Balancing fraud prevention and customer satisfaction

Using AI, machine learning and biometrics to reduce customer frustration with security in the contact centre

The contact centre industry is investing heavily in authentication

Annually, ID verification alone is costing the contact centre £1b – roughly equivalent to the cost of building the Burj Khalifa.

There are two key questions every organisation needs to answer:

1. How can you cut down this spend?
2. How can you stop authentication from adversely affecting customer experience?

Introduction

Today, a pressing challenge for the contact centre is how to upgrade fraud detection, without damaging customer or agent experiences. But how do you increase security without adding unnecessary barriers and friction between callers and their accounts?

As customers migrate from brick-and-mortar interactions to digital channels, remote interactions have increasingly become the default. But when remote channels like banking apps or user portals fail, the contact centre is the first place customers turn to for human interaction and support. Unfortunately for agents, this means by the time customers reach them, many are already confused, impatient or frustrated. If they then have to wait on hold or can't get immediate answers to their problems, their dissatisfaction grows.

During the pandemic, this situation intensified. Call volumes reached unprecedented levels, and the sensitivity of information being handled over the phone soared.

Plus, agents were often stretched, trying to adjust to remote working, or working in teams stretched by increases in staff sickness.

It was during this time that fraud reached an all-time high, with 79% of organisations seeing an increase[1]. Criminals preyed on the vulnerabilities of both organisations and customers and were quick to take advantage of the disruption. Identity fraud increased by 11% in the first six months of 2021[2] and a third of contact centres experienced higher fraud costs in 2020 compared to 2018[3].

The figures clearly point to a need for greater fraud prevention measures, but balancing increasing security with preserving the customer experience (CX) is challenging. In particular, many organisations are finding that knowledge-based authentication (KBA) protocols are a major source of customer dissatisfaction and unnecessary handling time. Customers who rarely used these procedures before the pandemic now struggle to remember their security answers or the passwords they set up, sometimes years ago, and are frustrated that resetting takes time and effort. Is KBA making CX worse?

If it's not handled properly, perhaps. But organisations can't ignore the fact that contact centre fraud is now huge business – especially in the banking and financial sector. It's critical that they stay several steps ahead of the professional fraudsters who are investing enormous amounts of money and time into sophisticated attacks.

This whitepaper will examine:

- key security challenges in the contact centre
- the types of attack to watch out for
- the five stages of fraud
- critical steps to protect your contact centre estate
- why BT for security in the contact centre
- streamlining authentication and redirecting fraudsters with Smartnumbers Protect
- authenticating customers and detecting fraud with Nuance AI-powered solutions.

Key security challenges for contact centres

So, what's holding organisations back from delivering an excellent CX that's protected from fraud? Based on our specialists' experience, here are the key challenges organisations often face:

1. **Siloed fraud and CX teams**
   Traditionally, most fraud and CX departments have little interaction and operate in separate areas of the business. This is counterintuitive, because - more often than not - the decisions made by fraud prevention and security teams have a direct impact on the everyday working lives of CX and customer service teams. And without effective cross-departmental communication, the daily frustrations and inefficiencies agents experience have no influence on fraud prevention decisions.

2. **Employee retention**
   Contact centres experience high staff turnover. As a result, retaining security expertise and customer service skills inside the workplace is particularly challenging and training costs can be high. Agents are on the frontline of customer service strategy, working under considerable pressure and stress as the first point of contact for dissatisfied customers. Laborious authentication processes and security protocols are a common source of frustration and aggravation for agents.

3. **Fraudsters are becoming more sophisticated**
   Today, contact centres are under attack from increasingly complex criminal manipulation. Fraudsters are going to more extreme lengths, generating a range of exploits which are testing agents in new and unpredictable ways. Static rules-based risk solutions struggle to keep up with the evolving threat landscape.

4. **The rapid shift to remote working**
   During the pandemic, the sudden unprecedented move to working from home left agents, at times, struggling to deliver a quality service. Without in-office technical support, this often forced them to find creative workarounds to challenges - from connecting their own devices to the network to downloading unsupported tools and software. With many workforces now continuing to operate remotely, organisations have to find ways to authenticate their employees at distance before they handle sensitive customer information.

