



UNIFY HOW 
YOU VERIFY

HUMANIZE + OPTIMIZE **THE WAY YOU RECOGNIZE** **EVERY CUSTOMER + CONTACT**

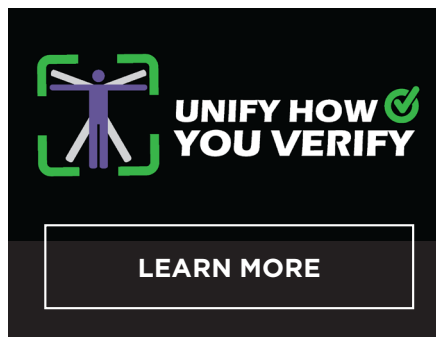
*Using Frictionless Biometrics Across All
Channels of Engagement*

Strategic Brief | November 2021





INTRODUCTION



Unify How You Verify is an important research initiative by the CMO Council and BPI Network, conducted in partnership with Daon, a global leader in identity assurance technology. It explores the critical role of authentication and identity verification in building better customer experiences and trust in today's digitally connected economy. This includes highlighting the value and importance of cross-channel identity assurance and the use of biometrics for customer onboarding and authentication.

In October, as part of this initiative, we issued an initial report based on the findings of a survey of 2,000 consumers in the United States, Canada, the United Kingdom and Ireland. Called *Authentication Frustration: How Companies Lose Customers in the Digital Age*, the findings demonstrate the critical need to address consumer demands for simplified and secure authentication.

Our new report, *Making Customer Help More Human: The Race to Secure the Omni-Channel Interface*, looks more deeply into what companies can do and are doing to improve the digital experience around authentication and identity protection. Our findings are based on both consumer survey data, and in-depth conversations with 12 leading executives and experts across security, identity, digital experience and marketing. We would like to thank the thought leaders below for their participation.

LEADERSHIP BOARD

MIKE GAMBLE

TSB
Digital Experience Leader



SUMEET GROVER

Alliant Credit Union
Chief Digital Officer



JAIRO OREA

Royal Caribbean
Chief Information Security Officer



SRIDHAR KOTAMRAJU

Goldman Sachs
Global Head of Fraud, Transaction Banking



NIAMH BYRNE

Layer
Chief Marketing Officer/
Digital Experience Leader



BILL GUINN

Serviceaide
Chief Technology Officer



ANDREA LINEHAN

CurrencyFair
Chief Marketing Officer



STEVE WILSON

Constellation Research
Senior Security + Identity Analyst



DWIGHT FLENNIKEN

Sunwest Bank
Chief Marketing Officer



CONOR WHITE

Daon
President of Americas



SHAWN JOHNSON

Concentrix
VP of Business Services
Sales and Customer Support Transformation



GENEFA MURPHY

Five9
Chief Marketing Officer



IMPROVING DIGITAL EXPERIENCE

It's a fundamental truth of doing business today: Digital experience now lies at the heart of your company's relationship with its customers. Since the onset of the global Covid pandemic, consumers have been forced to flock to digital channels of transaction and interaction. Now there's no turning back.

Yet far too many customers today say their digital experiences are less than satisfying. A recent study by the CMO Council, entitled "How Covid Has Changed the Channels of Engagement," found almost three quarters of consumers say they reevaluate their relationship with companies when they encounter frustrating digital experiences.

Executives and experts interviewed for this strategic brief recognize that digital authentication and customer onboarding represent a critical element of today's customer experience — and often one that causes friction, security concerns and dissatisfaction. Authentication and identity verification are a now major focus for improving digital experiences.

For the vast majority of our executive panelists, biometrics plays a major role in the effort to simplify and secure the future of identity verification. Executives say biometrics are rapidly becoming accepted by both customers and security experts as safer and easier to use than past methods of customer authentication and onboarding. Used in combination with other often password-less, front-end and back-end techniques, biometrics is helping deliver the seamless digital experiences most consumers are clamoring for.

“Authentication should be a top concern for executives focused on the customer and digital experience.”

