entersekt

and you're in.

Authentication re-imagined

New innovations in digital banking and payment security to fight fraud and poor digital experiences

www.entersekt.com

In this ebook:

Lessons from the evolution of customer and payment authentication. From the need for personalization, to passwordless options; browser authentication; delegated authentication for e-commerce transactions; behavioral biometrics, and the next frontier: **Context Aware™ Authentication.**

Foreword

Modern, new directions in authentication

In a world where one bad authentication experience — for example, a falsely declined e-commerce transaction — means the difference between a customer staying with you or switching banks, legacy solutions can hold your business back. To strengthen your institution's value proposition now, and secure its future, it's imperative to explore innovative authentication technologies to keep your customers' identities and transactions safe.

With the number of digital banking customers in the US alone reaching **over 200 million users**, a modern approach to authentication is a must to protect transactions from fraudsters. Since **89% of organizations** experienced a phishing attack in the past year, Financial Service Providers (FSPs) need cutting-edge customer and transaction authentication that is secure, quick to deploy, and easy to use.

While several authentication offerings and add-ons exist these days to help FSPs meet their goals, what many don't realize is that individual solutions don't cover the full spectrum of user devices or continuously evolving fraud attack vectors. The result? Gaps in coverage across an institution's channels, and frustration for the consumer when authentication experiences differ from one channel to the next.

> Entersekt has always taken a different approach to solving security concerns for FSPs, by considering the complexity of their existing legacy platforms and interactions with the rest of the banking and payment ecosystem.

Our customer authentication solution is unique as it provides not only secure, but consistent, cross-channel authentication experiences wrapped up in just the right amount of friction, at the right time, based on the context of these interactions. This approach – which we call **Context Aware™ Authentication** – is fast gaining momentum within the industry. Here's why.

Regardless of where, when, or how your customer transacts, with Context Aware™ Authentication in play, their experiences remain consistent with each other. That's because, with context, various factors are taken into consideration – including the device the customer uses – to surface the most appropriate authentication method for that customer, in the moment. FSPs benefit as there's no need for a separate authentication mechanism for each channel. They also don't feel weighed down trying to figure out how to orchestrate these sometimes-separate authentication journeys across multiple channels.

Banks must prioritize user experience and customer choice when establishing a safe environment for transactions to take place. Not only does updating the user experience mean more transactions, but if done via a cross-channel, context-aware solution, it also means better security.

Ultimately, while FSPs' individual security needs will always drive their approaches, the overall experiences they offer can either improve customer retention rates or cause them plummet.

And while many FSPs realize that authentication methods need to change, they may not know the next steps involved in finding the right balance between strong security and seamless customer experiences.

But that's where we can help.

Read on to learn valuable lessons from the evolution of customer authentication that can help enhance customer loyalty, market share, and revenue growth within a competitive industry. From the need for personalization to passwordless options; browser authentication, delegated authentication for e-commerce transactions, behavioral biometrics, and the next frontier: Context Aware™ Authentication.

Pradheep Sampath,
Chief Product Officer

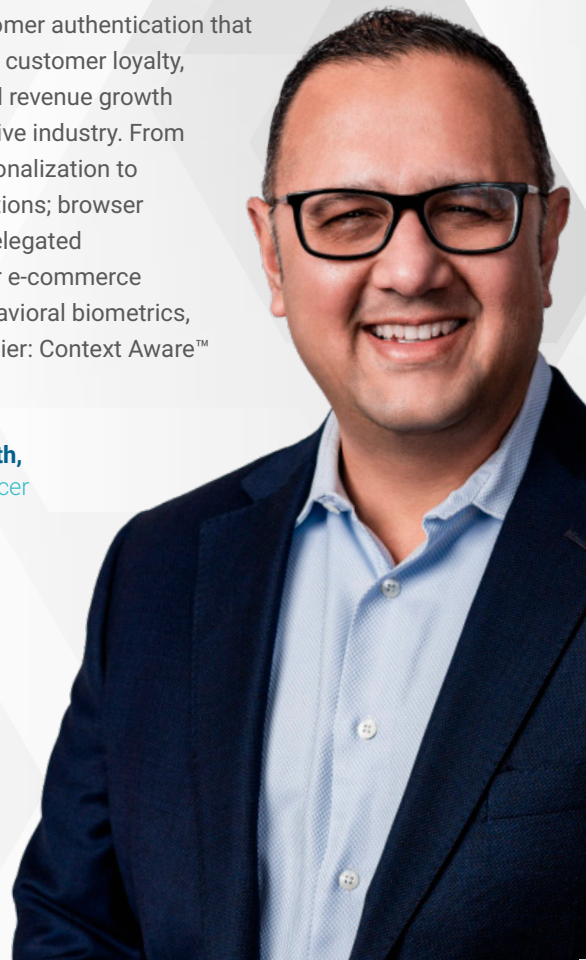


Table of contents

INDUSTRY VOICE

Digital banking transformation's surprising secret to success: Personalization

For banks, digitization entails far more than a direct transfer of branch-based processes to new digital platforms. It requires getting up close and personal with customers' needs.

Stessa Cohen
PIVOTASSETS

Stessa Cohen, a former research director at Gartner and founder of **PivotAssets**, is an internationally recognized expert on the digital transformation of the global banking industry. Her extensive network, skill with research methods and tacit knowledge are combined to counsel financial services companies, technology firms and investors on product, solution, and investment strategies.

Several years ago, I opened a bank account for my son who was then 13 years old. Last year, when he turned 18, he received a letter from the bank informing him that his account was no longer a minor account – it was his alone. Except that it wasn't. He couldn't change the primary telephone number (mine) associated with the account to his own mobile phone number.

So, every time he used his debit card, he triggered a fraud alert and each time I got the phone call from the bank. I had to remember to tell him and he, in turn, had to remember to call the bank to reassure them that there was no fraud (he was in high school; good luck). Inevitably the bank would lock him out of his debit card. He had to go to the branch to get a password to activate online banking, so he never did. The mobile app did not let him use Apple Pay as promised either.

Finally, he had enough. He went to the branch, just a block from our house, stood in line outside in the heat and humidity (because of the pandemic) to close the account. The customer service representative at the branch refused. Why? Because my name was on the account from when I opened it for him as a minor.

He opened a new account at another bank that immediately let him set up the mobile app and Apple Pay and connect to the other person-to-person (P2P) apps he used.

He now uses the mobile banking app several times a week. Yet, even with this much improved onboarding experience, he still gets phone calls about potential fraud activity on his debit card. Like most Gen Z (and Millennials and Gen Xers), phone calls are not the way to reach him – even with important news. The tellers at our local branch recognize him and greet him when he stops by to deposit money in his account. If only the bank could transport this in-branch experience to his digital one.

> In their quest to instill consumer confidence in digital channels, banks use security in unnecessarily clumsy, ill-considered ways. Too often, it's the wrong kind at the wrong time.

Watching his frustrating and increasingly adversarial experiences with his banks, I realized a few things. First, the banks were forcing him to use the two channels he least prefers to conduct their security checks: the branch and call center. Second, the banks didn't learn anything from his behavior – almost all his payments are mobile or debit card; he rarely, if ever, carries cash, and he always shops at the same merchants. Third, he always has his phone with him but rarely makes phone calls.

Customer journeys that answer customer needs

Too often, banks implement the wrong kind of security at the wrong time. They are missing out on the opportunity to create a customer experience that is aware of the customer's needs, starting from the time the customer opens an account through to the everyday tasks that we increasingly rely on mobile banking for: from ordering meals and grocery shopping to paying bills and sending money to friends. Consumers want hassle-free experiences, and are almost three times more likely to use a smartphone to purchase goods and services than computers, for instance.

