CCW CUSTOMER CONTACT WEEK DIGITAL

SPECIAL REPORT:

CONTACT CENTER SECURITY, AUTHENTICATION & FRAUD PREVENTION

AUTHOR: BRIAN CANTOR

August 15, 2018

NUANCE

FEATURING INSIGHTS FROM:

Brett Beranek

General Manager of the Security Business

Nuance Enterprise Division

Deb Brown

Manager, Individual Exchange & Direct to Consumer Customer Response Unit

Guardian Life Insurance Company of America

TalkTalk For Everyone

BARCLAYS WEALTH

Eastern Bank

SPECIAL REPORT: CONTACT CENTER SECURITY, AUTHENTICATION & FRAUD PREVENTION

Some refer to the contact center as the gateway to customer centricity. It is the point at which the brand achieves meaningful, lucrative connections with customers.

Fraudsters have a different perspective. They view the contact center as an opportunity for exploitation. It is the security weakness they can leverage for their nefarious intentions.

Many organizations underestimate the extent of this vulnerability.

As a result of the knowledge gap, increasingly sophisticated attacks and operational shortcomings, the contact center is under siege. Fraudsters are targeting contact centers, substantially hurting organizations, employees and customers in the process.

How should businesses respond?

The quick answer is not as simple as simply investing more heavily in security. Many security solutions and strategies are inefficient and ineffective. They subject organizations to enormous costs, while actually rendering the contact center *more ripe* for attacks.

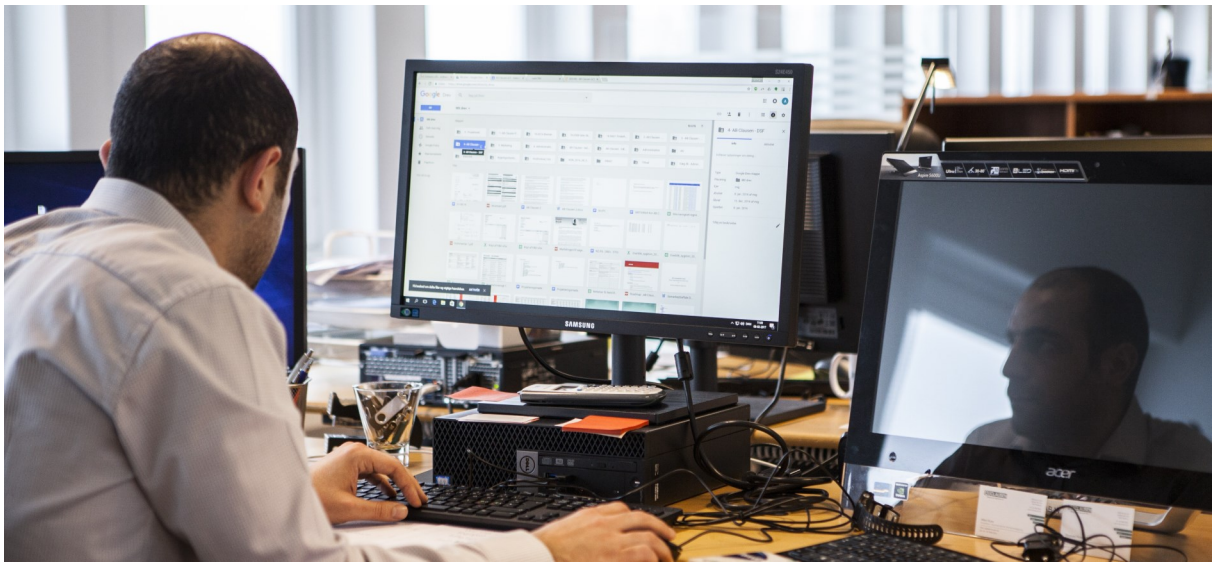
Worse, they often come at the expense of the customer and agent experiences. Customers and agents endure delays, frustration and generally unpleasant interactions without even getting the benefits of added security.

This report uncovers the *correct answer*: successfully blending authentication and fraud prevention. It explores visions, strategies, processes, technologies and measurements for more accurately authenticating customers, more successfully thwarting fraud and more effectively engaging with customers.

After exploring a set of imperatives for a customer experience security initiative, the report considers security through two key lenses: what are the truest demands of today's customers and what are the most debilitating challenges facing today's businesses?

It closes by revealing the philosophical and practical transformations that will improve security, optimize contact center performance and actually generate value for agents, customers and the overall business.

CX AUTHENTICATION & FRAUD PREVENTION: SIX IMPERATIVES



The foreword to this report highlights an unfortunate reality: not all organizations are presently in a position to successfully secure their customer experiences.

When working to remedy the issue, organizations must meet six imperatives. These pivotal steps create the framework on which a great, effective, customer-centric security strategy can be developed.

Acknowledge the problem

It goes without saying that properly authenticating customers and successfully defending against fraud are important objectives. Organizations are decidedly less clear, however, on the *severity of threats* to those goals as well as the *unique vulnerability* of the contact center.

To drive meaningful action, leaders must properly acknowledge and communicate the urgency of the matter. They must position sophisticated fraud attempts as a matter of when rather than if.

They, moreover, must understand how contact center people, processes, technologies and objectives exacerbate the challenge. By developing that understanding, they will truly recognize the need for meaningful transformation.