5. **Balancing security and customer service**
   Maintaining legal and regulatory compliance is critical. But customers can quickly become frustrated with what they feel are unnecessary security measures or verification procedures. For example, resetting passwords can be time-consuming and, in some cases, even require postal or physical verification. As a result, essential security and verification processes can have a negative effect on customers' perceptions of the service experience they've received. Yes, customers expect to be secure, but they also expect it to be seamless and swift.

6. **Mounting pressure to reduce call handle times**
   Right now, call volumes are higher than ever, and agents are under considerable pressure to reduce handle and hold times. However, reliance on KBA for identity management increases handle times and, as a result, the pressure on agents. This also affects the time they have on a call to focus on delivering a positive customer experience. Plus, issues with security processes in self-service channels such as IVR are driving more calls to agents and adding to their workload.

7. **Resistance and distrust from customers**
   Generally, younger, tech-savvy customers are used to remote transactions, banking apps and remote authentication protocols and accept them as part of the experience. But the older generation tends to be distrustful of online services and giving out sensitive information over the phone. They may be less aware of the value of KBA or how the information they share is protected, so are reluctant to take part in authentication processes, making their overall experience a negative one.

Recognising the most common forms of attack

If you don't properly understand your threat landscape, you can't effectively protect your organisation against new and emerging exploits. At present, these are some of the most common forms of malicious behaviour contact centres encounter:

Identity theft

This fraud tactic includes any attempt to pose as another person using stolen or purchased information, or information obtained through social engineering and IVR mining. Once a fraudster has gathered the right amount of data, they can open fraudulent accounts, destroy credit profiles, transfer assets, or even access medical information and claim government benefits.

In fact, just in 2021, there were 4.2 million complaints of identity theft and fraud to the Federal Trade Commission[4]. Common fraud tactics associated with identity theft include account takeovers, payment fraud, SIM swapping and credit fraud.

Social engineering

Social engineering is a key tactic used to support the end goal of identity theft – to be able to pose successfully as the real customer and gain access to their account.

Social engineering uses psychological and emotional manipulation to coerce victims into divulging personal or valuable information. Criminals might simulate distressing predicaments, urgent moral dilemmas, or even use distractions and diversions to deceive their victims. For example, they might exploit an agent's sympathy with a background audio of a child crying. Or they might play background noise to simulate an intense scenario, like loud traffic or shouting, which repeatedly drowns out KBA answers while the caller pretends to be under pressure and increasingly frustrated.

In the contact centre space, this type of attack can take multiple forms. Bad actors targeting agents can impersonate customers using information gathered from a range of public sources (social media, directory enquiry). They will then carry out multiple phone calls to scope out vulnerabilities and gather personal information for future attacks. They might also target customers under the pretence of being an agent to extract information from them.

Synthetic identity fraud

Sometimes, fraudsters use a combination of real customer information and forged information to create new, synthetic identities. These are often used to open credit accounts and borrow and spend money without detection. More commonly orchestrated by organised criminals, this tactic enables fraudsters to create a credit history under a false identity or set up new accounts, subscriptions and services without paying for them. Synthetic identities are also useful for money laundering, setting up rental properties as operating bases, and applying for utilities.

Interactive voice response (IVR) mining

IVR mining is a highly sophisticated form of criminal activity that leverages machine-to-machine manipulation and algorithms to systematically extract information or trick the contact centre's interactive voice system. Criminals gather information over time by conducting reconnaissance and identifying potentially at-risk accounts or flaws in systems.

IVR mining can be especially difficult to detect because it masquerades as genuine transaction activity. Plus, 64% of IVR reconnaissance is conducted from withheld numbers, making it difficult for organisations to detect[5].