We know banks long to improve customer experience and journeys. And they have digital transformation initiatives in place. Everyone from the CEO down is on board with the vision, mission and goals. They have also been upgrading and replacing their digital banking solutions to improve customer experiences. But they continue to deliver the same products and services, and fail to lead in adopting new services, such as mobile payments.

When implementing digital solutions, many banks simply focus on transferring their branch-based account opening processes to online and mobile banking apps without considering the entire customer experience. And this is their first mistake when trying to transform experiences.

Locating those hidden tribes in the customer base

> Banking has shifted from a sales-driven quest to sign new customers to a focus on loyalty and expertly crafted digital journeys, driven by omnichannel banking platforms.

The one thing that hasn't changed, however, is the way banks view and identify customers. Using the "**hidden tribes**" framework, I've created a new way for financial institutions to view their digital banking services and how to leverage them to grasp new opportunities. Banks and other financial services providers can use data and analysis to reveal these hidden tribes.

Uncovering them is essential to develop new services to address existing and future customer needs.

Needless to say, the current environment, in which we're all still trying to figure out how to live and work, is rich with potential in this regard. As a direct result of the pandemic, consumers have changed their buying and banking behaviors in a relatively short period of time.

Their increasing reliance on smartphones for more everyday activities presents an opportunity for banks to capitalize on by using mobile devices for more sophisticated forms of customer authentication to create intelligent friction.

Hidden tribes are those customers who reside underneath or out of sight of traditional customer segmentation. Traditional segmentation hides the multiple segmentations of customers who may or may not resemble each other. These segmentations challenge the bank's traditional assumptions.

Better service through intelligent friction

How does "intelligent friction" enter the picture? Financial institutions have major worries about security – from customer behavior and customer authentication to identity theft and data breaches.

Intelligent friction means that the bank has already collected data about which devices customers use and how they use their devices. From the moment a customer opens an account on a bank's digital platform, it can start collecting information about the customer's banking and spending habits and the channels they prefer for each type of transaction or interaction. This enables them to dynamically and intelligently adapt the level of authentication – and hence friction – required for that transaction.

Used in this way, intelligent friction can address both the consumer's and bank's security worries, all while transforming the customer experience for the better.

Intelligent friction is the use of authentication methods, both overt and covert, to balance necessary security with users' expectations and good UX.

It's about ensuring the right level of user interaction, presented in the right way, for a user to feel secure at the hands of their bank but still in control. The authentication solution must take the context into account, relating to the user and their preferences, as well as the transaction, to adaptively select the right flow.

A bank's posture also plays a role – if a bank is known to step up in certain instances, it becomes expected and should not change. Then, there's the threat landscape. If a bank knows of or detects an attack in progress, step up might need to occur more frequently. Nonetheless, intelligent friction should always result in an easy, unremarkable seeming experience, not an artificial step that surprises the user mid-transaction.

It shouldn't be this hard

After my son linked his Apple Wallet to his new bank account, his bank has rarely, if ever, interacted with him about his payments. Every time he uses his mobile banking app, he has to go through the same authentication steps, even when just checking his balance. When he moved out to university in another state, both his debit card and his mobile banking app failed to detect this and other changes in his location and behavior. At every point, the bank misses another opportunity.

The bank misses an opportunity to protect his banking transactions and purchases in his new location. The bank also misses opportunities to advise my son whether he should use his debit card or Apple Pay at a favorite take-out place, to alert him on how he is using his money, and to provide actionable advice on managing it better.

How banks can seize the opportunity

- Incorporate customer authentication and security teams into their digital banking transformation working groups
- Ensure their digital banking platform can connect to third-party security solutions that support intelligent friction across all channels and points of customer contact
- Digitalize account opening processes in a way that allows them to gather data for intelligent friction
- Be clear and transparent about the customer data they collect and how they use it for to protect their customers, while also explaining the real value of intelligent friction
- Build intelligent friction into mobile banking and payments first, and eventually include all channels and customer interactions
- Use the data they collect to identify the customer journeys and hidden tribes they may be missing and incorporate these discoveries into their digital banking transformation projects

PRODUCT PERSPECTIVE

The rise of passwordless authentication

The average internet user keeps around 150 online accounts, many “secured” by the same password. Experts agree, it is time to kick our password habit.

Arno van der Merwe

PRODUCT MANAGER: BROWSER EXPERIENCE, ENTERSEKT

Arno is responsible for pushing innovation that keep users safe and satisfied during browser interactions. Formerly part of the Research & Development team at Entersekt, Arno is naturally and relentlessly curious and passionate about the bleeding edge of browser technology, and envisions a safer, truly passwordless future for all.

It's no surprise that most people continue to grow frustrated by having to juggle passwords to access their ever-growing list of digital accounts. In the early stages of digitization, it made sense to gate-keep access to digital services with usernames and passwords. But, in a bid to simplify their access, some people started to reuse the same password for multiple accounts or choose simple passwords that are easy to guess, while others outsourced the task of monitoring their passwords to password management services.

The reality, however, is that over **80% of cyberattacks stem from passwords** and stolen credentials.

> What's quite remarkable, though, is that even when users suffer major data breaches or lose sensitive data and money, most do not update their passwords.

It is clear to everyone in digital security – and not only in banking – that there is a drastic need to kick our password habit. Fortunately, the future has finally arrived, and it looks like it could be passwordless.

KNOWLEDGE
Something you **KNOW**

POSSESSION
Something you **HAVE**

INHERENCE
Something you **ARE**

Passwords are out. Here's why.

To better understand the problem, let's first break down what a password is. In essence, it's "something you know" – a chosen combination of letters, digits and symbols that allows a user access to an account. You should never divulge your password but, even if you do 'keep it to yourself', it isn't totally secret. You share it over the internet and trust that it won't be intercepted in delivery or stolen in a breach.

You use it over and over again and, probably, in multiple places. Technically, it's called a static knowledge-based authentication credential.

There are two other types of authentication credentials: possession and inherence. Possession is "something you have" – for example, a token or digital device that can receive a one-time password (OTP), or an "Approve" button delivered via push notification in a mobile app. Inherence is "something you are" – a unique biological trait, like a fingerprint or facial ID.

How we modernize and become passwordless

All authentication is based on the premise that, when you can claim an identity by providing a username, and back up that claim with at least one type of authentication, you should be granted access. So, if we want a viable passwordless future, we need to leverage other forms of authentication.

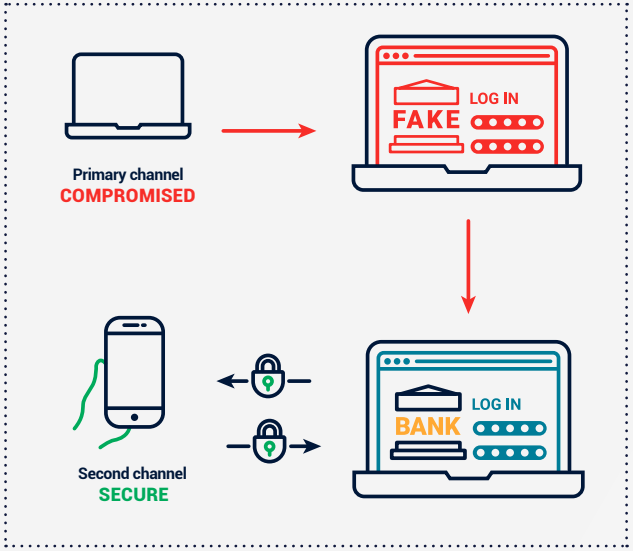
> Fortunately, we already have the means to leave the old days of passwords behind us, and many of these newer security options are already commonplace.

For example, most people now use biometrics, such as fingerprint technology or facial recognition, to access their mobile devices instead of a PIN (or nothing at all). In a **recent survey conducted in the US with PYMNTS.com**, 66% of respondents shared that they prefer using biometric authentication.

