transmit security

The Impact of Passwords on Your Business

Why Passwords Are to Blame for Loss of Revenue, Identity Attrition and Poor Customer Experiences

Passwords, despite their bad reputation, are still very much in use throughout all industries - inevitably leaving consumers to deal with poor user experiences and companies with an immense loss of revenue.

As our world continues to rely on digital services for almost every factor of our lives (think: banking, grocery shopping, work and socializing), our reliance on passwords and the need to manage our digital identities has become something that customers and vendors need to properly manage. In fact, it should be at the forefront of any customer experience journey and part of any security plan.

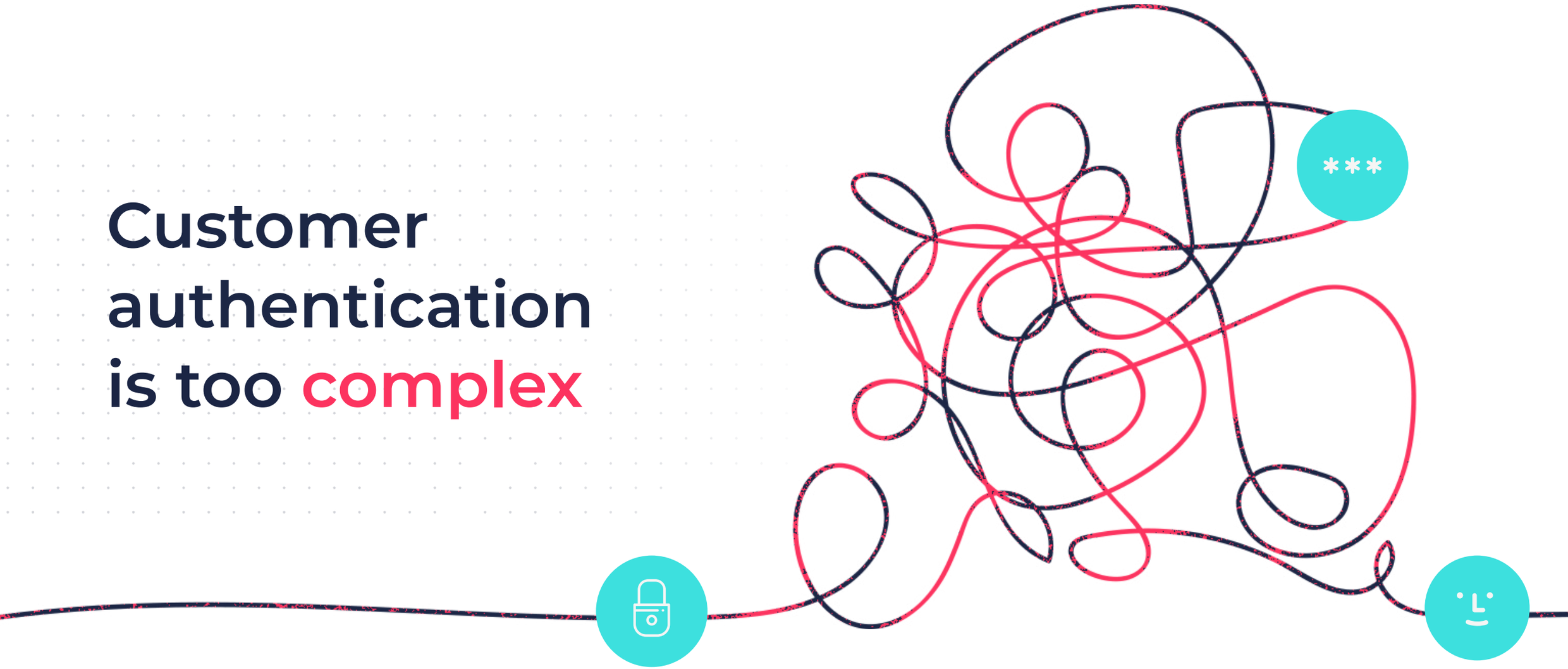
In this report, through the insights of 600 U.S based consumers aged 18 - 54, we'll show that the state of customer authentication, as it stands today, is certainly not up to par with the high demand for a seamless customer experience.

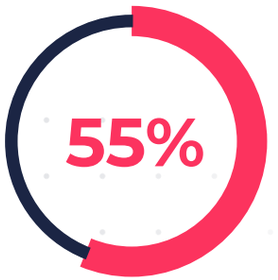
The findings of this report show how necessary it is for authentication to evolve beyond the use of passwords. More than necessary, the market is ready and equipped for change towards a passwordless future. This is evident considering that, today every mobile device for sale is designed with built-in device-based biometrics.

By getting rid of password dependency, companies will be able to meet the standards of customer service that consumers have come to expect across all industries, platforms and services.

Table of contents

Customer authentication is too complex

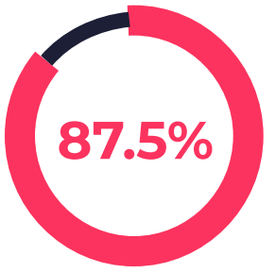




of consumers have stopped using a website because the login process was too complex.