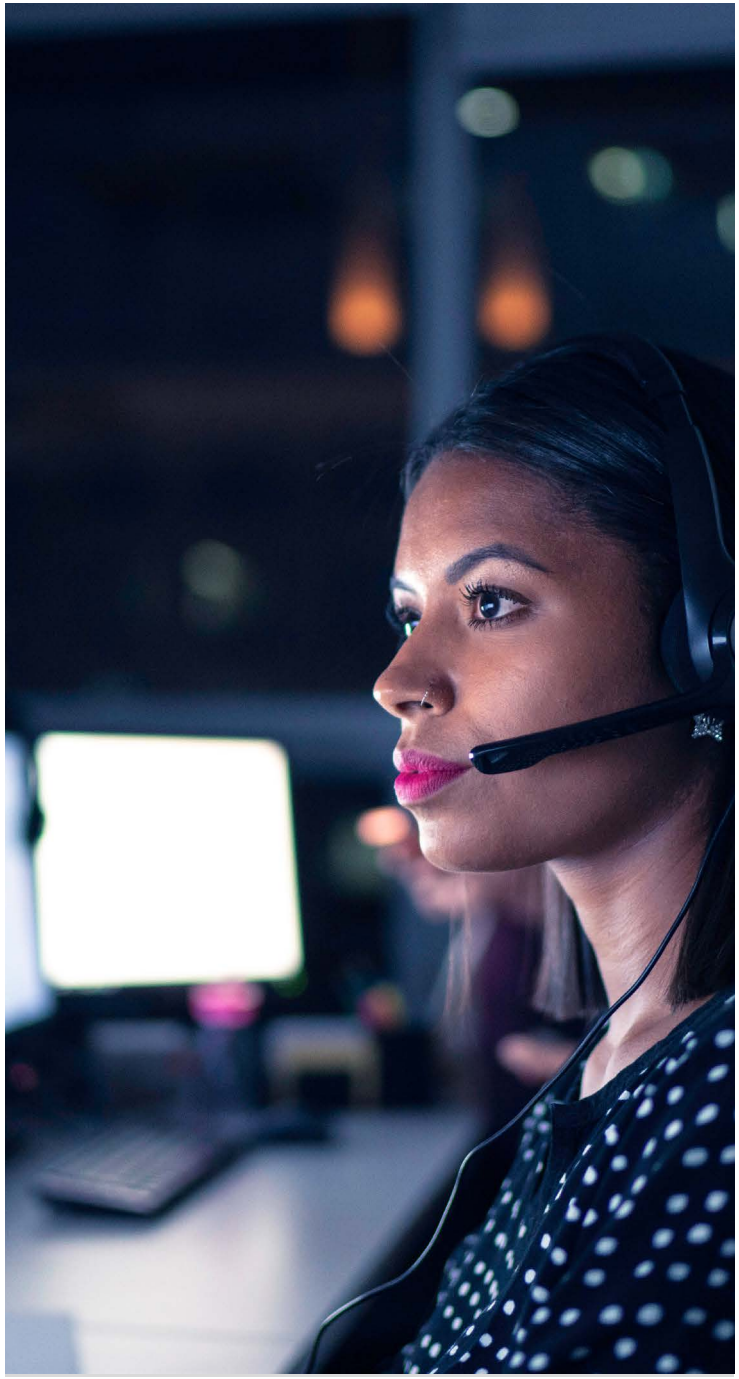
Criminals will use automated systems or bots to carry out extensive trial and error attacks, like repeatedly attempting to guess the answers to KBA questions or conducting account activity surveillance. Afterwards, data mined from these attacks might be used to support identity theft and synthetic identity fraud, or even sold to other criminal organisations.

64%

of IVR reconnaissance is conducted from withheld numbers, making it difficult for organisations to detect[5].

The five stages of fraud

While there are a lot of different types of exploits deploying a wide variety of tactics, fraudsters tend to follow a structured approach. Organisations can use a thorough understanding of this process to create effective fraud prevention strategies that intercept the fraudsters where it counts.



1. Harvesting

Fraudsters begin gathering credentials to impersonate their target using information leaked from data breaches, purchased illegally, or harvested using phishing or mail interception tactics.

