CIMPHONI WHITE PAPER SERIES

Modern Identity Management Promises to Improve BOTH Security and Customer Experiences

Ruben Moffett

cimphoni

Security and regulatory compliance rigor are no longer the enemy to effective and efficient CX design

We are at an inflection point – the digital economy has added complexity and cost to the process of delivering exceptional customer experiences (CX), while at the same time, technology innovations have raised customer expectations regarding how that experience should unfold.

The challenge of providing high quality CX is complicated by policies, processes and regulatory requirements aimed at addressing the pervasive data security breaches that seemingly occur monthly. And, while companies are rapidly improving tools and processes, they continue to lag in the methods they use to validate the identities of their customers when they engage. Methods to access customer-facing systems and to interact with customer service representatives are frequently not secure; they are costly, and they deliver a frustrating customer experience. Yet, according to a recent study by Visa, 86% of consumers are interested in using advanced technologies to verify their identities.

Billions of dollars are lost due to cybercrime and online fraud, but the potentially larger problem is customer frustration, which can lead to an erosion of customer trust. Consumers are frequently the losers as companies ratchet up their security policies and processes and typically force customers to spend excessive time confirming who they are before they can address the issues that they contacted the company about in the first place. This is an area that requires fresh thought and innovative solutions to improve the CX.

The 2018 Identity Fraud Study, released by Javelin Strategy & Research, found that $16.8 billion was stolen from 16.7 million U.S. consumers in 2017, up from $15.3 billion and 12.1 million victims just two years earlier.

Conveniently, with the deluge of publicized security breaches compromising consumer privacy, consumer attitudes and practices are changing. Two-thirds of consumers prioritize security over convenience when setting up passwords, and nearly half of consumers indicate that they would use two-factor authentication if available. These shifting attitudes will likely reduce the resistance to new technologies that can improve both the CX and Security simultaneously.

Billions of dollars are lost due to cybercrime and online fraud, but the larger problem is customer frustration, which can lead to an erosion of customer trust.

Many companies are beginning to implement solutions that significantly improve upon the traditional means of authentication. These solutions leverage advanced biometrics to authenticate users.

THE PATH TO MODERN IDENTITY MANAGEMENT

Companies have traditionally identified employees and customers in two ways: **What You Know** (Knowledge Based Authentication or KBA) and **What You Have**. For example, we use passwords, PINs, last 4-digits of our Social Security Numbers, Account Numbers, badges, key FOBs, tokens and any number of different means of engaging customer service, logging into websites and applications, and getting into buildings and secure rooms.

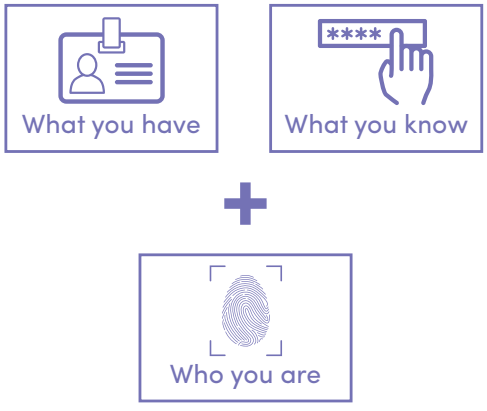
MULTI-FACTOR IMPROVES AUTHENTICATION, BUT DOES NOT PROVE IDENTITY

However, these means have proven to be insecure and inconvenient, resulting in staggering financial loss,

diminished privacy and control, and frustrating and time-consuming customer and employee experiences. Companies have tried to marry these two means of authentication as a second factor to improve security, **but this has not solved the problem**.

KBA is both regularly compromised and excessively complex for users to manage. Lack of password security is still the largest problem, with 81% of hacking-related breaches attributed to stolen or weak passwords according to Verizon's latest DBIR (Data Breach Investigations Report).