Defend every touch point

Today's customers are engaging in multiple channels, which means they are communicating personal information in multiple channels. It also means fraudsters have more touch points at which to levy attacks.

A robust authentication and fraud prevention strategy must account for this reality. Organizations must address security from an omnichannel perspective. Process design, initial authentication and ongoing monitoring must be equally robust—and wholly unified—across all channels.

> Because fraudsters don't limit themselves to a single interaction channel, fraud prevention needs to span all channels, including digital and voice," recommends Brett Beranek of Nuance.

Deliver a more customer-centric experience

At its core, security is about protecting *customers*. Achieving that security at the expense of customer satisfaction is, accordingly, counterintuitive.

When developing protections for the contact center, organizations must vehemently consider the impact on the customer experience.

> Authentication and fraud prevention are a priority, but they don't need to take place at the expense of friction, effort and CX," declares an encouraging Beranek.

Create an exceptional employee experience

The customer is not the only party involved in a service interaction. When developing authentication and fraud prevention initiatives, it is essential to account for the other party: the agent.

There are two elements to consider when accounting for the impact on agents. First, the organization must ensure agents are empowered to do their part in defending the customer experience. It cannot allow operational issues or training lapses to render agents vulnerable.

The organization must also ensure its security measures are not hurting the agent experience. Happy, productive agents are the key to a great contact center, and the organization cannot allow security to compromise either. Its authentication and fraud prevention efforts will, ideally, *boost* agent engagement.

Unite the organization

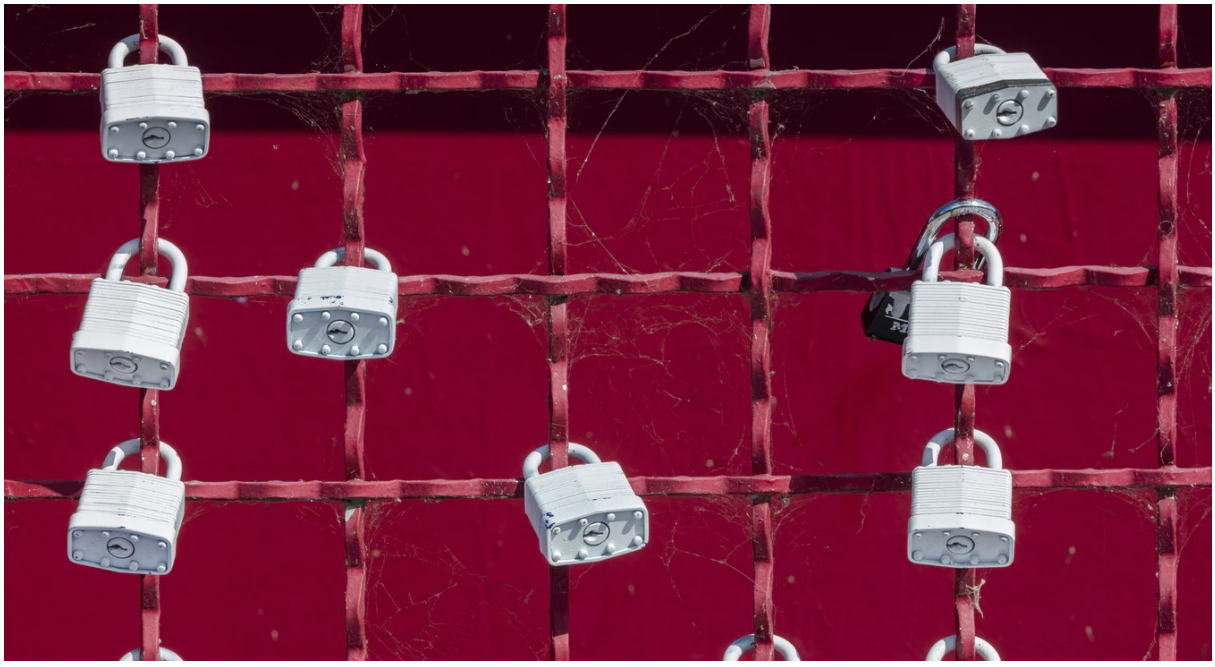
Chief Information Security Officers (CISOs) understand fraud. Customer contact leaders understand the customer experience. Key executives understand the financial stakes of security breaches and bad customer experiences.

It, therefore, behooves organizations to provide each entity a seat at the security table. Through this alignment, the organization can set the most appropriate objectives, consider the most likely challenges, and generate the most effective action.

