Daon®

4 Ways to Bring the Delight, Cost-Efficiency, and Security of Online Experiences to Your Contact Center

4 Ways to Bring the Delight, Cost-Efficiency, and Security of Online Experiences to Your Contact Center

"Your Call Is Very Important to Us…"

If you're like most organizations, you've come to embrace the "digital first" mindset, in which online customer interactions are prioritized, optimized, and continuously upgraded with the best security and usability technologies on the market.

Now is, truly, a golden age for digital customer experiences and transactions.

But there's a darker side to this story that isn't always acknowledged; in our zero-sum world of business investment, an increasing focus on optimizing online experiences has left other customer channels, most notably the contact center, more bereft of resources than ever.

If this is a golden age for mobile and desktop web, it's still a stone age for the vast majority of contact centers and their long-suffering customers, operators, and managers.

And that's a significant problem for two reasons:

First, customer-focused organizations know that trust and brand loyalty is built and sustained through the quality and consistency of multi-channel branded experiences over time. Hence, when your customers have pleasing experiences online, but then agonizing experiences over the phone, they come to view your organization, on the whole, as disjointed and unreliable.

Second, underserviced channels with obsolete technologies can lead to gaping security holes and vulnerabilities, and most fraudsters are savvy enough to quickly identify and exploit the least-secured channel in any multi-channel apparatus. Chances are, your contact center is "the path of least resistance" for hackers canvassing your organization. In fact, as companies have turned their attention to strengthening online channels, global call center fraud has increased by more than 45 percent over the past three years.

"Customer-focused organizations know that trust and brand loyalty is built and sustained through the quality and consistency of multi-channel branded experiences over time."

4 Ways to Bring the Delight, Cost-Efficiency, and Security of Online Experiences to Your Contact Center

Clearly, the time has come for customer-attuned organizations to realign their cross-channel strategies in ways that help propel contact center authentication experiences into the 21st century.

To help in this mission, here are four strategies successful organizations are adopting to bring the same delight, cost-efficiency, and security of their online experiences to that distant, final frontier—the contact center.

"Knowledge-based authentication (KBA), otherwise known as passwords and secret questions, has the dubious distinction of being the worst-in-class authentication factor from the perspective of both security and user experience."

Strategy 1: Active Voice Biometrics for Smarter, Safer IVR

It's a bitter pill to swallow that most of the calls reaching human contact center agents could have been resolved much more quickly—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. Knowledge-based authentication (KBA), otherwise known as passwords and secret questions, has the dubious distinction of being the worst-in-class authentication factor from the perspective of both security and user experience. In fact, Gartner estimates in some cases, KBA will reject 15-30% of legitimate customers while accepting up to 60% of criminals. With numbers like that, it's no wonder contact centers are so reluctant to trust even the least sensitive customer requests to their leaky automated systems.

But with the simple act of replacing KBA with active voice biometrics (a fast and easy upgrade that works "off-the-shelf" with most popular IVR systems), both the security and usability of your automated system can improve exponentially.

As a result, you'll contain more calls within the IVR, which translates to immediate cost savings, shorter wait-times, happier customers, and friendlier agents—who get to focus their time on the complex support cases most deserving of their human expertise.

How Do Active Voice Biometrics Work?

During the standard enrollment process, users are prompted to record a short audio phrase—or voiceprint. Subsequently, whenever they place a call to the contact center, they will be asked to speak this same phrase to confirm their identity. Biometric liveness technology then differentiates between a live voice and an audio recording (or a computer-generated synthetic voice). Because the spoken phrase itself is a constant, the voice biometric matching is extremely accurate and, in many cases, requires no additional authentication for most actions.

