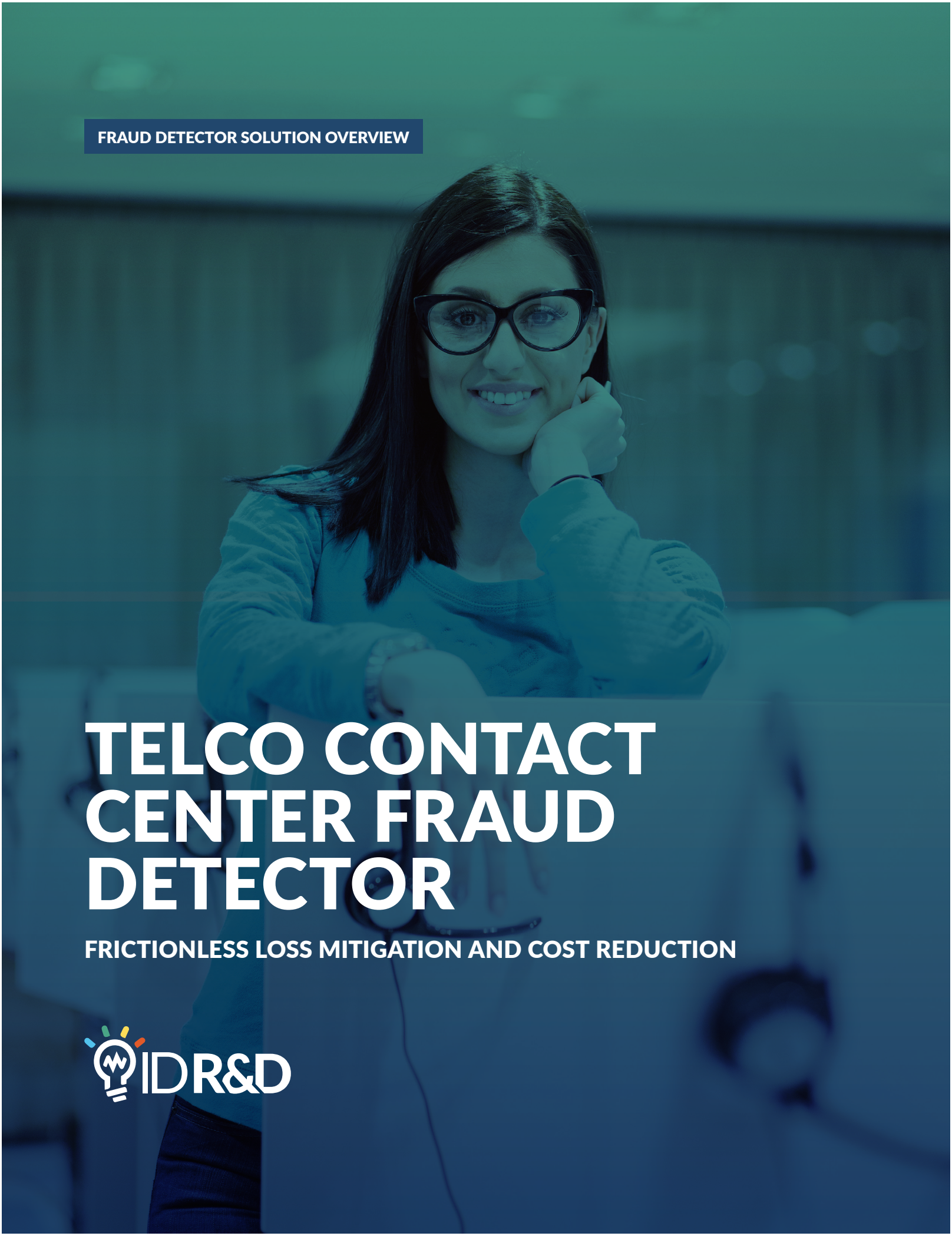
FRAUD DETECTOR SOLUTION OVERVIEW



TELCO CONTACT CENTER FRAUD DETECTOR

FRICTIONLESS LOSS MITIGATION AND COST REDUCTION

IDR&D

According to the analyst firm Aite Group, as much as 61% of account takeovers can be traced back to the call center. Account takeovers are only part of the fraud problem as companies across industries – from banks and telcos to retailers and healthcare providers – also struggle to stop new application and subscriber fraud. Javelin Strategy reports that new account fraud accounted for $3.4 billion in losses in 2018 in the U.S. alone, up from $3 billion in 2017.