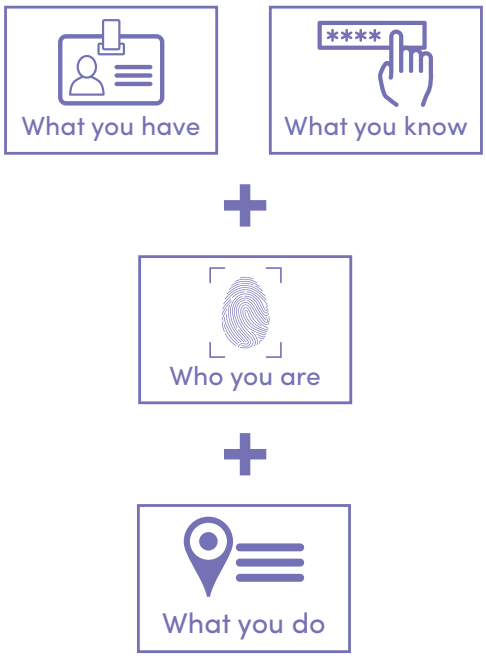
A third element frequently considered to be part of the authentication management methodology is **Who You Are** (e.g. a unique physical attribute like fingerprint, retina or face) and is generally validated using biometrics. Although biometrics have been around for years, very few companies have implemented them as a part of their pervasive authentication practices. The resistance has been due to the maturation and evolution of the underlying algorithms, costs to acquire and integrate, and effort to implement and adopt.



UNTIL RECENTLY, BIOMETRICS THAT CAN VERIFY UNIQUE IDENTITIES HAVEN'T BEEN PRACTICAL OR FREQUENTLY ADOPTED

But these technologies have evolved and have rapidly become viable means of identifying employees and customers. Advanced organizations are now actively looking to improve their security while reducing costs and improving user experiences with the addition of biometric identifiers that prove Who You Are.

Building on this foundation, a fourth dimension is further improving capabilities to prove identity by adding and tracking **What You Do**. These methods include the tracking of metadata about user behavior such as geolocation, usage patterns and other forms of information that can be leveraged forensically. This data not only supplements the other three categories of authentication, but also serves as a foundation for analytics and rapidly evolving Artificial Intelligence and Machine Learning applications that can derive even deeper business value.



COMPONENTS OF MODERN IDENTITY

FIVE WAYS MODERN IDENTITY MANAGEMENT WILL CHANGE OUR EXPERIENCES

With these advanced technical capabilities, companies are not only improving security; they are also transforming how employees and customers are managed and engaged. Here are five examples where advanced authentication technologies are poised to change our experiences:

Contact Center: Every customer has had their patience challenged when contacting companies for service who force them through onerous steps to verify their identity before finally attempting to address what is important to the customer. In addition to eroding customer satisfaction, companies incur significant costs as customers navigate Interactive Voice Response (IVR) systems and spend time with representatives trying to identify themselves. By allowing customers to biometrically self-authenticate through their mobile devices, and integrating that authentication into omnichannel technology platforms, users can bypass those authentication steps and immediately connect with a representative who can focus on their reason for calling.

Companies evaluating biometric authentication technologies must be sure to consider the customer journey and implement authentication methods strategically. No one wants to unnecessarily re-authenticate when switching from email to chat to a voice interaction. Thus, the technologies implemented must integrate seamlessly across channels and interaction points.

Unattended Access: Customers expect to be able to engage with companies and use their products and services on their terms. In response, companies are trying to make their brick-and-mortar locations available whenever the customer wants to use them. Hospitality, Fitness, and Real Estate industries are three examples in which customers want the flexibility to come and go around the clock. But 24/7 access has historically required companies to provide "front desk" staff who often offer little-to-no customer value, and only exist to validate customers and allow access to the location. By providing customers with the ability to biometrically authenticate using their mobile devices, companies can maintain security and controls, reduce cost and improve customer experiences.

