


A man with glasses and a headset is smiling and talking on a phone. He is wearing a light blue button-down shirt. In the background, other call center agents are visible, also wearing headsets. The setting appears to be a modern office or call center.

Reducing Fraud Loss With Proactive Omni-Channel Defense From Pindrop Protect

**We defend some of the largest
organizations **on the planet.****

Along with rapid changes to the economy, the operating structure of businesses, and global consumer behavior, have come unprecedented spikes in call volumes and fraud attempts.

The Advantages of
Proactive Fraud Defense 

5 Technologies on 1 Platform

Protect Offers Specially
Adapted Anti-Fraud Technology

A continuously learning AI, IVR specialized technology, and deep relationship analysis enable omni-channel risk mitigation capabilities.

ON PINDROP PROTECT

Protect defends across channels, accounts, and time, leveraging IVR data, and graph algorithms to predict fraudulent activity 60 days before it occurs.*We've compiled data from a well-known yet anonymized Pindrop customer to illustrate how Pindrop Protect impacted their consumer experience and improved operational efficiency. Because of our business's nature, we have shielded our client names—reach out if you want to learn more about these cases and their outcome.

The Starting Environment



The Situation

Waystar Financial Services* suffered significant losses due to account takeover and card, not present fraud.

Waystar financial services, like most other organizations, had no monitoring or analysis of their IVR; this allowed fraudsters to turn a friendly, customer-focused tool into a free-entry amusement park for cheats. A place where opportunistic individuals and organized crime rings could come to test PINs, validate phone numbers, and collect other data from "low-risk" transactions in the IVR.

Waystar* was losing millions and had no idea that they were enabling the organizations and persons seeking to defraud and steal from them.

Waystar implemented Pindrop Protect from IVR through agent interaction and saw a dramatic decrease in account takeover and card not present fraud, \$3.8 million in fraud savings within six months.



Their Challenge

Account Takeovers Plagued The Contact Center

Waystar Financial fought the fraudsters valiantly. They strengthened their front-line protection - their customer service agents and provided their contact center with tools to help them fight fraud once the call was connected.

However, fraudsters were validating and making the first steps towards seizing these accounts inside the IVR, sometimes calling hundreds of times and never reaching an agent.

Our Solution

IVR Adapted Technologies Identify Fraudsters Real-Time

For the IVR, Protect uses multifactor analytics developed specifically for the IVR environment and runs in every call background. Protect combines **5 technology engines into one platform** which analyze risk across time and accounts to determine if an incoming caller exhibits anomalies that indicate high-risk or suspicious behavior, activities; fraud or fraudulent reconnaissance.

A photograph of a male customer service agent with dark hair and glasses, wearing a headset with a microphone. He is smiling and looking towards the left, with his hands on a keyboard. He is wearing a dark plaid shirt. The background is a blurred office setting with a computer monitor and a lamp. An orange diagonal graphic element is in the top right corner.

Protect correlates risky behavior across accounts and time to identify organized fraud rings and informs omni-channel fraud strategies.

Their Challenge

CNP Fraud Increased

Waystar implemented tools and strategies that reduced overall fraud via the phone channel but were still seeing spikes in the form of card not present fraud.

Our Solution

Protect Predicts Fraud Across Channels Using IVR Data

Protect's predictive analytics and relationship analysis capabilities connect fraud activity across multiple channels, accounts, and time. Protect fed data from the analyses and other accountbased risk information into the customers' crosschannel risk orchestration platform to identify cross channel risk at the account level. The result was for Waystar Financial operationally was the ability to predict which accounts would fall victim to card not present fraud several weeks before it would occur.



Their Problem

Low Visibility Enabled Data Validation and Sourcing

The fraud organizations attacking Waystar were using its IVR to perform surveillance on targeted accounts, and to optimize their operations, formulating new strategies to avoid barriers or reach their ill-gotten bounty sooner.

Our Solution

Protect Gave Waystar X-ray Vision

Protect's preemptive fraud detection capabilities produced less false positives and improve review rates, canceling the noise for analysts. .

How We Did It

Protect analyzes thousands of indicators across the fraud event lifecycle - from account mining and reconnaissance in the IVR to social engineering attacks against agents. As agents engage with callers, Protect analyzes audio, voice, and metadata of the caller.



\$3.8 Million Saved



2.7 Million Call Volume



6 Month Initial Deployment



DEVICE

Phoneprinting®

Analyzes over 1,300 characteristics of a call's full audio to determine its risk and catch first time fraud calls



VOICE

Deep Voice™

Next-gen voice identification, optimized for noisy conditions, speaker aging, & multi-voice enrollment



METADATA

Network Analysis

Analyzes ANI risk/velocity, account and carrier risk, smart white/blacklisting, phone number reputation



BEHAVIOR

Heuristic Analysis

Non-monetary transactions, robotic dialing, keypress habits,



CONNECTIONS

Trace Technology

Graph analysis of relationships between activities, accounts, and calls across time