Today, companies like Apple, Microsoft, and Google all facilitate more modern authentication solutions — passwordless technology called passkeys, a new form of sign in-technology. Instead of using a password, a passkey grants passwordless access and is also more secure and easier to use. (Take a look further down in this section, on **page 17**, where we discuss passkeys in more detail.)

Mobile-enabled biometric authentication is another step towards passwordless solutions.

It's a great example of how you can very successfully swap one type of authentication for another to improve both security and the user experience. But why stop at a simple one-for-one exchange? We can combine multiple authentication types – one of which, ideally, should be communicated through an out-of-band channel – for even greater security, provided it does not impact the user unnecessarily.



Backed by strong device ID, users can prove that they have more than one of the devices or channels linked to their identity, so that if one authentication channel is compromised by a malicious party, there is another form of authentication that can still provide a barrier to prevent bad actors gaining access.

Combining authentication methods to improve security

When authentication solutions use a combination of authentication methods, this is called two-factor authentication (2FA) or multi-factor authentication (MFA). Multi-factor authentication is the best way to secure an account. However, MFA can be less effective if one of the factors is an SMS one-time password (OTP). SMS OTP may be a form of MFA, but they are extremely vulnerable to man-in-the-middle and SIM-swap attacks. In 2021, **Americans lost $68 million to SIM-swap attacks**.

Therefore, to ensure a passwordless future, we need to educate people how to use these authentication methods. In the meantime, however, there are other forces at play that may speed up adoption.

Considering that **by 2025, consumers will conduct about 60% of their e-commerce transactions via mobile devices** globally, they expect an experience that doesn't interrupt their purchase experience, but is still secure.

With biometric capabilities now available on most smartphones, we are starting to see consumers use this authentication option for more than device access. In fact, **research indicates** that 68% of consumers that use mobile apps to access digital accounts are willing to use login methods other than passwords.

This behavior, combined with industry leaders starting to align themselves to an international standard called Fast IDentity Online (FIDO), will have a major impact on security and authentication across industries. The objective of the FIDO international standard is to make passwords obsolete by replacing them with possession and biometric factors. The standard also uses encryption technology to ensure that users' credentials cannot be accessed or stolen.

Biometrics and hardware devices are in

What all these changes mean is that the barriers to implementing secure authentication through biometric or hardware devices are lessening significantly. Leading web browsers, smartphone platforms, software providers and hardware providers are already releasing FIDO-certified hardware as well as certifying their platforms for FIDO authentication.

Several tech giants – Google, Microsoft, and Apple – already support this standard too.

> Because FIDO simplifies the risk and process of using biometrics or hardware for authentication, more online services and hardware — such as smartphones, laptops, and desktops — will adopt this method of authentication.

As a result, a higher percentage of the population will utilize and trust biometrics for all services that require authentication as it significantly eases the authentication process and increases security.

Biometrics, PIN keys, and second-factor devices are all FIDO-secure methods of authentication that have demonstrated decreased checkout abandonment and fraud incidence rates. However, authentication using biometrics results in the least amount of friction for consumers in the authentication process.

Additionally, for payment institutions requiring absolute certainty and verification of user devices, the registration protocol outlined by FIDO includes an attestation procedure, which further minimizes the risk of fraud.

In the US, for instance, **consumer trust biometrics is growing**. This growing familiarity, combined with the industry-wide use of FIDO and the promotion of Passkeys by large corporations like Apple, Google, and Microsoft, could be the solution that will finally free us from the burden of endless passwords, opening the door to a brighter, passwordless future.

Passwordless authentication options at a glance

These technologies offer viable alternatives to passwords, especially if used in combination for a cross-channel authentication approach.

Fingerprint technology

Uses a smartphone's fingerprint recognition feature to securely authenticate users at login or when completing a transaction. Fingerprints are unique and represent both possession and inherence factors.

Facial biometrics

Verifies users' identities remotely using smartphone cameras for facial recognition and document scanning. This method supports remote online account opening and can be used at scale.

Mobile push and FIDO2-enabled apps

Phone-as-a-token authentication allows users to verify their identity and approve transactions in-app, simply by tapping Yes. This is arguably the best user experience, and offers the most flexibility to layer security for a seamlessly integrated, passwordless experience.

Hardware keys

Securely authenticates users signing onto a device using a physical hardware key in the form of a USB, near-field-communication (NFC), or Bluetooth device. Hardware keys offer great security and a good mix of usability and deployability.

QR codes

On login, users scan a Quick Response (QR) code, which binds the session to their smart device. An in-app message then displays, prompting users for a biometric scan to validate their identity. The limited lifespan of a QR code prevents hijack or session replay attacks.

Behavioral analysis

Confirms users' identities by combining non-identifiable but unique behavioral factors, like typing speed, login history, IP address or browser used. This enables a secure, completely invisible authentication experience.

Zero knowledge proofs

A challenge/response protocol requiring users to prove their knowledge without revealing their secrets. This method transforms a password into an abstract sequence, which is transferred to a server and stored, eliminating the risk of data exposure during authentication.

Passkeys

The latest innovation, which we touched on before, is passkeys. Passkey technology is a more advanced form of MFA than SMS OTPs, and provides a modern, secure way for users to sign into their banking app on their mobile or through a website.

Passkeys use biometrics and leverage FIDO to prove the person signing in is who they say they are. The technology relies on the WebAuthn standard, which enables passwordless authentication for added security, and is supported by all major operating systems. Since most mobile phones and computers are also equipped with native biometric capabilities, the process of transitioning to passkeys should be smooth for most users.

Supported by Apple, Google and Microsoft Passkeys are designed to sync across a user's devices securely within an ecosystem. This means that instead of having a password that you copy around to use on all your devices, your passkeys are available on all your devices in a seamless way.

"Unlike passwords, passkeys are resistant to phishing, are always strong, and are designed so that there are no shared secrets."
– FIDO Alliance

Find out more about passkeys in our insightful fact sheet – free to download.
Click here

SOLUTION SPOTLIGHT

Widening the web with browser authentication

Browser authentication, risk analysis, and orchestration are the keys to improved online security as the growth of financially sensitive web-based transactions accelerates.

Andries Maritz

PRINCIPAL PRODUCT MANAGER,
ENTERSEKT

Andries helps ensure that Entersekt's customers take ownership of high-quality software solutions that meet their needs, when they need them. He has worked on several of Entersekt's product lines during his tenure as product manager. With an everchanging technological landscape, that experience together with his curiosity and holistic approach, breathe life into products that must be as adaptive and fluent as the environments in which they run.

A rising wave of online fraud and crime is compelling businesses – particularly those in the banking and financial services sectors – to re-evaluate and improve the security of their web-based operations. Per a recent US PYMNTS.com survey, 64% of FIs reported an increase in credit card fraud attacks.

This upward trend parallels the increase in web activity as a growing number of consumers interact with organizations online and expect the experience to be as uncomplicated, yet secure, as possible.

Entersekt's browser authentication solution, which uses a powerful combination of sophisticated behavioral analysis and business logic technologies, ensures that when consumers log in to a website, they experience the right balance of security and convenience.

It allows customers to transact safely and ensures businesses build trust among users while reducing the fees they pay for fraud insurance. This is done without complicating the user experience. The solution is relatively simple to deploy and integrate and does not require replacement of existing infrastructure.

A trusted browser

The easy way to add MFA to your web channel

1. A fully orchestrated experience
2. Integration with existing identity platform
3. Works with or without an app

Password problems

Many institutions still make use of old authentication methods, like simple username and password combinations, which are not multi-factor. Because anyone could assume someone else's identity by reading a password off a sticky note attached to a monitor, for example, this is not ideal.

To ensure a user is who they say they are, organizations can employ different authentication factors comprising of something they know, like a password; something they possess, like a smartphone; or something they are, like fingerprints or retinal scans. Ideally, at least two of these mechanisms should be used to identify someone logging into a transactional website.