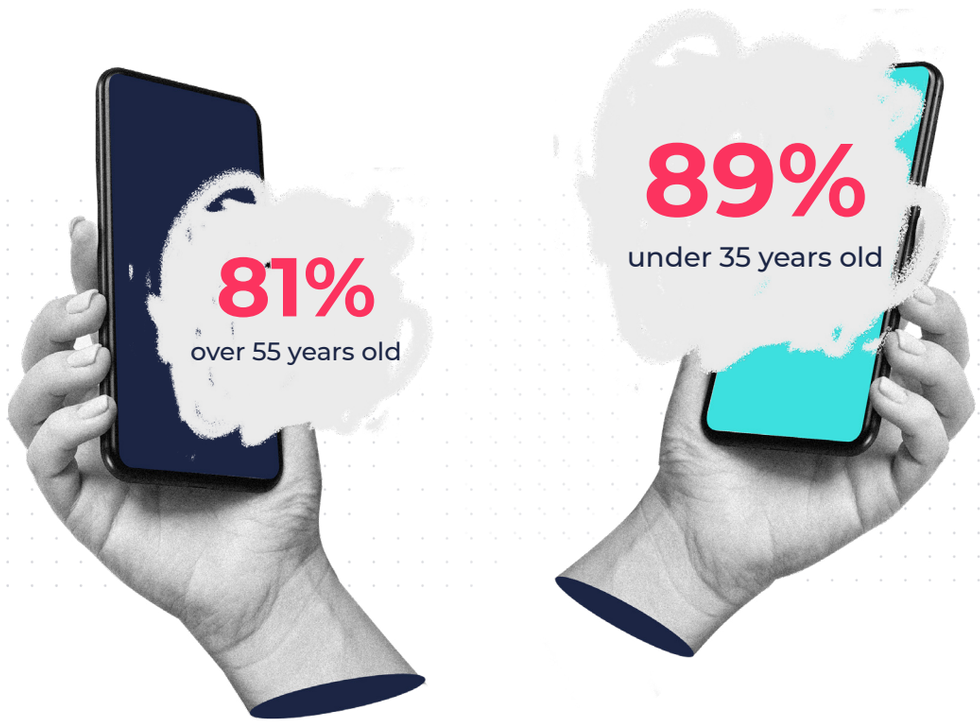
There's long been an understanding in the industry that passwords need to be retired due to the complexities they bring to customer authentication. Identity and authentication practices tend to either ensure high levels of security or an optimal user experience - but usually not both. In many cases, if you are in search of strong authentication that usually comes at the price of usability. Traditional methods of 'strong' authentication include knowledge-based questions, one-time codes sent via text messages or email or the use of hardware devices. Basically, a process full of complexity, roadblocks and frustration.

Due to these complexities, many consumers find themselves locked out of their own accounts. Causing only more frustration and irreparable brand damage.



of consumers found themselves locked out of an online account due to too many failed login attempts.

Of those locked out, **young consumers** are locked out slightly more. This could be due to a higher number of accounts than those that are older. However, the numbers remain high across all age groups.



Transmit Security's CEO, Mickey Boodaei attributes the the high frequency rate of failed logins to the following factors:

Technical issues

- Unknowingly using caps lock or the wrong language keyboard.
- Complex password requirements such as the use of a symbol or capital letter.

Too many passwords

- With too many passwords to remember, customers resort to guessing until they are locked out.
- With some sites forcing users to update their passwords regularly, customers don't remember the most recently updated password for an account.

Attackers failed attempts

- When hackers unsuccessfully try multiple passwords, via guessing, during an attack the account is blocked.

What are the implications of getting locked out of an account to both customers and vendors?

Customer frustration and stress

88% of users are less likely to return to a website after a bad user experience *(Designers[1])*

Session abandonment

About a third of online purchases are abandoned at checkout because consumers cannot remember their passwords *(MasterCard[2])*.

Increase in support calls and inquiries

Up to 40% of a service desk's call volume is just password resets *(Gartner[3])*.

- https://www.toptal.com/designers/ux/ux-statistics-insights-infographic
- http://www.cs.ox.ac.uk/files/9113/Mobile%20Biometrics%20in%20Financial%20Services.pdf
- https://ayehu.com/wp-content/uploads/2015/05/AD-Password-reset-tool.pdf

