THE STATE OF STRONG AUTHENTICATION 2019
ADOPTION RISES UNDER THREAT OF NEW RISKS AND REGULATIONS

January 2019

Sponsored by:

fido™

Independently produced by:

JAVELIN

TABLE OF CONTENTS

Overview 3
Executive Summary 4
Key Findings 4
Recommendations 6
Introduction 7
What is Strong Authentication? 8
Vulnerabilities Stack Up in Traditional Authentication Methods 11
Consumer Authentication 13
Beyond Security: The Other Benefits of Strong Authentication 17
Meeting Customer Expectations 18
Enterprise Authentication 21
What is FIDO? 26
Strong Authentication Industry Case Studies 27
Google 27
Tradelink 27
Visa 28
Methodology 29

TABLE OF FIGURES

Figure 1: Authentication Strength for Consumer and Enterprise Applications 9
Figure 2: Authentication Solution Table 12
Figure 3: Adoption of Strong Authentication for Consumer Applications 13
Figure 4: Adoption of Online Authentication Methods (Consumer) 14
Figure 5: Adoption of Mobile Authentication Methods (Consumer) 15
Figure 6: Impact of Regulatory Pressure on Current and Future Authentication Methods 16
Figure 7: Adoption of Strong Authentication by Sensitivity of Data Processed 17
Figure 8: Most Desired Authentication Features Among Consumers 18
Figure 9: Perceived Effectiveness and Ease of Use of Customer Authentication Solutions 19
Figure 10: Most Important Factors when Choosing an Authentication Solution 20
Figure 11: Adoption of Strong Authentication within the Enterprise 21
Figure 12: Adoption of Online Authentication (Enterprise) 22
Figure 13: Adoption of Mobile Authentication Methods (Enterprise) 23
Figure 14: Use of Non-Password Authentication to Protect Corporate Data Assets 24
Figure 15: Reasons for Using Only Passwords to Authenticate Employees and Contractors 25

FOREWORD

This original report, sponsored by the FIDO Alliance, examines the ways that organizations authenticate consumers in digital channels and employees within the enterprise, including the evolving role that strong authentication is playing in protecting accounts and securing access to valuable data and critical systems.

This research report was independently produced by Javelin Strategy & Research. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

Digital channels are more important than ever to how businesses reach their customers. And within the enterprise, communication and collaboration are more digitally-oriented than ever before. At the center of keeping it all secure is how users are authenticated, and that security is under siege. Weak authentication is being abused by criminals to compromise consumer accounts at depth and en masse. In response, regulators are raising the standards they expect businesses to implement to protect consumer accounts – not just for how strongly users are authenticated, but also how their data is protected. These threats to authentication extend beyond consumer applications into the enterprise as adversaries are gaining access to organizations' internal systems to impersonate corporate users through weakly authenticated entry points, stealing data and facilitating fraud. Fortunately, adoption of strong authentication, which can mitigate attacks from criminals and other adversaries across consumer applications and within the enterprise, is on the rise as organizations respond to these threats and pressure from regulators.

This study explores how businesses are implementing authentication to secure consumer applications and the enterprise, the factors they consider when choosing an authentication solution, the role that strong authentication is playing within their organizations, and the benefits that these organizations are realizing. For real-world examples, this report also includes case studies of organizations that are leveraging FIDO-compliant solutions to protect customers' accounts and the enterprise.

EXECUTIVE SUMMARY

Key Findings

Adoption of strong authentication has grown dramatically since 2017. With vulnerabilities affecting traditional authentication solutions on the rise, organizations are bolstering their authentication capabilities with strong authentication. The number of organizations using cryptographically-backed multifactor (MFA) authentication has tripled since 2017 for consumer authentication and increased by nearly 50% for enterprise authentication. The fastest growth is in consumer mobile authentication because of the growing availability of biometric authentication.

Strong authentication holdouts underestimate the risk to their businesses and customers. Organizations that do not currently use any strong authentication tend to see usernames and passwords as among the most effective and easiest to use methods for authenticating users. Other organizations fail to see the value of the digital assets they hold, despite cybercriminals' continuing to target a wide variety of consumer and business information. Two-thirds of businesses that use only passwords to authenticate their employees do so because they believe passwords are good enough for the type of information they are protecting.

Nonetheless, passwords are on a steady path to the grave. Over the past year, the reliance on passwords has declined significantly for both consumer and enterprise applications (44% to 31% and 56% to 47%, respectively) as these organizations increase their adoption of both traditional MFA and strong authentication.