When it comes to identity fraud specifically for telcos, fraudsters target the contact center with scams that include:

1. **SYNTHETIC IDENTITY FRAUD.** Criminals combine real and fake identity credentials to create a new "synthetic identity". For example, a stolen social security number is combined with a falsified name and address. Synthetic identities enable fraudsters to open new accounts and obtain phone service and devices, then disappear without paying.

2. **TRUE IDENTITY FRAUD.** The use of a stolen identity in the application process or the use of stolen credentials and social engineering to impersonate a real user. True identity fraud enables criminals to control a victim's account, open new accounts, and make purchases in the victim's name.

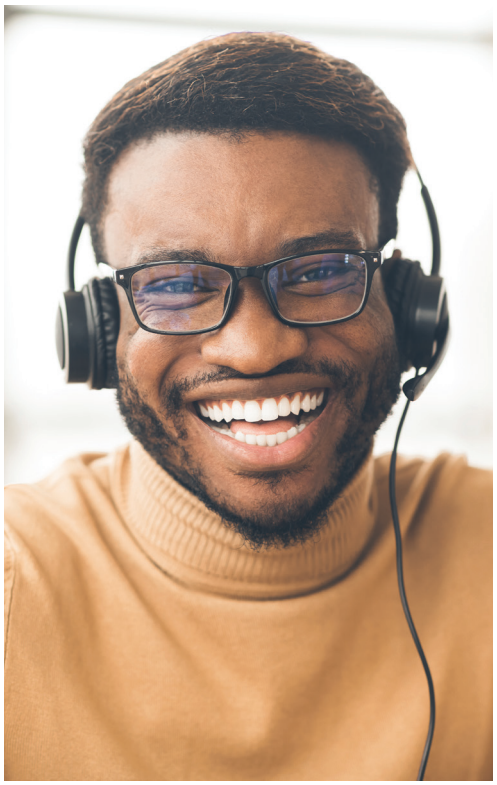
3. **FRIENDLY FRAUD.** Friendly fraud is a type of first person fraud in which a user makes purchases and later claims them as unauthorized. For example, they may use their mobile phone account to set up a new telecom contract, order a new device and then claim that they didn't place the order and that the device wasn't received, as if someone else had stolen their identity. A study conducted by Chargebacks911 suggests that between 60-80% of all disputes are probable cases of friendly fraud.

Fortunately, the latest scientific advances in voice biometrics combined with a clean and simple software application can be implemented to cost effectively address these fraud problems. The remainder of this document describes the solution in detail, further explaining how to quickly get started.

HOW CRIMINALS OBTAIN INFORMATION FOR IDENTITY FRAUD:

- Breached data available on the dark web
- Phishing and vishing attacks
- Public social media profiles
- Mail theft and dumpster diving

CHALLENGES IN THE FIGHT AGAINST CONTACT CENTER FRAUD



Contact centers predominantly rely on technology such as ANI matching and ***knowledge-based authentication*** (KBA) to verify caller identities. But skilled professional fraudsters make quick work of finding the needed information online in public records, social media, and the dark web, or using social engineering tactics to obtain it.

When using the call center to onboard new customers, telcos rely on weak KBA tools. This leaves a wide opening for fraud, which damages both brand reputation and the bottom line. Yet, with aggressive customer acquisition goals, telcos can't afford to turn even a small number of legitimate customers away with stringent and time-consuming security measures.

As a result, fraudsters gain access, reap the benefits, and then disappear in significant numbers. Efforts to combat this fraud typically involve performing verification checks as thoroughly as possible on the customer's background and calling the new customer before setting up the account. But of course fraudsters anticipate these steps and in many cases, know how to circumvent the process. Some telcos attempt to manually review suspicious calls, but the cost trade-off of staffing to perform checks is prohibitive given the large volume of new customers that a telco typically onboards. In the end, the telco only learns after the fact that fraud has occurred and must act to cut losses as quickly as possible.