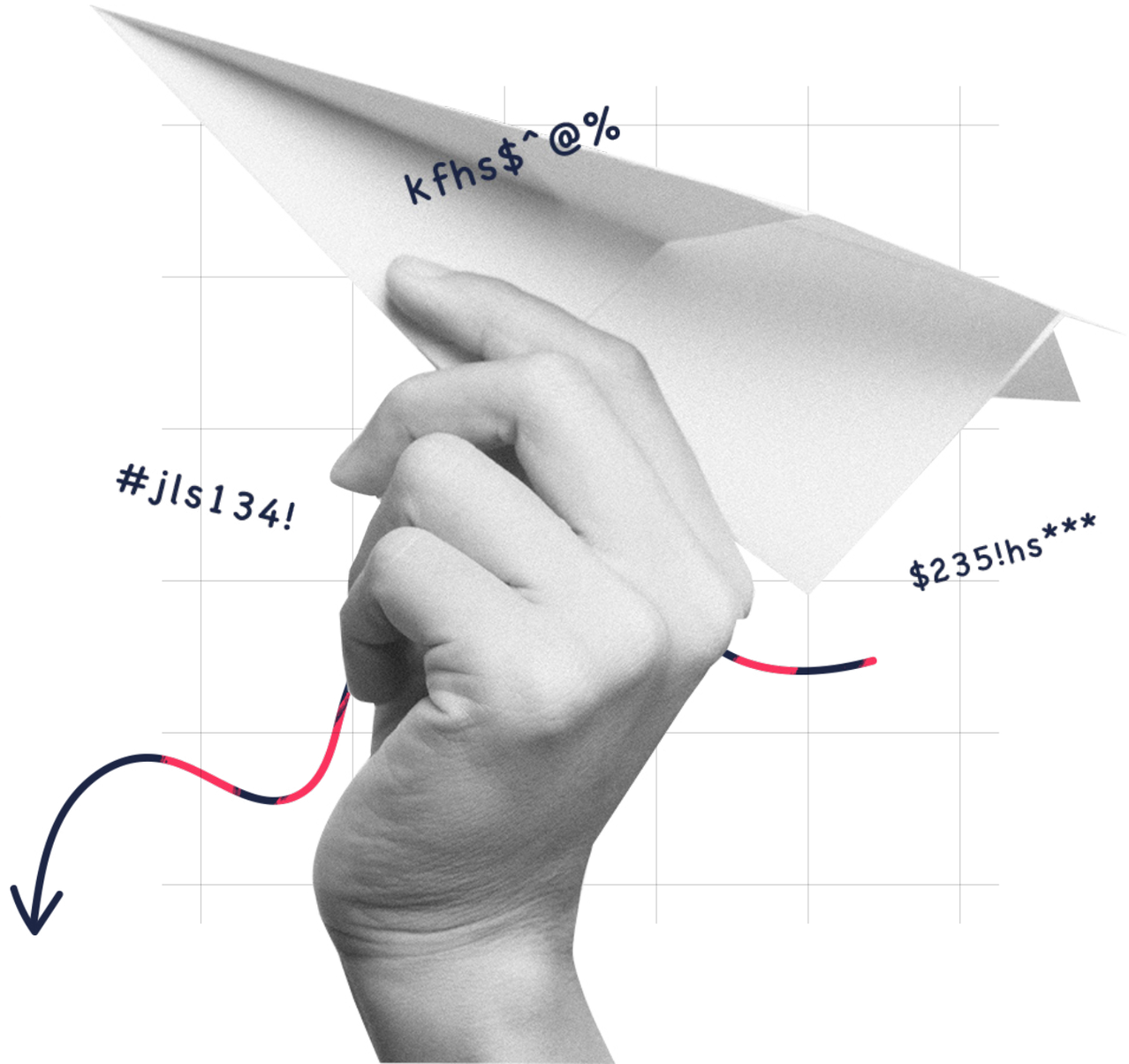
How a passwordless approach can solve the issue of complex authentication

As you can see from the numbers above, failed login attempts are an extremely common scenario that consumers have to deal with. Getting rid of passwords entirely would solve the issue of customers not remembering their passwords and therefore getting locked out of their accounts. By eliminating passwords all together, all the frustration and friction within authentication today would automatically be taken out.

- Customers wouldn't have to worry about remembering multiple passwords.
- Organizations won't have to deal with the endless volume of password reset inquiries.
- Vendors could offer a more secure and user-friendly customer experience.

By replacing passwords with biometric technology and device-based authentication, customers will be able to seamlessly and effortlessly access their online accounts. Due to this improved experience, vendors will benefit from an increase of customer loyalty which naturally leads to more profit. With no passwords in sight, the move to biometrics also reduces the ability of hackers to perform account takeover attacks as there is nothing to 'steal'.

