Fraud in the contact center:

Shore up your vulnerabilities on a path to better customer experiences.

Nuance in partnership with

ConvergeOne

provides premier security and biometrics solutions for enterprises globally.

NUANCE®

Table of contents

1 Current State / p2

2 Contact centers: The chink in the armor of fraud prevention / p2

3 Traditional identification and verification is no longer effective / p3

4 Biometrics to the rescue / p4
– Aite Group: “40% of FIs have voice technology on their one- to two-year contact center roadmap” / p5

5 Beyond authentication and voice / p5
– Biometrics use case: Barclaycard / p7

6 Layered defenses / p8

7 High profile, high priority, high impact / p9

8 Conclusion / p10

Current state

Currently businesses are under a great deal of stress. Policies, processes, and procedures are constantly changing. Inbound call traffic is at an all-time high. Companies have had a reduction in hours and / or contact center employees have left. Customers have more time than ever to talk to agents, stay on the line, and work toward getting the information or satisfaction needed. Longer talk times, changing policies, reduced staff and hours are all contributing factors to the increase in volume and decrease in satisfaction both on the part of the employee and customer.

Speaking of the customer, multiple passwords which age are not convenient. Member numbers, pins, and the need to protect personal data is difficult. Many people have all these items written down or buried in email or a file for quick reference. When all you want is to be recognized and get a response to your question, customers are dissatisfied.

Unfortunately, the criminals who intend on stealing personal identity and compromising institutions know these facts. It is easy prey to attack an otherwise unknowing agent gathering vital personal information in order to take over the account… then another account… then another.

Solutions that can help satisfaction, reduce handle time, and mitigate fraud loss are the forefront of many conversations today.

Contact centers: The chink in the armor of fraud prevention

Whether it's financial services, government agencies, telecom, healthcare, or retail, fraud is on the rise across customer-facing interaction channels. But experts agree: The contact center may be the most vulnerable channel that represents an easier target for thieves. Fraud was on the rise prior to the pandemic. Sources report at least 30% of fraud entered the contact center prior to March of this year. Now reports are indicating this trend is upwards of 75% with no end in sight

A closer look

Imagine you manage the contact center at a financial services firm. Your highly trained customer-service agent answers an inbound call from Tim Underhill, who reports that he's having trouble accessing his brokerage account – he says he's forgotten his account password. Your rep follows the protocol, asking for the account number, Social Security number, and answers to a few knowledge-based authentication questions. Satisfied with the answers, your rep activates the password reset protocol, and the caller has access to the account. **But should he?**

When the line rings in your contact center, a crucial question arises: Is it a valued customer, or is a fraudster at the other end of the line, aiming to steal money, products or services? Is it a true accountholder – or someone armed with breached data and social-engineering tactics preparing to wipe out an account? This vexing question is becoming ever-more crucial. For, while telecommunications and financial-services firms and government agencies have taken countless measures to strengthen the security of their online resources, criminals have begun to eye a far more appealing and lucrative target: **the contact center.**

There's little doubt that the contact center is the weakest link; where many organizations struggle to limit the widespread impact. Certainly, there is the devastating financial toll on the organization – regardless of industry.

From hard-dollar losses to wasted time and added overhead to combat the problem, institutions are spending significant money to combat fraudsters responsible for billions of dollars of losses. For the customer (think: the real Tim Underhill), contact center fraud can wipe out more than an account.

It can wipe out the customer's trust. And in the broader market, as the organization's reputation suffers PR damage, the public can lose confidence – sometimes permanently.

That's because organized fraud rings are probing institutions for the information they need to access customer funds and account information. The contact center – staffed by people whose mission is to provide high-quality, friendly customer service – is often the point of least resistance, representing "easy pickings" for a determined fraudster. This rising tide of fraud represents unacceptably high business and financial risks that forward-thinking businesses must address immediately.

This white paper examines the challenges that organizations face and how voice, behavioral and multi-modal biometrics successfully detect and prevent fraud while improving customer experience by reducing effort for legitimate customers.

