Smaller banks that do not have dedicated fraud investigation resources sometimes need to rely on their customer service reps / agents to flag an ongoing call as high risk depending on blacklists or preset business rule violations. However, detecting fraud is not their responsibility. CSRs are trained to help customers and solve problems. AI based fraud detection can take over the burden of real time fraud monitoring from the agents and allow them to focus on serving customers.

Most fraud is concentrated within 2% of the call volume. AI predictive models can find the "needle in the haystack" helping to focus the fraud team's effort and time for maximum impact.

Predictive Fraud Alerting

Fraudster tool kits are constantly growing. For example, due to the Equifax and Facebook data breaches fraudsters have a lot of data about millions of consumers. In combination with caller ID spoofing, voice synthesis, deepfake and robotic dialing technologies, fraudsters can now leverage that data on a large scale. Self-serve surfaces such as IVRs provide grounds for fraudsters to test out these data mining exercises and to conduct deep account reconnaissance which could go unmonitored. Once they reach the agent the fraudsters have already gained enough intel to present themselves as a genuine customer and to take over their accounts. AI can alert the organization to these surveillance and reconnaissance attempts before they are lost. AI can alert the organization to these surveillance and reconnaissance attempts before they are lost. Pindrop Research demonstrates that by monitoring suspicious activity in the IVR and by matching these alerts to the related accounts, organizations can predict fraud several weeks in advance and help ensure the vulnerable accounts are protected.[1]

[1]) Pindrop Research Labs - IVR Fraud Case Study"

CONSIDERATIONS

The successful deployment and operationalization of AI, like any other technology, is predicated on several questions such as:

> **How can I make it work?**
>
> **What are the costs and tradeoffs?**
>
> **What pitfalls do I need to avoid?**
>
> **How will AI fit in my infrastructure, processes and workflow?**

Answering these questions is crucial in order to derive the most benefit from AI. Following are some considerations to keep in mind to leverage AI for CX and protection.

Big Data

AI, in particular machine learning and deep learning, require a certain level of data engineering resources and effort for mining data across large and diverse datasets The efficacy and accuracy of AI predictions is directly dependent on how richly the data models have been trained.

Reinforcement Learning

The consistent accuracy of AI depends on fraud and authentication feedback data provided back to the AI for tuning of the prediction models.

Memorization vs. Generalization

It is important that the machine learning model trains well on "seen" data and conditions. But that might result in the system memorizing the training data, and possibly failing on the "unseen" data test where the distribution is different from the training data.

Machine Bias

Organizations need to avoid bias in AI particularly in terms of protected categories such as race, ethnicity, language, age, gender, etc.

Domain Adaptation

Supervised and unsupervised models need to be utilized for training of datasets. The former requires labeled data and the latter does not. The reason unsupervised learning is needed is due to the lack of consistent availability of labels.

Score Calibration

The risk scores and authentication scores provided by AI need to be operationalized according to the needs and workflows of the organization. Depending upon what the scores indicate, the workflow needs to be able to respond with follow up action (either allow the interaction to go ahead, step-up authentication, or to redirect the call to the fraud team).

> **Fairness in AI/ML is critical. In the long term any bias embedded in the model gradually starts eroding the accuracy of predictions.**

Anomaly Detection

Fraud is a hard problem because of the imbalanced nature of the training data where the fraud is a minority compared to genuine cases. So special attention needs to be given to effectively train and validate fraud models.

Reduced Computational Complexity

The architecture and the size of the machine learning model should be chosen in a way to meet requirements agreed upon in terms of time real-time constraints, memory footprint and CPU usage.

BEST PRACTICES

Following are some recommendations to extract the most value from AI.

1

All AI models are not the same. Different AI models specialize in various functions such as speech recognition, voice biometrics, intent recognition, fraud detection etc. The more closely the AI model resembles your business, regulatory and operational environment, the better its performance. **Therefore selecting an AI model that is purpose built and optimized for the financial industry is highly recommended.**

2

The ability of AI to deliver accurate results, over a period of time is directly correlated with the amount of time and data used in training of the AI models. The models could be trained using data from publicly available datasets, internal data collection efforts, from crowdsourced datasets and other data sources from live use cases. **In addition, the models need to be tuned with constant feedback and optimized for newer use cases.** The best practice is to either have a dedicated data engineering team or to leverage a specialist AI focused vendor that is knowledgeable about the banking industry and its regulatory environment.