Password sharing implicates business, revenue and security



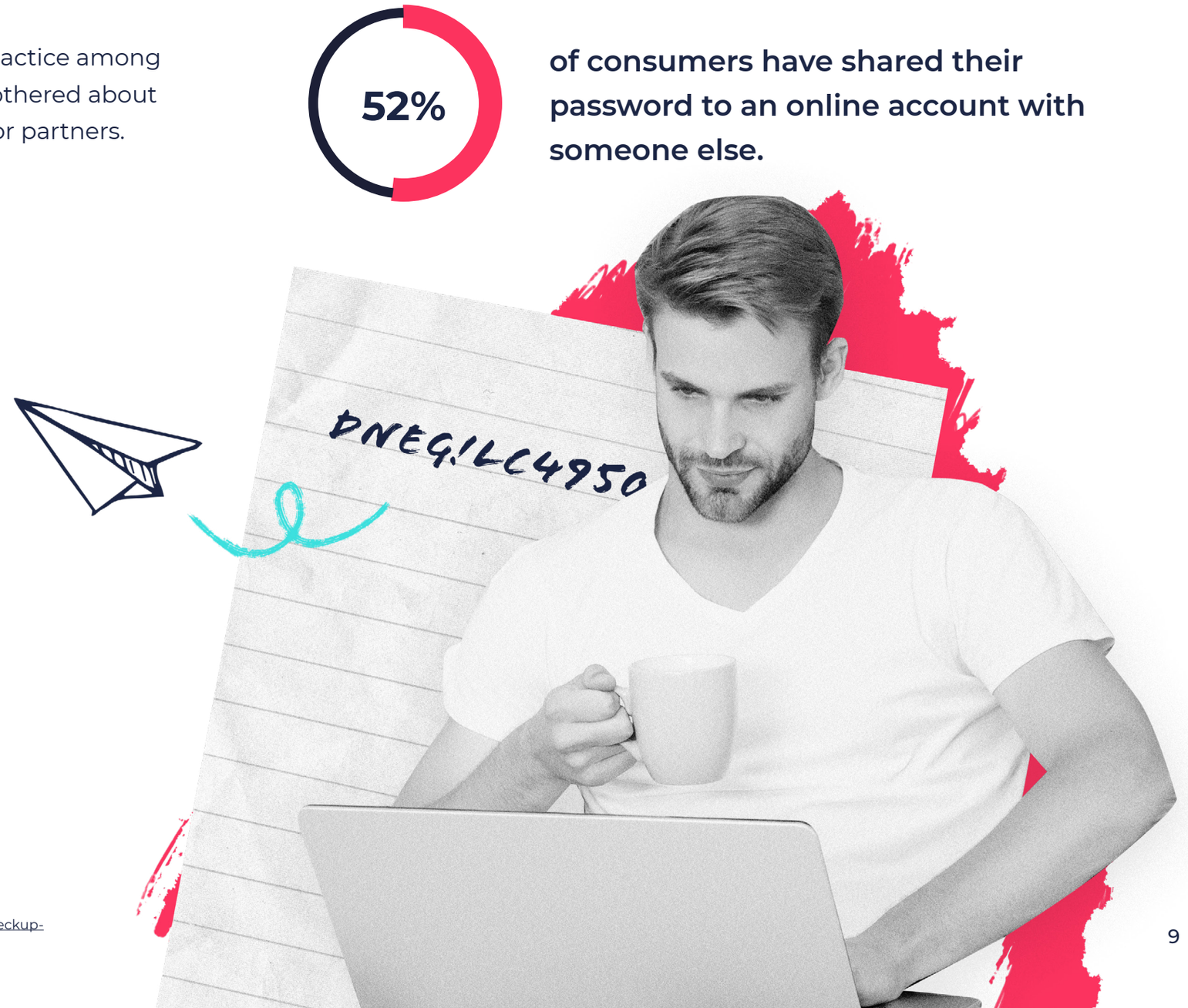
As you can see, password sharing is a common practice among many consumers. Customers don't seem to be bothered about sharing their passwords with colleagues, friends or partners.

41%

of consumers said they share their passwords often.

1 in 10

Californians still have access to a password belonging to an ex-partner, a former roommate or colleague *(Google[4])*.