Keeping fraudsters out

Today, there are around **24 billion credentials available for sale online**, which implies that people often reuse username and password combinations. Fraudsters use these credentials to try to log into a wide variety of websites.

Our browser authentication solution leverages risk-based authentication (RBA) to track, identify and handle interactions in real-time. The authentication happens silently if the risk is low and with step-up authentication (which incorporates other authentication mechanisms, such as out-of-band authentication) if the risk is high. But in both cases, delivering a seamless, secure user experience.

Browser authentication decoded

> Browser authentication provides cutting-edge browser security that is swift and silent.

Using Browser ID (a cryptographic ID) to uniquely identify the browser, and FIDO standards, customers can authenticate without an app, but rather via physical security keys or biometrics for a more secure, dynamic user experience.

That differs from current trends — using cookies or browser fingerprinting.

Browser fingerprinting falls foul of privacy regulations because it collects potentially sensitive information that fraudsters can use to identify a specific user.

Consumers have issues regarding the privacy of browser fingerprinting. One **academic study** found that 85% of users were concerned about browser fingerprinting. Browser authentication, on the other hand, allows the user to remain anonymous while still providing a strong possession factor. Our browser authentication can uniquely identify any browser.

Browser authentication is also not subject to “drift”. A fingerprint looks at a set of metadata (for instance, the browser’s language, installed fonts, installed plugins and time zones) which can change over time.

Analyzing behavior

Behavioral risk analytics, conducted in partnership with Mastercard's NuData Security, BioCatch, or Featurespace is another important component of our offering. It looks at users' behavior – such as how people use their mouse or how quickly they type, as well as the time of day and usual geographical location – and builds a hyper-dimensional model of that interaction.

Because the model looks at patterns in a "big data" context, behavioral deviations can be flagged in distinct transactions without the need to know anything specific about who the user is.

The model simply detects that the user's behavior is uncharacteristic or different to that of the typical user.

It's already known from the certificate that the browser is legitimate, and the analytics indicate that the user is behaving in the way they usually do. If those two things match, then there is a high level of confidence that the user is authentic. At this point, the user has not necessarily provided any information such as a username or password yet.

Business logic

Orchestration, or business logic, is another component of browser authentication. It directs interactions between a bank and their customers' devices, helping to coordinate appropriate responses.

It determines how the technology will behave in certain situations. For example, what happens if a one-time PIN fails, or if the browser certificate does not provide the correct response to a challenge? Does the login fail or does something else happen?

Entersekt provides policies that can be configured without having to write code. A single bank can even have multiple operations – like private or retail banking – and they define what these policies are per channel. Entersekt also offers risk-policy advice. In such instances, we review each interaction, assess the risk score and then advise the institution what steps to take next — whether to step up or not, or decline the transaction outright.

Balancing security with convenience

The challenge for banks and financial services organizations, as well as the wider business community, is to offer their customers secure web-based transactions that are easy and convenient.

> Entersekt's browser authentication provides a straightforward way for organizations to add multi-factor authentication to their web channels, without having to replace the systems they currently use to identify their customers.

Browser authentication significantly expands the reach of our Strong Customer Authentication (SCA) solution, from mobile apps only to web browsers. It brings us closer to securing digital transactions from anywhere, at any time on any consumer device.

Banks that use Entersekt's cross-channel authentication solution (a single authentication platform across all digital channels) prevent gaps in coverage, where single vendor solutions fail to gather the full context of each customer transaction. The result is a seamless, secure customer experience.

TECH FORECAST

Delegated authentication set to improve secure online shopping experience for consumers and retailers

Understand delegated authentication, which allows FIs to outsource Strong Customer Authentication (SCA), as defined by EU regulation, to a third party – like a merchant.

Gerhard Oosthuizen

CHIEF TECHNOLOGY OFFICER, ENTERSEKT

Gerhard is responsible for accelerating strategic initiatives at Entersekt, driving research and development. He has over 20 years' experience in the software industry, developing and managing solutions in electronic funds transfer, electronic payments, digital banking, and digital security. As you would expect of a highly creative thinker and inventor, this is his second time around helping to shape a fast-growing software company into a global industry leader. He is passionate about making the online world a safer place.

The adoption of European Payment Services Directive 2 (PSD2) – and soon, PSD3 – security standards for digital payments will make online shopping more secure. However, depending on how FIs implement these measures, they could have a negative effect on the overall customer experience by creating friction and increasing cart abandonment rates – something merchants want to avoid at all costs. They want to provide customers with a simple, intuitive checkout experience. Thanks to delegated authentication, they can offer this while complying with the latest regulations.

Delegated authentication (also called merchant delegation) – means online retailers can take control of authenticating e-commerce transactions from the traditional gatekeepers, credit, and debit card issuers, giving consumers numerous new benefits. Certainly, it promises online shoppers faster, simpler, more intuitive checkout experiences that look and feel consistent with their go-to retail brands.

Cart abandonment issues

In 2022, the **average cart abandonment rate was 58%** due in part to user experience issues. These issues include any transaction friction — the frustration at the time-consuming process of being authenticated and having their payments authorized.

> While e-commerce fraud may grab the headlines, hundreds of millions of dollars in sales are lost every year because the process of paying for goods and services online is too complicated and frustrating for consumers.

Active online shopping can fail to convert into sales for two main reasons. The first is when the customer abandons their cart at the payment authentication step. The second is when payment is declined, rightly or wrongly, for risk reasons. Something out of the ordinary has triggered an alert, flagging the transaction as potentially fraudulent. When – erring on the side of caution – the system blocks a legitimate cardholder, it's called a "false decline."

Unfortunately, this means the consumer is usually directed away from the merchant's domain to the issuer's domain at checkout for authentication – and then back again. This redirection breaks the consistency of the online shopping experience and often leads consumers to abandon the transaction, whether out of confusion or fear, or that momentary intrusion of reality ("Do I really have the money to spend on these headphones?").

To succeed, all transactions need to be authenticated either in the background or by involving the consumer actively, and currently this responsibility typically sits with the issuing banks.

Better experiences to come

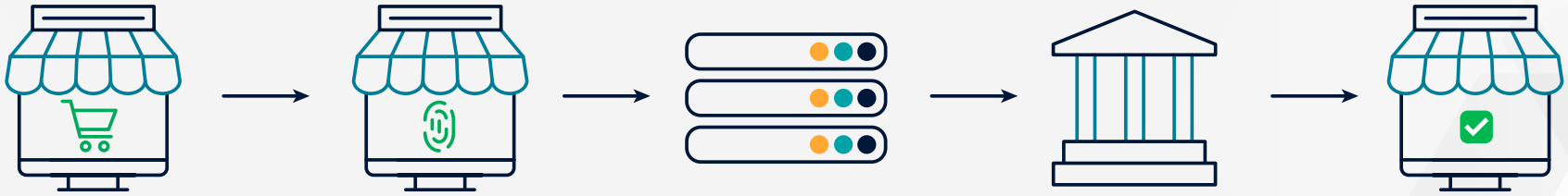
Nowadays, merchants can offer their customers a simple, intuitive checkout experience by utilizing delegated authentication. This is due to the European Banking Authority's PSD2 regulation, which allows the process of Strong Customer Authentication (SCA) to be outsourced to a third party such as an online merchant or e-wallet provider.

Merchants who qualify and have an SCA-compliant solution can perform SCA on behalf of the card issuer or submit recently performed SCA under certain conditions, which helps reduce friction at checkout. They can decide when and how to authenticate their customers, keeping the online shopping experience as consistent and hassle-free as possible.

It's a win-win

> One of the main benefits of delegated authentication for online shoppers is that the entire shopping experience remains consistent, from the moment they browse to the site to the time they pay.