Geneva Murphy, Chief Marketing Officer
Five9



Yet, executives also agree that identification verification will remain a moving target in the coming years. Sophisticated hackers and fraudsters will continue to develop new technologies and strategies to steal identities and data. Security and other business leaders will need to continue to stay ahead in this ongoing arms race.

Our research clearly demonstrates that, in today's digital-first economy, customer onboarding and authentication must become a board-level and C-level concern. Companies need to take action to simplify and strengthen customer authentication or risk losing customers.

“There needs to be someone thinking about customer experience in every organization. You might think that authentication is chiefly the concern of the CISO and security team, but it shouldn't be,” says Geneva Murphy, CMO at Five9, a leading cloud contact center platform

provider. “This really needs to be the concern of a chief customer officer or chief digital officer who is continuously thinking about removing friction from the digital experience and making sure that across every touch point you’re making it as easy as possible to authenticate and move users through customer journey in a seamless way.”

AUTHENTICATION FRUSTRATION WILL COST YOU CUSTOMERS



***6 in 10
consumers
have abandoned
a transaction
because of
Authentication
Frustration.***

The rapid rise of digital channels, combined with an equally dramatic increase in identity theft, account break-ins and fraud, is driving the need for businesses to modernize, streamline and fortify authentication and identity assurance.

While digital business was already on growing rapidly, the forced march into a digital-first world during the Covid pandemic has accelerated the timeline for many companies to create more seamless and satisfying digital experiences.

For too many consumers, the process of customer onboarding and authentication is major area of digital frustration. How you establish, verify and protect identities increasingly will make or break your relationship with customers. Unequivocally, consumers are demanding that authentication be highly trustworthy and secure — but also as simple and consistent as possible. In many cases, they will leave your brand if the experience is too challenging.

Our own research verifies this point of view. A survey we conducted in September of 2021 of 2,000 consumers in the United States, Canada, the United Kingdom and Ireland shows that customers overwhelmingly desire and demand more simplified, consistent and secure authentication processes. As outlined in our report, “Authentication Frustration: How Companies Lose Customers in the Digital Age,” frustration with difficult and time-consuming identity verification is causing customers to abandon transactions and look for other digital experiences.

Some 61 percent of consumers say authentication frustration has caused them to quit a transaction they would otherwise have completed. In addition, some 81 percent say they prefer to do business with companies that make authentication easy and safe. And 85 percent report that a difficult authentication process reflects negatively on a company, with 53 percent saying it has a “major” or “significant” negative impact.

Not surprisingly, consumers are particularly fed up with passwords as an authentication method.

“The easiest way to improve customer satisfaction scores is ease of resolution.”

Shawn Johnson, Vice President
Concentrix



Our survey found that the top frustrations with password include keeping track of too many passwords (55 percent), needing to recreate passwords (43 percent) and being forced to strengthen them (33 percent).

Most consumers want to get what they need from a digital interaction in very short period of time. Some experts estimate consumers expect to be able to access a transaction or other interaction in as little as 15 seconds, according to Jairo Orea, chief information security officer at the Royal Caribbean Group. If the authentication process requires 15 seconds or a minute, “you’ve lost them,” says Orea, who has also held CISO and senior information security roles with Kimberly-Clark, United Health Group and ING. “Simplifying access is key.”

Customer satisfaction scores, such as CSAT and Net Promoter Scores (NPS) are often used to measure customer attitudes toward customer support. “It’s not rocket science,” says Shawn Johnson, VP of Business Services Sales and Customer Support Transformation for Concentrix, a leading global provider of customer experience (CX) solutions and major customer support outsourcing and solutions company. “The easiest way to increase your CSAT is ease of resolution. That’s why we want to remove unnecessary barriers in authentication and other processes.”

THE TRUST FACTOR

Ease of use, of course, is not the only issue of concern to customers and businesses. Companies face a raft of increasingly strict regulatory requirements around privacy and data protection. These run the gamut from GDPR in Europe, the PCI standard in the payment card industry and the California Consumer Privacy Act, to Know Your Customer (KYC) and Anti-Money Laundering requirements in banking. Compliance with these standards is helping drive the need for stringent security around authentication and identity.