Shared Content: With machines disguised as real people posting comments on websites and social media, public perception is harder and harder to gauge. From topics as critical as health care and net neutrality to restaurant and product reviews, companies and governments need to distinguish fact from fabrication in the world of online content. By enhancing the authentication layers of these types of platforms, organizations can ensure that posts and comments are validated as coming from identified sources, while still maintaining the option of retaining the anonymity of the public-facing post.

Subscription Models: Streaming content providers are some of the fastest growing companies doing business today. However, all of them are wrestling to protect their revenue streams and combat the common practice of shared passwords. While this practice does violate piracy laws, the legal threat is doing little to curb user behavior. Companies are fighting back because of the millions of dollars at stake. According to a Bloomberg article in December of 2017, "Tom Rutledge has had enough. The chief executive officer of Charter Communications Inc., which sells cable TV under the Spectrum name, is leading an industrywide effort to crack down on

password sharing. It's a growing problem that could cost Pay TV companies millions of subscribers—and billions of dollars in revenue—when they can least afford it."

Not only can modern identity management validate unique identities biometrically, it can also validate the devices from which the content is being accessed. This provides companies with the ability to limit and manage both the quantity of endpoint devices and quantity of users included in each subscription.

This technology has the power to transform the management of these subscription models and potentially recoup millions, if not billions, in unrecognized revenue.

Physical to Systems Access Bridge: While providers of Single Sign-On technologies have been helping companies streamline login processes across applications for employees, the ability to also integrate and streamline physical access through those same authentication processes has been missing. These platforms can now be augmented so that biometric authentication can both open front doors and provide systems level access, further reducing friction for employees while increasing the levels of security.

As the stack of authentication technologies continues to evolve, organizations will be better equipped to leverage these capabilities to improve experiences like the ones described above, and many others. Technologies that provide flexible levels of security based on use case will be the most valuable. For example, a platform that allows companies to pick and choose between the four identification categories and then pick and choose between specific methods within each category will equip organizations with tremendous value and control. An on-device fingerprint might be sufficient to open front office doors, whereas a biometric plus a trusted token-approved device will be required for access to an application. And finally, a combination of What You Know, What You Have, Who You Are, and What You Do might be required for access to critical facilities such as data centers and high value inventory storage locations.

Cybercriminals are constantly searching for and exploiting gaps across the varied layers of security. But technology innovation is now providing organizations with practical and effective tools to improve their security, while also designing improved experiences for their employees and customers. It is essential that companies implement these tools to seamlessly integrate security into the CX across all customer interaction points before their customers move on to companies that have already done so.

ABOUT THE AUTHOR

Ruben Moffett, Partner

Ruben leads Cimphoni's customer experience practice, combining extensive technology, operational and business expertise to help clients maximize and align technology with their strategic objectives. He has more than 20 years of experience in technology, product development, service delivery and operations functions in the business process outsourcing (BPO) industry. Ruben's specialties include customer experience, workforce optimization, business intelligence, software development, infrastructure, cloud solutions and professional and technical services management.

Some of Ruben's recent projects include leadership of Post-Merger Integrations in the Road Service, Insurance & Travel industries, as well as an Interim-CEO assignment for a technology provider in the rapidly growing Identity and Access Management market. Prior to joining Cimphoni, Ruben was COO of TantaComm, a leading workforce optimization solutions provider. He has a Bachelor's degree in history and sociology, and an MBA from the University of Iowa. Ruben spends his free time playing hockey and attending his children's soccer games, cross country and track meets and dance competitions.

About Cimphoni

Cimphoni is built on the premise that technology, when properly applied and led, can deliver practical solutions that transform businesses and improve the products and services we use every day. The Cimphoni team is comprised of highly experienced technology and business leaders with a thirst for innovation, an understanding of the value and application of new technology, a passion for solving problems and a hands-on approach to execution. Founded in 2012, we serve customers throughout the United States from our offices in suburban Milwaukee.

Contact Cimphoni

P.O. Box 80
Hartland, WI 53029

t: (888) 470-0448
e: info@cimphoni.com

www.cimphoni.com

cimphoni