Stopping Fraud at The New Front Door (Spelled "IVR")

opusresearch

opusresearch | Report »

Stopping Fraud at The New Front Door (Spelled "IVR")

»

Interactive voice response (IVR) systems are now hubs for both customer care and associated fraud. This document describes how an end-to-end approach that spans time, channels and multiple data sources can detect activity by fraudsters and prevent their efforts to mine personal data and, ultimately take over accounts.

»

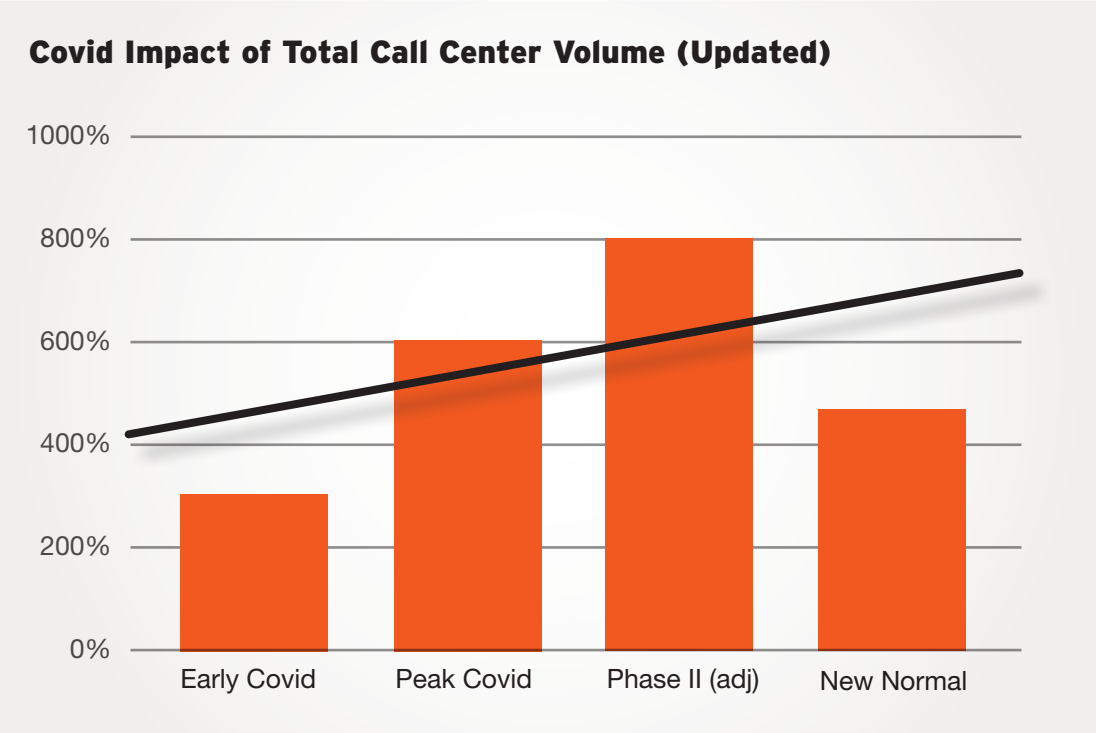
October 2020

Dan Miller, Lead Analyst & Founder, Opus Research

Opus Research, Inc.
893 Hague Ave.
Saint Paul, MN 55104
www.opusresearch.net

ENTERING 2020, interactive voice response systems (IVRs) were thought to be following a long, slow downward arc toward irrelevance. Then the COVID-19 pandemic hit. Now a new history is being made. Life under lock-down led people to discover their new “happy paths” to reach the companies with which they had urgent business. Nearly all cases included a phone call. As a result, as illustrated in Figure 1, call volumes for some industries tripled in the first month and reached as much as 800% of average volume during the next three.

Figure 1: Dramatic Increase in Call Volume



As millions of homebound individuals felt an urgent need to get in touch with their banks, cable companies, healthcare providers or airlines, virtually all these conversations were involuntarily disjointed, asynchronous and multi-channel. Still, over 60% involved a phone call, and, in almost every case, those calls landed on an IVR. Millions of calls from thousands of fraudsters followed a similar path. That’s why the IVR has become the new hub for both customer care and associated fraud.