Strategy 2: Passive Voice Biometrics for Frictionless Live Agent Interactions

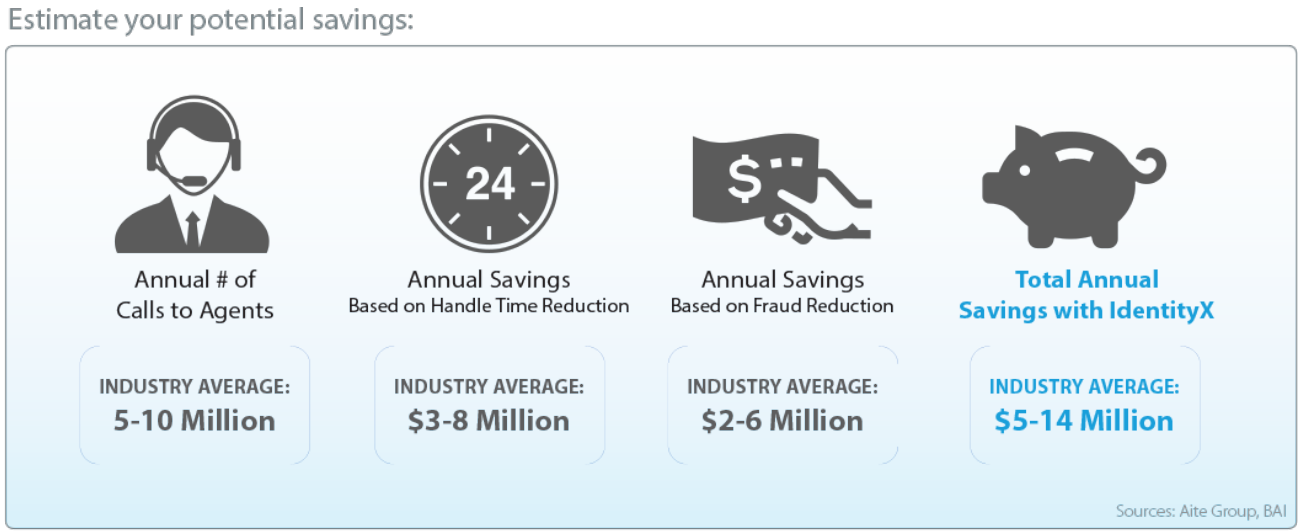
As previously mentioned, active (sometimes referred to as text-dependent) voice authentication, in which a user speaks the same phrase every time, has the highest degree of matching accuracy. On the other hand, text-independent voice authentication can be done passively (i.e., without bothering the user), which in many cases is the preferred customer experience.

The key to passive voice authentication is that it gets better as it goes. In other words, the more you speak, the more confidence the passive voice algorithm has that it's really you doing the talking. For this reason, passive voice biometrics are extremely well suited to lengthier, more conversational situations like interactions with a live contact center agent.

In this scenario, as a customer describes their reason for calling, the agent is receiving a voice-based identity confirmation—with increasing levels of confidence—in real time.

If, for some reason, the voiceprint cannot be verified, the agent is notified to take an additional verification step, which could include either a device-based biometric "push" authentication (the kind we'll describe in the following section) or a traditional KBA.

The art of step-up authentication is to create the minimum possible friction commensurate with the risk introduced by a customer's intended actions. Today, with passive voice biometrics, many of the lowest-risk transactions can be authorized without any customer friction whatsoever.



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

Comparing the technological capabilities of a landline phone with a smartphone or desktop computer is like comparing a live contact center agent with a potted plant. So it stands to reason looking for ways to utilize the advanced capabilities of these web-enabled devices makes good business sense in any channel, including (naturally) the contact center.

Devices, particularly smart mobile devices, are increasingly becoming the lynchpin of cross-channel customer journeys—and with good reason. But the problem with overreliance on state-of-the-art smartphones and computers is that not everybody has one. And the "capabilities gulf" that separates the oldest from the newest devices on the market today is massive and often seemingly insurmountable.

As a result, organizations feel forced to find the lowest common denominator for device-based authentication—often a one-time password (OTP) delivered via text message that's a) far too easy for fraudsters to intercept, and b) at best an authentication of the device, not the user.

Device-based biometrics solve this problem. Better yet, an open, all-inclusive platform for device-based biometrics (like Daon's IdentityX) brings state-of-the-art biometric capabilities to even the oldest smartphones.

In our contact center scenario, the IVR or live agent leverages this capability by sending a biometric authentication "push" to the customer's mobile or desktop device while the call is ongoing. The customer chooses their preferred biometric factor (face, fingerprint, voice, even palm recognition), and the agent is notified instantly of the match or non-match.

Strategy 4: Cross-Channel Continuity for Truly Magical Customer Experiences

Now here's where the real fun begins.