Traditional identification and verification is no longer effective

The incidence of fraud in the contact center continues to grow rapidly. Gartner estimates that, by 2020, 75 percent of omni-channel customer-facing organizations will endure a targeted, cross-channel fraud attack with the contact center as the primary point of compromise. For many years, most contact centers' voice-based services have been isolated – organizationally and architecturally – from other channels - such as web self-service or mobile applications, which means they fall outside the careful fraud-prevention and loss-prevention measures that focus on digital channels.[1]

The scope of these attacks is significant as well. An earlier study by Javelin Strategy & Research[2] reports that:

- Identity-fraud victims increased 8 percent to 16.7 million U.S. consumers
- Fraudsters netted 1.3 million more victims in 2017, stealing $16.8 billion from U.S. consumers
- Victims paid an average of $290 out of pocket and wasted 15 hours each to resolve these incidents

Years later, the same types of metrics apply and are often used to secure funding to stem the fraud loss annually.

Let us not forget that voice enabled channels are on the rise, from IVR with natural language to voice assisted devices in our homes to company applications allowing for voice in order to converse with the organization.

[1] Phillips, Tricia and Care, Jonathan. (March 2, 2017). Don't Let the Contact Center Be Your 'Achilles Heel' of Fraud Prevention. Gartner.

[2] Pascual, Al; Marchini, Kyle; and Miller, Sara. (February 6, 2018). 2018 Identity Fraud: Fraud Enters a New Era of Complexity. Javelin Strategy & Research. Retrieved from: https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity#

Unfortunately, traditional identification and verification (ID&V) is no longer anywhere near up to the task of controlling unauthorized access. As Forrester notes, an eight-character, non-dictionary password with two nonidentical numbers, one uppercase letter, and two special characters can be cracked… in nine hours. Given the rise of clustered computers and exponentially greater computing capacity, soon the password will no longer protect payment-grade or high-risk transactions.[3]

Another reason for the death of password-based security? Breaches. Consumers have endured a constant barrage of data breaches and widespread compromises of personal data and user credentials: 145 million Equifax accounts, 130 million Heartland Payment Systems accounts, 110 million accounts at Target, 250 million Epsilon accounts and 15 million accounts at Experian, to name just a few. As a result of these and dozens of other breaches, the traditional PIN and password paradigm is over. Not only can fraudsters easily elude it, customers hate being forced to remember – and change – a portfolio of complex passwords across multiple sites and services. According to Gartner analyst Avivah Litan, 15-30 percent of legitimate customers fail an identification test – while 60 percent of criminals can pass.

Quite simply, it's now far too easy for a fake "Tim Underhill" to answer those questions from your contact center agent, perform an account takeover and clean out the account – whether it's stolen airline loyalty points, government benefits, big-ticket merchandise or retirement funds. However, adding friction to the verification process isn't an appealing option either.

Biometrics to the rescue

Of course, traditional methods of shoring up those vulnerabilities create unwelcome compromises and further scrutiny, especially as companies and organizations embrace digital transformation, not to mention an increased cost in customer and agent time. "There's a real discrepancy here – consumers are glad their bank is protecting them, but they're frustrated that the protection is making it harder for them to open accounts and make purchases," said TJ Horan at FICO. "When it comes to digital transformation, a smooth customer experience is going to be vital. The winners will be the firms that can balance this against the need to stop fraud."[4]

To balance customer experience with the need for security, industry experts are increasingly calling for the use of biometrics as an important strategy for identity verification in numerous security applications. Biometrics is something that you "are", not something you need to remember. Gartner, for instance, recommends that contact centers should implement fraud-prevention technology to improve customer authentication and reduce call

[3] Csar, Andras and Spiliotes, Alexander. (February 6, 2018). Forrester Research TechRadar: Biometric Authentication, Q1 2017 "Adoption of User- and Mobile-Friendly Biometrics will Kill the Password." Forrester Research.

[4] Orem, Tina. (July 11, 2018). Everybody Is Sick & Tired of Online Security Measures, Poll Finds. Credit Union Times. Retrieved from: https://www.cutimes.com/2018/07/11/everybody-is-sick-tired-of-online-security-measure/

[5] Phillips, Tricia and Care, Jonathan. (March 2, 2017). Don't Let the Contact Center Be Your 'Achilles Heel' of Fraud Prevention. Gartner.

times for legitimate customers, while identifying high-risk calls for appropriate scrutiny. Core to this is integrating voice biometrics to enable velocity detection of fraudulent callers and morphing across accounts, and to identify confirmed fraudulent voiceprints.[5]

Fortunately, biometrics can play a key role in the contact center and across multiple interaction channels through authentication and fraud prevention. It starts with the voice. When the purported accountholder calls the contact center, a biometrics system compares his voice with its stored "voiceprint" and can confirm that the caller is who he claims to be. There is no other information to provide and no verification questions to answer, so the process is fast and secure. That allows the service rep to proceed with confidence to deliver a high-touch experience to the customer.