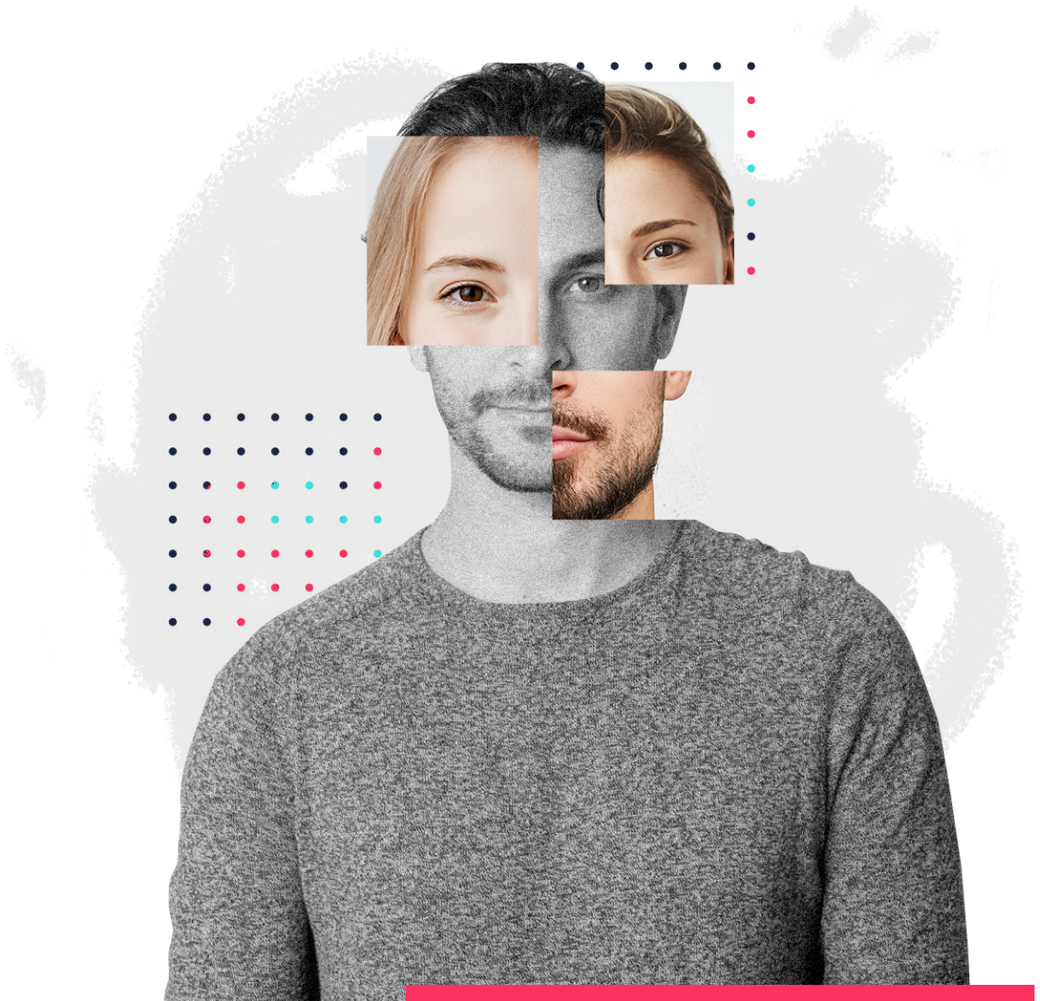


of consumers have shared their password to an online account with someone else.

https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf

Passwords are a pain for users to remember, keep track of and maintain. Since many users have dozens of online accounts they rarely update their passwords. Meaning, if their password is shared once the likelihood of someone abusing one or more of their accounts is high. Once a password is shared there is very little control on how it's used further.

This implicates businesses directly in the following ways:



Licensing abuse

If users have access to a password for an already paid account they are effectively avoiding paying (which means less revenue for you as a service provider) for a second account. Think of how many people share Netflix accounts!

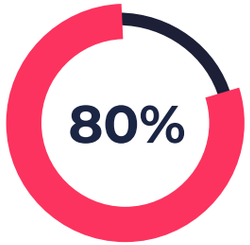
Usage monitoring and personalization

If accounts are being shared by multiple users, service providers are less likely to accurately monitor usage and are unable to correctly personalize their offerings - their user experience can't be optimized or personalized to meet their users expectations. Service providers can't give their customers what they want because they are unable to see clear user activity. This inability directly impacts potential revenue.

Password sharing also poses a threat to security

Given that **65% of users re-use the same password across multiple accounts** (Google[5]) once users share that one password with someone else they are essentially handing over access to multiple accounts they own.

Hackers know (and use) this too



80% of hacking-related breaches are linked to passwords (Verizon[6]).

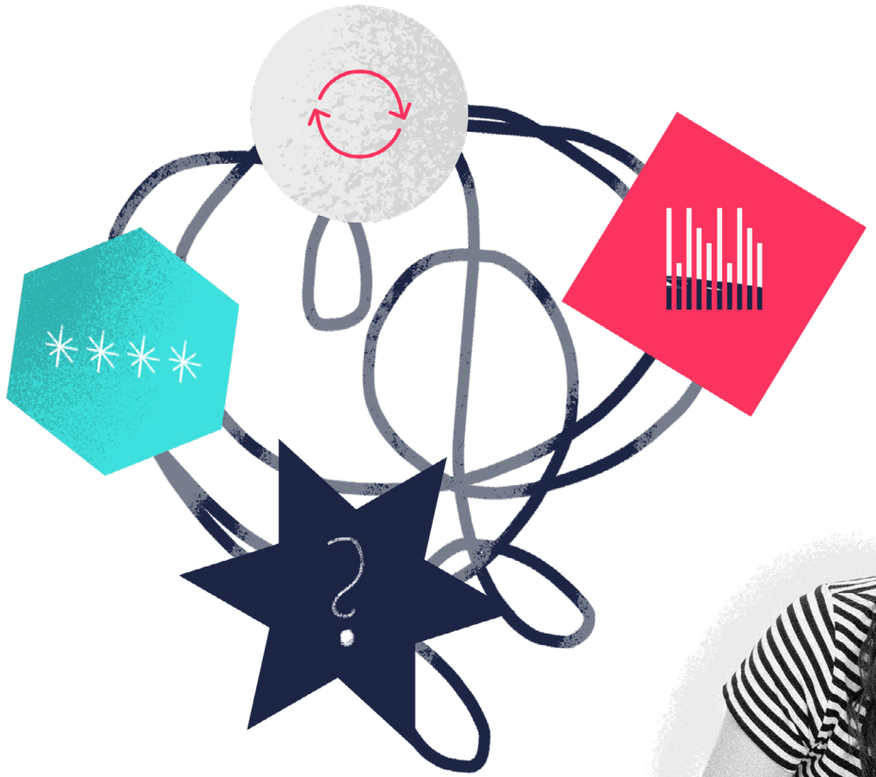
Once hackers gain access to one account they often try the same password, or variants of it, to try and gain access to more accounts.

