Daon

4 Strategies for Protecting Your Contact Center

while saving money and improving customer experience

4 Strategies for Protecting Your Contact Center

while saving money and improving customer experience

4 Strategies for Protecting Your Contact Center

while saving money and improving customer experience

"Your call is very important to us..."

In the current business landscape, most organizations dedicate a significant portion of their budget toward protecting online assets—and rightly so. Not only is the frequency of digital threats growing, but the methods used to commit cybercrime continue to evolve, making combatting bad actors a constant struggle.

To make sure they aren't the subject of the next data breach or identity fraud headline, organizations are forced to prioritize and continuously upgrade their online security with the best technologies available on the market. In our zero-sum world of business investment, however, an increased focus on optimizing online security can leave other customer channels, most notably the contact center, forgotten and, subsequently, at risk. This often ends up meaning contact centers lag behind in not only security, but in efficiency and customer experience—a significant problem for two reasons.

First, it's widely accepted that a customer's perception of a business is heavily weighted toward the worst experience they've had with that organization. It's estimated that it takes as many as 10 exceptional customer experiences to erase the effects of a single negative one. When your customers have positive experiences online, but frustrating ones over the phone, their view of your organization in general can trend negatively. This is even more crucial when you consider that the contact center is where customers turn when they need a more personalized experience or cannot resolve an issue through digital channels.

Second, most fraudsters are savvy enough to exploit a business's least-secure channel. Most contact centers offer "the path of least resistance," making them vulnerable to an attack. In fact, Aite Group reports that 61% of organizational fraud losses can be traced back to the contact center.

Modern organizations need to refocus their technology investments, prioritizing the contact center as a key piece of both their security and customer experience strategy.

"It's estimated that it takes as many as 10 exceptional customer experiences to erase the effects of a single negative experience."

"Knowledge-based authentication, which includes passwords, pins, and security questions, has the dubious distinction of being the worst-in-class authentication strategy for both security and user experience."

Strategy 1: Empower Your IVR

A significant percentage of the calls handled by human contact center agents can be resolved quicker—and more cost-effectively—through an Interactive Voice Response (IVR) system. So what's preventing contact centers from containing all those calls within the IVR?

In most cases, it's security—or lack thereof. The majority of IVR systems use knowledge-based authentication (KBA), which includes passwords, pins, and security questions, and has the dubious distinction of being the worst-in-class authentication strategy for both security and user experience. Gartner estimates that, in some cases, KBA will reject 15-30% of legitimate customers and accept up to 60% of fraudsters. Even the least sensitive customer information cannot be entrusted to a security system with that kind of track record.

The good news is that a better solution—one that's simple to implement and exponentially more secure and user friendly—is available. Implementing **biometric voice authentication** into your IVR system provides the highest level of identity accuracy and can significantly expand the data access your organization can automate. And with frictionless passive authentication, once a customer is enrolled, they won't even know they are being authenticated.

You can contain more calls within the IVR, which translates to immediate cost savings, shorter wait times, happier customers, and agents that can focus their time on complex support cases that most deserve human expertise.

Active vs. Passive Voice Biometrics: What's the Difference?

With active (also known as text-dependent) voice biometrics, a customer enrolls a voice print by speaking a specific, short phrase. Then, to authenticate during future calls, they are asked to repeat the same phrase, which is biometrically matched to the voice print.

Passive voice biometrics is significantly more natural and requires no specific customer effort. Once a customer gives consent for their biometric template to be captured, it is automatically generated as the customer conducts their business, with the actual capture taking just a few seconds. Then, during future IVR or agent interactions, the customer's voice is automatically authenticated, in seconds, while the agent addresses their issue.

Strategy 2: Passive Voice Biometrics for Frictionless Interactions

While active voice authentication has the highest degree of matching accuracy and eliminates most of the user friction inherent with KBA, it still requires directed customer interaction, which creates a small amount of friction and requires the authentication take place in IVR. A failed match, while relatively rare, could also be a source of frustration since the customer is an active participant in the matching process and in dealing with an automated system.

Passive voice authentication remedies these issues. Once a user is enrolled, successful passive voice authentication is frictionless and adds no additional time to the call. In fact, the customer never even knows authentication is taking place.

Another benefit is that passive voice authentication improves in accuracy as it analyzes more speech samples. While it has the capability to authenticate a user during a brief IVR call, a lengthier, more conversational situation, like an interaction with a live agent, allows for a deeper analysis. As the conversation continues, the confidence percentage climbs, subsequently increasing the agent's comfort with sharing sensitive information.