However, consumers themselves are another major driver for change. As digital interactions continue to grow, consumers have become increasingly sensitive to and aware of the dangers of identity theft and account break-ins.

“There is a big push on the consumer side to have better protections in place as people see hacking and other fraud activities on the rise and understand these threats are now a daily fact of life in the digital world,” says Niamh Byrne, CMO of Layer, a fintech leader based in Ireland

that provides a digital banking platform and solutions for banks, credit unions and insurance companies.

Consumer attitudes and concerns about authentication are evolving. Consumers were initially worried about their wallets and credit cards. Now they're increasingly concerned about identity theft and data privacy, says Orea.

Johnson believes consumers should be particularly concerned when using knowledge-based authentication methods that ask the customer to provide personal identity information. "So sitting out on the web is the make, model and year of my first car, the name of my first pet and my mom's maiden name. I have to give that information to satisfy the security requirements of different companies. I know it's only a matter of time before one of those places get hacked."

“Consumers are increasingly concerned about identity theft and data privacy.”

Jairo Orea, CISO
Royal Caribbean Group




Royal Caribbean Group



BIOMETRICS TO THE RESCUE

All of the executives interviewed for this report agree that biometrics should and will become a core standard for identity proofing and authentication, especially in highly regulated industries and high-value transactions. Facial, fingerprint, voice and behavioral recognition are simply safer and easier to use.



Consumer acceptance and preference for biometric authentication are growing rapidly

Customer acceptance of biometric authentication is growing rapidly. Indeed, our consumer poll shows that people overwhelmingly prefer biometrics over passwords and other forms of authentication. When asked if they believe biometrics are an easier and better way to verify one's identity, 44 percent of respondents said "absolutely." Another 34 percent said "yes, as long as it is more secure." Only 10 percent said they preferred passwords or other forms of authentication over biometrics.

While not all consumers will fully embrace digital, the vast majority will, and biometrics will be key to that experience, says Mike Gamble, director of analysis & design at TSB, a large retail and commercial bank based in the U.K. "There's

very little that a customer will access without using some form of biometrics. It's a natural extension to their banking. If banks were the only ones asking you to look at your phone when logging in, that might be something of an outlier. But people are doing that all the time to access devices and different applications. It's become basic hygiene."

"I think this (biometrics) will become the norm at some point," says Dwight Flenniken, CMO of Sunwest Bank, which is and continues to integrate biometrics into its digital experience. "The goal is always to make security better while making security features easy to use. We also need to worry about the privacy of our users. There has to be balance between privacy and security."

"The mobile phone is becoming a digital passport."

Mike Gamble, *Digital Experience Leader*
TSB



Biometrics integrated with the mobile phone is rapidly becoming a major facilitator in delivering more frictionless authentication experiences. Gamble says TSB can rapidly and securely onboard customers using their mobile phones. New customers take a picture of their passport or driver's license and then holds the phone in front of them to make a short video selfie, in which he or she moves their head and speaks.

The mobile app then provides seamless access to a variety of banking services. TSB also recently launched live chat within its mobile app so that customers can now move from a

digital to a human interaction within the app. In addition, the bank is developing the capability for customers to use their mobile phone to call the bank and speak with someone while automatically being authenticated by the phone.

"The mobile phone is becoming your passport, your gateway into TSB," says Gamble.

UNIFY HOW YOU VERIFY

A major source of customer frustration with identity is the lack of continuity across digital and nondigital channels. Many companies treat identity as a standalone event, using a different method of verification in each channel.

"Part of consumer frustration stems from inconsistencies in authentication within different channels in the same company," says Byrne. "For example, opening up your banking application with a fingerprint on your phone is seen as non-invasive and welcome protection," she says. "But that same customer may experience a lot of friction from the same bank when they're making an online payment. I think authentication frustration partially comes from the fact that different authentication methods are being used in different areas of the same company. Some experiences are really easy and welcomed, but others are too difficult."