2. Reconnaissance

Fraudsters exploit the contact centre to validate any harvested information by testing IVR systems or contact centre agents to confirm data. Then, they'll start to perform low-risk actions or 'scoping' for additional information like emails or account balance. They might learn through repeated calls what information is requested during the verification process or gather the names of contact centre agents and managers in an attempt to build credibility for further questions.

3. Preparation

Once they've passed security checks, the fraudsters will start making preliminary changes to the account. This could include changing login or address details, requesting a new debit card, or adding payees onto the account.

4. Monetisation

At this point, the fraudsters can lift money out of the account with a simple bank transfer and carry out transactions without anyone noticing or preventing them.

5. Legitimisation

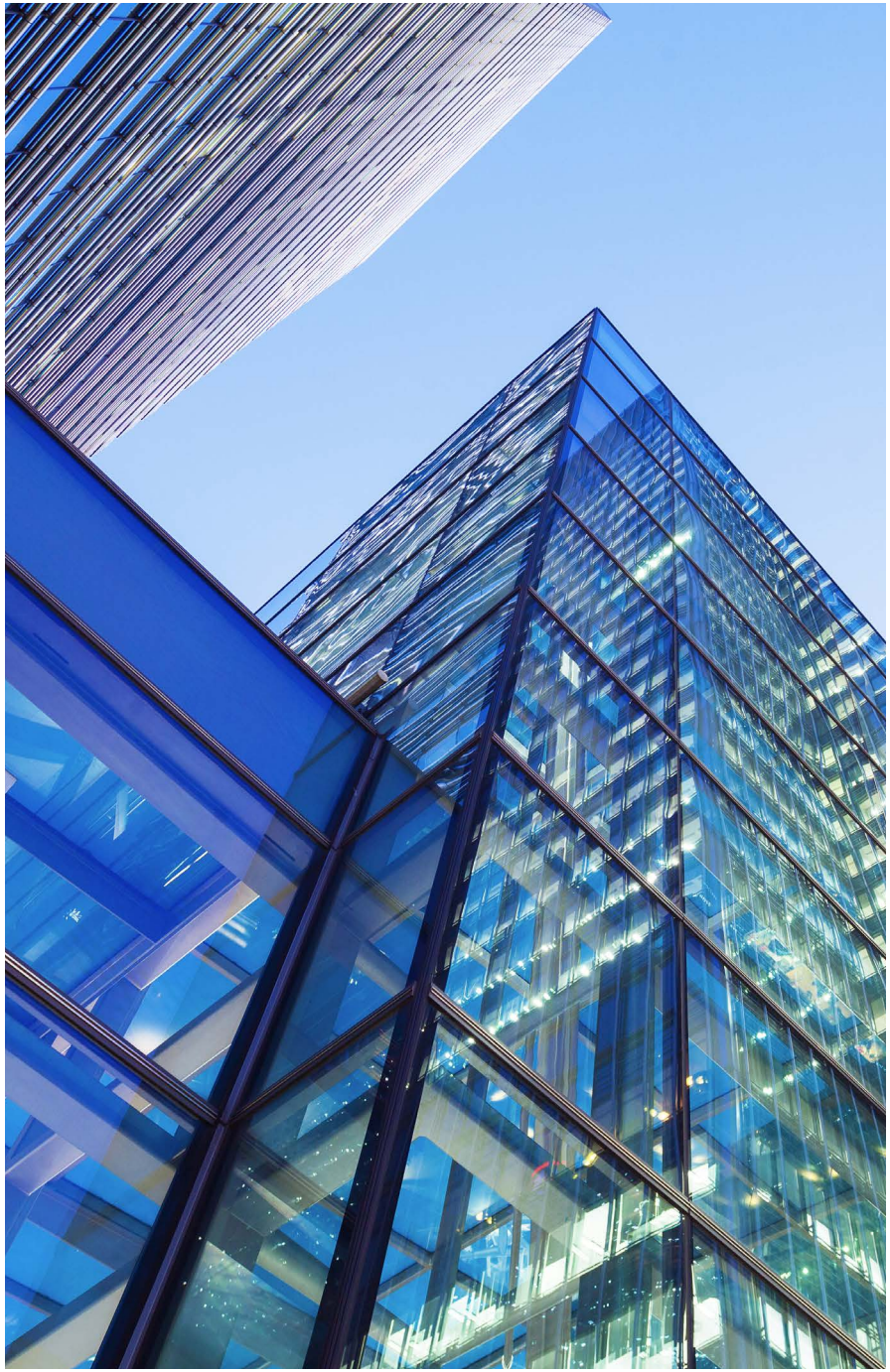
To avoid detection, fraudsters will start to launder proceeds from their activities, transferring money into foreign bank accounts, moving it across into another 'clean' account or using money mules to move funds around through cheques, wire transfers and direct mail.