Step-up authentication continues to be dominated by easily compromised authentication modalities. For consumer authentication, around a quarter of organizations use SMS OTP (one-time password) to authenticate users at step up, essentially tied with static and dynamic security questions. This necessitates the use of supplemental technologies to mitigate their inherent vulnerabilities, which increases costs. Use of more robust authentication methods, like hardware cryptographic keys, sees much lower use, at around 5% of organizations.

An evolving regulatory environment holds promise for accelerating strong authentication adoption for consumer applications. With the introduction of PSD2, along with data protection regulations in the EU and U.S. states such as California, businesses are feeling the heat. Nearly 70% of businesses agree they face strong regulatory pressure to provide strong authentication for their customers. More than half of businesses believe their authentication methods will not be sufficient to meet regulatory standards in a few years.

Organizations that adopt strong authentication are considerably more likely to value customer experience. Among all the factors organizations consider when choosing a solution for consumer authentication, organizations with strong authentication are 50% more likely to specify that a low-friction experience is a determining factor compared with other organizations (18% vs. 12%, respectively).

Laying a strong authentication foundation enables businesses to shift their focus from meeting regulatory requirements to delighting customers. While the most important factor in

selecting an authentication method among organizations relying on single-factor authentication or traditional MFA is meeting regulatory requirements, organizations that already use strong authentication instead are able to focus on selecting authentication methods that drive higher customer loyalty.

Regulation is less of a factor in the enterprise as businesses will look to practical concerns when selecting authentication methods. Ease of integration (32%) and cost (26%) are the most significant factors businesses consider when selecting an enterprise authentication solution. Ease of use is close behind, but compliance with industry standards and regulation fall to the bottom.

In the age of business email compromise (BEC) and other deception schemes, corporate email portals are frequently the weakest link. With just a quarter of enterprises employing either traditional MFA or strong authentication to protect access to corporate email accounts, fraudsters have an opening to deceive legitimate users into providing access to sensitive data or increasing permissions associated with an account they have compromised, or even convincing other employees to transfer funds to accounts under the control of criminals.

Google has doubled down on strong authentication. More than two years ago, Google published the result of its internal implementation of FIDO U2F security keys, reporting impressive outcomes. According to the company, there has not been a successful phishing attack against its 85,000-plus employees since it required use of physical security keys. Since the publication of this report, Google has taken a number of other notable steps toward integrating FIDO protocols into its consumer and enterprise authentication flows.

Tradelink has driven adoption across banking and now into government ID. Tradelink has driven adoption across banking and other public services in Hong Kong. After examining different technologies and standards worldwide, Tradelink decided to recommend and promote the use of FIDO based authentication starting in 2016. Since that time, acknowledgment by the relevant regulators has been a major factor in adoption by banks. In fact, the HK Government has indicated that it will leverage the FIDO standards to authenticate citizens online for the new HK Electronic Identity (eID) initiative from 2020.

Visa has made FIDO a central part of its new ID Intelligence service. Visa recently released its ID Intelligence suite of services to help organizations better identify and authenticate users. Through this service, these organizations can easily obtain authentication capabilities from a trusted provider via a single point of integration. Visa has chosen to make a FIDO-based implementation of biometrics one of these offerings as it aligns with their strategic approach to authentication.

Recommendations

Implement strong authentication online and in the mobile channel. Cryptographically-backed MFA standards for strong authentication infuse the benefits of traditional MFA with greater resilience against data compromise by eliminating the need to transmit actual authentication data (passwords, one-time codes, or biometric information) from the user's device to the authentication server. Additionally, by standardizing the protocols used by authentication methods when communicating with the central server, it becomes easier to implement new authentication methods as they become available, lowering the cost of keeping up with regulation, customer expectations, and ever more sophisticated fraud schemes.

Plan to sunset one-time passwords (OTP). The vulnerabilities inherent in OTP have become increasingly evident, with cybercriminals using social engineering, phone porting, and malware to compromise these authenticators. While OTPs still have some advantages in their near-universal reach to users, the security benefits are growing slimmer.

Leverage risk-based authentication to judiciously apply step-up. Using solutions such as device recognition, geolocation, and behavioral biometrics and analytics, organizations can invisibly assess the risk associated with logins or post-login activity. This enables businesses to restrict authentication challenges to only the most high-risk events, avoiding unnecessary burdens for legitimate users.

Use strong authentication as a marketing tool to build confidence among users. Strong authentication can improve actual security. In addition, making customers aware that a business supports strong authentication can bolster public perception of that business's security — an important factor when there is considerable customer demand for strong authentication methods.