Approximately 95 percent of callers "get a "match" with their stored voiceprint. It's the remaining 5 percent who merit additional levels of scrutiny. In a growing number of cases, that caller is an unauthorized individual intent on defrauding the accountholder and institution.

> "Technologies that are transparent to the end user, such as behavioral analytics and voice printing technologies, are preferred by FIs, which reserve the intrusion and cost of stepped-up authentication for only a small percentage of customers… When asked whether they plan to invest in voice technology as one method of protecting their contact centers, **25% of FIs indicate that they either have a pilot underway or are working on a production rollout, while another 40% have voice technology on their one- to two-year contact center roadmap**."
>
> Aite Group[6]

Beyond authentication and voice

While some vendors emphasize authentication, others focus on fraud prevention. Combating fraud requires a dual-pronged strategy of authentication and fraud prevention to improve the customer experience and reduce effort for legitimate customers while preventing fraudulent access.

Since fraudsters don't limit themselves to a single interaction channel and are increasingly targeting contact centers as the weakest link, companies must deploy **authentication and fraud-prevention** measures that span interaction channels (e.g. web self-service, mobile applications, and the contact center).

What's more, those omni-channel measures must leverage both biometric and non-biometric modalities. When the inbound caller fails the voiceprint check, the contact center can't simply refuse to serve the caller – that would needlessly create hundreds or thousands of justifiably angry customers.

Instead, the contact center can follow a series of biometric and non-biometric checks to proceed carefully in ways that reduce or eliminate fraud exposure.

Combating fraud requires a dual-pronged strategy of authentication and fraud prevention to improve the customer experience and reduce effort for legitimate customers while preventing fraudulent access.

[6] Inscoe, Shirley. (April 27, 2016). Contact Centers: The Fraud Enablement Channel. Aite Group. Retrieved from: https://www.aitegroup.com/report/contact-centers-fraud-enablement-channel

Step #1:
Compare to list of known fraudsters
When the account holder's voice fails to match with the voiceprint on file, the contact center can compare the failed recording with a list of known fraudsters – people who've previously committed fraudulent transactions. If a match is found, that call enters a "gray zone" and gets handled differently. The call may be transferred to the fraud department. The contact center might place an outbound call to the accountholder to confirm access and transactions. It might freeze accounts and transactions and email the accountholder. Increasingly, however, merely asking security questions is an ineffective screening technique..

Step #2:
Analyze the conversation
If the caller doesn't match the accountholder's voiceprint but also doesn't match a known fraudster's voiceprint, we can still apply patented biometrics technology to analyze the caller's voice, speech pattern, sentence structure, and even grammar – the so-called "conversation print." Instead of focusing solely on voice characteristics, this test compares the caller's speaking manner with the accountholder's known speech characteristics to determine if they match. What's more, like voiceprints, we can compare conversation prints with a library of known fraudsters and confidently determine:

- This is not how the accountholder normally speaks
- This is how a previously known fraudster speaks

Just as important from an omni-channel perspective, the conversation print speech-pattern-recognition technology isn't restricted to voice calls. It can also be applied to text-based chat with your agents, which are popular ways for fraudsters to attempt to impersonate accountholders because they can disguise gender and speech accents. Integrated conversation analysis is an easy, effortless, high-touch way to enable the agent to transparently authenticate the consumer and prevent fraud – on the fly.

Step #3:
Other behavioral biometrics
Customers behave in distinct ways, and biometrics can recognize and assess those behaviors to match them to known patterns – for accountholders and fraudsters alike. These can include everything from typing patterns (key-press strength, travel, and sequence), mouse usage – even how they hold or use a smartphone (including pressure, hit zone, and more). Behavioral biometrics, of course, can improve fraud prevention across different engagement channels.

