VERIDIUM
TRUSTED DIGITAL IDENTITY

WHAT PASSWORDLESS AUTHENTICATION MEANS FOR YOUR BUSINESS

BENEFITS INCLUDE FASTER CUSTOMER ONBOARDING, STREAMLINED CLINICAL CARE AND SCA COMPLIANCE

Since all organizations use passwords, the benefits of passwordless authentication – improved security, a streamlined authentication experience and reduced password management costs – apply to all industries.

But what other factors are driving passwordless methods, which, according to Gartner, 60 percent of global companies will implement by 2022?

To find out, we asked organizations why they eliminated passwords or are looking to. They said that passwordless authentication and digital IDs let doctors access lab results faster, allow a law firm's clients to easily share evidence with lawyers and streamline customer onboarding at banks, among other uses. Eliminating passwords is also factoring in to digital transformation projects. Organized by industry, here are their stories.

A major Swiss bank reduced password management costs by 80 percent by adopting passwordless authentication for its employees

FINANCIAL SERVICES

People expect a digital approach to conducting financial transactions. Typing in a password to transfer money with a bank's mobile app doesn't appeal to them. Neither does gathering paper documents and submitting them at a bank branch to comply with know your customer and anti-money laundering regulations. They'd prefer modern approaches that leverage passwordless authentication and digital IDs.

The convenience associated with passwordless authentication is why bunq, a European challenger bank, partnered with Veridium to bring it to their customers. Instead of entering a password, bunq's customers use their biometrics and smartphone to authenticate.

Veridium also helps provide a better customer onboarding experience. Instead of submitting paperwork for know your customer requirements, a bank's customers can use Veridium as part of a digital ID program to confirm their biometrics against the ones stored in a database. Using digital IDs lets financial services organizations spend less time manually confirming a person's identity.

Financial services organizations can also see operational benefits from going passwordless. A major Swiss bank reduced password management costs by 80 percent by adopting passwordless authentication for its employees. Using Veridium eliminated password resets and token maintenance and gave employees an easier, consistent authentication experience, regardless of device.

INSURANCE

In the insurance industry, digital IDs offer an easier and more convenient approach for customer onboarding and fulfilling know your customer requirements. Instead of submitting paperwork (or typing in a password) to prove who they are, customers can use passwordless authentication as part of a wider digital ID program.

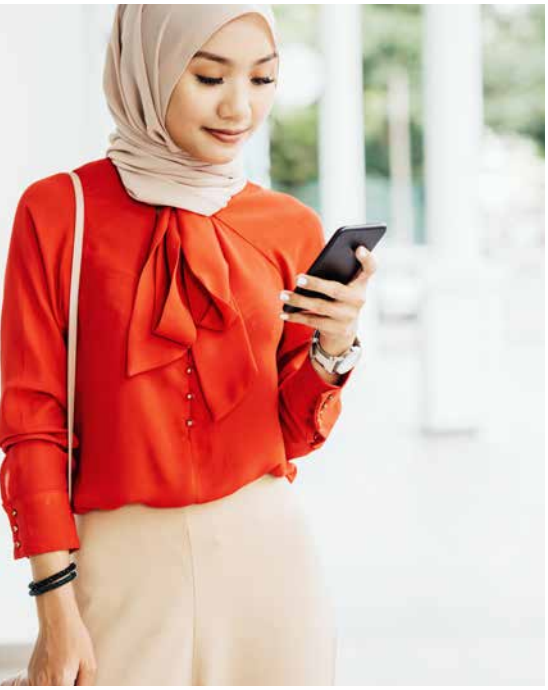
Passwordless authentication also benefits insurance agents who upload documents to a portal for a claim. Getting rid of passwords means agents don't have to remember them or waste time resetting them. Going passwordless lets agents be more productive and spend more time helping customers instead of dealing with authentication.

HEALTH CARE

Modernizing how health care providers authenticate fits with digital transformation projects hospitals are undertaking around using technology to provide better care. For example, many hospitals are deploying Citrix Workspace as part of digital transformation projects to improve clinical workflows. TThey're also looking into introducing passwordless authentication into Citrix Workspace since it fits with the projects' greater goal of making practicing medicine more efficient and productive. Going passwordless means doctors and nurses don't have to remember passwords to access lab tests or fumble with a key card to unlock a workstation.

Passwordless authentication also provides superior protection of patient data. Some hospitals use password management tools that allow single sign on to make authentication easier. But attackers that infiltrate these tools have access to a care provider's passwords and all the patient information they guard. Eliminating passwords also eliminates an attacker's opportunity to use them to access patient data.