A Look at IVRs: Past, Present and Opportunistic

Over the years, IVR scripts remained remarkably static and universally annoying. For decades, the large commercial banks, insurance companies, telcos, and brokerage houses deployed IVR systems that were closely linked to Automated Call Directors (ACDs). Their prime directive was to ascertain the purpose of a call and route it to the correct agent. They offered callers a familiar set of choices starting with “If you know your party’s extension, enter it now…” and then marching through the list of no-more-than-five high level options. For banks, these included, “Press 1 to learn your current balances, Press 2 for assistance with your checking or savings account, Press 3 to find the nearest branch, Press 4 to report a suspicious charge or credit card activity….” Each option triggered the routing of a call to a specific department or pool of assistants.

Change took place at telephone systems' characteristically slow pace. Working with vendors or integrators, banks could add new options. Popular new options included "assistance with online banking," rapid "activation of credit or debit cards" or "instructions for downloading and use of our mobile app." Innovative banks also introduced functions far beyond ascertaining intent and routing calls.

Today, banks have gone the distance of adding a number of common informational and transactional services. They started with lightweight authentication in order to provide callers with current balance information and, in the case of credit cards, informing them of payment history, balance due and the payment due date. For a bank's customer or cardholder, such offerings are a convenience.

For a fraudster, this is a golden moment. It is an indicator that they "got a live one." In one, innocent phone call, they have confirmed that the number they obtained on the "Dark Web" is a real account holder. They can ascertain the value of the assets in an account. Given that it might be one of many calls to the same number, using the same account number, think of it as "just another brick in the wall."

TAKE AWAY

As they do more, IVRs are a growing "threat surface" for fraudsters. They are rich source of information to support three specific activities:

INFORMATION MINING – Gleaning any and all information piece-by-piece that is available about an individual or his account.

ACCOUNT SURVEILLANCE AND RECONNAISSANCE - Ascertaining changes over time. In a new use case, enabling fraudsters to see if activity initiated on another channel (for example through the web or mobile app) have taken effect

PASSWORD CRACKING – Gaining access to an account by stealing an individual's password either by brute force "guessing" or by employing a purchased asset.

In addition to being the initial landing zone for inbound calls from legitimate customers, IVRs are a rich source of background information for criminals engaged in a set of patient processes or workflows that they hope to find richly rewarding, including identity theft, currency theft and account take over.

A Picture Tells the Tale in Advance

As mentioned above, committing fraud is not a single event. It is a process that takes place over time, often months. Nor does the culmination of phone fraud always take place over the voice channel. Instead, a complex "Fraud Graph" is created that captures the relationships between known fraudsters and targeted customer accounts. As depicted in Figure 2 below, the identity of the fraudster can be associated with originating phone numbers (or ANIs) and when observed over time, can generate a fascinating visual graph.