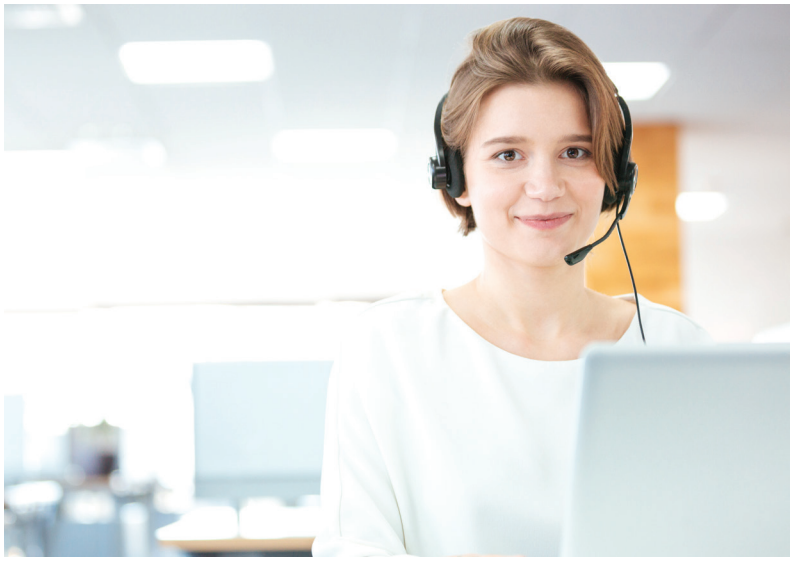
VOICE AS YOUR FIRST DEFENSE

The tools available to verify identity are something you know, something you are, and something you have. In the case of a new account opening, a call center agent must rely on something the new customer knows to validate an identity. Because the account is new, there is no mobile device to check and no biometric information. Until now...

ID R&D now makes it possible to leverage the "something you are" category of identity validation, ***the customer's voice***, to detect and prevent the three types of fraud previously described. This is possible because of fraud patterns and the power of ID R&D's best-in-class Text Independent voice biometrics.

THE SOLUTION

PART I: TEXT INDEPENDENT VOICE BIOMETRICS



Voice biometrics is the science of using a person's voice to verify identity and much like a fingerprint, it is largely unique based on the physiology of the person's vocal tract. Although current science cannot resolve identity using voice with the same precision as face recognition or fingerprint readers, the latest advances in voice biometric technology provides enough precision to be extremely useful for fraud detection, and in a call center, voice is the only biometric available!

Voice biometrics technology typically works in one of two modes: Text Dependent and Text Independent. Text Dependent voice biometrics involves verifying someone's voice based on a phrase the person speaks, essentially a passphrase. This mode is used by some financial institutions, but it is generally not popular due to the amount of friction during enrollment, user confusion on how to use it properly, and the fact that fraudsters have discovered ways to thwart the technology.

The other mode of voice biometrics is Text Independent, which determines identity based on conversational voice, regardless of what the person is saying. The caller's conversation with the call center agent is used as the source of the audio for Text Independent matching. Obviously, Text Independent voice biometrics is the best option for fraud detection and prevention:

1. **Requires nothing extra of the caller; therefore, no friction is added to the new customer onboarding experience**
2. **Fraudsters have no information to help them thwart the voice biometric system**
3. **Beating the system is challenging: a fraudster would need to alter his/her voice during the entire conversation with a call center agent**

Using Text Independent voice biometrics, like any other biometric process, requires the user to enroll or "register." Enrolling a person's voice using Text Independent voice biometrics typically requires 30 seconds of a person's conversational speech, although useful results begin with as little as 15 seconds.

Fortunately, the call center scenario for customer onboarding is well suited to match these requirements with onboarding calls generally lasting five minutes or more. Although the agent is speaking much of the time, the system can usually collect enough speech from the caller to perform a reliable enrollment.

Once you have gathered enough speech for enrollment, only a few seconds of speech is necessary to verify against that enrollment for 1:1 matching, although for the sake of accuracy, it is better to use 5 or 10 seconds of audio, even more, if possible. The term for 1:1 matching is "verification," because the process is verifying the claimed identity. You will see later that 1:1 matching is useful for friendly fraud detection. In this case, you have the customer's voice when he/she ordered, and you can compare the voice on the confirmation call in a 1:1 match test.