When a customer interacts with your brand, she wants you to see her as a single person with a single, consistent identity profile—not multiple, separate profiles in stovepipes. Otherwise, she'll be treated like a friend in one channel but a stranger in another, or she'll be forced to restate the same problem multiple times, which is both frustrating and patently unnecessary.

4 Ways to Bring the Delight, Cost-Efficiency, and Security of Online Experiences to Your Contact Center

Solving this problem requires a model we call Identity Continuity—the process of consolidating a lifetime of disparate, cross-channel identity interactions into a single, seamless view of the customer. Furthermore, orienting your cross-channel strategy in this manner lets you personalize and continuously optimize the customer experience, regardless of when, where, how, or why an interaction takes place.

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, truly 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 her screen, right next to the customer's verified identity and engagement history. Without a word, the live agent knows instantly who's calling, why she's calling, and even which app screen she's stuck on.

In the very near future, Identity Continuity strategies like this one will work behind the scenes to help seamlessly bridge all the many stovepipes 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.

USAA By the Numbers:

In just its first three months using Daon's IdentityX, USAA's contact center reported 33,000 minutes of call time saved and a 50% reduction in transfers and customer wait times. Perhaps even more impressive, USAA has publicly stated that it has found zero evidence of fraud through the mobile channel since implementing IdentityX.

33,000 MINUTES OF CALL TIME SAVED | 50% REDUCTION IN TRANSFERS AND CUSTOMER WAIT TIMES | ZERO EVIDENCE OF FRAUD THROUGH THE MOBILE CHANNEL SINCE IMPLEMENTING IDENTITYX

Daon®

Jason Beloncik, Head of Solutions Engineering, Americas, Daon

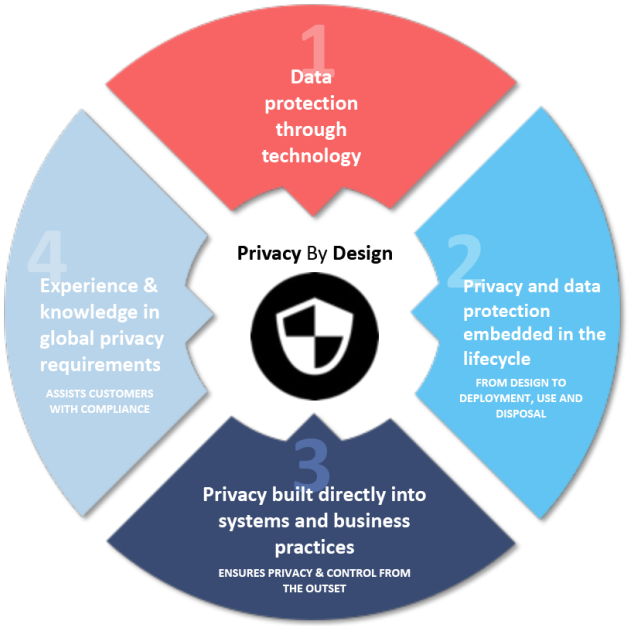
Ask the Expert:

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

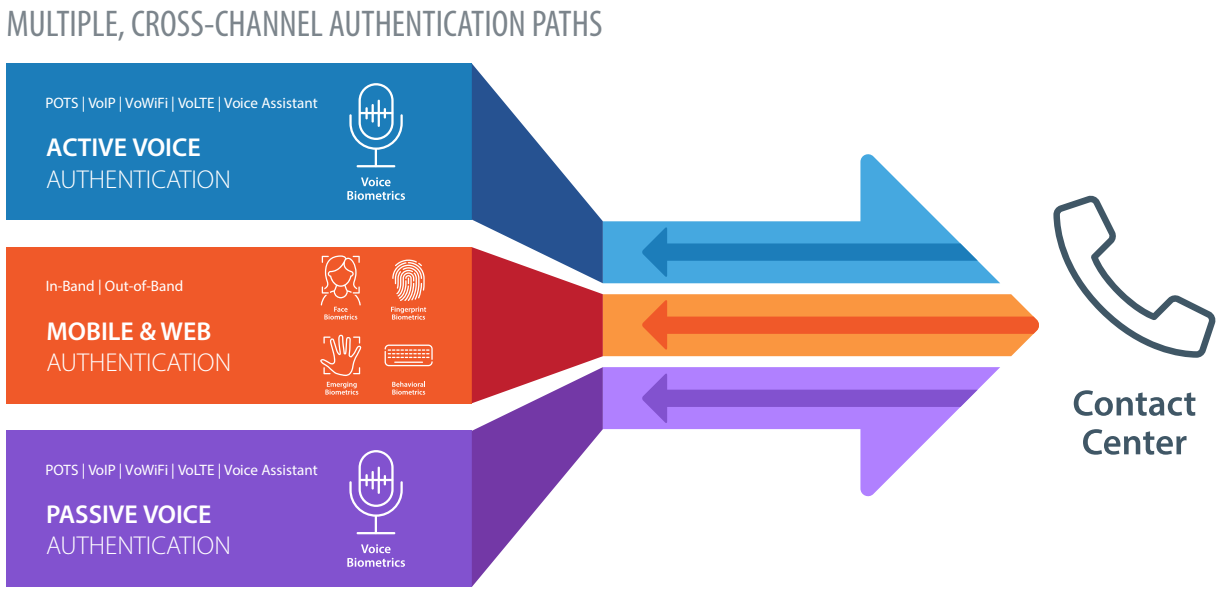
A: *"Device- and server-side deployments each have strengths and weaknesses. As a board-level member of the FIDO Alliance, Daon is naturally a strong proponent of device-side biometric authentication (in which private information never leaves a customer's personal device) for many use cases. That said, most of the contact center capabilities we've 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 this PII at all times using, among other tools, state-of-the-art encryption methods. In addition, Daon advises organizations not to retain biometric PII for any length of time, and to instead create anonymous biometric "templates" of the data that work for matching purposes but are utterly useless to hackers and fraudsters attempting to reverse-engineer the personal records. In doing so, organizations can immediately delete the biometric PII from their systems so that they need not worry about protecting a honey pot of personal data.

Daon also specializes in Privacy by Design, having implemented four layers of privacy into each of our client deployments (data protection through technology; privacy and data protection embedded in the lifecycle, from design to deployment, use, and disposal; privacy built directly into systems and business practices to ensure privacy and control from the outset; and experience & knowledge in global privacy requirements to assist customers with their compliance mandates). 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."



Daon®



Don't Pick One:
Tailor and Combine Strategies to Fit Your Organization's Diverse Needs

Given the urgency of this problem (according to Aite Group, 61% of organizational fraud losses can be traced back to the contact center, and the Bank Administration Institute reports an average loss of $1,653 per fraudulent call), one might reasonably decide to grab a single strategy and run with it.

But this would be a mistake.

Perhaps the most enticing feature of the four methods covered in this eBook is their ability to fit together seamlessly in the service of a multi-faceted, versatile solution that transcends its individual pieces. Such is the reason why, for instance, most savvy organizations aren't putting all their eggs in the passive voice authentication basket, or even voice authentication more broadly. Indeed, it's a fair bet that any organization now choosing to rely on a single strategy, technology, or authentication modality will face a painful reckoning in a matter of years if not months.

Furthermore, it has been roundly demonstrated that giving customers an array of choices and the ability to steer their own identity experiences is at the heart of building lasting brand affinity. Hence, many of the world's most iconic brands have leveraged the unrivaled openness and inclusiveness of Daon's IdentityX platform as a central component of their identity infrastructures—with new and ingenious use cases emerging all the time.

Every contact center is undoubtedly unique, as are your organization's requirements. But in nearly all cases, a biometric-based multi-modal platform solution for the contact center can dramatically improve its bottom line by minimizing fraud, friction, and the total cost of operations.

By bringing seamless, multi-modal biometrics to your customers, agents and IVR, Daon's IdentityX platform helps you prevent fraud losses, reduce your average handle time by 25-45 seconds, contain more calls within IVR, and deliver markedly better customer experiences from any phone, anywhere.

And don't forget to explore Identity Continuity both within and without the contact center for a single, central view of your customer across all channels and encounters.

To see how these and other strategies work first-hand, please visit **daon.com/request-a-demo** for a personalized tour of today's most delightful (and secure) contact center experiences.

"Giving customers an array of choices and the ability to steer their own identity experiences is at the heart of building lasting brand affinity."

Daon®