Make a thorough inventory and honest assessment of corporate data assets, and protect them accordingly. Even apparently low-risk data, like customer contact information, can provide significant value to fraudsters and expose companies to regulatory ire if compromised. Identifying core company data assets is the first step in establishing appropriate access safeguards.

Use strong authentication within the enterprise; especially where it counts. Certain systems are higher-profile targets for criminals. These include anything internet-facing and internal systems that could present attractive targets for insider threats, such as treasury management systems or data warehouses. Strong authentication reduces the opportunity for criminals to gain unauthorized access while also making it easier to track with certainty when an insider has conducted malicious activity.

INTRODUCTION

Authentication portals have emerged as the hottest target for cybercriminals. This trend is driven by a number of factors, from the U.S. transition to EMV cards forcing fraudsters online to the growing prevalence of online and mobile commerce. With this focus has come a maturing of fraud tools and tactics — from device and location spoofing tools to sophisticated social engineering schemes designed to deceive users into giving up their credentials.

Fortunately, authentication technologies have been maturing as well, with many newer authentication methods and architectures improving resilience against these fraud tactics. Cryptographically backed authentication standards, such as the ones put forth by the FIDO Alliance, provide powerful answers to phishing schemes and similar attacks on customers and users.

WHAT IS STRONG AUTHENTICATION?

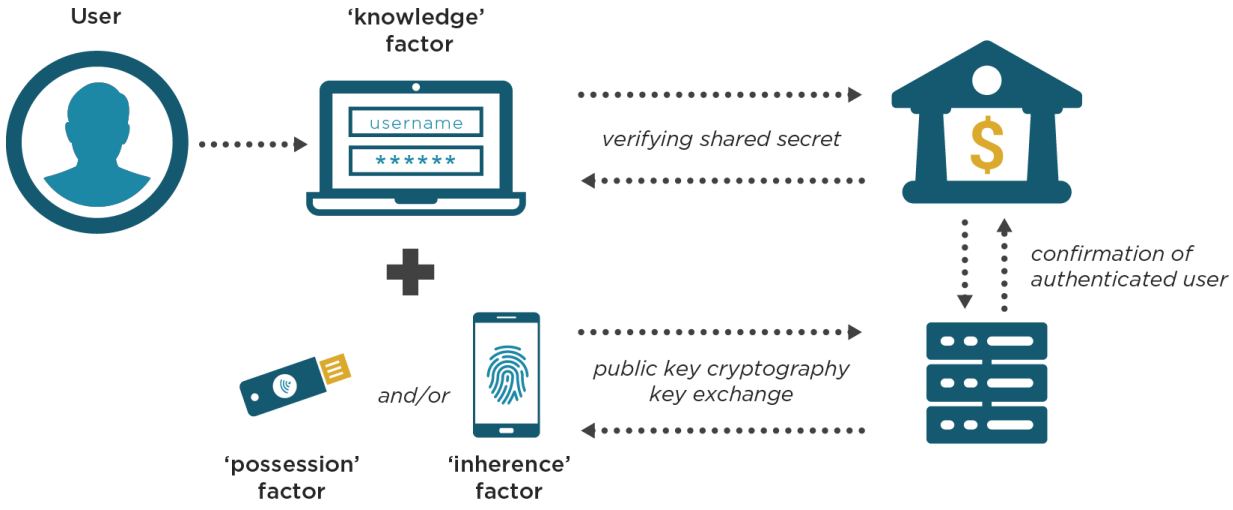
Strong authentication[1] uses multiple methods, or factors, to verify the identity of the user:

- Knowledge: a shared secret between the user and the entity authenticating that user (e.g., passwords, answers to security questions, etc.)
- Possession: something the user has (e.g., a mobile device, cryptographic key, etc.)
- Inherence: something the user is (e.g., a fingerprint, behavior, etc.)

Attempts to defeat multiple factors significantly increases the failure rate of fraudsters, since circumventing or fooling different authentication methods requires deploying multiple types of tactics and technologies to fully impersonate the targeted individual.

Crucially, at least one of the authentication factors at play in strong authentication must use a public-key-cryptography-based authentication method. Cryptographic standards, like the ones put forth by the FIDO Alliance, have a number of advantages over other, authentication methods… When a user wants to access online resources, a device prompts the user to authenticate themselves via a cryptographic key exchange using methods ranging from simple "tap-to-approve" verifications through an app or push notification to more involved authentication methods, such as biometric modalities. The device sends a digitally signed approval to the online resource, typically a web page or mobile app , validating the authentication process. If the public/private key pair match and other checks are validated the user is granted access This process makes cryptographic authenticators significantly more resilient against phishing because no sensitive data is passed over the wire.