They can also prove they are the legitimate cardholders by using authentication methods they are familiar with – like PINs, passwords and biometrics that are already enabled on their mobile phones or computers.



Merchants who qualify and have an SCA-compliant solution can perform authentication on behalf of the card issuer.

Merchants benefit by retaining control of the consumer's online experience because authentication happens within their own web page or app – shoppers are not bounced out to a third party for authentication.

The whole checkout process is smoother, reducing the chances of shoppers abandoning their carts. The payment networks validate the authentication results directly, reducing the chances of the issuer requiring a step-up authentication involving the customer.

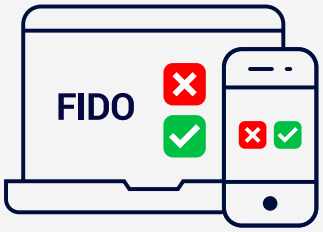
Banks benefit because, for them, it's all about being front-of-wallet. Their card will be chosen above others if the experience is superior to others, and this means more revenue. Their customers are authenticated with SCA without the need to delegate this function to a third party. Authentication results are validated by the payment networks on their behalf.

Following protocols

There are two primary ways for a merchant to implement delegated authentication:

Generic PSD2-compliant SCA

- authentication takes place directly in the merchant's app or browser, which results in fewer issuer challenges as regulatory compliance is covered by the merchant.



FIDO (Fast IDentity Online) via WebAuthn

- authentication takes place on the users' preferred devices, with an Application Programming Interface (API) built into browsers on both desktop and mobile using biometrics or a security key.

FIDO protocols use standard public key cryptography techniques to provide stronger authentication, reducing reliance on passwords. It is supported by Microsoft, Google, Apple, Amazon, Facebook, and Entersekt. WebAuthn enables online services to use FIDO authentication, which provides a higher level of security than passwords alone and is supported on Safari, Chrome, and Firefox browsers.

Allowing online merchants to stay in complete control of the customer experience means consumers are in for a more satisfying online buying experience.

Aside from the security benefits, merchants with frictionless checkout using delegated authentication will be able to claim a greater share of the already burgeoning consumer appetite for e-commerce.

Everything you need to know about FIDO, in one ultimate guide.
Download your copy!

Secure Payment Confirmation (SPC) is a more secure authentication method developed by the World Wide Web Consortium (W3C). SPC streamlines payment authentication by allowing issuing banks or their payment service providers to directly authenticate their customers using Application Programming Interface (API) technology.

Not only is it easy to adopt, but it also exceeds the standards set by Strong Customer Authentication under the PSD2 regulations. Consumers no longer need to navigate away from the merchant's site to verify their identity, plus no external hardware or dongle is needed. This means smooth, fast and safe transactions.

INDUSTRY VOICE

Focus on behavioral biometrics

Companies are increasingly turning to behavioral biometrics to augment their authentication systems, discovering that it can cut friction while further reducing fraud.

Alan Goode

CEO & CHIEF ANALYST, GOODE INTELLIGENCE

Alan heads **Goode Intelligence**, a London- based research, consulting, and events company for the identity and biometrics sectors, and is chair of the International Biometrics Forum. He is a respected expert on information security and fraud management and has frequently presented and written on these subjects. Mobile technology is a special interest, Alan having been one of the first to predict its utility in user authentication and digital identity. He has been a judge for the GSMA Global Mobile Awards since 2012.

Biometric authentication is now a popular method to authenticate account holders securely and conveniently. Millions of us can unlock our smartphones by just touching or looking at our devices, and large numbers of banks and payment service providers are leveraging biometric technology to help secure access to bank accounts and to authorize payments. Biometrics is now even part of important financial services regulations and industry protocols, including the European Union's Regulatory Technical Standards on Strong Customer Authentication and secure communication and EMV 3D Secure.

It is not just about morphological biometrics like fingerprints and faces, of course. A fast-developing biometric technology is based on our unique interactions with digital devices. Behavioral biometrics is a dynamic biometric that continually collects unambiguous user data to help verify someone's identity. The technology works passively in the background and analyzes how a user types on a keyboard, holds or swipes a mobile device, and other details, building up a profile of that individual customer's online behavior.

Behavioral biometrics enhances authentication solutions by detecting abnormal or unexpected behavior, including automated and scripted activity, and detecting traffic from bots, while at the same time ensuring that legitimate customers can access their digital services and transact in an increasingly frictionless way.

The approach is at its most effective when combined with other class-leading Strong Customer Authentication solutions, which offer low-friction step-up authentication processes to avoid false positives, for example, or to comply with regulations mandating direct user involvement. These also allow users to give active consent to or acknowledge certain interactions for compliance and non-repudiation purposes.

> Customer experience is becoming a critical component in delivering competitive digital services. For those services providers and relying parties that do not get this right, consumers and banking customers will go elsewhere.

This is especially true for e-commerce providers and online merchants that must contend with EMV 3D Secure while reducing cart abandonment rates that can be as high as **70% to 80%**.

Cart abandonment is caused by many things, some of them unavoidable. A **recent report** revealed that 18% of consumers abandoned an online purchase because they had forgotten their username or password. Consumer frustration with clunky and complicated authentication methods – remembering passwords, PINs, and your favorite teacher from the 1990s, makes sense. We can do a lot to improve things in that department.

A layered approach to authentication

Passive - Biometric and behavioral analytics in the background help identify users in real time, without impacting the digital experience.

Active - Reaching out to users for explicit verification or approval using any of a wide range of authentication factors.

Behavioral biometrics at Entersekt

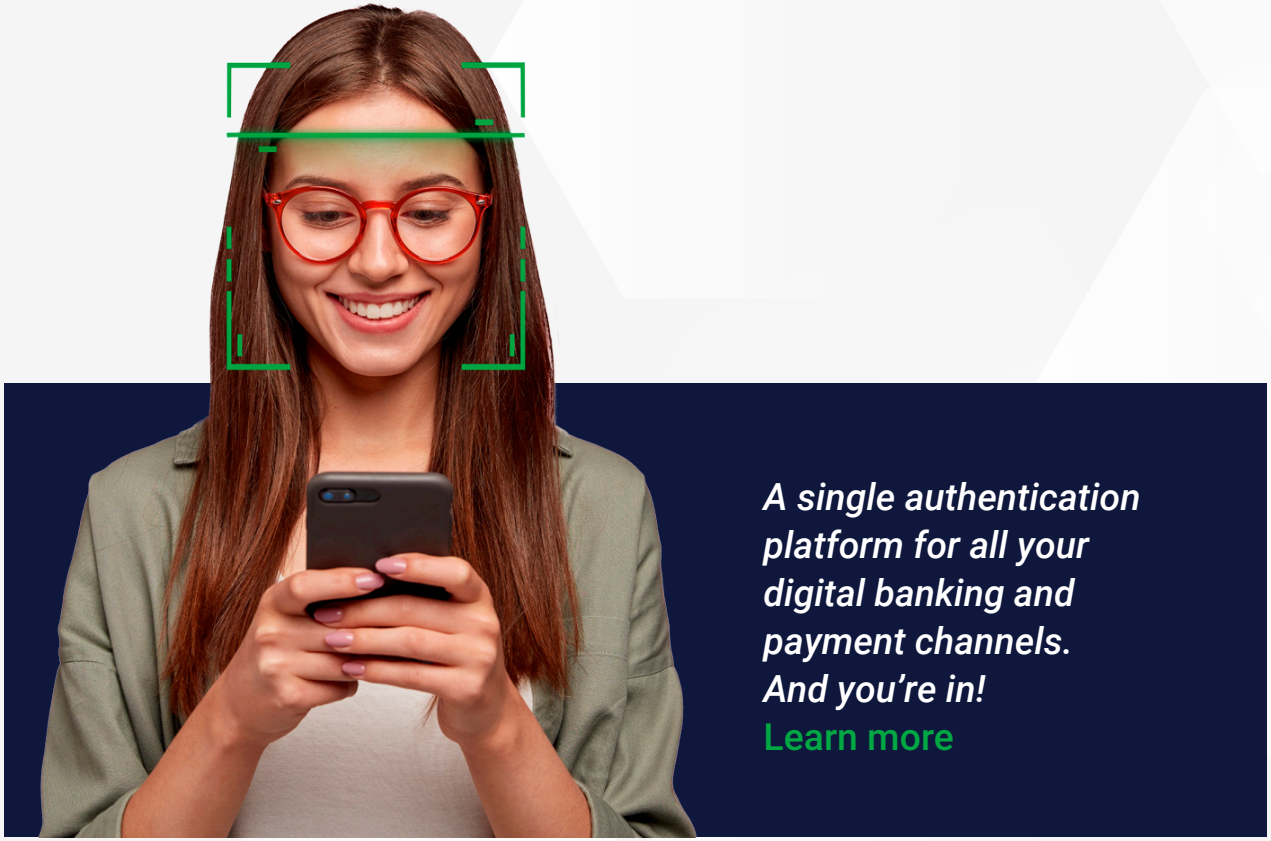
Entersekt offers a solution that combines behavioral biometrics and advanced strong device ID, whether on mobile or browser. Our patented technology issues strong IDs to consumers' devices, including mobile phones and personal computers — transforming apps and browsers on these devices into trusted endpoints that can be leveraged as strong possession factors during users' authentication journeys.