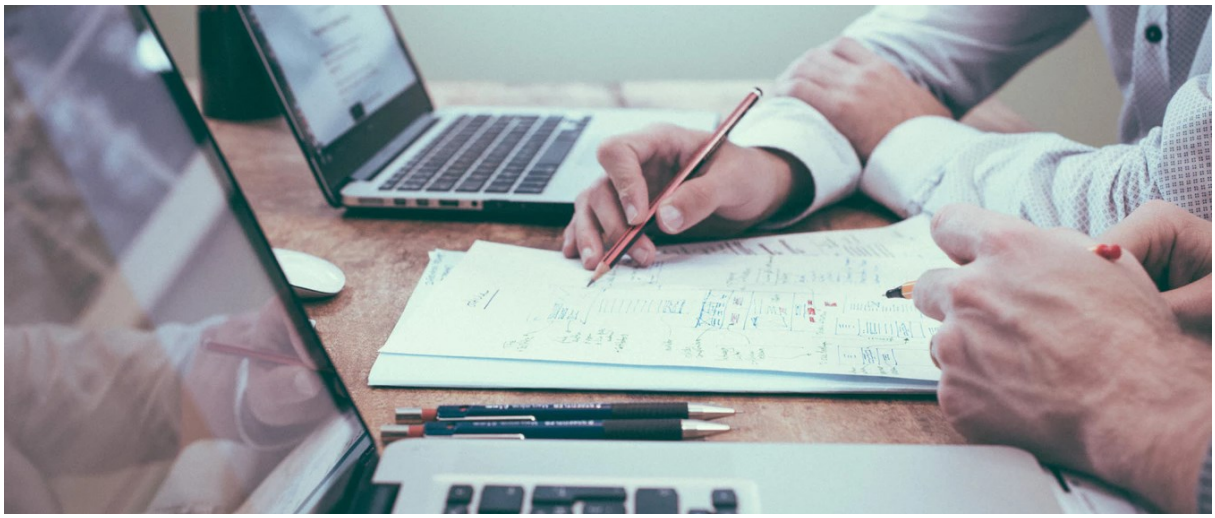
> CISOs are responsible for fraud prevention while contact centers own CX," details Beranek. "CISOs focus on digital channels and are less familiar with contact center voice services and concepts like CX, CSAT, etc. To provide the best levels of security, including authentication and fraud detection/prevention, CISOs and contact center leadership needs to partner.

Create a multi-dimensional security strategy

Never appropriate in the era of customer centricity, a "set it and forget it" mentality is particularly problematic in a fraud prevention context. Fraudsters are creative and relentless; they will not stop because they hit one firm line of defense in one particular scenario. To truly transform and secure the customer experience, the organization must adopt a multi-tiered, continuously evolving approach to authentication, fraud prevention and monitoring. If customer data is ever in play, the organization must have an ability to identify and eliminate any threats.



AUTHENTICATION THROUGH THE CUSTOMER'S EYES



On the one hand, security is a fundamentally customer-centric endeavor. While the specific parameters may be defined by laws and regulations, the ultimate goal is to protect customers from the nefarious desires of fraudsters and other criminals.

Customers, in fact, demand security. CCW Digital research reveals that eighty-two percent of customers actively value enhanced authentication measures during at least some brand interactions.

On the other hand, some security initiatives *undermine* customer satisfaction. Some measures complicate the interaction process, in turn leading to frustration for customers—and the agents tasked with serving them. While other measures may avoid that complexity, they do so at the expense of security. Customer data remains vulnerable, and customer confidence evaporates.

Operating in the era of customer centricity, today's businesses know they must compete on the customer experience. To win that competition, they must devise an authentication and fraud prevention strategy that simultaneously creates exceptional interactions and demonstrates bulletproof security.

To achieve that best-of-both-worlds scenario, they must account for several realities.

Customers expect personalization

Customers are not necessarily demanding intimate conversations, but they absolutely expect brands to *know* them. They loathe repeating personal information during interactions with businesses, and they value tailored conversations that produce uniquely relevant resolutions.

Business leaders recognize this demand. They, in fact, identify personalized interactions as the #1 sign of customer centricity.

To deliver these interactions, organizations must gather, store, and leverage specific, personal data about customers in all channels. Agents will need to access this information when providing support. Customers, meanwhile, will aim to access and modify this information within self-service environments.

With personally identifiable data always in play, effective authentication and fraud prevention measures are essential.

Customers are demanding fast, frictionless experiences

Personalization may be important, but it pales in comparison to the demand for fast, frictionless experiences. If given the choice between reducing effort or increasing personalization, 80% of customers would choose the former.

A simple interaction that yields a fast resolution is, in fact, the #1 customer demand.

This demand for easy, efficient interactions presents a clear ramification for security: the slower and more complex the authentication process, the less satisfying the experience.

While 82% of customers theoretically value enhanced authentication, 68% would only accept slower processes in particularly high-stakes scenarios.

Granted, customers do hate falling victim to fraud. They still wholeheartedly expect the business to protect their personal data.

Organizations, accordingly, must overcome a pivotal dilemma when building their security strategies. How can they create a protocol that is seamless and simple for customers yet still bulletproof against fraud?

> “The customer wants something that’s easy and simple for them to use, so that they actually get their query resolved or go through to the right agent or service first time,” says Sarah Bramwell of TalkTalk.

The dilemma is markedly more challenging for organizations that face regulatory requirements.

> Automated authentication is something that we are looking into to make it less onerous on the consumer," says Deb Brown of Guardian. "How can we do that and still not put ourselves at risk [from a compliance perspective]?