Conor White, President Americas for Doan, a global leader in identity assurance technology, believes that identity continuity needs to be a core objective for businesses in the digital economy. He believes companies need to look for a single platform that integrate authentication across every channel and interaction.

“As a consumer, I want my bank to understand me, to know me and have continuity with me. I don’t want a different system, a different experience when I’m using my mobile app than when I’m contacting the call center. Consumers want continuity across all of their interactions with a company, across authentication factors, and across time. They want a compelling experience that is consistent and unified,” White says.

Sumeet Grover, Chief Digital and Marketing Officer at Alliant Credit Union, concurs. “Companies need to simplify and unify. Today there are many points solutions. These can create a very disjointed and inconsistent experience without solid oversight. Cross channel integration and unification are critical to both improving the customer experience and improving security.”

Because Alliant is a branchless credit union, digital is core to the customer experience. “Our members expect us to provide a very secure, frictionless experience from when they open an account to when they return to use it ongoing. They let us know when we’ve failed, so we have to constantly monitor and adjust accordingly,” says Grover. While some Alliant customers still prefer to use passwords, the credit union is increasingly integrating biometrics, device registration and multi-factor authentication into its identity verification processes.

“‘Identity Continuity’ is essential to today’s digital experience.”

Conor White, Daon President of the Americas



“Companies need to simplify and unify authentication and identity management.”

**Sumeet Grover, CDO and CMO
Alliant Credit Union**



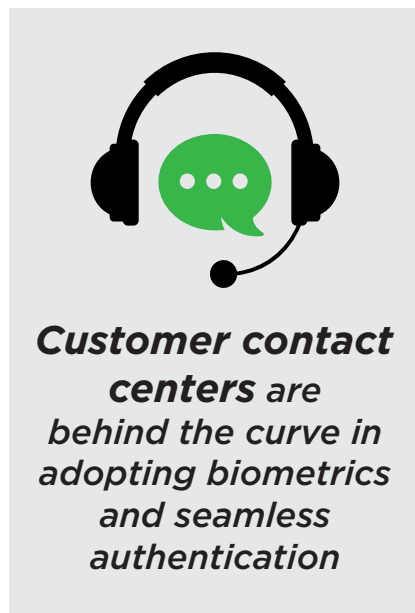
At the back-end, companies like Alliant are integrating technologies and methods like AI and behavioral analytics to provide additional layers of security and protection.

Identity assurance strategies need to incorporate intelligent authentication, says Orea, using behavior analytics to understand the customer’s behavior in terms of access, location, risk profile, device usage, etc. “If I detect that you’re connecting from a place or a device that is untrusted, then I can raise the bar (for authentication),” he says.

BIOMETRICS IN CUSTOMER SUPPORT

The contact and customer support center is frequently a siloed island and source of frustration and risk when it comes to authentication. Aite Group, for example, has found that 61 percent of all fraud losses can be traced back to the contact center.

Many contact centers use legacy IVR and PBX systems, which can be more challenging to integrate “because you’re no longer just passing through into a backend application. You’re passing through a phone system and an application and through a voice system to a human,” says Bill Guinn, chief technology officer at Serviceaide, a global provider of intelligent IT and enterprise service management solutions. However, Guinn notes, contact centers are beginning to adopt technologies that solve the problem.



White agrees that contact centers are too often late to the game when it comes to seamless authentication. Many still use knowledge-based authentication, or KBA, which requires something the customer knows to verify their identity. The authentication process can be both frustrating and unsecure. The chances are slim that the knowledge being shared is something that only the customer knows.

However, voice biometrics can now be integrated into existing IVR systems to provide seamless authentication experiences, White says. The most advanced systems dynamically recognize vocal quality and customer speech patterns. They can also differentiate between live speech, recorded speech, and computer-generated speech by detecting subtle acoustic distinctions that a human being would probably miss.

THE CONTINUING ARMS RACE

For the foreseeable future authentication and identity management will be a continuous process of improving security, privacy and ease of use. Hackers and fraudsters will continue to invent new ways to penetrate defenses and companies will need to adapt. Oversimplifying authentication can be a risk.