> Entersekt has partnered with leading behavioral biometrics and analytics specialists across the world to deliver a fully integrated Strong Customer Authentication with passive biometric technology.

The two approaches complement each other well, combining possession with inherence for a powerful, regulatory-compliant multi-factor authentication solution that is especially user friendly.

Entersekt's 3D Secure authentication solution, enhanced by behavioral biometrics, can help card issuers and other organizations in the payments ecosystem to drive down cart abandonment. It is augmented by risk-based and data analytics techniques to ensure that the majority of consumers can transact without the need to actively authenticate. For users whose payments are deemed high risk, step-up authentication can take many forms.

Entersekt provides a state-of-the-art in-app push solution, but also uses biometric authentication underpinned by FIDO, SMS one-time-passwords, and mobile-network- initiated USSD.



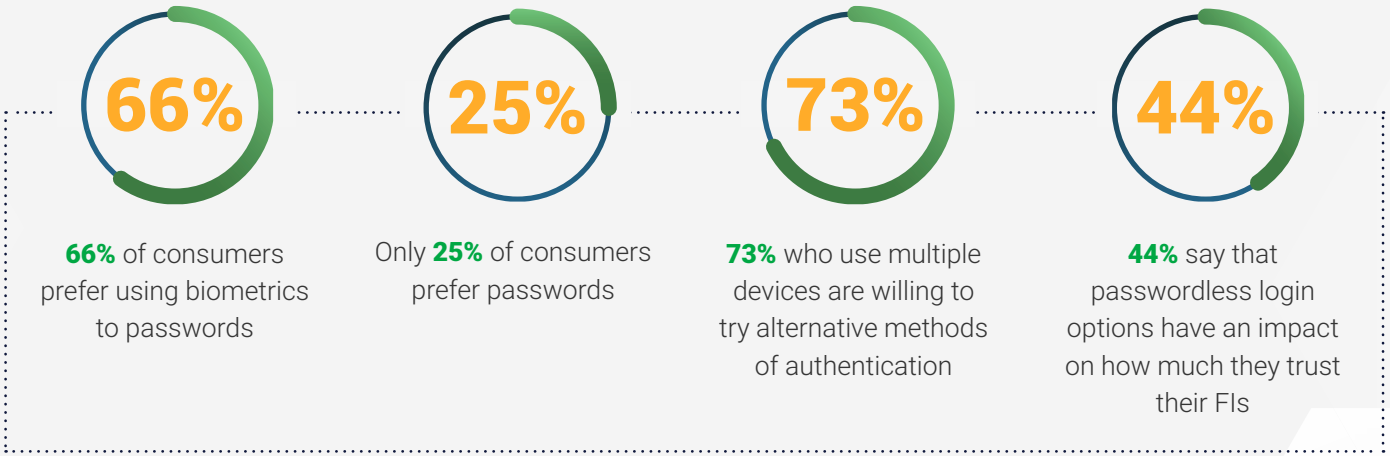
Biometrics score well in Entersekt's consumer surveys

Biometric authentication is growing in popularity with consumers. In two recent surveys, conducted in June and November 2022 with global news platform, PYMNTS.com, the evidence is clear that consumers value the growing simplicity and convenience of modern authentication technology.

Today's banking customers want to perform transactions across all their devices without any interruptions. And it's no surprise that only 25% of consumers who use a password actually prefer password authentication.

The data shows that 73% of consumers, who use multiple devices for their banking, are willing to log in to their accounts with alternative authentication methods. What's more, 66% actually prefer using biometrics to verify their identity, and view biometrics and multi-factor authentication as the most secure ways to verify their identity.

Not only do they value the efficiency of these authentication experiences (or rather the absence of disruptive processes), but also 44% shared that passwordless login options have a big impact on their trust in their financial services provider.



66% of consumers prefer using biometrics to passwords

Only **25%** of consumers prefer passwords

73% who use multiple devices are willing to try alternative methods of authentication

44% say that passwordless login options have an impact on how much they trust their FIs

ENTERSEKT IN PARTNERSHIP

Game-changer: Entersekt's biometric authentication for Q2

Entersekt's biometric solutions are now available on the Q2 Digital Banking Platform, offering financial institutions advanced biometric authentication and protection against modern fraud vectors.

Mzukisi Rusi

VP PRODUCT: IDENTITY & AUTHENTICATION, ENTERSEKT

Mzukisi (or Mzu, for short) is passionate about leveraging technology for change within the financial services industry. In his role as the VP Product: Identity and Authentication at Entersekt, he achieves this by leading innovative IT projects and building high-performing customer success teams. Thanks to his deep understanding of consumer interactions across banking channels, Mzukisi played a pivotal role in developing Entersekt's cross-channel, Context Aware™ Authentication solution.

The Q2 Partner Accelerator is a program that's part of the Q2 Innovation Studio. These programs enable in-demand financial services companies — that already use the Q2 software development kit (SDK) — to pre-integrate their technology into the Q2 Digital Banking Platform. The core benefit for banks and credit unions is the ability to rapidly deploy their standardized integrations to their customers.

From an Entersekt perspective, the partnership makes perfect sense, as helping financial institutions ensure that their customers can transact securely and easily remains at the heart of what we do.

Savvy authentication: Zero friction equals zero workability

While there is a major push in financial services to remove friction from the authentication process, delivering zero friction is a misnomer. Because, if you think about friction, you can't remove it completely.

With banking transactions, there will always be some sort of friction. Think about a banking customer performing a high-risk transaction. In this case, the risk engine assesses the transaction silently, and determines that it's high risk. Step up authentication is needed at that point. The customer then verifies they are who they say they are via an SMS OTP, or biometrics, and finishes up their transaction.

Alternatively, if financial institutions went completely frictionless with all transactions, and a high-risk transaction occurred, it would be declined. In other words, when the same customer tries to make a payment, the transaction will be declined at checkout. They might retry it, but it will be declined again. At that point, they would have to call their bank to find out why the payment was declined. A very time-consuming exercise for banking customers!

If we consider the above scenarios, which one actually contains less friction? If you look at the user journey, you can decide where that friction point is, but the transaction will never be completely frictionless.