Customers are increasingly fearful of fraud

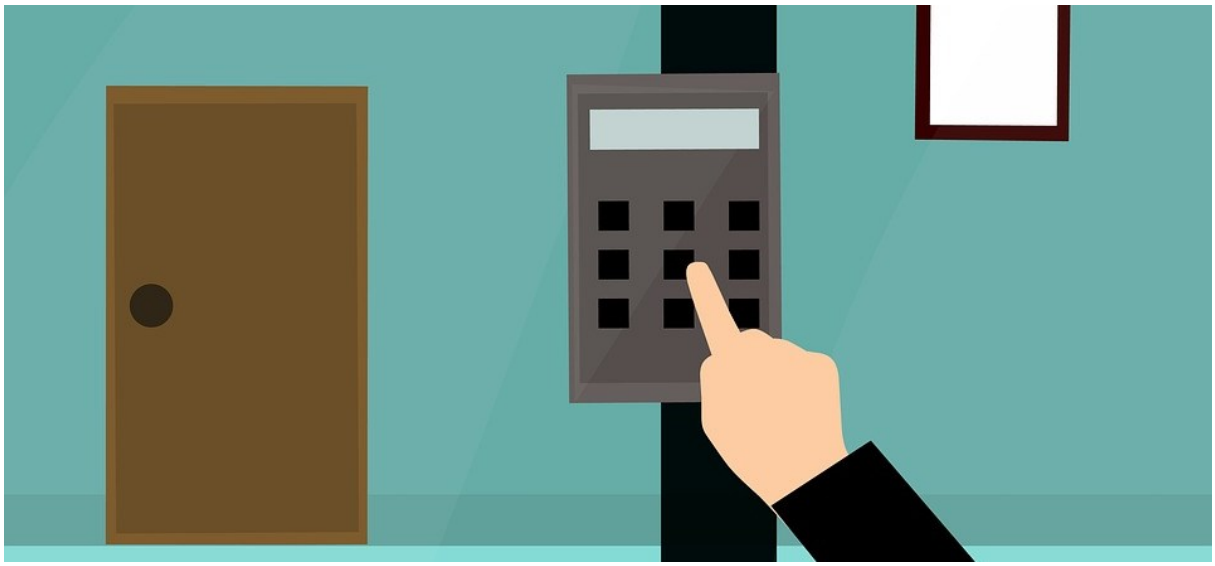
Technology professionals know that digital interactions are often more secure than voice conversations. For customers, however, the digital revolution underscores the vulnerability of their data.

It bombards them with the reality that specific information about their identities and finances is sitting in a database that can, theoretically, be accessed and exploited.

The string of recent headlines about data misuse and fraud only compounds that fear. These horror stories educate customers on the vulnerability of their data and, in turn, drive them to demand heightened security measures from their businesses.

Indeed, fraud prevention is an experiential demand in its own right. Customers cannot take security for granted; they require businesses to demonstrate firm, unwavering commitment to defending the experience.

AUTHENTICATION: LIMITED BY BUSINESS REALITIES



Forced to account for growing security threats without hindering the experience for customers, all organizations face an exceedingly daunting challenge.

Within many organizations, operational limitations serve to exacerbate the security challenge. The very way they choose to manage their contact centers (including the agent behaviors and customer interactions within those contact centers) inherently cripples efforts to bolster security.

Before pursuing stronger authentication and fraud prevention measures, organizations must break free of these restrictive business realities.

Organizational silos

Operational misalignment is the #1 performance challenge, #1 technology issue and #1 source of agent frustration.

Unsurprisingly, it is also a major bottleneck on security initiatives.

Given their different areas of expertise and focus, information technology and customer experience professionals predictably approach authentication and fraud prevention from different vantage points. IT and security professionals may have a better grasp on the overall idea of protection, but they lack the CX team's familiarity with agent and customer demands. If these groups do not work in concert, the organization will be unable to optimally balance security and customer centricity.

Additional fragmentation may also exist *within* the customer experience function. Many organizations isolate the traditional voice "call center" from digital channels. They may also divide the different engagement functions—sales, marketing, support, billing—into separate teams. As a consequence of these fracture points, the organization cannot establish a consistent, omnichannel approach to security. Some channels will be more vulnerable, giving criminals an access point for exploiting customer data.

Incorrect vision

Some organizations treat security measures as “necessary evils.” They are ways to mitigate corporate risk, limit liability and prove compliance. They are not sources of value for the organization.

Insofar as organizations do not fully appreciate the growing volume and magnitude of threats **(35% do not even view customer data protection as a priority)**, this complacent, cost-conscious mindset becomes easier to justify.

Organizations will, as a consequence, resist making heavy investments or sweeping changes. They will rely on the conventional approaches that seem to work well enough.

Reliance on conventional methods

The problem is that conventional methods do not work well enough. Traditional identity and verification (ID&V) methods, such as PINs or passwords, are the epitome of an ineffective, inefficient contact center practice. They subject *actual* customers and agents to slow, frustrating processes, while giving savvy fraudsters a legitimate shot at crossing the line of defense.

> The world has changed, and contact centers are at a crossroads,” says Beranek. “Traditional identification and verification is no longer effective because data breaches have rendered PINs, passwords and personal information virtually useless.

These ineffective processes, moreover, create a troublingly false sense of security. Aware that it has authentication measures in place, the organization will refrain from continuously monitoring and protecting against fraud. Criminals that break the initial line of defense are thus afforded carte blanche to do damage.

“Plug and play” mentality

The aforementioned two factors—a dismissive approach toward security and irrational confidence in conventional authentication measures—contribute to a problematic “plug and play” mindset. Organizations should not reduce customer experience security to a series of disparate steps and solutions. As long as they implement compliant, promising authentication and fraud detection platforms in their experiences, they believe they are creating a secure environment.

This mindset leaves organizations vulnerable. Fraudsters are always developing new skills and constantly looking for new ways to exploit customer data. If organizational stakeholders are not constantly monitoring all pieces of the experience journey and constantly collaborating to improve security measures, they expose themselves to future risk.