Finally, by providing frictionless authentication at the onset of a call, step-up authentication for high-value transactions becomes less burdensome with passive voice authentication. From the customer's perspective, they are only required to authenticate once—and the value of that authentication is evident.

Strategy 3: Device-based Multi-modal Biometrics for a More Secure "Push"

While mobile devices are a key component of online security, their value in contact center fraud prevention is often overlooked. Many organizations are surprised to learn that the device their customer uses to call in with is key to creating truly secure contact center transactions.

Historically, authentication factors like PINs or security questions were the standard for call centers, due to the limitations of landlines. Now, in the U.S., only 37% of homes have a landline at all, and less than 2% have no mobile devices. In the UK, greater than 80% of contact center calls originate from mobile devices. The prevalence of advanced telecommunication technology has made it easy for businesses to move to more advanced and secure authentication techniques. The most secure of these is a push request for biometric authentication, which can use any of the biometric capabilities of the user's device—most commonly a fingerprint or face scan.

By pushing the request to the customer's device, you are technically using 2 authentication factors in a single action. Your organization is identifying that the customer is in possession of a registered device and then checking their identity against a biometric template. This can be taken to an even higher level of security if the push is to check the identity against a server-based template.

Strategy 4: Identity Continuity for Seamless Customer Experiences

The future of customer identities means providing simple, consistent experiences by establishing singular identities for each customer, ensuring no matter how they interact with your business, they are recognized and provided with the personalizations that keep them coming back. It also means making sure customers don't have to jump through any hoops to get the care they deserve.

This future is realized through **Identity Continuity.**

Identity Continuity is an approach to digital identity and access management where every phase of the customer journey exists on a single, cross-channel platform. Every customer establishes a single digital identity during their onboarding process and then uses that identity for access when interacting with any part of the organization (personal account, ecommerce, finance, support, etc.), through any channel (web, mobile device, phone, kiosk, service center, etc.). The result is that your customer can interact with your business at anytime, from anywhere, and is guaranteed the same high-quality experience.

Both customer experiences and business processes improve dramatically with the implementation of Identity Continuity. A singular view of your customer improves data security by consolidating all customer information in a single location, while the convenience of biometric identity proofing and authentication means that customers won't abandon transactions due to added friciton.

Today, modern organizations are only scratching the surface of what's possible through Identity Continuity, but the results have already been impressive. For instance, USAA, one of the world's most innovative and customer-attuned financial services organizations, uses Identity Continuity to seamlessly merge their mobile and contact center experiences. With one click, an in-app-initiated VoIP call connects the customer to a live agent without the need for further authentication, thanks to the multi-modal biometric authentication already embedded in the USAA mobile app.

Better yet, information about the user's recent behavior on the app helps silently route the call to the most appropriate agent, who then receives the complete contextual information on their screen, right next to the customer's verified identity and engagement history. Without a word, the live agent knows instantly who's calling, why they're calling, and even which app screen they're stuck on.

This may sound like the future, but Identity Continuity strategies like this one can be used now, behind the scenes, to help seamlessly bridge all the siloes in your multi-channel customer engagement structure—creating a single, seamless, and continuously evolving profile of your customer that extends from the contact center to mobile, desktop, IoT devices, and even kiosks or other physical locations.

ASK THE EXPERT

Jason Beloncik
Head of Solutions Engineering, Americas, Daon

Should I be concerned about the security and privacy of biometric data in the contact center?

"Daon specializes in privacy by design. Each of our client deployments features full lifecycle privacy and data protection, from design to deployment, use, and disposal. Our business systems and practices are built on privacy and a key focus of our technology is data protection. Our knowledge of global privacy requirements and experience provides valuable assistance with compliance mandates.

Device- and server-side deployments each have strengths and weaknesses. As a board-level member of the FIDO Alliance, Daon is naturally a strong proponent of device-side biometric authentication (in which private information never leaves a customer's personal device) for many use cases. That said, most of the contact center capabilities discussed in this eBook necessitate sending some quantity of personally identifiable information (PII) in transit for server-side biometric data processing.

Given that necessity, Daon takes extraordinary care to secure PII at all times using, among other tools, state-of-the-art encryption. In addition, Daon advises organizations to create anonymous biometric "templates" that are useless to hackers and fraudsters attempting to reverse-engineer personal records, eliminating the need to protect biometric PII.

Let us know the needs of your organization, and we'll help you devise a tailored deployment strategy that satisfies any and all of your unique privacy requirements."