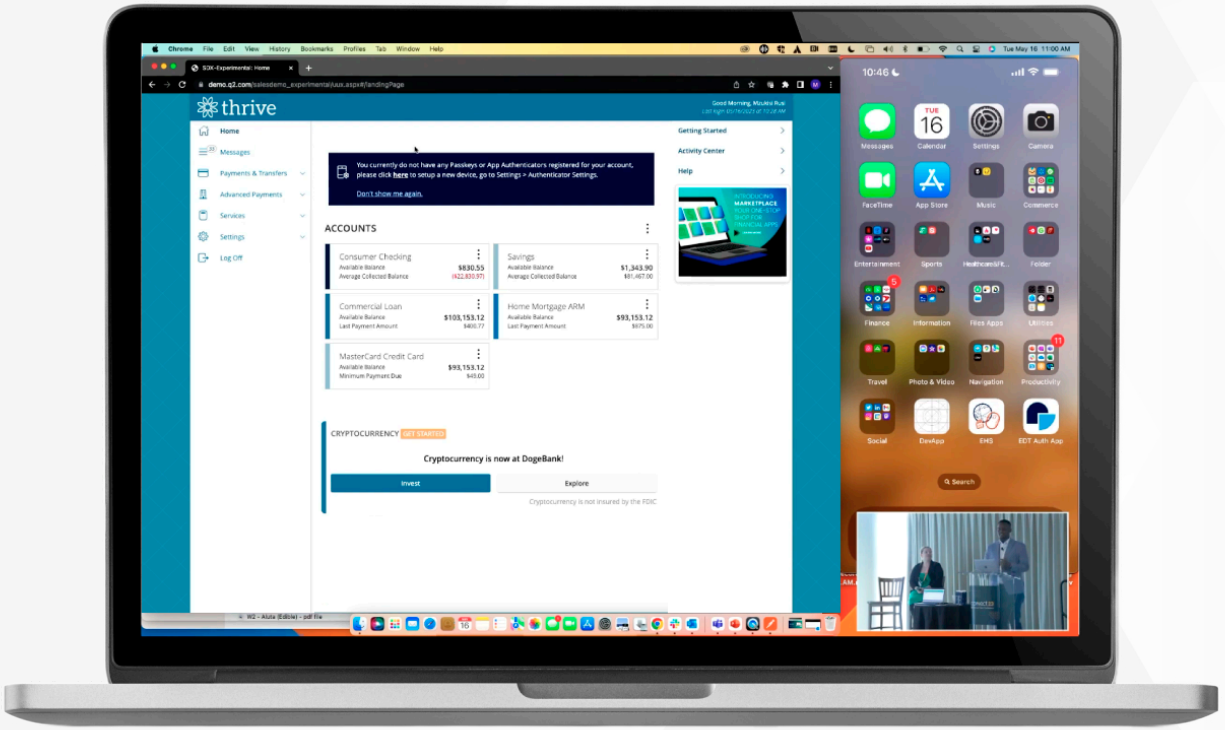
> Biometric authentication, which Entersekt offers on the Q2 platform, provides strong security and a streamlined user experience.

Entersekt's cutting-edge authentication solutions

Entersekt provides a single, cross-channel solution for FIs that balances convenience with banking-grade security for simple, secure authentication. Together with SMS OTPs, Entersekt also offers biometric authentication for Q2 customers. Financial institutions can provide the secure, personalized experiences tech-savvy consumers expect.

With Entersekt's app-free biometric authentication, FIs can deliver:

- Seamless multi-factor authentication options
- Strong device and endpoint security
- Secure authentication without an app
- Security that eliminates account takeover fraud



Case study: 4Front Credit Union's success with biometric authentication through Q2

4Front Credit Union (CU), a Q2 customer, recently expanded its MemberPass authentication solution, which is powered by Entersekt, to bring biometric authentication to members for online and mobile banking systems.

Here's their success story.

The need: Streamlined multi-factor authentication experiences

"Ensuring the financial protection of our members is paramount to our mission and strategy at 4Front," said Jack Martin, Chief Innovation Officer at 4Front Credit Union. "MemberPass enables leading-edge authentication for our call center, branches, and interactive teller machines (ITMs)."

According to Martin, it was important for the business to reduce reliance on SMS one-time passwords (OTPs) and knowledge-based authentication methods, which are easily intercepted by fraudsters. They wanted to extend the solution across all their channels, offering better protection to members against account takeover fraud, SIM-swap fraud, and phishing attacks. According to the FBI, $68 million was lost to SIM-swap attacks in 2021 alone.

The solution

By adding the extended authentication capabilities to their Q2 digital banking platform, 4Front CU members can now seamlessly use MemberPass to authenticate their identity and sensitive transactions using passwordless, biometric authentication across all channels – powered by Entersekt.

"MemberPass's extended functionality from Entersekt provides unmatched biometric authentication for our digital banking platform, while being in tune with members' unique preferences for user logins and payments," says Martin.

> Forward-looking financial institutions are realizing that they can offer more secure, user-friendly login and payment experiences that also protect members against modern fraud schemes without adding unwanted friction.

At Entersekt, we are committed to empowering banks and credit unions to conquer fraud and move towards a passwordless, Context Aware™ Authentication strategy.

"MemberPass credit unions have led the industry by enabling advanced technologies to authenticate members across multiple channels including contact centers, branches, and ITMs," added John Ainsworth, President/CEO at Bonifii. "By adding the capabilities from Entersekt, MemberPass further extends their protection to include user login for online and mobile banking."

Multi-factor authentication needs to fulfill two of the three elements:

- Knowledge: Something that the member knows, like a password or, in this case, an SMS OTP.
- Possession: Something that the member possesses, like a mobile device or a computer.
- Inherence: Something that the user is; namely, biometric information like a fingerprint.

When a member logs into their credit union profile, two of the three factors listed above should be independent of each other to make it harder for cybercriminals to access their account. Ideally, the authentication method should strike a balance between robust security and a smooth experience.

Members who enrolled in MemberPass found biometric authentication to be "fast and easy," with others saying that they are more inclined to use this method going forward.

4Front's extension of MemberPass on their Q2 online banking platform enables members to register their devices on both channels, providing safer and easier authentication for logins and high-risk transactions.

THE NEXT FRONTIER

From cross-channel to Context Aware™ Authentication

Cross-channel authentication is changing the game for digital banking security and customer experience. Context Aware™ Authentication will take this approach one step further.

Schalk Nolte

CHIEF EXECUTIVE OFFICER,
ENTERSEKT

As CEO, Schalk's vision for Entersekt is to bridge the gap between identity, authentication, and payments. He is responsible for overseeing the company, its investors and continued growth and development, and has been instrumental in facilitating the implementation of Entersekt's technology in more than 45 countries to date.

Not all banking customers are tech-savvy. Many are not proficient in identifying common attacks, unintentionally creating opportunities for fraudsters to target these vulnerable customer bases.

What's more, institutions deploying different solutions per channel at login, during a transaction, or at checkout during online shopping, create a disjointed authentication experience and are less effective against attacks. These measures only prompt fraudsters to jump to a different channel or change the nature of their attack — meaning fraud is seldom eliminated.

The limitations of single-channel authentication

The big risk with this type of single-channel approach is that it inhibits authentication platforms from obtaining and leveraging the additional context needed to eliminate friction and combat fraud. And this has a big impact on customers. Forcing them through a rigid journey on a device or channel that is not available or familiar to them will inevitably cause friction and a great deal of frustration.

On the technology side, single-channel authentication also prevents solutions from accessing the context from one channel to inform and improve authentication journeys on another. Both these factors create a disjointed experience that can break the customer's trust and result in transaction abandonment and customer churn.

Quite simply, banks must prioritize the user experience when establishing a safe environment for transactions. Not only does fixing the user experience mean more transactions, but if done via a cross-channel solution, it also means better security.

> Though many financial service providers realize that authentication methods need to change, they may not know the next step to create the right balance between strong security and seamless customer experiences.