> The majority of fraudulent transactions occur in authenticated interactions," notes Beranek. "Contact centers must have integrated authentication and fraud prevention strategies to be successful. They can't have one or the other.

Vulnerable agents

Capable of forging empathetic, emotional connections, human agents are uniquely valuable to the customer experience. They are also uniquely vulnerable to fraud.

While agents may receive basic training about authentication and fraud prevention, they rarely become experts on the subject. They certainly do not amass as much knowledge as the most sophisticated data criminals.

Leveraging their expertise and clever social engineering practices, these criminals can take advantage of agents to gain access to personal customer data. They recognize humans as a weakness.

The redundancy of conventional authentication creates additional problems. Due to the repetitive nature of the process, agents may become complacent and unfocused. In turn, they become vulnerable to even unimposing attacks.

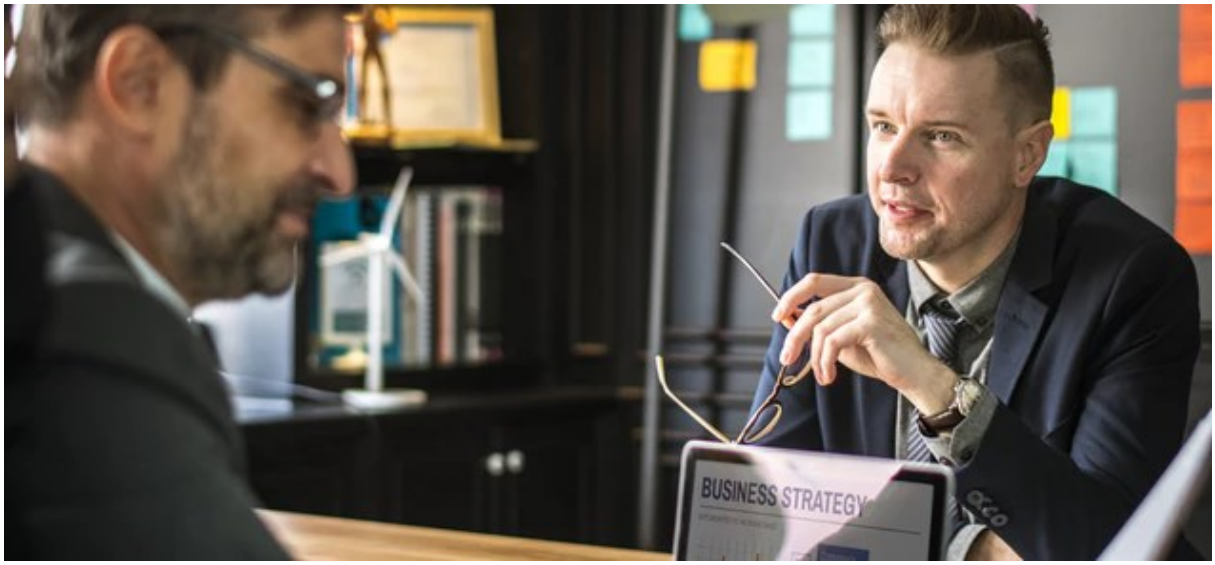
Conventional authentication measures also create a broader employee engagement issue. By forcing agents to spend time focusing on repetitive, mechanical tasks, organizations risk reducing agent satisfaction. The fear associated with security issues may compound that dissatisfaction.

Agent-led authentication efforts also come at the expense of productivity.

> Call times increase as agents become focused on investigation, rather than assistance," explains Beranek.

It is important to note that these increases in call times will not yield any additional value for the business. Agents make their impact when supporting customers rather than when leading security. The time they spend authenticating a customer is time they should be spending actually helping someone.

STRENGTHENING AUTHENTICATION & FRAUD PREVENTION



Securing the customer experience is an active pursuit. It is not enough to merely eliminate strategic and systemic roadblocks; the organization must also take action to elevate all facets of its security program.

With a revised vision for protection, the use of modern technology, improved training, and a more quantitative approach to monitoring, the organization will attain a heightened, more customer-centric form of security. More importantly, it will allow itself to continuously improve its authentication and fraud prevention efforts.

Establish a customer-centric security objective

While it is nice to assume all stakeholders will instantly see the value in collaboration, reality does not work that way. Departmental leaders tend to be set in their ways—and fixated on their own objectives.

To combat this resistance, executive leadership must target those objectives. If the technology team and contact center are suddenly held accountable for improving security *and* customer-centricity (across engagement channels), the notion of collaborating becomes much more logical and intuitive.

The modified objective may not eliminate all organizational silos, but it will ensure all customer contact functions and all business departments are united in their effort. It will turn customer-centric security into an organizational pursuit, thus eliminating the blind spots and inconsistencies that emerge in a more fragmented organization.

Optimize security by monitoring for risk

Not every interaction is equal—or equally risky to the business.

Savvy organizations take advantage of this reality. By understanding their customer journeys and evaluating the potential risk associated with each interaction, they can take the right security measures at the right time. They can use deep, multi-layered authentication for high-stakes interactions, while allowing simple, low-risk calls to more immediately reach the “engagement” phase. They can also focus their fraud prevention strategies on the riskier calls.