How a passwordless approach can solve the issue of shared passwords

If online vendors offered a passwordless solution that used device-based biometrics, effectively removing passwords from the entire process then service providers could ensure that for every account there is only one intended user. More than that, service providers could more accurately monitor and personalize their user journeys leading to more potential revenue.

- https://services.google.com/fh/files/blogs/google_security_infographic.pdf
- https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Customers face inconvenient user experiences



A lot of money goes unspent in the online world. Many organizations are losing millions in potential revenue simply because customers can't remember their passwords (or refuse to participate in a long and complicated sign up process). Customers will spend valuable time adding items to their cart but when asked to re-enter or update their information they flee. Why? Because it's inconvenient and they know they can hop on over to the next site that won't make them jump through hoops to sign up or check out successfully.

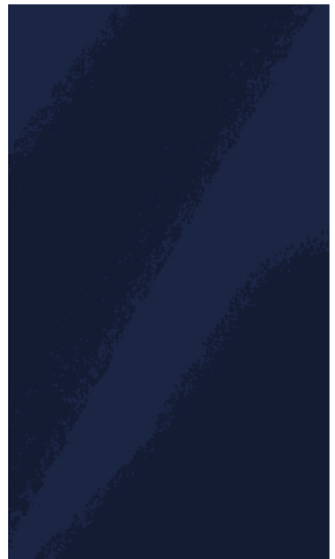
Consumers are already overloaded with logins and passwords.

1 in 4 consumers will not set up an account because they don't want to remember yet another password (FIDO[7]).

The friction and frustration involved in opening up an account is enough to make any consumer abandon a session no matter how badly they want your product or service - it's just not worth it.

66%

of consumers will leave a website if the registration process is too complex.

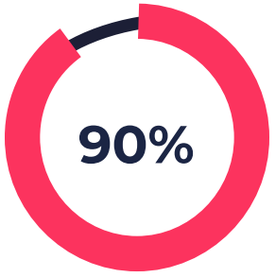


92%

of users would rather leave a website than recover or reset their login credentials.

64.5%

of consumers will abandon a website if asked to create a username and password.



90% of consumers flip between multiple devices in one day. (Google[8])

A single consumer uses a multitude of devices every day depending on their needs and environment. More inconvenience is faced when customers have to login or sign up to the same service across different devices. Many online services do not provide a seamless cross-channel experience which leads to more frustration and a drop in customer loyalty.

How a passwordless approach can solve the issue of inconvenient user experiences

Account opening and registering a password is a generally unpleasant and stressful experience for consumers. Therefore, when faced with this task consumers abandon the registration process all together. It's clear that processes that involve passwords are not successful in converting customers throughout the entire buying process. This has a direct impact on any business.

By eliminating passwords and using a passwordless solution, consumers are much more likely to proceed in the journey as they won't have to deal with opening an account, signing up or remembering a password. Authentication without passwords enables customers to experience a unified cross-channel experience when signing in to various accounts across multiple devices. Websites that avoid the reliance of passwords have a significantly higher chance of reducing user attrition.

- https://fidoalliance.org/wp-content/uploads/2020/12/FIDO-Alliance-E-Commerce-Infographic-2.pdf
- https://services.google.com/fh/files/misc/multiscreenworld_final.pdf