Enhancing security and customer experiences with cross-channel authentication

Cross-channel authentication means using a single authentication platform across all digital channels. This breaks down the silos between channels, improving security and creating a seamless and familiar customer experience.

There are many authentication offerings available today, including app-based authentication, FIDO authentication, risk-based authentication (RBA), and more. Individually, these methods contribute to combating fraud and mitigating threats, but they fail to gather the full context of each customer's transaction. That's because they're often deployed as a single vendor's solution that either does not talk to the rest of the ecosystem or takes a lot of effort to facilitate a valuable data exchange. Furthermore, no individual solution offers 100% coverage across the spectrum of user devices or fraud attack vectors.

The result is gaps in coverage across an institution's channels, either through their customer authentication mechanisms, the use cases they offer, or the authentication methods available to customers.

Why Entersekt's approach to customer authentication is different

Entersekt's customer authentication solution is unique as it provides not only secure, but near-frictionless cross-channel authentication experiences.

How? Well, if a transaction is assessed as low risk, a customer's payment should go through without friction. However, depending on an organization's policy and risk tolerance, they may choose to challenge the customer for certain transactions. Cross-channel authentication adds tremendous value at this stage. For the customer, this step-up authentication is a secure and seamless experience because they validate the payment using the same authentication mechanism used to log in or perform other transactions with the bank. It's a familiar and hassle-free experience.

Benefits for banks are that there's no need for a separate authentication mechanism. Nor do they need to get bogged down trying to integrate their current authentication solution with their ACS.

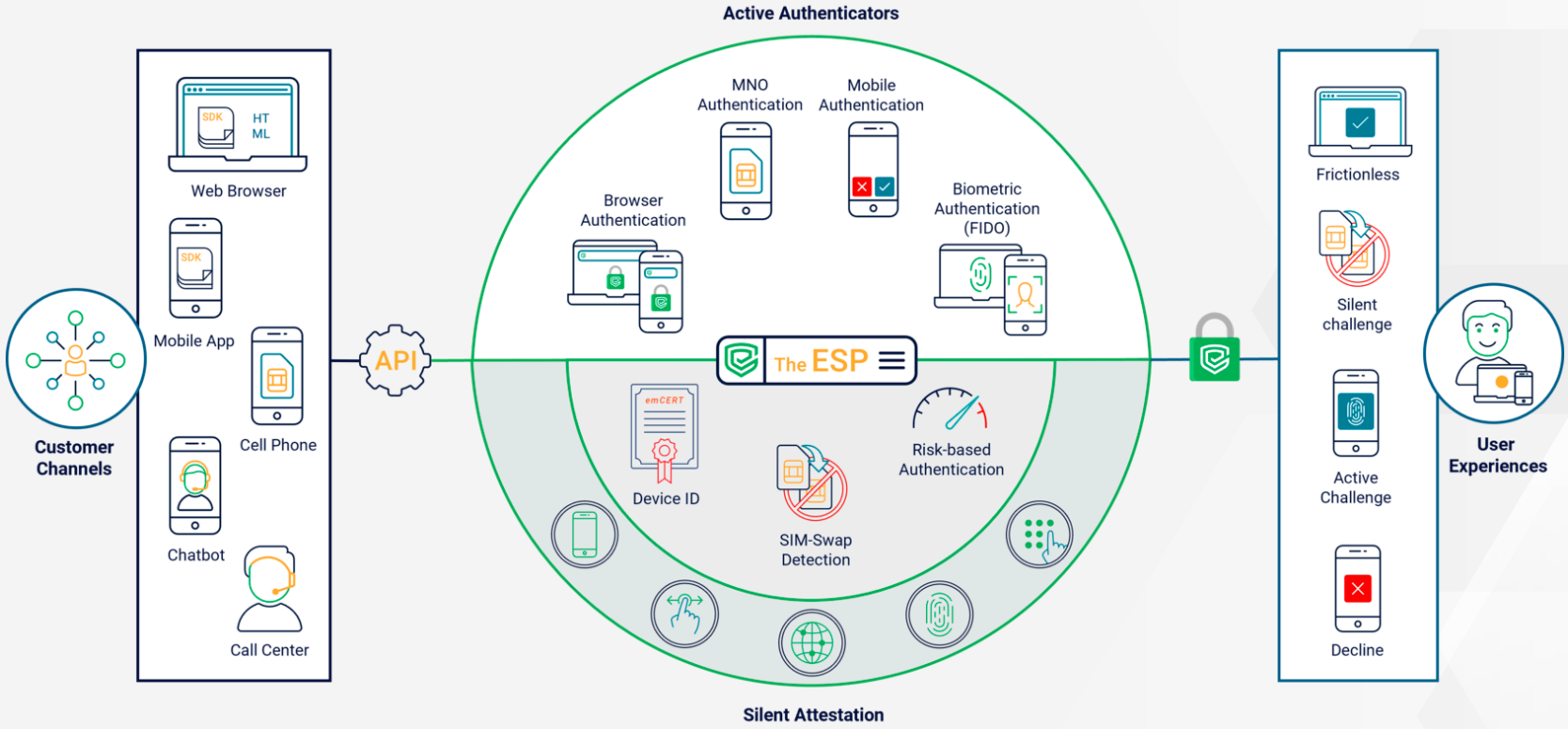
Entersekt's partnership with Capitec Bank in South Africa demonstrates how FIs can enhance the security of e-commerce payments and reduce friction at checkout.

Capitec uses Entersekt's market-leading 3D Secure solution, which harnesses the power of RBA provided by NuData Security, a Mastercard company. RBA enables the solution to silently track a user's behavior and identify high-risk interactions in real-time for a seamless, secure user experience. Yet, this is only the tip of the iceberg.

The next frontier: from risk-aware to Context Aware™ Authentication

Context Aware™ Authentication is the next frontier and, by intelligently layering RBA within our cross-channel solution, Entersekt is taking the entire authentication experience up several notches.

By combining an ecosystem of third-party integrators and a collection of both silent and active authentication mechanisms, banking customers experience the most secure and seamless authentication journey possible, across all digital channels.



The Context Aware™ Authentication ecosystem: A combination of third-party integrators and both silent and active mechanisms.

Ultimately, Context Aware™ Authentication provides a complete, context-rich picture of both the user and the interaction in real-time and allows for a curated authentication journey for the customer, for that specific interaction.

Unfortunately, banks using static, single-channel authentication policies do not take additional context into account, and their customers need to jump through extra hoops just to approve their transactions on another device or channel, which might not even be enrolled with them at the time of authentication.

> Entersekt's Context Aware™ Authentication solution leverages the context of each interaction between the customer and the institution to determine the best authentication mechanism to employ in the moment.

This is the key to building the next generation of authentication solutions.

Security needs to have great user experience. But to achieve that, you need to know what your customer is doing, where they are doing it from, and on which device, along with details of which authenticator is available. Only then can the best, most secure authentication experience be selected for that transaction.

Context gives us all that.
Hello, Authentication 2.0!

Learn more about Context Aware™ Authentication!
Click here

About **Entersekt.**

Entersekt provides transaction authentication to financial institutions that is both secure and free from unnecessary friction. Our single, cross-channel platform empowers these institutions to build great user experiences for their customers, helping to drive revenue growth without adding further costs and complexities to their ecosystems.

For over a decade, we have enabled some of the world's most prominent financial brands with the tools and confidence to conquer fraud, compliance, disparate customer journeys, and the related bottom-line impact of reputational damage and customer loss. Backed by companies like US-based Accel-KKR, one of the world's top private equity firms, Entersekt continues to innovate and expand its global footprint.

For more information about Entersekt, or to speak to an expert, please visit www.entersekt.com or email info@entersekt.com.

/Entersekt

@Entersekt

/Entersekt

Copyright © 2023 Entersekt. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.