Critical steps to protecting your contact centre estate

Our experts strongly recommend that any organisation seeking to protect customers and agents from fraud in the contact centre should follow these critical steps:

1. **Understand your current environment**
   Set your fraud prevention strategy in the context of a wider cybersecurity strategy, starting with a thorough knowledge of your data ecosystem. Without this, in the event of an attack your technical team will be working in the dark and potentially exposing your network and services to more threats and greater damage as they try to solve the issue.

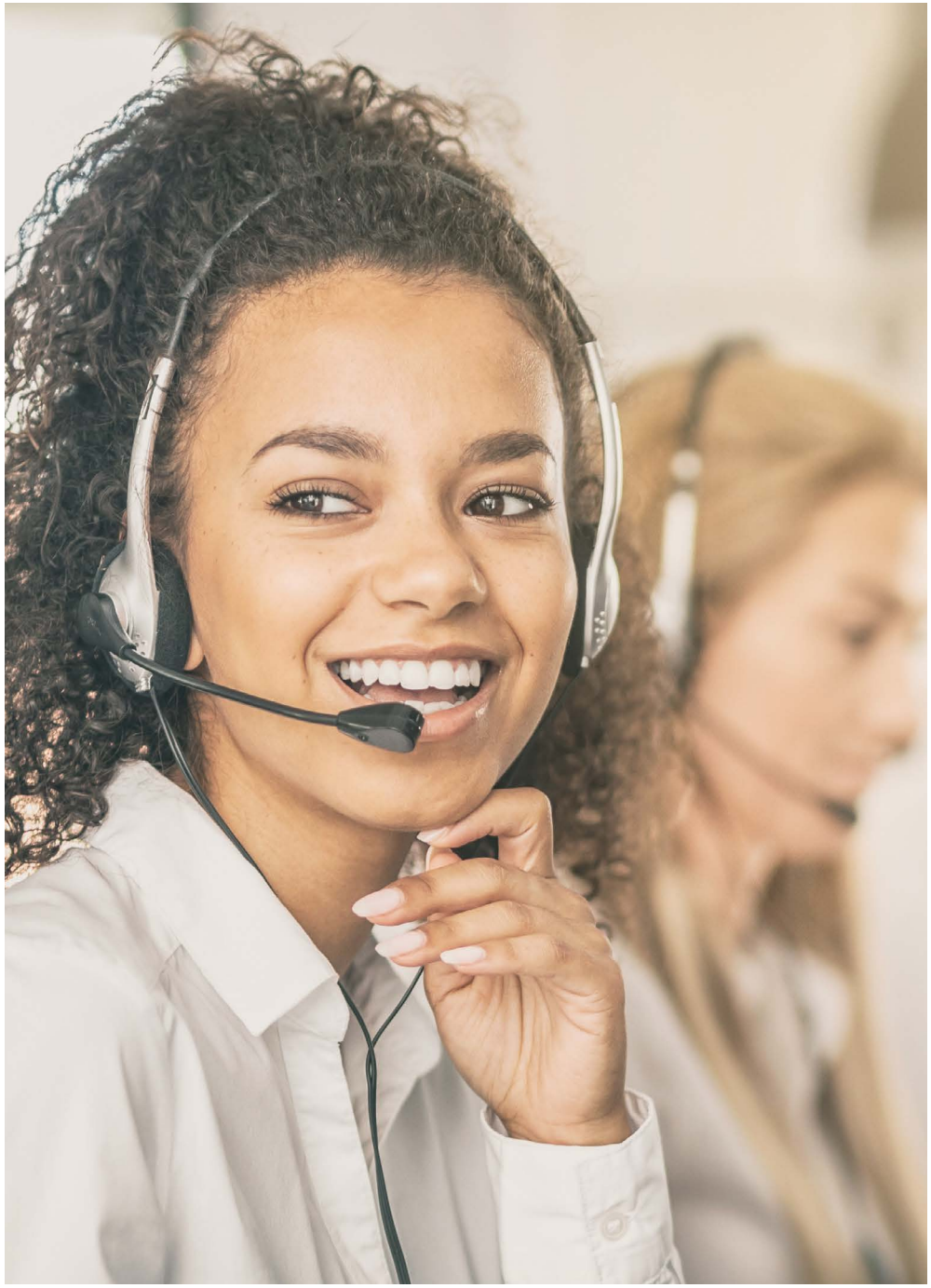
   Layer this insight on top of how your contact centre operates. Think about analysing call drivers, implementing call listening and working on identifying process and agent vulnerabilities to build the full picture of what optimal operations look like.