However, for the other elements of fraud detection, 1:1 matching is not possible. The telco does not have any prior voice information from a new customer because the customer is new. Instead, a different voice biometric method is necessary. This other method requires taking a voice and comparing it to a list of voices to determine if that voice matches any voice in the list. Imagine the list is a blacklist and you can see why one to many matching, usually referred to as 1:N matching, is essential.

1:N matching is called "identification," because you do not know in advance who the person is, but instead you desire to find out the person's identity from the list of possible voices, also recognizing that the person may not be in the list.

1:N matching with voice is not well suited where N is a large number, say 100,000. However, it is still useful for spotting the best matches out of a possible list. Although not perfect, voice biometrics once again provides a massive labor savings compared to humans attempting the same task. The next sections describe these advantages in greater detail.

PART II: HOW TO APPLY VOICE BIOMETRICS TO DETECT FRAUD

This section describes how to use the power of Text Independent voice biometrics to detect and prevent fraud in each of the three main fraud categories outlined in the first section. You will see that both 1:N and 1:1 matching contribute to fighting fraud. Age and Gender voice biometrics also help.

SCAN FOR KNOWN FRAUDSTERS

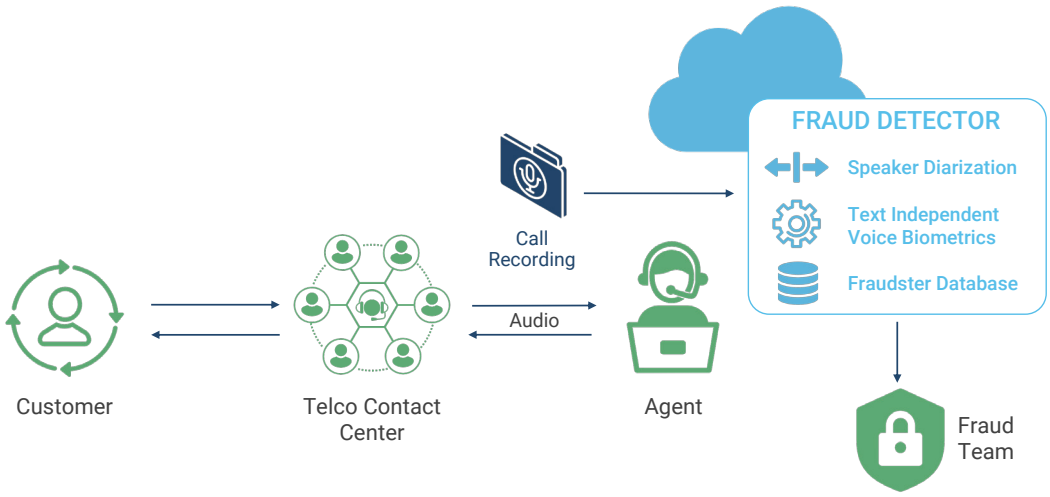
The simplest approach to preventing fraud is to scan all new customers to see if they are known fraudsters who previously created new accounts using either synthetic or stolen identities. However, for this to work, the telco must already have audio of known fraudsters to enroll in the voice biometric system. It then becomes possible to perform a 1:N comparison of each new customer against each of the entries in the database of fraudster voices.

Where does the telco get audio from known fraudsters? All calls to a telco are recorded, so if a new customer call is later discovered to be fraudulent, the telco now has a recording of the fraudster's voice. This audio becomes the source for enrolling a fraudster. The name isn't known, but the voice is now registered as a fraudster.

A problem that arises in many call centers is that audio is stored in a manner that saves disk space. As a result, most call center audio is compressed to lower quality and saved as a monophonic recording that contains both

the caller's voice and the agent's voice. This compressed, monophonic recording is unsuitable for use with Text Independent voice biometrics, which expects to process only a single voice.

To address this limitation, ID R&D provides Speaker Diarization to split the caller audio from the agent audio. This is a highly sophisticated use of voice biometrics technology that works in an offline mode. Accuracy is typically greater than 96%, which is less than the 100% that occurs if the call center conversation is recorded in stereo, but is adequate for the task of comparing voices. Likewise, compressing the audio to smaller size and lower quality diminishes the precision of voice biometrics, but again, the precision remains good enough to be impactful.