Typical Strong Authentication Process (Online Banking Login Example)



Source: Javelin Strategy & Research, 2018

[1] Previously referred to in the 2017 Strong Authentication study as 'High-assurance strong authentication'

This provides significant advantages, in terms of both security and ease of use over either single-factor authentication or traditional MFA.

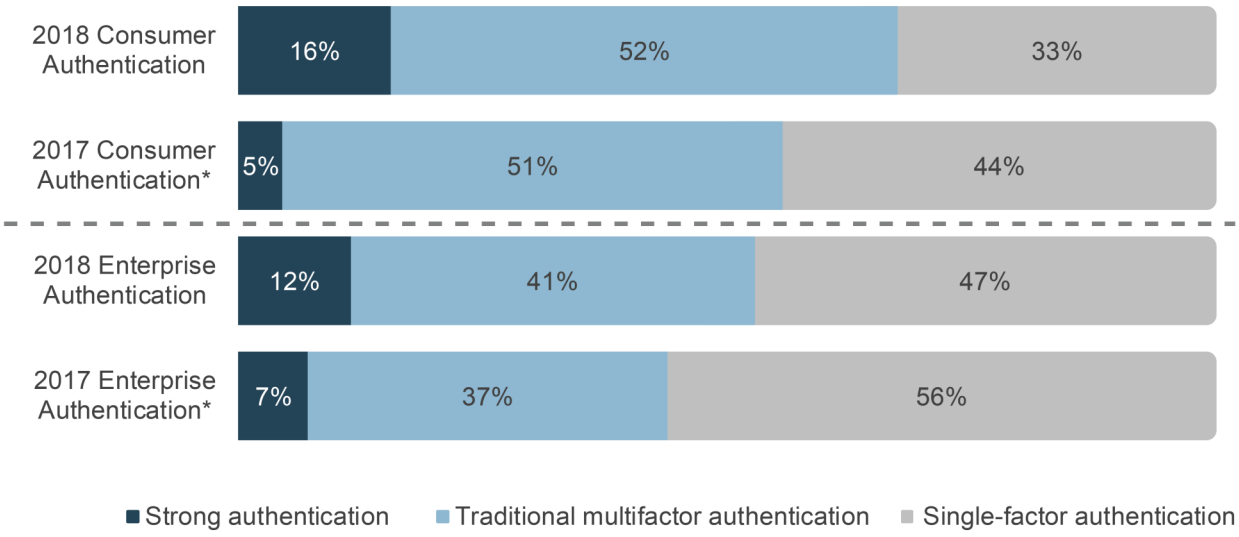
As the name implies, single-factor authentication verifies users' identities using only a single factor, typically knowledge. While multiple authentication methods within this category may be used by organizations, all rely on the same factor — in essence, knowledge-based shared secrets, such as passwords and static or dynamic security questions.

Traditional MFA uses multiple factors to authenticate the user, such as use of both a password and an SMS one-time code, but none of the authentication methods in use provides a standards-based cryptographic handshake during the authentication process. Typically, this means that the authenticator — a code, password, or biometric template — is directly transmitted from the user's device to the authentication server. While much stronger than relying on a single factor, this authentication scheme is still vulnerable to interception and replay, through any number of potential tactics such as phishing websites, social engineering attacks, or malware.

Fortunately, since last year, use of both traditional MFA and strong authentication is gaining ground in both consumer and enterprise applications. Use of strong authentication in consumer applications has grown particularly quickly — tripling from 5% of enterprises with customer-facing digital channels in 2017 to 16% in 2018. Much of this can be attributed to increased availability of mobile biometric authenticators capable of supporting Public Key Cryptography (PKC)-based standards. In addition, heightened regulatory pressure through EU regulations such as PSD2 and GDPR, have had ripple effects even outside of their primary geographic area.

Adoption of Strong Authentication Rises for Customer and Enterprise Use

Figure 1: Authentication Strength for Consumer and Enterprise Applications



*2017 responses calibrated for longitudinality with 2018 data set
Source: Javelin Strategy & Research, 2018

Use of strong authentication within the enterprise – to authenticate employees, contractors, or vendors – has also seen strong growth, rising from 7% of enterprises in 2017 to 12% of enterprises in 2018 (Figure 1). Unfortunately, strong authentication within the enterprise still lags behind consumer authentication, with just under half (47%) of businesses using only a single factor to authenticate their employees. Many businesses are still entrenched in weak authentication, with ignorance around the value malicious parties put on the data they hold and apathy toward implementing strong authentication that opens up even more risk to security conscious companies.