Figure 2: The Fraud Graph

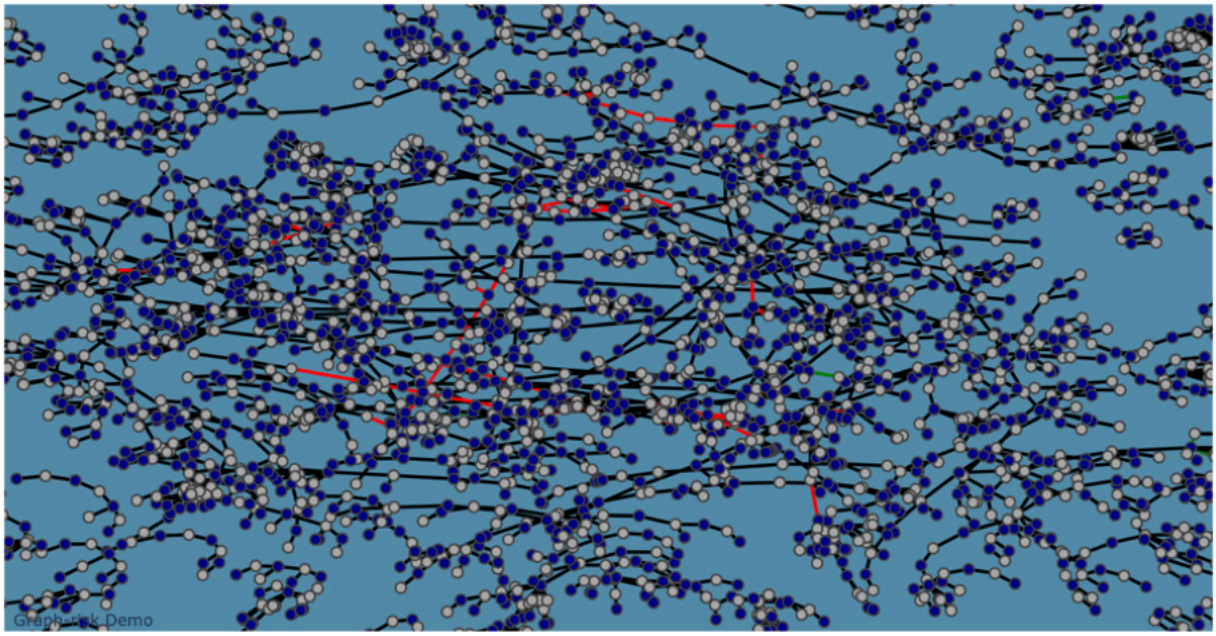


Figure 2 illustrates a graph algorithm that connects disparate data sources and analyzes relationships between behavior, accounts and calls across time. Gray dots are caller IDs and blue dots are accounts. The red lines are confirmed frauds and green lines are genuine activities

While traditional, discrete analytics help to connect call risk with account exposure, graph algorithms take it to the next level by using a network effect to quickly discern and extract insights from complex databases and uncover relationships between multiple accounts, fraudsters and activities based on millions of calls over time.

Modern enterprises interact with customers over multiple devices and channels. In the voice channel, specifically, information security provider Pindrop has found it useful to separate fraud detection capabilities across three distinctive “legs” in the communications path from customer to agent:

- **The Telco Carrier Leg** – Pindrop detects and identifies cause for suspicion based on known fraudulent telephone numbers (ANIs) and other suspicious characteristics of the device in use or network origin.
- **The IVR Leg** – Pindrop detects anomalies in characteristics of the mobile device, in the metadata associated with the call as well as caller behaviors, such as time it takes for a caller to respond to prompts.
- **CSR/Agent Leg** – Once a call is routed to a live agent, Pindrop can perform authentication once again, either passively or explicitly; however, consensus is building that “social engineering” that takes place in the “agent leg” is one of the weakest links in all company’s fraud prevention fabric.

WELL BEFORE FRAUD IS COMMITTED, THE IVR CAPTURES ANOMALOUS INDICATORS OF FRAUD IN THE CONTACT CENTER. THEY CAN CAPTURE AND LOG SUSPICIOUS ACTIVITY ASSOCIATED WITH A CALLER, DEVICE OR ACCOUNT AND TRIGGER THE PROCESSES THAT PREVENT THE FRAUD FROM TAKING PLACE.