BY THE NUMBERS

33,000 MINUTES OF CALL TIME SAVED

50% REDUCTION IN TRANSFERS AND CUSTOMER WAIT TIMES

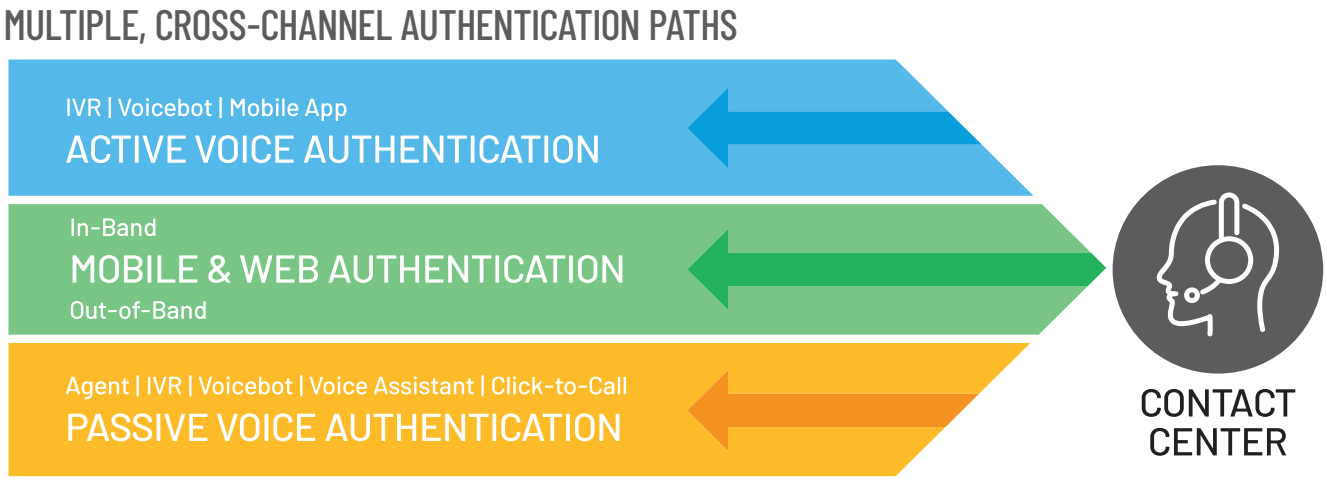
ZERO EVIDENCE OF FRAUD THROUGH THE MOBILE CHANNEL

Just three months into employing Daon's xVoice application on our IdentityX platform, the contact center in a large, US-based financial services institution reported 33,000 minutes of call time saved and a 50% reduction in both transfers and customer wait times. Perhaps even more impressive, the organization publicly stated that it has found zero evidence of fraud through the mobile channel since implementing Daon solutions.

Tailor and Combine Strategies to Fit Your Organization's Diverse Needs

The Bank Administration Institute reports an average loss of $1,653 per fraudulent call. Add that to the previously mentioned 61% of fraud coming from the contact center, and you have a scenario that creates an understandable sense of urgency. Still, it's important to avoid rushing into a single solution without considering the benefits of multiple products working together.

None of the solutions mentioned thus far are mutually exclusive. In most cases, they seamlessly integrate, creating identity strategies that transcend the individual solutions' capabilities. Savvy business leaders will recognize that meeting the needs of all customers requires solutions that maximize versatility while also minimizing fraud. To do this, employing a tool set that focuses on options is paramount.



Today's customers want control over their interactions with service providers. Allowing them to steer their own identity experiences is at the heart of building lasting brand affinity. The ability to offer this unparalleled level of flexibility is one of the reasons some of the world's most iconic brands put their trust in Daon to supply the technology for their digital identity efforts.

4 Strategies for Protecting Your Contact Center

while saving money and improving customer experience

While every contact center is operationally and financially unique, in nearly every use case, a biometric authentication solution can dramatically improve your business's bottom line by minimizing identity fraud, friction, and the total cost of operations in the call center.

Daon xVoice can help you prevent fraud losses, reduce your average call handle time by 25-45 seconds, complete more calls within IVR, and deliver markedly better customer experiences from any voice communication device, anywhere.

By adding the capabilities of Identity Continuity, you can build a single, central identity for each of your customers—across all channels and points of access—to create a seamless, convenient user experience and a clear point of visibility for your organization.

"Allowing your customers to steer their own identity experiences is at the heart of building lasting brand affinity."

To learn more about xVoice, the application central to our contact center solutions, visit

daon.com/xvoice

Daon®

The **Digital Identity Trust** Company