The result will be an optimized experience for both customers and the business. Customers will not have to endure any more effort than is absolutely necessary to secure their particular interactions. Agents, meanwhile, will have a clear sense of which interactions may require additional scrutiny. No longer over-authenticating, these agents will become more productive.

Leverage multi-modal, multi-layered biometrics to successfully authenticate

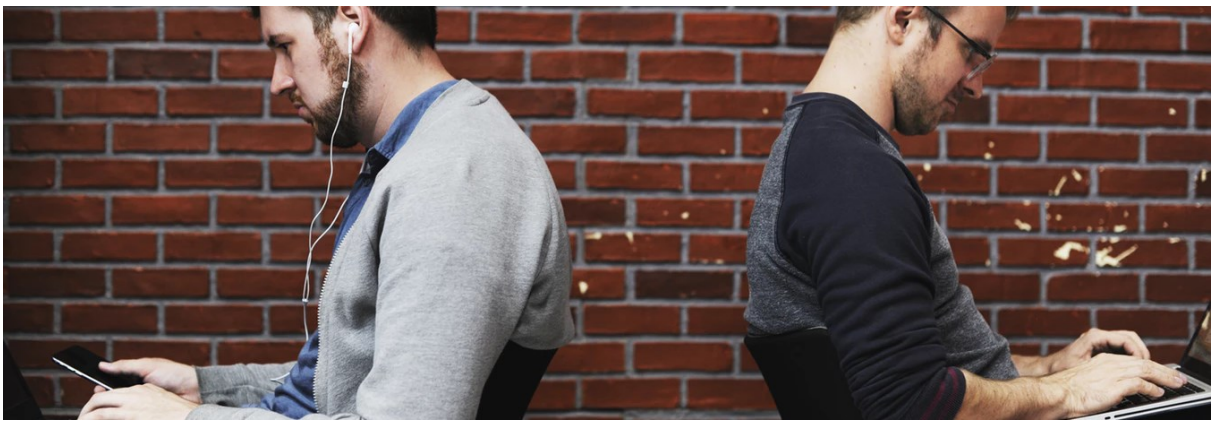
Not every risky interaction is equal—or taking place in the same context.

Because the voice channel is the attack vector of choice for fraudsters, it is critical to fortify defenses with voice biometrics. Organizations should nonetheless consider additional security measures to cover the broader omnichannel journey. A customer traveling on a crowded train, as an example, may prefer to authenticate using a selfie rather than a voice password.

Using voice and multi-modal biometrics technology, an organization can accommodate these preferences. It can maintain a highly secure, highly reliable authentication process while also accounting for customer preferences and convenience. It, most importantly, can implement the authentication process in all channels.

Depending on the particulars of the industry and the interaction, the organization may also want to implement a multi-layered form of biometrics authentication. This markedly strengthens security, but insofar as it is still automated, organic and seamless, it does not markedly increase customer effort or frustration.

The biometrics process also accounts for the agent experience. By eliminating a redundant task, biometrics technology helps agents focus on the work they prefer to do—and tend to do better. And insofar as the automated authentication is more effective, the agent experience gain does not come at the expense of security.



Pair authentication with fraud prevention

As a more reliable means of authenticating than traditional ID&V methods, multi-modal biometrics will provide a much firmer line of defense against fraudsters.

In the unlikely event that fraudsters circumvent these defenses, post-interaction behavior can still help organizations understand how to up-level security in the future.

Collectively, the factors justify a simple best practice: from an operational perspective, organizations must pair authentication with fraud prevention.

Strategies for the two should be operated in tandem. Employees should be trained to spot and defend against opportunities for fraud throughout the journey. Systems, moreover, should be capable of blocking criminals at every conceivable touch point.

Biometrics assists in creating this synergistic, persistent approach to security. Voice and other identification biometrics can authenticate customers at the onset of the interaction, while behavioral biometrics can detect suspicious behavior at later stages of the interaction.

Prepare agents for success

Agents are generally not well-suited for security, which explains why automated options are so valuable.

The idea that they can be completely eliminated from the security process is not, however, consistent with reality.

With the contact center under siege and agents representing the Achilles heel because of their susceptibility to social engineering, conversations are always facing a conceivable risk. They, moreover, are always great platforms for learning about weaknesses and opportunities within the experience.

Consequently, organizations will greatly benefit from coaching agents on security. By training them to identify riskier calls, spot warning signs and more promptly take action in the event something seems amiss, the organization turns agents from a weakness into a strength.

Measure success

As a consequence of their complacent attitude toward authentication and fraud prevention, many organizations fail to properly assess and scrutinize their efforts. They know when major compliance violations or data breaches occur (or when customers complain), but they do not have granular, day-to-day insight into the success of their programs.

That needs to change. In order to make sure their tools are working to protect their customers, organizations must establish a robust monitoring effort, as well as clear, intermediate success metrics. How many would-be fraud attempts are being thwarted? How many false negatives are arising due to the enhanced security program? How are factors like talk time and agent productivity changing as a result of automated authentication?

REDEFINING AUTHENTIFICATION & FRAUD PREVENTION

When crafting authentication and fraud prevention strategies, there is a noteworthy tendency to focus on compromises and balances.

Organizations think about how to protect data without significantly hurting the customer experience. They focus on bolstering authentication measures without dramatically reducing agent productivity. They aim to protect against the cost of fraud without meaningfully spending on authentication and fraud prevention efforts.