2. **Uphold data integrity and compliance for maximum security**
   As part of creating this secure context, review how you handle data. Always avoid capturing unnecessary customer data and consider a cloud access security broker to monitor access to all the data you have in the cloud. Without the right expertise onboard, you'll struggle to navigate the complexities of the regulatory landscape. Consult regional compliance advice and, if necessary, bring reliable experts in from elsewhere to support you through this process. Plus, explore how to incorporate data encryption and take additional steps to secure your call recording.

3. **Strengthen your human firewall**
   Humans and, more specifically, human error can be your biggest weakness. Help your agents appreciate the impact that organised fraud can have and make it easy for your people to do the right thing by strengthening your 'human firewall'. Support your agents with training so that they're on the alert for social engineering, and apply the same identification and verification standards used for customers to your remote agents. No matter how well trained they are, your agents are going to make mistakes, especially if they're stressed. That's why it's critical to find ways to take the pressure off by putting solutions in place that prevent fraud without relying on human perfection. AI-driven voice biometrics, for example, identify customers and fraudsters using the unique characteristics of their voice, freeing up your agents to focus on delivering high-quality, personalised service.

4. **Work with a trusted partner**
   It's critical to address these strategic points with the support of a fraud prevention technology partner. Look for one with a range of solutions that boost your security posture and improve the service you can provide. Confidence in your partner is key, so start by understanding who you're working with. The right partner should have the depth and breadth of expertise and experience to navigate you through the complexities of fraud detection and authentication, including how to stay up to date with all the latest industry regulations. Ask about their ability to integrate their solutions with current interaction channels, particularly how they enable intelligent IVRs and virtual agents with biometrics.



Why BT for security in the contact centre

Our detailed knowledge and experience of fighting fraud

We have a strong track record in helping customers defend their contact centres against telephony, card and online fraud. We use our wider security expertise to cover all potential aspects of attack, often seeing new threats emerging before they become entrenched problems, helping our customers to head off issues before they can do significant damage.

Our valuable partnerships and strong alliances

We have strategic partnerships with Smartnumbers and Nuance, which means we can integrate these solutions into any contact centre.

We understand customer experience

We don't just provide and implement technology – we understand the human context, too. We regularly conduct research into what people want when they deal with organisations and run this awareness throughout our practice. As a result, our contact centre security solutions work for the consumer, as well as the enterprise.

We take an industry-specific approach

We have experience in implementing solutions across every sector, working with customers who have to navigate even the tightest of security regulations. For example, we've been an active member of the banking and financial services industry for over 50 years. We work closely with the Financial Conduct Authority and financial regulators to shape policy and make sure our solutions always deliver risk and compliance outcomes that are fair, explainable and auditable.