Once the telco enrolls known fraudsters they can compare the audio from new customer calls against the fraud database. Two options are available:

1. **Capture audio in real-time and stream it to the voice biometric system for comparison against all the voices in the fraud database, plus check that the age and gender match the purported identity**
2. **Perform a call recording, and at the end of the day, compare each call recording against the fraud database, also checking age and gender**

Capturing call center audio in real-time and sending it to the voice biometric system involves integrating audio capture into the call center operation. This requires a fairly intensive project with ongoing infrastructure expenses. Pulling calls out of the call center recording system, on the other hand, is far simpler with no disruption to existing call center processes.

Did you know? Humans are about 95% accurate with assessing gender. ID R&D's voice biometrics exceeds this rate and can help affirm an identity. That is, if an identity should be a female of age 45, ID R&D's Age and Gender voice biometrics can confirm these values.

Due to the quality of the audio due to compression and diarization, plus the fact that voice biometric precision is not 100% accurate to 1 in 10,000, the results from scanning the fraud database for a match of a known fraudster will not be with 100% certainty. Instead, the voice biometric system will return a list of possible matches above a threshold of probability along with the probability score.

The system may miss some fraudsters and may also provide a handful of matches to known fraudsters that will need manual follow-up. But if only 80% effective at catching fraudsters before they cause more damage, the telco is that much better off than when using previous methods. Moreover, the solution can be implemented at an extremely reasonable cost, especially if starting by simply scanning existing files.

SCAN FOR UNKNOWN FRAUDSTERS WHO ATTACK REPEATEDLY

New fraudsters appear on the scene frequently, so only scanning for known fraudsters means that the telco must first suffer fraud, capture the audio from the original call, and enroll the new fraudster in the database. The telco can take advantage of fraudster patterns to reduce the amount of new fraud.

The basis for this second method of fraud detection and prevention is that professional fraudsters treat their activity like a business:

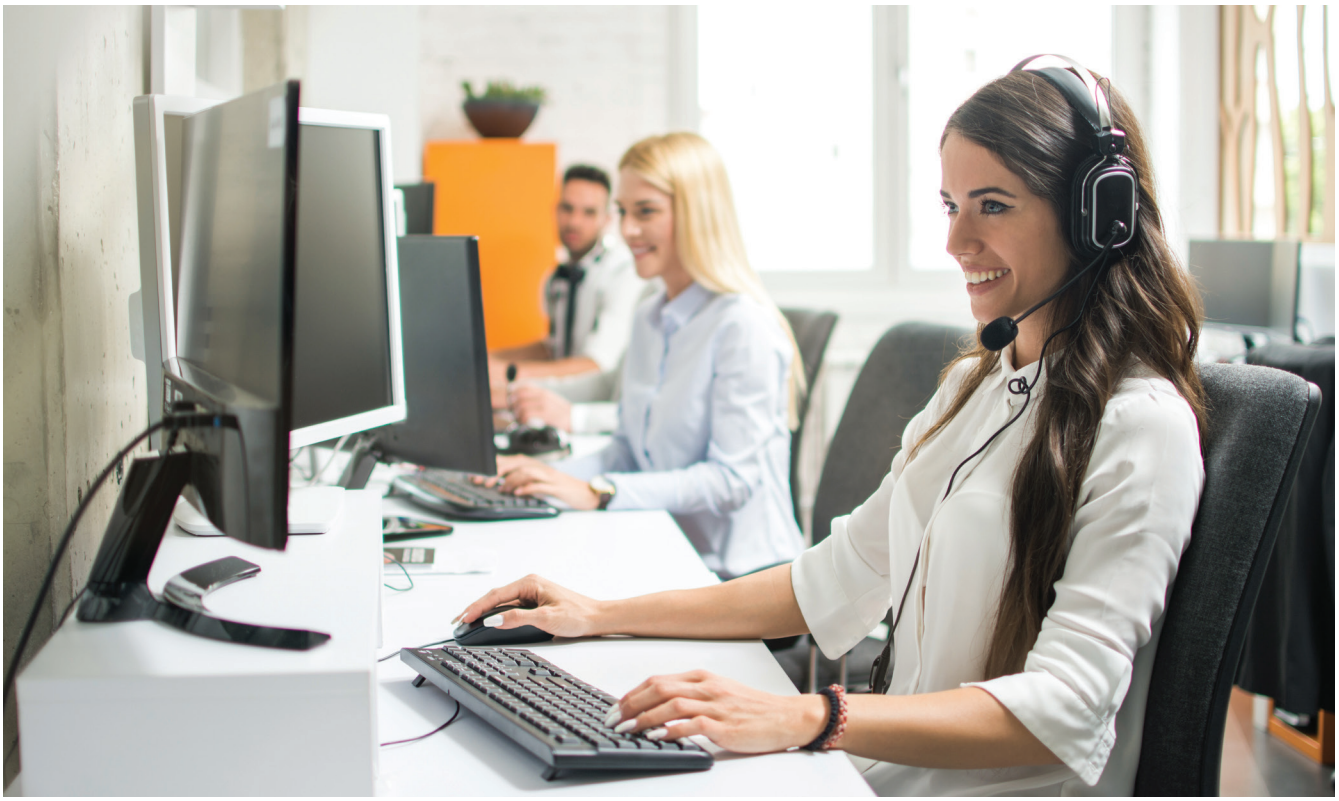
1. **They try to get the best return on their investment of time and effort**
2. **If they find low hanging fruit, they will keep picking the low hanging fruit**
3. **They seek the path of least resistance**