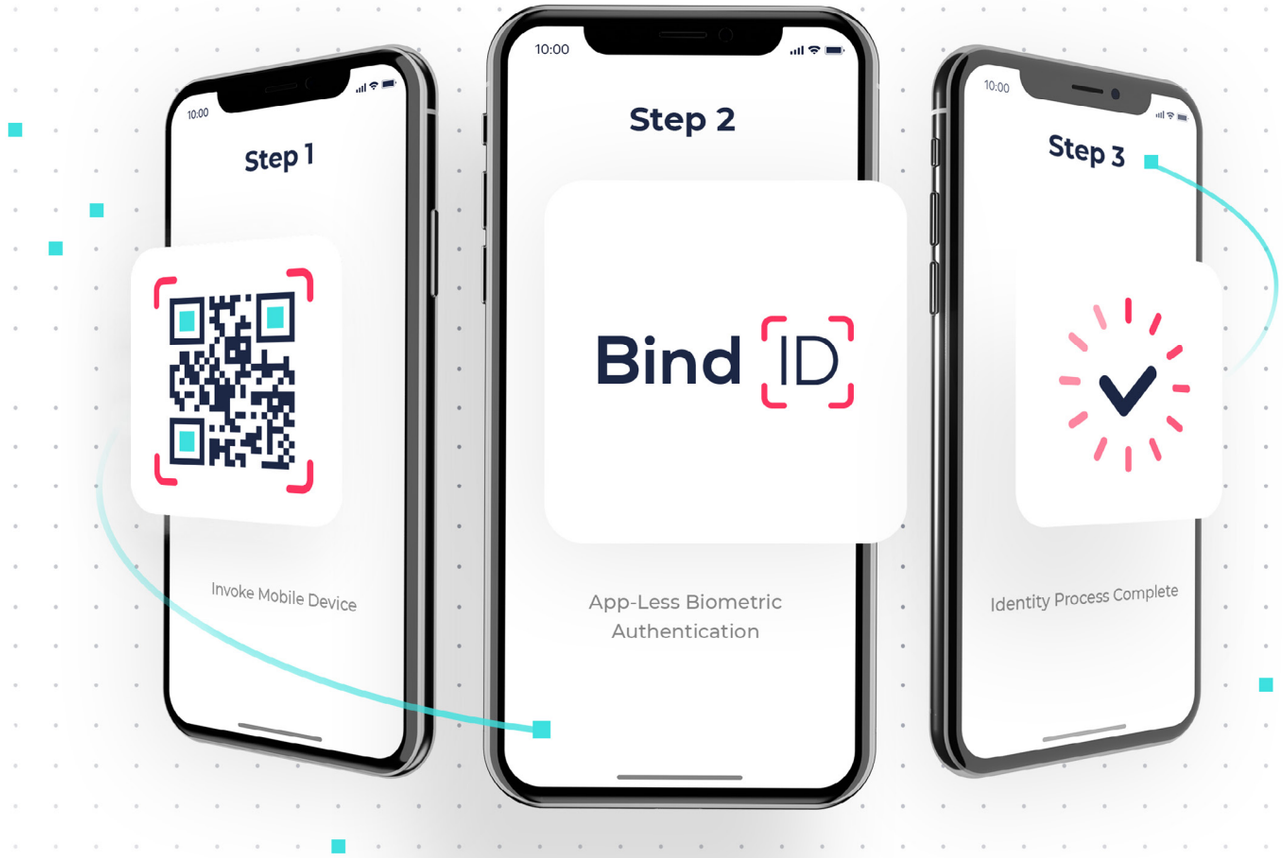
Key takeaways

Organizations are losing potential customers and therefore substantial amounts of money due to passwords.

Organizations suffer financially because potential customers drop off during a transaction or checkout process due to password management complexities.

Organizations are losing money due to customers who stop using their website because they are locked out or refuse to recover their account.

Bind ID:
The future of customer authentication



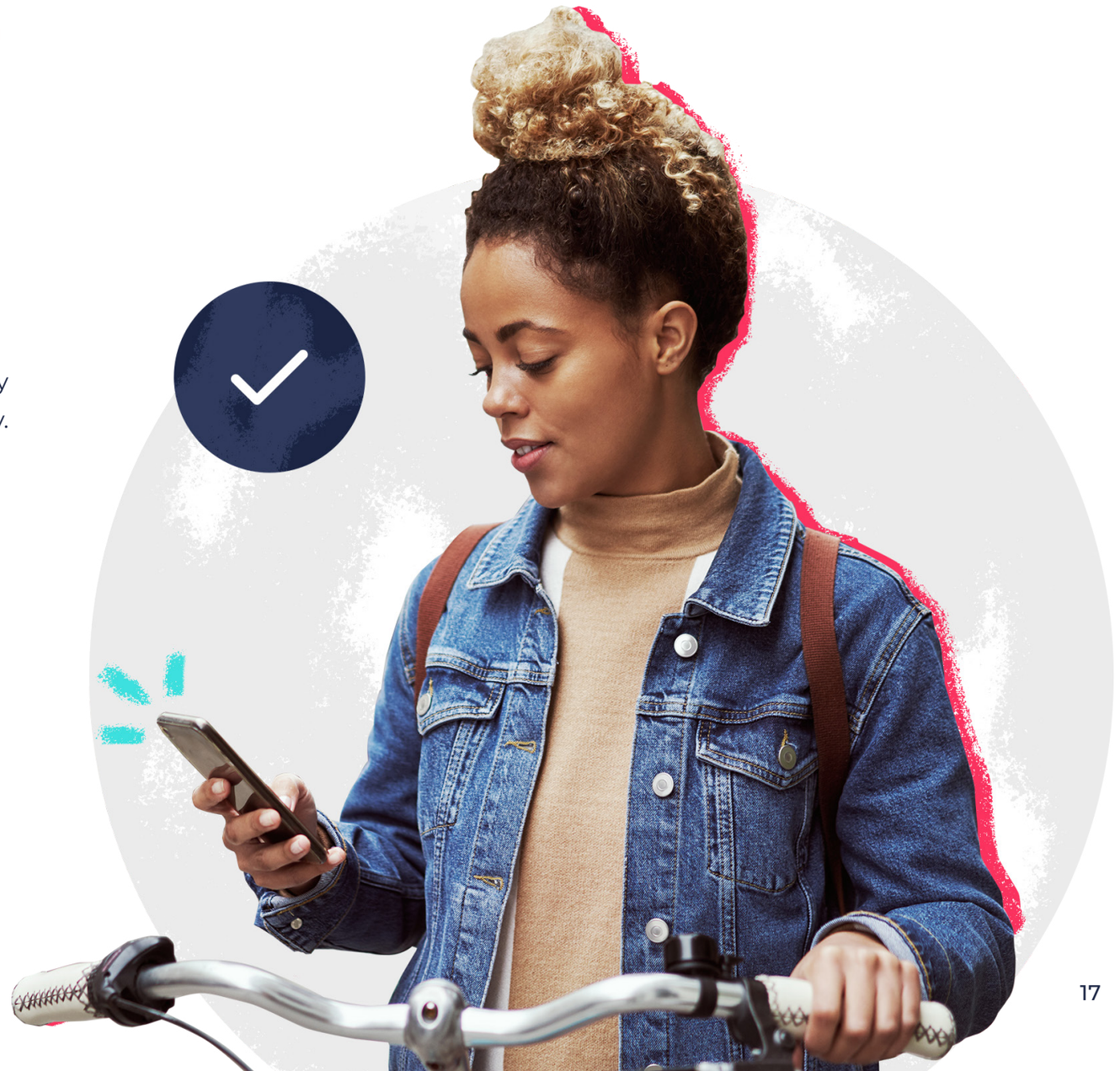
Given the current state of customer authentication, Transmit Security set out to create a passwordless solution that would cover all the issues discussed above.