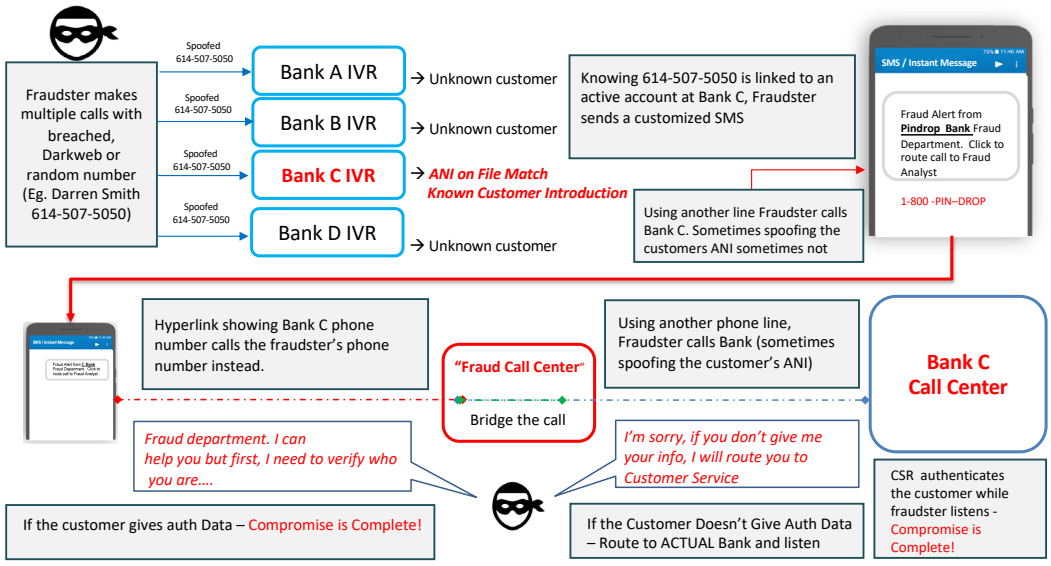
When fraud detection is performed in the "IVR Leg" firms take advantage of two positive outcomes. Just as important, identifying a fraudster or potential fraudster in the IVR removes the human element from the fraud equation. Practiced fraudsters can no longer charm helpful agents into unwittingly advancing them along the path to account take over or identity theft.

Taking an End-to-End Solution to Stop Imposters and Predict Fraud

Fraudsters make their money in multiple steps, over time and by employing multiple channels. They turn to the IVR when it is the easiest source of information to support their endeavors. Looking exclusively at conversations taking place in "the IVR Leg", a business can perceive anomalies that signal the potential for future fraud. Examples include repeated calls from the same number. Because speech-enabled IVRs are being called upon to do more types of self-service activities, they provide security personnel with more raw material to monitor and detect potential fraud.

Note, also, that fraudsters treat IVRs as a font of knowledge to support their illegal activities. At a minimum, they know when a targeted account is genuine. As illustrated in the case study below, by simply completing a call to a known account, they can initiate a series of actions that result in a full account take over or other forms of fraud that take place over other channels.

Figure 3: Case Study: A "Man in the Call Attack"



In the example illustrated above, an imposter carries out a particularly insidious scam, following this playbook:

1. Fraudster calls into multiple banks' IVR using a "spoofed" telephone number as an ID. As soon as the ANI on file matches a known customer's caller ID, the IVR immediately greets it as a known customer. This information itself is very valuable to fraudsters since it confirms that the ANI is linked to a specific account at the bank.

2. Pretending to be the bank, the fraudster sends a customized text alert message, including a hyperlink, informing the genuine customer that a "fraud" that's taking place.

3. The customer follows the hyperlink in the message to speak to the bank.

4. That conversation is intercepted by the fraudster, who uses the conversation to gather more data from the customer under the pretense of verifying his or her identity. If the customer refuses to provide the info, then the fraudster routes the call to an agent at the real bank, but stays on the call and listens in while the customer provides the identity verification to the agent.