If executed in accordance with the best practices detailed in this report, an organization will be able to achieve those optimal balances. They will secure their customer experiences without compromising their ability to perform.

There is no reason to stop there.

Leading organizations recognize that security is not merely a way to mitigate risk; it is a way to generate positive value.

The customer satisfaction opportunity

When done right, authentication and fraud prevention create a best-of-both worlds scenario for customers.

Organizations that leverage contextual, automated solutions like biometrics enable customers to confirm their identities in the quickest, most convenient, most comfortable way possible. They can move right to the heart of the interaction: resolving their problem.

By deploying heightened authentication measures within digital and self-service channels, the organization also gives customers a greater ability to handle matters on their own terms. This further reduces effort (customers do not have to wait to speak to a live agent) and further increases satisfaction (customers feel that their preferences are being honored).

These experiential benefits come alongside—rather than at the expense of—stronger security. Robust, biometrics-driven solutions do not simply make authentication easier; they make it better.

Ultimately, organizations should view enhanced security measures as a way to improve the overall customer experience.

The benefit is not simply theoretical; organizations are truly improving their experiences through automated, biometrics-driven authentication.

TalkTalk, for example, reports a reduction in authentication time by 80%, as well as a 1-minute decrease in handle time.

> “Voice biometrics allows our customer to get service in the most natural and intuitive way, through their voice,” adds Bob Rivers of Eastern Bank. “The end result is a better and more effortless experience for our customers.”

> “In our implementation of voice biometrics, we focused on the clients and carried out some really valuable focus groups to understand the issues,” details Iain Hanlon of Barclays Wealth and Investment Management. “We found that between 7 and 10% of customers calling in were actually being rejected by the security processes, prior to voice biometrics. We ran some client satisfaction surveys after the implementation and clients rated the service at least 9 out of 10 in all cases, which translated into a customer advocacy rating of 60%—a significant uplift on our previous ratings.”

The agent satisfaction opportunity

By taking the burden of authentication off agents' plates, organizations can dramatically increase workplace satisfaction. Employees will neither face the stress of worrying about security nor the burden of going through a convoluted authentication process.

They will simply get to focus on what they do best: connecting with customers.

When done right, an authentication and fraud prevention strategy positively impacts every relevant employee metric. Performance will be stronger, while satisfaction, retention, engagement an advocacy will be higher.

> Over 65% of calls are now verified by voice biometrics and instead of having to wait two to seven minutes to be verified, the opportunity is now there to have a much better conversation with customers earlier in the experience," says Paul Scales of Barclays Wealth and Investment Management. "A big positive result is that we've had a 90% reduction in complaints regarding our security service since we've implemented voice biometrics.

> What we've found with our clients is that agents embrace the voice biometrics technology for two reasons," reveals Beranek. "1) In many cases, it eliminates the need for agents to interrogate callers. 2) It allows agents to focus on what they do best: engage and support customers as efficiently as possible.

The personalization opportunity

When confident in its authentication measures, an organization can collect and process meaningful customer data at all touch points.

As a result, it can personalize the customer experience. Aware of the individuals they are supporting, agents and self-service platforms can *instantly* tailor conversations to customers. They can also seize opportunities for additional value, such as delivering relevant, proactive support, sales and marketing messages.

Bad authentication measures take personalization off the table. Lacking confidence in their security measures, organizations may refrain from collecting data—and thus render personalization impossible—in some cases.

In other cases, agents will spend so much time authenticating that there is no way to efficiently personalize the conversation. By the time the "support" part of the interaction begins, the agent has no choice but to rush to resolution.

The branding opportunity

With tales of data loss, misuse and exploitation dominating news cycles, security is top-of-mind for today's customers.

Organizations that can demonstrate an unwavering shield against fraud and data breaches, accordingly, stand to generate a considerable competitive advantage.

Rather than hoping potential customers will take security for granted, these organizations can attract customers who actively care about security.

With so many brands competing on the customer experience—and so many boasting similar core service "experiences"—security represents a fresh, immensely valuable way to achieve differentiation.

Illustrating the branding opportunity, Virginia Credit Union is an example of an organization touting its success in leveraging biometrics to improve security and reduce fraud without hurting the customer experience.

Per an official statement, the financial institution redesigned "its authentication strategy, while maintaining a personal, high-touch experience for each member… The service, which is free to members, can be used to verify a member's identity without requiring the typical list of security questions."

The initiative has yielded a 24% reduction in talk time, while thwarting 5,000 calls that did not match the voice record on file.

AN OPPORTUNITY WITH A THREAT

As a result of its clear, obvious security vulnerabilities, the contact center is under siege. Fraudsters know they can finesse their way past voice channels and their human gatekeepers—sometimes without much effort—and exploit the data these organizations are supposedly collecting in the name of customer centricity.

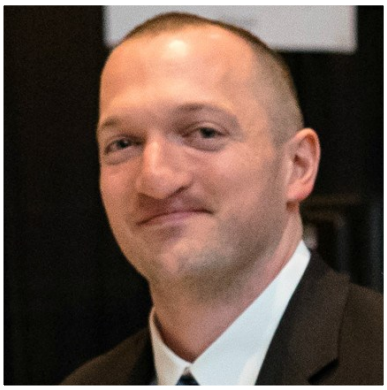
Organizations, consequently, have no choice but to take action. They have no choice but to educate stakeholders on the importance of security and develop comprehensive strategies for combating the threat.