Streamlining authentication and redirecting fraudsters with Smartnumbers Protect

Smartnumbers Protect is a contact centre solution that identifies suspicious callers before they reach the contact centre. This protects the IVR from reconnaissance and saves time verifying the identity of trusted callers, as well as reducing the risk of being defrauded.

The Smartnumbers solution determines each call's risk-score in real-time by analysing call signalling, caller behaviour and if it is associated with a confirmed fraudster already highlighted in the fraud database. High-risk calls can then be diverted to specialist teams while authenticating legitimate callers to create frictionless experiences for genuine customers.

The solution uses machine learning to keep on top of the tell-tale signs of changing fraudulent activity and is constantly learning about new tactics to stay one-step ahead of fraudsters.

Smartnumbers offers rapid authentication by verifying the authenticity of the number before they even reach an agent. Also, when the transactions become more complex and security more of a risk, it layers brilliantly with Nuance Gatekeeper to provide a multifactor authentication solution. This multifactor authentication approach increases IVR containment to increase customer self-service while further streamlining authentication for agent-answered calls. It ensures better experiences, reduced contact centre costs and considerably fewer risks.

Some of the key benefits of Smartnumbers Protect are:

- **streamline authentication**: rapidly answer legitimate customer calls by validating call authenticity before the call is even answered
- **reduced financial loss**: protect your contact centre from fraud loss and accurately identify suspicious callers before they speak with an agent or enter IVR
- **improved customer experience**: authenticate customers before answering to streamline their journey
- **reduce operational costs:** significantly reduce average hold times and agent call duration with quick recognition and escalation of trusted callers to self-service options in the IVR
- **evolving alongside fraudsters**: machine learning and behavioural analytics spot the changing tactics used by fraudsters to ensure you remain protected.

Smartnumbers in action: fighting financial fraud and streamlining authentication

The challenge

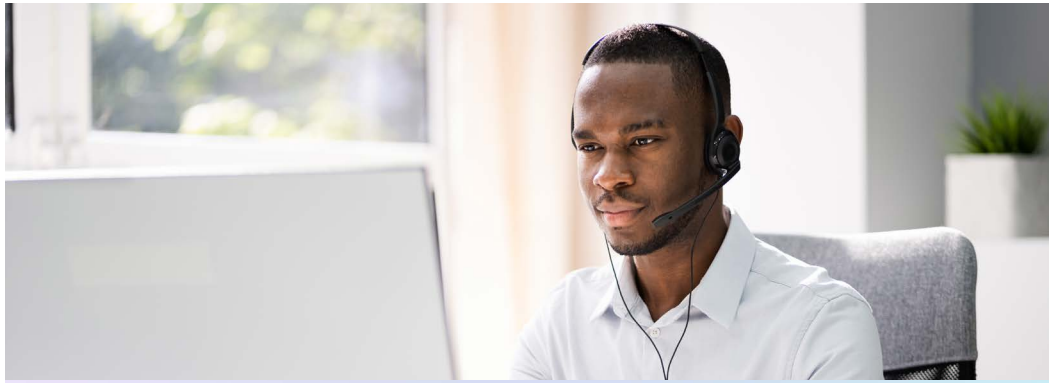
A bank offers its customers self-service through IVR. However, it discovered that its audio monitoring solution was insufficient for identifying fraudsters abusing the IVR to validate their compromised data, so it needed to improve both customer authentication and fraud prevention.

The solution

We helped the bank adopt Smartnumbers, to enhance its customer service strategy and reduce potential fraud losses. Now, when a potential customer calls, the solution provides the bank with a risk score to improve detection and reduce telephony and downstream fraud such as Authorised Push Payment (APP) and card fraud. The aim is to streamline customer journeys as well as cut operational costs throughout its multiple business units.

The result

Because of Smartnumbers, the bank has improved caller experience by 35-40% with the increase in the IVR containment and successfully reduced authentication times for agent-answered calls. This takes friction out of the customer journey while preventing card, online, telephony and APP fraud. As the bank continues its efforts in fighting fraud, it now views Smartnumbers as the solution for preventing fraud across the business and building better service delivery while strengthening customer relationships.