Modernizing how health care providers authenticate fits with digital transformation projects hospitals are undertaking around using technology to provide better care



MEDIA

The multitude of streaming services available means people will always find something to watch. But it could also mean an increase in piracy as some decide to share passwords instead of purchasing several streaming services.

Streaming services, which once tolerated and accepted password sharing, are now looking to crackdown on the practice. The economics behind streaming require it. Streaming services have spent billions on original programs and the rights to older shows. To make a profit, these services need paying customers.

Passwordless authentication lets streaming companies address privacy by linking one account to one user. Since biometrics can't be shared, only paying subscribers can stream content. Features like geolocation can limit account access to locations near a subscriber's billing address while behavioral biometrics add another layer of security to authentication.

Customers expect to easily stream content from any device but passwords hinder this experience, especially when customers forget their password when logging in to a streaming service from a new device. A forgotten password means a password reset, a process that can prove complex. Removing passwords removes this complexity and lets people access content quickly and easily.

Using your smartphone and biometrics for transaction authentication preserves the fast online shopping experience people are accustomed to while providing SCA

RETAIL

People expect a seamless and quick online checkout process. Retailers in Europe are figuring out how to offer this while meeting the strong customer authentication (SCA) component of PSD2, which requires two-factor authentication for some online purchases.

Many retailers (and payment processors as well) struggled with implementing SCA, resulting in an 18-month extension to comply with the regulation. In fact, a Deloitte study found that maintaining a positive user experience when applying SCA was the top concern among banks. Ideally, approving a transaction wouldn't require entering a password or PIN. Waiting for and then entering the PIN that needed to complete your online purchase is a hassle. Using your smartphone and biometrics for transaction authentication preserves the fast online shopping experience people are accustomed to while providing SCA.

Passwordless authentication can also be used to provide a customized brick-and-mortar shopping experience. After entering a store, an associate can scan a customers' fingerprints and pull up their account, which can show information like color preferences and previous purchases. Having this information readily available can help associates make better product recommendations, leading to increased sales and satisfied customers.

GOVERNMENT

Passwordless authentication and digital IDs can improve how people access government services while reducing fraud. In the U.S., using a digital ID for identification instead of a Social Security number could decrease tax fraud. Fraudsters launch phishing campaigns during tax season to deceive people into divulging personal information such as Social Security numbers and birth dates. With these details, they can file a fake tax return and obtain a person's refund. But using a digital ID makes filing a fraudulent tax return with stolen credentials more challenging.

Decreasing fraud is why one Latin American country is considering having small business owners use digital IDs to file taxes. Currently, small business owners gather documents proving their identity and take them to a government office to obtain tax refund forms. Some owners used forged IDs to illegally obtain other business' refunds. Using digital IDs would allow the government to ensure that valid business owners receive refunds while saving business owners a trip to a government office.

Governments are considering several other uses for digital IDs. One country may use them to better confirm a prisoner's identification before distributing medication. The department of agriculture in one European country wants to use them to combat fraud around farmer subsidies. Instead of submitting paperwork for a subsidy, the farmers would use a digital ID to confirm their identity. Other governments are looking into using digital IDs for how people submit visa applications and border control at airports.

Passwordless authentication provides law professionals with a secure, universal authentication experience whereever they're working

LEGAL

Law firm employees, who may work from a court house or a client's office, need an authentication process that's as flexible as their work environments. Often times, authentication in the office calls for a user name and password while authenticating in the field requires either a hard or soft token. But hard tokens are a hassle for employees to carry around and IT departments to maintain. And threat actors have become more skilled at intercepting soft tokens like one-time passwords. Passwordless authentication provides law professionals with a secure, universal authentication experience whereever they're working.

In a profession centered around billable hours, law firm employees need a way to quickly and easily access work applications and services. Using passwords can stymie this objective. Inevitably, a password will be forgotten and have to be reset, leading to time spent on authentication instead of a client's case.

An international law firm is looking into passwordless authentication as part of a larger digital transformation project around improving its client portal. Among other features requested, clients want to upload documents via the portal. That practice is prohibited since the portal is password protected and passwords don't provide irrefutable proof of a person's identity.

Going passwordless would let clients upload documents to the portal using their biometrics, providing non-refutable proof of who uploaded the document.