Biometrics use case

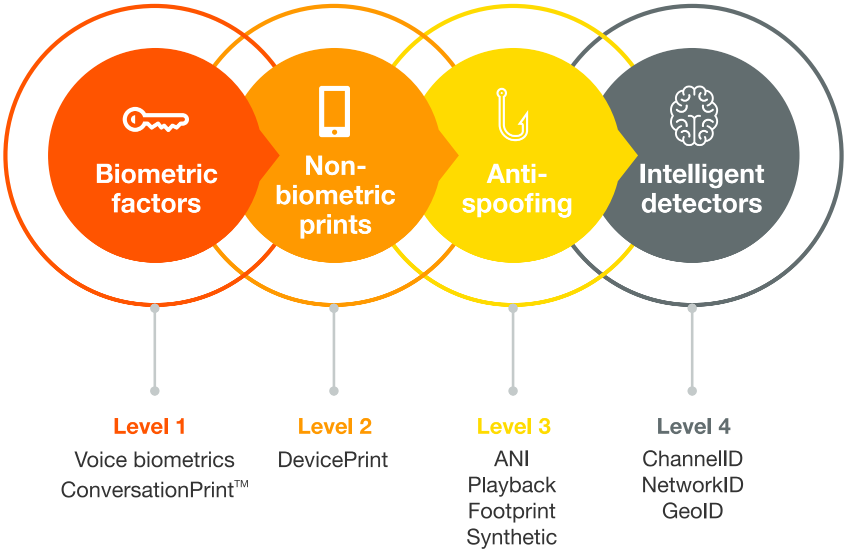
Barclaycard reduces account takeover fraud by 40%
The Card and Payment Awards recognize excellence and innovation in the UK and Irish card and payments industries. In 2015, client Barclaycard won the award for Best Security or Anti-Fraud Development.

In describing why Barclaycard was selected, the judges wrote, “Barclaycard wished to protect its customers without cumbersome procedures. Barclaycard implemented a dynamic fraud-detection solution using Nuance voice biometrics to protect its customers without disruptive processes. The financial services leader compiled a comprehensive library of known fraudsters’ voices and, using Nuance technology, implemented a near-real-time’ pilot matching incoming voices against this blacklist. Incoming audio is assigned a risk score and alerts are investigated by experienced Barclaycard fraud agents who, when necessary, contact customers, protect the customer’s account, and add new fraudsters to the blacklist.

“As the first UK financial institution to implement voice biometrics, Barclaycard **reduced account takeover fraud by more than 40 percent in a short timeframe, and nearly 75 percent of high-risk alerts were confirmed as fraud**. Adverse impact on customers has been negligible. What’s more, timely and clear contact with fraud victims has created very positive customer experiences.”
Card and Payment Awards Ltd., London

Layered defenses

While biometrics can provide exceptionally accurate levels of authentication and fraud prevention, there are other clues that we can automatically observe that can indicate signs of potential malfeasance. Collectively, biometric and non-biometric techniques create a layered defense.



Through this “layered defense,” we can look for other clues when a voiceprint and conversation print both fail to produce a match for the named accountholder:

- **Device ID**
  A company can register the unique device ID of a laptop or mobile phone. If that device ID doesn’t match the one on file, the system can issue an alert. Of course, two challenges arise. First, users change and upgrade devices, creating transactional friction that erodes the customer experience. Another, perhaps more troubling, factor is that some of the interactions are done by family members, caretakers, and other trusted associates – people who have easy access to the accountholder’s registered devices.
- **Anti-spoofing measures**
  Some of the key non-biometric techniques for fraud prevention include automatic number identification (ANI), detection of voice playbacks, gender mismatches, and synthetic vocalizations.
- **Intelligent detectors**
  If the accountholder device is associated with the U.S., but the inbound call to your contact center is originating from a remote country, or the inbound text chat originates from an IP address that is a known trouble spot – or even a phone number that is fraudulent – that may indicate an attempt at fraud. Even something as simple as channel choice can raise a flag. If the accountholder typically calls on a landline, but the incoming call is from a disposable mobile phone, that could indicate fraud.

High profile, high priority, high impact

With a robust platform for authentication and fraud prevention, all organizations including government agencies and financial services can achieve significant benefits.