3

Fairness in AI/ML is critical. Various biases such as race, gender, language, age etc. enter the AI model through corrupt data practices as well as from the way the solutions are built. In the long term any bias embedded in the model gradually starts eroding the accuracy of predictions. Even worse, any bias in the bank's decisions arising out of AI predictions could pose regulatory and legal challenges. But there are ways to address the builders' biases and help protect the solution from the input of "bad" data. Diverse and fact-based inputs which are derived from sampling of wide population groups are required to address selection biases and ensure that few, isolated factors do not influence decisions. By combining varied voices, thought processes, and capabilities from diverse groups of developers, an AI could be created with such diverse and varied inputs, that it learns to operate outside of the conflicting biases of its makers.

4

Leverage both supervised vs unsupervised learning. Having true and accurate labels for training of the data models is typically costly and impractical. Therefore, it is important that the **machine learning tools are able to learn from unlabeled data.** Therefore techniques like unsupervised clustering, domain adaptation and transfer learning are needed in practice to maximize the performance of real-world systems.

5

As banks become smarter, fraudsters also continue to bolster their arsenal. To try to beat AI existing fraud detection techniques, fraudsters attack in the form of rings. The reason fraud rings work is because banks tend to store fraudster data in silos which makes it easier for fraudsters to form groups that are hard to detect with a single threaded approach. **Graph algorithms can help.** Graphs are built to detect complex relationships between various data points that are several steps removed from each other. The key is to understand that any single data point such as a caller ID or an account by itself may not be suspicious but that caller ID could be connected to another device, voiceprint or account which may have a risk alert. Connecting the dots between seemingly innocuous data points to reveal a connected set of actors behind the scenes is a game changer. Banks can use graph analysis to enhance the coverage, accuracy and precision of AI models in order to help protect their networks from complex fraud rings.

6

Interpretability of AI results is an essential component in the deployment of an AI system especially in the domain of contact center security. AI need not be considered as a black box that delivers a risk score but it can provide insights into the specific risk factors that contribute to a suspected fraud call's score. These insights can help banks to smartly allocate resources that are being spent to catch high profile fraudsters.

7

Not just the amount of data but also the changing statistical distribution (eg. fraudsters changing carriers or ANIs) is something that needs to be taken into account while training AI models. Different banks can have different fraud rates/attack vectors that would need AI modules to dynamically learn from historical data to deploy the models given the constraints that the bank sets.

IS YOUR AI CAPABLE OF THIS?

AI needs to fight on multiple fronts to detect risk in a customer interaction and to provide a pathway to help protect genuine customers for superior CX.

Is your organization's AI capability equipped on these fronts?

WHO ARE YOU INTERACTING WITH?

REQUIRED CAPABILITIES	WHY?
VOICE ACITIVITY DETECTION	Identifies whether a call contains speech or not in order to improve quality of voiceprint
SPEAKER IDENTIFICATION	Identifies a speaker among a set of known speakers. It is a 1:N problem.
SPEAKER VERIFICATION	Increases accuracy of authentication of a repeat caller. It is a 1:1 problem.
SPEAKER DIARIZATION	Identifies multiple speakers on the same call to improve authentication accuracy and avoid voice blending
VOICE CLUSTERING	Enrolls multiple voices on the same account to ensure frictionless authentication of known account holders
SPEAKER & CHANNEL INVARIANCE	Ensures consistency of enrollment and authentication across varying conditions of microphones, distance of speaker, harsh background noise, reverberation etc.
BACKGROUND NOISE REDUCTION	Reduces background noise in a variety of acoustic conditions to increase accuracy of authentication
SPEAKER SPECIFIC SPEECH ENHANCEMENT	Reduces background noise to ensure better speaker voice recognition
AUDIO EVENT CLASSIFICATION	Identify the various noises that are heard on the phone calls. For instance, some fraudsters explicitly add specific noise to try evading positive voice bio identification (e.g. baby crying, pet noises, etc.).