The problems with passwords – negative user experience, high reset costs, security risks – transcend industries and apply to all enterprises

ENTERPRISE

The problems with passwords – negative user experience, high reset costs, security risks – transcend industries and apply to all enterprises. The companies Veridium talks to are especially interested in using passwordless authentication for employee authentication, consumer authentication and transaction authentication.

EMPLOYEE AUTHENTICATION

Passwordless authentication lets employees forget their passwords forever. There's nothing for them to remember or complex password management policies to follow. This improves the user experience. Employees have a faster, easier way to authenticate so they spend less time resetting their password and more time working.

For organizations, passwordless authentication improves their security posture since there aren't any passwords for threat actors to steal and use in attacks. It also saves companies on the costs associated with password resets and lets IT staff handle more important tasks.

CONSUMER AUTHENTICATION

Customers are accustomed to accessing accounts, services and products using websites and mobile apps. Often times, using these digital channels requires entering a password. But knowledge-based authentication sometimes fails at providing a positive user experience. Passwords have to be remembered and are easily forgotten. And resetting them can prove cumbersome.

Meanwhile, smartphones have changed people's expectations around authentication. They've grown accustomed to touching a fingerprint sensor or using facial recognition to authenticate and not entering a password. To them, authentication shouldn't be a complex process, especially when their smartphone is involved. This is true whether they're accessing a mobile banking app, home thermostat or Amazon account.

Passwordless authentication provides consumers with the consistent and seamless authentication experience they want across devices and channels. Accessing accounts and services is efficient and fast whether the person is using a laptop browser or mobile app.

Passwordless authentication provides consumers with the consistent and seamless authentication experience they want across devices and channels

TRANSACTION AUTHENTICATION

Passwords can be lost, borrowed or stolen and are cumbersome to use, so they're not the best method of transaction authentication. That includes all types of transactions, such as signing legal documents, authorizing stock trades and approving online purchases.

Going passwordless makes transaction authentication faster and more secure. Maintaining the quick checkout process associated with online shopping is a priority for bank and payment providers as they implement two-factor authentication on some transactions to meet the strong customer authentication component of PSD2. Using passwords and PINs for a second factor could slow down the checkout process and lead to lost sales. Passwordless authentication utilizing biometrics preserves the effortless experience that online shopping is known for while meeting the requirements for SCA.

Passwordless authentication makes distancing yourself from high-risk transactions challenging. Unlike a password, biometrics are something you are and can't be easily used by someone else. Even if a biometric is stolen, liveness detection and behavioral biometrics make someone else using it nearly impossible.

UTILITY PROVIDERS

Mobile devices and apps are standard equipment for field workers at utility companies. Devices like smartphones allow them to do their jobs more efficiently by providing them with immediate access to job information and apps and services they need in the field. This makes fast and secure authentication critical. Password resets and other issues that prevent field workers from accessing mobile devices, apps and cloud services lead to missed appointments, project delays, upset customers and increase project costs.

Some utility companies want to eliminate passwords to improve how customers pay bills and access services using mobile apps and Web browsers. Customers frequently forget their passwords, necessitating a password reset. But often times, resetting a password takes a significant amount of effort, more effort than people would associate with paying a utility bill online and leads to a negative customer experience.

Not using passwords lets field workers quickly and easily access mobile devices by eliminating password resets. For customers, switching to passwordless authentication for account access makes bill paying easier and faster.

Not using passwords lets field workers quickly and easily access mobile devices by eliminating password resets

CALL CENTERS

Call centers are key channels for customers to learn about products, place orders, review account information and obtain support. But call centers are vulnerable to fraud leveraging social engineering tactics and information people post on social media. Asking customers for their security password, which is sometimes their mother's maiden name or the last four digits of their Social Security number, can't protect a person's account from a skilled threat actor. Scammers can use call centers to access customers' accounts and make unauthorized purchases, cancel plane tickets and change mobile phone plans, among other malicious acts.

Passwordless authentication helps businesses fight call center fraud. Instead of asking customers a knowledge-based authentication question that could be obtained by reviewing social media posts, call center employees can confirm callers' identities using their biometrics.

AND THERE'S MORE TO COME

With organizations just starting to adopt passwordless authentication and digital IDs, the use cases for this technology are emerging. As more businesses rethink authentication, expect passwordless authentication to play greater roles in how employees access applications, consumers access services and approve transactions. And look for passwordless authentication to appear in digital transformation projects as organizations look for modern ways for employees and customers to access services and information.

As more businesses rethink authentication, expect passwordless authentication to play greater roles in how employees access applications, consumers access services and approve transactions