Biometrics is the future, says Johnson. “It continues to get more sophisticated and more accurate. But I also know that it will be a race to stay ahead of the hackers, who you know will be trying to invent deepfake techniques and figure out ways to trick the system. The technology will have to continuously improve.”



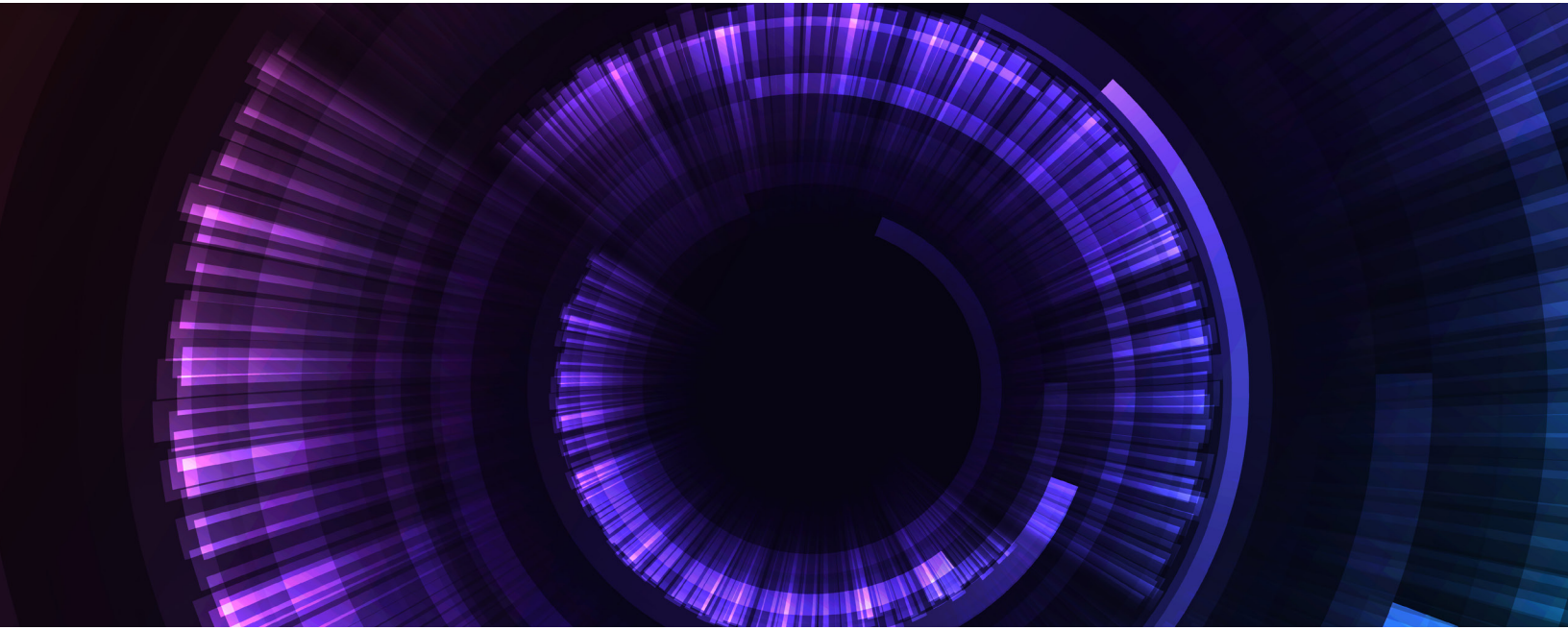
Hackers will continue to develop new techniques to trick the system. Identity technology must continue to improve.

Steve Wilson, a vice president and senior analyst for Constellation Research focused on digital identity and privacy, says consumers should be careful about what they ask for. Many people think they want what's called single sign-on. Once a person has logged on to their computer and established their identity, they should be able to access any website or interaction.

The move toward federated authentication, in which different web properties agree to share the same authentication is fraught with problems, particularly for highly regulated industries and high-value transactions. Social identities from Facebook and Google do not offer the level of security and privacy required. "You won't find a single bank in the world that allows you to log onto an internet banking site using Facebook handle."