BindID is the industry's first app-less mobile authenticator that uses FIDO2 certified built-in device biometrics for reliable and consistent customer authentication across every device and channel.

Using innovative technology, customers can finally experience a truly passwordless method of authentication without downloading any additional app. Guaranteed seamless authentication experiences every time allows for satisfied customers and an increase in customer loyalty. No matter how large your enterprise, you can effortlessly implement and scale BindID across all your channels.

of customers believe that authentication via biometrics (fingerprint or face scan) is more or equally trusted than a regular password.

From this statistic it's clear that customers are open and receptive to a new, more modern way of authentication. By providing an easier and more convenient method of authentication, customers are able to build trust with vendors and in turn increase customer loyalty.



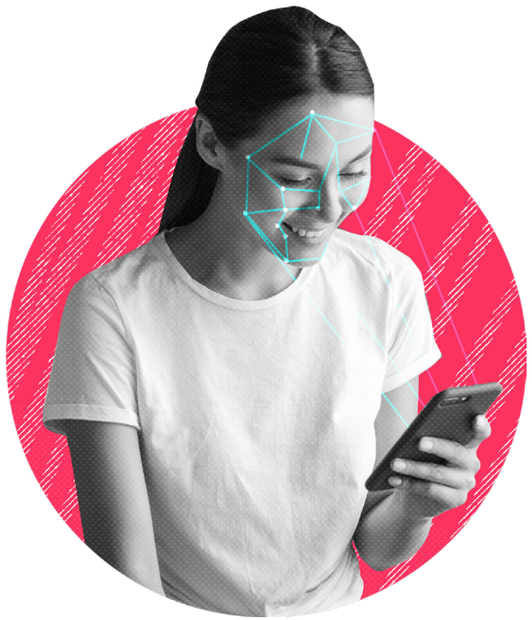
transmit security

BindID marks the end of an era. No more multiple IDs and credentials needed for each website. No more password resets and locked accounts. For the first time ever, customers can authenticate using biometrics using just their mobile device. BindID makes authentication simple, unified and much more secure.

- Mickey Boodaei

Paving the way towards a biometric future

As a committed board member of the FIDO Alliance, Transmit Security has embedded the latest biometric technology within all of our products. In a study conducted by the FIDO Alliance it was made clear that consumers prefer retailers that enable them to log in and make transactions simpler by using their built-in device-based biometrics.



68%

of consumers would prefer to use fingerprint or FaceID than traditional two-factor authentication methods *(FIDO[9])*.

- https://www.biometricupdate.com/202011/two-in-three-prefer-biometrics-to-mfa-for-online-retail-fido-alliance-research-reveals
- https://fidoalliance.org/new-research-reveals-consumer-frustrations-with-online-retail/

60%

of consumers believe retailers offering on-device authentication care more about their customer experience *(FIDO[10])*.

By utilizing the latest FIDO protocol, which ties the biometric profile of a user to an ID, we're able to offer a passwordless solution that:

1. Uses safe built-in, device-based biometrics.

2. Ensures a delightful and seamless experience free from passwords, user ids and failed logins.

3. Is easy to implement across all channels and devices.

4. Satisfies customers which means better business and customer loyalty.

About Transmit Security

Transmit Security, the identity experience company, is at the forefront of creating frictionless identity experiences for both customers and workforce across all channels. Our user-centric solutions, which includes the industry's first app-less biometric authenticator, are proven to ensure an effortless and truly passwordless experience - effectively reducing all forms of identity attrition and saving enterprises substantial costs.

Transmit Security was co-founded by serial entrepreneurs and investors, Mickey Boodaei and Rakesh Loonkar in 2014 with the aim of changing the security identity landscape. In 2020, Deloitte recognized Transmit Security as the 5th fastest growing company in North America. Today, our powerful technology is used by millions of end-users worldwide spanning across all industries and platforms.