As it pertains to the telco, if fraudsters discover an exploit, they will keep working that exploit. For example, if a skilled fraudster successfully sets up a new account on Monday, they will likely try again multiple times that day or shortly thereafter. Due to the large number of call center agents a telco has, the fraudster will likely be able to defraud a different agent each time. This pattern of repeating fraud in a relatively short time period opens up another opportunity to stop them.

Scanning for unknown fraudsters uses call recordings of new customers to compare against all the other new customer call recordings over a given time period. If the fraudster is working the exploit over a day, a few days, or a week, the voice biometric system will discover the same voice but with different new accounts, clearly indicating the work of a professional fraudster. The telco should deny all of those new accounts. Furthermore, that audio file can be enrolled as a new known fraudster.

Again, the accuracy is not 100%, but whatever the system discovers will be a significant improvement over the status quo.

TIP: To get immediate results with Fraud Detection and Prevention, first try to use the call center recordings and transfer them daily for batch voice biometric processing. The onboarding process usually takes at least 24 hours, thus allowing enough time to scan the files in batch mode, which takes only 2 to 4 hours.



PREVENT CONTRACT DENIAL FRIENDLY FRAUD

The previous two fraud detection and prevention methods address synthetic and stolen identity fraud. This third method addresses a type of friendly fraud where the customer claims they did not set up a contract – in essence, claiming that they were the victim of fraud. When successful, the telco takes a loss.

To prevent this fraud from happening, telcos can leverage voice biometrics to monitor the existing process of confirming a customer's order. That is, the process for onboarding a customer includes a step to verify the customer's order by placing an outbound call to the number provided when setting up a new account. Using a 1:1 matching scheme with the call recordings from the orders and the call recordings from the confirmations, the telco can easily compare and ensure that these voices are the same. If the customer denies making the purchase and the voices are the same, the telco has strong evidence that the customer is attempting fraud. If the called party denies and is telling the truth as shown by the voices being different, then the telco knows the original call to place the order was fraud. Therefore, in either instance of denial, the telco can confidently add the original caller's voice in the known fraudster database.

This simple solution can be implemented with a short turnaround time, allowing telcos to quickly enhance their Contract Denial fraud prevention.

PART III: ID R&D CONTACT CENTER FRAUD DETECTOR

IDFraud™ Contact Center, ID R&D's software for detecting all of the fraud types described earlier, is available as Docker image file, completely self-contained, for handling both streaming real-time audio and batch audio file processing. Because of our high efficiency algorithm design, a single server instance provides enough computer power to handle batch processing of a call center handling 40,000 new customer orders per month in only a few hours per day.

For batch processing, simply notify IDFraud Contact Center where the audio files for the day reside along with a metadata file linking a customer ID, age, and gender to each audio file. The solution does the rest, generating an HTML report and CSV file of results for matching known fraudsters, scanning for the same voice associated with different customer IDs, verifying age and gender conform to the expected results, and confirming all customer order calls match the voice on the customer confirmation calls.