Continued on next page

REQUIRED CAPABILITIES	WHY?
FRAUDSTER VOICE MATCHING	Increases accuracy of matching of repeat fraudster's voice against previously recorded voiceprint
DEEPFAKE DETECTION	Identifies real human voice vs synthetic deepfake audio to stop fraudulent activities
REPLAY ATTACK DETECTION	Identifies whether fraudster is replaying a legitimate customer's voice
SHORT UTTERANCE DETECTION	Recognizes customer voices with short utterances so that they can be authenticated in the IVR or low speech environments
VOICE ATTRIBUTE ASSOCIATION	Estimate the gender, the age and the language of the speaker
AUTOMATIC SPEECH RECOGNITION	Speech-to-text. It could be useful for speech analytics tasks.
NATURAL LANGUAGE UNDERSTANDING	Understands natural human language to facilitate voice based interactions including voice assistants

WHAT IS THE MODE OF INTERACTION?

REQUIRED CAPABILITIES	WHY?
PHONE NUMBER SPOOF DETECTION	Identifies whether a caller ID has been spoofed which in turn helps assess risk level of the call and its treatment in the call center
NUMBER PORTING DETECTION	Identifies whether a phone number or SIM has recently been ported which points to the risk level of the call
GATEWAY DETECTION	Identifies if the call originated from Skype, Google hangout, or other gateway services.
CARRIER PATHWAY DETECTION	Identifies the pathways a genuine vs high risk call takes through multiple carriers
GEO-LOCATION DETECTION	Identifies the location from where the incoming call originated relative to the caller's device and carrier

HOW SECURE IS THE INTERACTION?

REQUIRED CAPABILITIES	WHY?
RISKY ACCOUNT ACTIVITY DETECTION	Detects the account(s) that could be connected to a high risk call (or vice versa) and are vulnerable to fraud
RISKY CALLING PATTERN DETECTION	Identifies calling pattern in the IVR or agent leg that is anomalous relative to a particular caller ID or device's historical patterns
ACCOUNT RECONNAISSANCE	Detects suspicious activity in the IVR or agent leg that indicates account takeover, account mining or information gathering attempts
ROBOTIC DIALING DETECTION	Analyzes DTMF tone patterns to detect robot attempts vs genuine customer's patterns
ANI TRAWLING DETECTION	Detects whether fraudsters are testing multiple spoofed caller IDs in the IVR
ACCOUNT & ANI VELOCITY	Identifies if any ANI / Account has a sudden burst. This typically is related to fraudulent activity.

THE TAKEAWAY: BET BIG ON AI

AI is and will continue to fundamentally reshape the way banks do business. By automating internal processes, securing and personalizing customer experiences and stopping fraudsters, AI can continue to bolster banks' revenues and profitability. By investing in AI - particularly in high scale machine learning, deep learning and workflow automation - banks could reap long term benefits such as increased customer satisfaction, efficient resource utilization, fewer fraud losses and a highly productive workforce.

Investing in AI is not just about the technology but also about strengthening the underlying processes, empowering people and making sure the AI strategy is in sync with the business strategy and operations. Moreover, banks would need to think and act comprehensively from strategic, regulatory, operational and financial perspectives to ensure an effective deployment and operationalization of AI. Finally, banks would need to be cognizant of several best practices regarding data, modeling, training and optimization of AI engines to ensure they connect the dots between desired business goals and the power of AI.

These best practices can be developed internally through robust investment in data scientists, AI experts, extensive research, training and fine tuning of AI models over time. In addition banks can also leverage specialist vendors that possess the financial industry expertise and deep AI acumen that can help them leapfrog their competition.

ABOUT PINDROP

Pindrop® Solutions are leading the way to the future of voice by establishing the standard for identity, security, and trust for every voice interaction. Pindrop Solutions protect some of the biggest banks, insurers, and retailers in the world using patented technology that extracts an incredible amount of intelligence from every call and voice encountered. Pindrop Solutions help detect fraudsters and authenticate genuine customers, reducing fraud and operational costs, while improving customer experience and protecting brand reputation. Pindrop's Deep Voice® Network, is a deep neural network AI based voice biometric engine, which is leading the industry in innovation and powers both Passport® and Protect® for authentication and fraud detection respectively. Pindrop Security Inc., a privately held company, headquartered in Atlanta, GA, was founded in 2011 by Dr. Vijay Balasubramaniyan, Dr. Paul Judge and Dr. Mustaque Ahamad and is venture-backed by Andreessen Horowitz, Citi Ventures, and Felicis. Pindrop is also the parent company of Next Caller, Inc., whose Verical® Technology leverages advanced machine learning for caller ID validation and spoof detection.

in Pindrop

@Pindrop

@PindropSec

@Pindrophq

pindrop®

pindrop.com