Even with biometric forms of authentication, there are risks and challenges with false positives and false negatives.


The more a system seeks to prevent false negatives, the greater the likelihood of a false positive. This challenge is greater with one-to-many systems that store large volumes of biometric data. Wilson believes that one-to-one methods, which are supported by the FIDO Alliance, are a better solution. The user's biometric information is stored and secured on their mobile phone and can be used to access other digital services and transactions. Because it stores only the user's biometrics, accuracy is higher.



CONCLUSION

Digital experience is now a core competitive issue for business. Because of Covid, customers have flocked to digital channels of engagement and transaction, and most executives believe this digital transformation will be permanent.

For far too many companies, identity assurance and authentication are currently a major stumbling block in delivering satisfying and seamless digital experiences. Consumers are fed up with difficult and inconsistent authentication processes that frustrate and impede their digital lives and business transactions. The vast majority of consumers say they want to do business with companies that make authentication both easier and safer. Some 61 percent of consumers told us they have abandoned transactions because of poor identity experiences.



The authentication challenge is now an issue that reaches far beyond the realm of the CISO and security team.

Biometrics are viewed by consumers and business leaders alike as a technology that can help solve both ease of use and security challenges around authentication. However, biometrics need to become more than point solutions that are used effectively in isolated digital channels. Biometrics must be part of a unified, cross-channel system for understanding, recognizing and satisfying customers.

The authentication challenge is now an issue that reaches far beyond the realm of the CISO and security team. It's impact on customer relationships, revenue and brands is too great. It must become a major focus of business leaders across the enterprise, including chief marketing, revenue and digital officers.

SPONSORS AND PARTNERS



The Business Performance Innovation (BPI) Network is a peer-driven thought leadership and professional networking organization reaching some 50,000 heads IT transformation, change management, business re-engineering, process improvement, and strategic planning. It is dedicated to advancing the emerging roles of the Chief Innovation Officer and Innovation Strategist within today's enterprise. The BPI Network brings together global executives who are champions of change within their organizations through ongoing research, authoritative content and peer-to-peer conversations. These functional area heads (operations, IT, finance, procurement, sales, marketing, product development, etc.) and line-of-business leaders are advocates for Innovation as a fundamental discipline and function within 21st Century organizations. They seek to demonstrate where and how new inventive solutions and approaches can advance business value, gratify customers, ensure sustainability and create competitive advantage for companies worldwide. For more information, visit www.bpinetwork.org.



The Chief Marketing Officer (CMO) Council is dedicated to high-level knowledge exchange, thought leadership and personal relationship building among senior corporate marketing leaders and brand decision-makers across a wide-range of global industries. The CMO Council's 16,000+ members control more than \$1 trillion in aggregated annual marketing expenditures and run complex, distributed marketing and sales operations worldwide. In total, the CMO Council and its strategic interest communities include over 65,000 global marketing and sales executives in over 110 countries covering multiple industries, segments and markets. Regional chapters and advisory boards are active in the Americas, Europe, Asia Pacific, Middle East and Africa. The Council's strategic interest groups include the Customer Experience Board, Digital Marketing Performance Center, Brand Inspiration Center, Marketing Supply Chain Institute, GeoBranding Center, and the Coalition to Leverage and Optimize Sales Effectiveness (CLOSE). To learn more, visit www.cmocouncil.org.

SPONSORS AND PARTNERS



Daon is an innovator in developing and deploying biometric authentication and identity assurance solutions worldwide. Daon has pioneered methods for securely and conveniently combining biometric and identity capabilities across multiple channels with large-scale deployments that span payments verification, digital banking, wealth, insurance, telcos, and securing borders and seamless travel. Daon's IdentityX® platform provides an inclusive, trusted digital security experience, enabling the creation, authentication and recovery of a user's identity and allowing businesses to conduct transactions with any consumer through any medium with total confidence. Get to know us on [Twitter](#) and [LinkedIn](#). For more information, visit www.daon.com.