SOLUTION COMPONENTS

- ID R&D's top rated voice biometric engine, IDVoice
- Speaker diarization for the ability to quickly isolate multiple voices in call center recordings and split them into separate audio files
- Database of voiceprints of known fraudsters
- Temporary database of voiceprints of recent customers

IDFraud Contact Center offers configuration settings that enable customized setup without having to write custom code. Examples include threshold settings for declaring a fraudster match, how many days of history to process for the repeated fraudster attack scans, and what level of audio quality is acceptable for processing.

The ID R&D Difference

ID R&D is not the only company in the world producing voice biometrics. However, certain elements of the ID R&D solution provide a distinct advantage compared to alternatives.

HIGH ACCURACY	ID R&D's modified x-vector technology for Text Independent voice biometrics performs exceptionally well compared to all other earlier generation voice biometrics. The evidence is in ID R&D's superior results in global challenges, such as the 2019 National Institute of Technologies and Standards (NIST) Speaker Recognition Evaluation, and customer results.
SPEED OF 1:N IDENTIFICATION	When checking a voice against a potentially large fraudster database, speed is important. Otherwise, the system will take excessively long to process the information or will require substantially more hardware working in parallel. ID R&D's Text Independent voice biometrics performs on the order of 1000 comparisons per second with a simple, general purpose CPU, making it feasible to scan the fraud database and get near real-time results.
CHECKS AGE AND GENDER	To validate the new customer's identity against what identity databases report is that person's gender and age, ID R&D's technology makes it possible to perform an added check with accuracies well above what a human achieves.
WORKS EVEN WITH NOISY DATA	Contact center audio data is often low quality due to compression and noise. Many voice biometric systems work well with "clean" audio but degrade quickly with noisy data. ID R&D's neural network technology is trained with noisy data and provides valuable results even with typical call center audio recordings.
ACCURATE DIARIZATION OF MONOPHONIC AUDIO	Because call center recordings are often reduced to monophonic audio where both the caller and the agent are stored in the same track, accurately diarizing or "splitting"the audio for the purposes of using voice biometrics, becomes a critical success factor. ID R&D's diarization technology, embedded as part of IDFraud Contact Center, provides highly accurate, fully automated separation of the caller from the agent.
LANGUAGE AND ACCENT INDEPENDENCE	A telecom must support the languages and accents of its customer base. ID R&D's modified x-Vector Text Independent technology works with any language and accent out of the box. No tuning or training data is necessary to operate in any country.

USE CONTACT CENTER FRAUD DETECTOR TO:

- **Make it possible to detect fraud before it happens**
- **Detect if a caller is a repeat fraud offender**
- **Catch if a caller opening a new account recently opened an account using a different identity**
- **Transfer the labor intensive burden of identifying repeat fraudsters from the fraud team to the technology**
- **Reduce fraud losses and lower operational costs**
- **Get up and running easily – no integration with contact center hardware or software required**

With IDFraud Contact Center, telcos catch fraud ***before*** it happens. As criminals learn that the contact center is no longer vulnerable in the same way it was previously, the amount of fraud will decrease. This fast and easy-to-implement solution offers a high ROI at a low cost of deployment and ownership. Then the next step is to leverage the power of ID R&D's voice biometric engine installed with IDFraud for additional fraud prevention measures within the telco.

Talk to us today to learn more.

About ID R&D

ID R&D is an award-winning biometrics company on a mission to deliver the next generation of "zero-effort" frictionless authentication and fraud prevention. With extensive expertise in the science of biometrics and the industry's leading R&D team, we deliver a new breed of AI-driven voice, face and behavioral biometrics, and unique voice and face liveness detection capabilities. Our SDKs run on iOS, Android, Linux, and Windows, and work across mobile and web applications, telephone channels, and conversational interfaces to improve security while ensuring a frictionless UX. ID R&D was the TechCrunch Top Pick in Fintech at Disrupt SF, a Finovate finalist for Identity and Access Management, and a 2019 VOICE Summit finalist for Best Banking Experience.

1441 Broadway, Suite 6019
New York, New York 10018 USA
info@idrnd.net
www.idrnd.ai