Customers using Smartnumbers report:

- typically a 20-30 second reduction in average handling time (AHT)[6]
- on average, a four times return on investment on fraud savings alone[6]
- a 10% increase on IVR containment[5]
- on average, 24p savings per call[5].

Authenticate customers and detect fraud with Nuance AI-powered solutions

Nuance Gatekeeper replaces outdated verification factors and reactive fraud prevention with seamless biometric authentication and intelligent fraud detection.

Through Gatekeeper, organisations can authenticate the actual person behind the device or on the other end of the phone, increasing trust in every interaction. Customers can use their voice as their password, eliminating the need to remember obscure information and allowing secure, frictionless authentication.

During an engagement, Gatekeeper analyses how a person sounds, how they talk or type, and how they behave, while checking their device, network, location and other factors for signs of fraud. Within seconds, powered by deep neural networking, Gatekeeper authenticates legitimate customers, flags suspicious engagements for additional verification and identifies known fraudsters.

Some of the key benefits of Nuance Gatekeeper are:

- **passive verification:** works in the background of interactions, authenticating from natural conversations with agents or speech-enabled IVR
- **increased agent satisfaction:** liberates agents to focus on helping, not interrogating individuals – 60% reported improved satisfaction[7]
- **faster customer service:** fast, reliable authentication takes customers quickly to their preferred destinations, reducing average handle times (AHT)
- **biometrics can't be forgotten:** no more remembering passwords, PINs, or security question answers. No need to update or reset a password
- **extremely difficult for fraudsters to defeat:** layers voice, conversational and behavioral biometrics to protect against spoofing, deepfakes, synthetic speech, and replay attacks
- **reduced costs:** biometric authentication slashes average handling time and increases self-service and containment in IVR and digital channels, further reducing costs.

Nuance in action: deploying passive authentication for major financial institutions

The challenge

One of the largest asset managers in the world was looking to authenticate their customers before they reach an agent. The aim was to eliminate the need for passwords and security questions to improve experiences and reduce overall costs.

The solution

Working closely with Nuance's experts, the company extended their Nuance voice biometrics solution into its IVR and tuned the system to authenticate callers from minimal voice utterances. Now, it identifies customers during their voice-controlled navigation of the IVR and helps agents know who a customer is and why they're calling before the conversation begins.

The result

Since deploying Nuance's voice biometrics for customer authentication across its contact centres, the company has enrolled more than 6.5 million customers and is achieving a 99% authentication success rate on live agent calls[8] — streamlining and protecting customer calls while reducing average handle time and other operational costs. Plus, passive voice authentication in the IVR makes customers feel recognised and welcomed by agents.

Customers using Nuance report:

- 99% authentication success rates[9]
- 90% detection of fraudsters in real-time[9]
- 0.5 seconds audio to authenticate a customer[9]
- 85% increase in customer satisfaction[10].

More than 80% of consumers view biometrics as the safest method for authentication[11].

A secure, satisfying experience for customers

Balance the risk of fraud with the importance of customer experience and start your journey to an end-to-end secure contact centre.

Get in touch with your account manager to talk through your contact centre requirements.

References

[1] ACFE, Fraud in the wake of Covid-19: Benchmarking Report, 2020
[2] CIFAS, Identity Fraud Surge 2021, 2021
[3] Aite Novarica, Improved Customer Experience, Reduced Fraud and Cost: Contact Center Solutions, 2020
[4] Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime, 2021
[5] Smartnumbers, Insight from Smartnumbers analysis of annual customer data
[6] Smartnumbers, UK leading retail bank improves customer experience while fighting fraud with Smartnumbers, 2022
[7] Nuance, Happy agents = Happy customers. How AI helps you augment live agent interactions, 2021
[8] Nuance, Cloud-native biometric security for every channel, 2022
[9] Nuance, Major financial institution deploys passive voice authentication in the IVR, 2021
[10] Nuance, Authenticate the actual person, 2022
[11] Experian, Experian's 2022 Global Identity and Fraud Report, 2022

Offices Worldwide

September 2022