Their lack of choice does not, however, mean organizations have to view security as an unfortunate, unavoidable cost. They can, instead, view it as an opportunity.

Better security is valuable in its own right—it offers a distinct, marketable advantage in an environment overflowing with competition.

It, moreover, produces meaningful improvements on the customer and agent experience fronts. It, in essence, offers an opportunity to accomplish the objectives customer-centric leaders truly want to be completing.

MEET THE AUTHOR



Brian Cantor

Principal Analyst, CCW Digital Director
Customer Management Practice

#CCWDIGITAL

Brian Cantor is the principal analyst and director for CCW Digital, the global online community and research hub for customer contact professionals. In his role, Brian leads all customer experience, contact center, technology and employee engagement research initiatives for CCW Digital's series of reports. CCW Digital's articles, special reports, commentaries, infographics, executive interviews, webinars and online events reach a community of over 150,000.

A passionate advocate for customer centricity, Brian regularly speaks on major CX conference agendas. He also advises organizations on customer experience and business development strategies.

leader by Wilson Joseph from the Noun Project; Traffic Light by Amy Stuart from the Noun Project; lightbulb by Maxim Kulikov from the Noun Project

2018 Special Reports Calendar

Special Reports Calendar is subject to change.
Updated as of 8/15/18

Publish Date	Report Topic	Sponsorship Deadline
Jan. 2	2018 Predictions	**Dec. 15, 2017**
Jan. 16	Retail CX	**Dec. 20, 2017**
Feb. 1	Omnichannel	**Jan. 18, 2018**
Feb. 15	Messaging	**Feb. 1, 2018**
Mar. 1	CX Automation	**Feb. 15, 2018**
Mar. 15	Customer Intent	**Mar. 1, 2018**
Apr. 2	Brand Reputation	**Mar. 16, 2018**
Apr. 17	Outsourcing	**Mar. 30, 2018**
May 1	Customer Contact Executives	**Apr. 13, 2018**
May 15	Customer Journey Mapping	**Apr. 27, 2018**
Jun. 1	Agent Performance	**May 18, 2018**
Jun. 15	Self-Service	**Jun. 1, 2018**
Jul. 1	FP3 Experience	**Jun. 15, 2018**
Jul. 15	Learning & Development	**Jul. 2, 2018**

2018 Special Reports Calendar

Special Reports Calendar is subject to change.
Updated as of 8/15/18

Publish Date	Report Topic	Sponsorship Deadline
Aug. 1	Actionable Analytics	**Jul. 19, 2018**
Aug. 15	Contact Center Security, Authentication & Fraud Prevention	**Aug. 1, 2018**
Sep. 4	The Digital CX	**Aug. 21, 2018**
Sep. 17	Chatbots	**Sep. 3, 2018**
Oct. 1	Outbound & Proactive Engagement	**Sep. 18, 2018**
Oct. 15	Remote Agents	**Oct. 2, 2018**
Nov. 1	Future Workspaces	**Oct. 18, 2018**
Nov. 15	Knowledge Management	**Nov. 2, 2018**
Dec. 3	Live Chat	**Nov. 16, 2018**
Dec. 17	CX Automation Pt. 2	**Dec. 3, 2018**

SPONSORING A SPECIAL REPORT:

LEAD SPONSOR
(LIMITED TO 1)

A senior executive from your company will be interviewed by one of our CCW Digital Analysts. These thoughts and comments will be incorporated throughout the report. Your executive's analysis will be inserted into the final copy. Your company logo will be on the front page of the report.

BRANDING SPONSOR
(LIMITED TO 2)

Your company logo will be on the front page of the report.

INTERESTED IN SPONSORING? CONTACT US AT INFO@CCWDIGITAL.COM

UPCOMING EVENTS

Customer Experience Automation
September 5-7, 2018
Embassy Suites Milpitas, San Jose, CA
www.customerexperienceautomation.iqpc.com

CX Week Canada
September 12-14, 2018
The Radisson Admiral Harbourfront
Toronto, ON, Canada
www.cxweekcanada.iqpc.com

CCW Online: The Blueprint for the Customer Experience
September 25-26 2018
Register for FREE
register.customercontactweekdigital.com/ccwfallonline/

CCW Austin
October 9-12, 2018
Renaissance Austin Hotel, TX
www.customercontactweekfall.com

Service Design Week
October 15-18, 2018
Hilton Boston Back Bay, MA
www.ccoexchange.iqpc.com

Chief Customer Officer Exchange
November 4-6, 2018
Hotel Colonnade, Coral Gables, FL
www.servicedesignweek.iqpc.com

CCW Executive Exchange
December 2-4, 2018
Hotel Colonnade, Coral Gables, FL
www.ccwexecexchange.iqpc.com

MEET OUR ANALYSTS

Brian Cantor

Principal Analyst &
CCW Digital Director

Michael DeJager

Principal Analyst,
Experience Design Series

Max Ribitzky

Head of Commercial
Research

Nadia Chaity

Senior Analyst, CCO Series

Sandy Ko

Research Development
Analyst, CCW Series

GET INVOLVED

Ben McClymont

Business Development Director

E: Ben.McClymont@customermanagementpractice.com

Simon Copcutt

Head of Strategic Accounts

E: Simon.Copcutt@customermanagementpractice.com