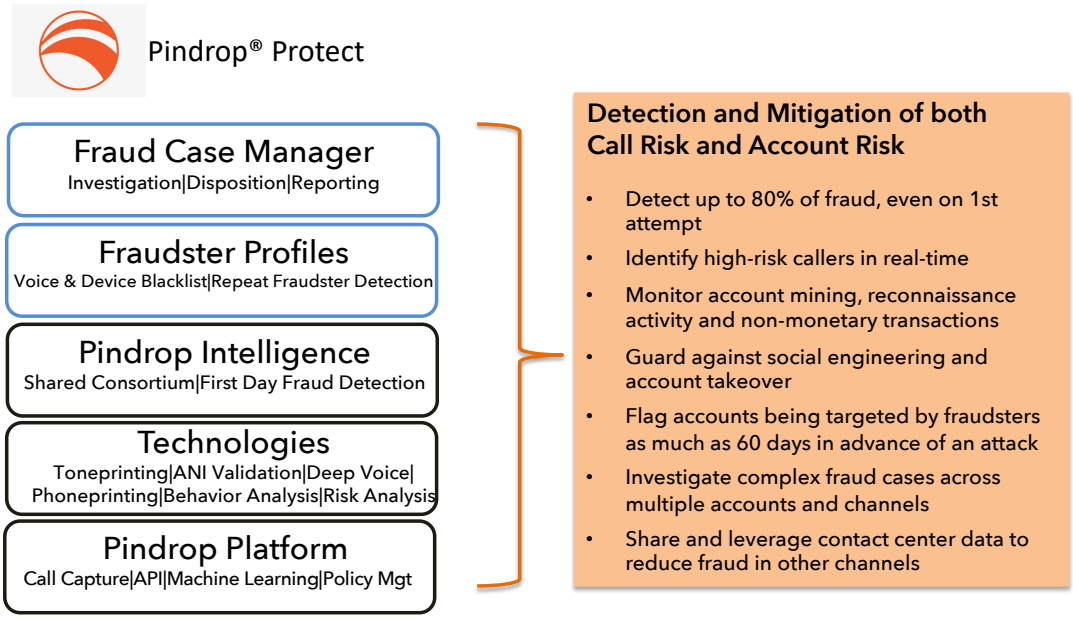
5. The fraudster now has complete identity data of the customer and can use this data to compromise the account. The fraudster will usually wait a few days and start with smaller transactions to avoid suspicion.

As a countermeasure, even if there is no voice interaction involved with the IVR, a business can detect anomalous IVR activity that is a precursor to major fraud. Working with Pindrop, a bank has an end-to-end look at a series of contacts over time, which can be associated with suspicious phone numbers, devices or activities and linked to specific accounts. They can also be associated with activity on other channels and to information about individuals who have previously been identified as fraudsters.

Employing Pindrop Protect

Pindrop's solution incorporates a comprehensive database of known fraudsters referred to as "Consortium". It is comprised of cumulative data on the characteristics of known fraudsters based on analysis of 1.5 billion calls that are from customers in a variety of industries. Working closely with sophisticated financial services companies, Pindrop has already moved well past that simple Blacklist/Whitelist approach to take data and metadata from a multiplicity of sources into account in the IVR and render a risk score within five seconds of the initiation of a call.

Figure 4: Pindrop Protect's Layered Approach



Fraud detection and mitigation in the IVR is an extension of existing capabilities of part of Pindrop Protect. As depicted in the figure above, it is a multifactor fraud mitigation solution that analyzes and provides insights about every call into a company's contact center. It has augmented Pindrop's core technologies surrounding "Toneprinting, ANI Verification, Phoneprinting, behavioral analysis, and risk analysis with data and metadata from a number of sources. When deployed together, they can detect a significant percentage of phone fraud at the very first attempt.

In addition, Pindrop Protect can also detect if a caller ID has been spoofed based on the carrier signaling data and elevate the fraud risk score of calls that have the most spoofing risk associated with them. This spoof risk score further increases the ability to detect fraud even before the fraudster starts to perform any suspicious behavior in the IVR.

In real time, it is able to flag known fraudsters and it knows enough about the behaviors of individuals who are "mining" for account information that it is able to flag suspicious activity even when no voice is involved and no transaction takes place. Because it is familiar with the activities that fraudsters take and it looks for patterns that are different in the course of carrying out fraud, the solution can, in effect, predict fraudulent activity as much as 60 days in advance of an actual occurrence.

Performing risk assessment and necessary blocking in the IVR has the additional advantage of keeping live agents out of the authentication and fraud detection role.

The Advantages of an Account-Based Approach

Fraud prevention tactics most often focus on rapid identification of a blacklist of known fraudsters. Calls originating from known malign individuals, devices or networks are tagged, blocked or otherwise routed according to rules established by the Fraud Department. Yet the internal listing approach should be seen as a starting point for a more comprehensive set of factors, such as the frequency or velocity that a known suspect dials into the IVR and the characteristics in the "carrier leg" of the call that are associated with known fraudsters.