- **Lower costs**
  Integrated, omni-channel solutions for authentication and fraud prevention can dramatically improve the performance of the contact center – from increased use of self-service options, to reductions in average handling times and reduced processing times for high-risk calls. These all directly improve the bottom line.
- **Improved customer experience**
  Properly implemented fraud prevention initiatives should reduce (or nearly eliminate) any disruptive friction in the contact center. That transparent improvement in both security and customer experience creates meaningful increases in Net Promoter Scores (an indication of customer loyalty) and customer satisfaction rankings. Customers prefer voice biometrics for its simplicity, transparency and effectiveness.
- **Increased agent satisfaction**
  By eliminating the need to interrogate (and potentially irritate) callers, contact center agents find that voice biometrics simplifies their jobs and improves job satisfaction which can reduce absenteeism and employee churn. Agents spend more time helping customers and less time on security matters.
- **Brand differentiation**
  For financial institutions, biometrics are creating an important point of differentiation that they are aggressively promoting. Consumers are recognizing the importance of security, and financial institutions are increasingly marketing their use of biometrics directly to consumers.
- **Reduced fraud**
  Of course, the most important metric is the amount of money institutions can save by preventing or mitigating fraud. One Nuance customer identified

Thinking about taking that next step is important to your company's customer experience and financial health. Time is of the essence given the increase in fraud over the last few months. This trend of change is likely not to stop soon. It is predicted that we are going to continue change, and rapid change over the next few years.

We recommend the following steps on your path to fraud prevention through biometric authentication.

1. Work with your security, risk, and fraud teams to educate them on the technologies discussed to mitigate the risk to the business. Many companies are more concerned with database breaches and phishing scams and are writing off this fraudulent debt. The customers are left with a feeling of mistrust and are likely to move on to other companies that will provide them a more effortless experience.

2. Understand the amount of time taken today to validate through the traditional methods used. This information will be important to establish the efficiency side of the business case. The savings in handle time, increased IVR containment rate and fraud detection and prevention will yield a compelling financial result.

3. Determine which methodology (passive or active enrollment) is right for you.

4. Receive a proposal from a reputable partner

5. Implement the solution

6. Check back to see how you've improved with a streamlined process, customer satisfaction, employee satisfaction, and fraud prevention.

7. Enjoy the rewards of better customer and agent experience.

Conclusion

More than ever, authentication and fraud prevention are the foundation of forward-thinking strategies for customer engagement – for almost any customer-facing organization, including financial services, government agencies, insurance, healthcare, and high-value retail. It's also increasingly clear that organizations can no longer view their channels as independent silos. Omni-channel communications require omni-channel security strategies and initiatives.

What's more, those strategies – encompassing both authentication and fraud prevention – must blend biometric and non-biometric layered defenses to create a pleasing, fraud-free, low-friction customer experience across voice and digital channels.

As more traditional methods of passwords and knowledge-based authentication are compromised and therefore recede from the scene, biometrics and other fraud-prevention strategies that span interaction channels (e.g. web self-service and mobile apps) are gaining greater importance.

About Nuance Communications, Inc.
Nuance Communications (NASDAQ: NUAN) is the pioneer and leader in conversational AI innovations that bring intelligence to everyday work and life. The company delivers solutions that understand, analyze, and respond to people – amplifying human intelligence to increase productivity and security. With decades of domain and AI expertise, Nuance works with thousands of organizations globally across healthcare, financial services, telecommunications, government, and retail – to create stronger relationships and better experiences for their customers and workforce. Explore Nuance Security Suite, and for more information, visit www.nuance.com.

About ConvergeOne
ConvergeOne is a leading global IT services provider of cloud collaboration customer experience and technology solutions with decades of experience assisting customers to transform their digital infrastructure and realize a return on investment. Over 14,000 enterprise and mid-market customers trust ConvergeOne with collaboration, enterprise networking, data center, cloud and cybersecurity solutions to achieve business outcomes. Our investments in cloud infrastructure and managed services provide transformational opportunities for customers to achieve financial and operational benefits with leading technologies. We deliver solutions with a full lifecycle approach including strategy, design and implementation with professional, managed and support services. More information is available at convergeone.com.

To get started, please contact:

NUANCE

Nuance Communications, Inc.
1 Wayside Drive
Burlington, MA 02155
cxexperts@nuance.com
781-565-5000

ConvergeOne

ConvergeOne
10900 Nesbitt Avenue South
Bloomington, MN 55437
contactus@convergeone.com
888-321-6227