IVR-based fraud detection is even more effective when it is employed as input to an "account-based" approach to fraud risk assessment. Fraudsters, themselves, treat "account takeover" (ATO) as their ultimate and, often, most lucrative outcome. It only makes sense for enterprises to frame fraud detection efforts from the perspective of protecting an account. That means looking at the frequency and mix of calls into the IVR and contact center, determining how many different phone numbers (ANIs) are used to originate those calls and even assessing activities associated with that account on the Web or through the mobile app. These are known "tells" that suspicious individuals have initiated efforts to commit fraud.

The risk score for an individual account changes significantly over time as fraudsters pursue known patterns to mine personal information, ascertain balances or discover vulnerable passwords. The risk score equates to a predictive model for fraud prevention as it can take months for a fraudster to pounce by initiating a funds transfer, making an address change or to take over an account altogether.

You Can Teach Old Tech New Tricks: With Profitable Results

Given the sophisticated, organized and patient approaches that rings of fraudsters take, it is no longer sufficient to build a blacklist of voiceprints or block specific ANIs associated with known fraudsters. Pindrop's approach detects suspicious patterns in the IVR and generates a risk score associated with these anomalies. Taking a holistic, account-based approach, that score can be transmitted throughout an enterprise through APIs and be merged with data from other systems in order to provide more accurate risk scores, issue alerts and trigger action.

FRAUDSTERS ARE CHANNEL AGNOSTIC. OVER TIME, THEIR ACTIVITIES SPAN EMAIL, TEXT, MESSAGING AND HYPERLINKS, IN ADDITION TO THE PHONE CHANNEL.

Figure 5: Case Study in Detecting IVR Fraud

Call Risk and Identity

Annual Calls	60 M
Calls analyzed (60 Days)	8 M
Unique no. of accounts	3 M

Account Risk Monitor

High Risk Acc'ts Flagged	50K /1.8%
Accounts with confirmed fraud	7,800
IVR Account Fraud Rate	1 in 390

Accounts monitored for 90 days after "high-risk" flag:
- ~25% reported b/w 30-40 days
- ~35% reported b/w 40-50 days
- ~20% reported b/w 50-60 days

Financial Impact

Gross Fraud Loss	$13.4 M
Net Fraud Loss (after Recovery)	$ 1.6 M
Fraud Detection Lift	$584 K
Annualized Fraud Lift	$ 3.5 M

Sources of Fraud:
- 63% Card Not Present
- 18% Account Takeover
- 14% All others

In the case study illustrated in Figure 5, a company that sees 60 million calls in a year is able to detect and mitigate over $13 million in gross fraud loss. The figures will vary by size, call volume and vertical industry, but one thing is sure:

In the era of increased call volumes and novel demands on IVRs, they have stepped up to their role as communications hubs connecting telephone lines with enterprise systems, including fraud departments.

Pindrop's Fraud Detection & Prevention suite is a natural integration point both physically (as the front door to the contact center) and architecturally (as network component with hooks into CRM, ERP and Fraud). Leveraging an existing technology at the front end of a fraud prevention solution that spans multiple channels and timeframes is proving both secure and cost-effective.

The end-to-end approach to customer care, self-service, security and digital transformation overcomes a tendency to find new platforms and technologies to meet emerging demands. Enterprises can now implement Pindrop Protect in ways that leverages tried-and-true self-service technologies, informed by databases with profiles and attributes of known fraudsters. Combined, these technologies are already showing impressive results and ROI.

About Opus Research

Opus Research is a diversified advisory and analysis firm providing critical insight on software and services that support multimodal customer care and improved customer experiences. Opus Research is focused on “Conversational Commerce,” the merging of intelligent assistant technologies, conversational intelligence, intelligent authentication, enterprise collaboration and digital commerce. **www.opusresearch.net**

For sales inquires please e-mail info@opusresearch.net or call +1(415) 904-7666