Vulnerabilities Stack Up in Traditional Authentication Methods

Even as many organizations remain reliant on outmoded single-factor authentication systems, the vulnerabilities in traditional strong authentication are becoming more evident. One-time passwords — typically six- to eight-digit numeric codes — delivered by SMS text message remain the most prevalent form of authentication besides knowledge factors, to the extent that in the popular press, references to "two-factor authentication" or "two-step verification" almost invariably refer to authentication with SMS one-time passwords.

In 2016, the National Institute of Standards and Technology (NIST) updated its authentication guidelines to deprecate SMS one-time passwords, a move that was quickly softened after industry outcry. Since then, the weaknesses inherent in SMS OTP have become more evident. There are a variety of methods that fraudsters use to compromise SMS messages:

- **SIM swap:** Impersonating victims to their mobile carriers to have their account transferred to a device under control of the fraudster has proven to be a popular and effective tactic for compromising the accounts of high-profile victims. In one particularly prominent case, hackers were able to compromise cryptocurrency investor Michael Terpin's AT&T account to steal nearly $24 million in cryptocurrencies, resulting in a lawsuit from Terpin claiming that AT&T was at fault due to lax authentication measures leading up to the swap.[2]
- **Malware:** One of the earliest features of mobile malware was the interception and forwarding of text messages, even when mobile malware was largely an extension of the Zeus desktop banking Trojan. Similarly, man-in-the-browser and man-in-the-middle attacks can capture one-time passwords as they are entered on infected laptop or desktop devices.
- **Social engineering:** When fraudsters are aware that a victim has SMS one-time passwords enabled, they may contact the victim directly, impersonating a trusted organization such as her bank or credit union to deceive the victim into providing the code she has just received to authenticate herself.

While alternative delivery methods for one-time passwords can mitigate some of the vulnerabilities in this authentication method, others remain inherent in the system. Stand-alone code-generator apps are the most resilient delivery method against interception, since it is largely impossible for even malware to directly interact with the code generator, but the OTPs can still be intercepted as they are entered into the browser, captured through an overlay on a mobile app or received directly from the user through social engineering.

Supporting multiple risk assessment tools, such as device recognition, geolocation, and behavioral analytics, goes a long way toward addressing vulnerabilities, but no single solution is bulletproof. Layering authentication technologies with a comprehensive risk assessment framework can help judiciously apply step-up authentication and identify the most appropriate authentication method to be used.

2 https://www.reuters.com/article/us-cryptocurrency-at-t-lawsuit/us-investor-sues-att-for-224-million-over-loss-of-cryptocurrency-idUSKBN1L01AA, accessed Oct. 8, 2018.

No Single Authentication Solution Is Bulletproof

Figure 2: Authentication Solution Table

Authentication	Factor	Description	Key Vulnerabilities
Password, PIN, and Passcode	Knowledge	A fixed value that can include letters, numbers, or a combination thereof	Can be intercepted or stolen and replayed, brute-forced, or guessed
Knowledge-Based Authentication	Knowledge	Questions designed to elict an answer known by the respondent	Can be intercepted or stolen and replayed, or guessed
Hardware-Based One-Time Password	Ownership	A stand-alone device that provides a single-use code	Can be intercepted and replayed, or device stolen
Software-Based One-Time Password	Ownership	An application (e.g., mobile app, email, browser, etc.) that provides a single-use code	Can be intercepted and replayed, or device can be stolen
SMS-Based One-Time Password	Ownership	A single-use code delivered through a text message	Can be intercepted and replayed, or device stolen
Smartcard	Ownership	A card that contains a secure IC chip which leverages public-key infrastructure	Can be physically stolen
Security Key	Ownership	A compact device that contains a secure IC chip which leverages public-key infrastructure	Can be physically stolen
Device Fingerprinting	Ownership	A process that creates a profile of a device, often through the use of JavaScript, or uses markers such as cookies and Flash Shared Objects to certify a device's identity	Markers can be stolen, or device characteristics obscured or emulated
Behaviometrics	Inherence	Analyzes how the user interacts with a device or session	Behavior can be emulated
Fingerprint Scanning	Inherence	Compares fingerprint on record with new scans captured optically or electrically	Image can be stolen and replayed
Eye Scanning	Inherence	Compares characteristics of eye on record, such as iris or eye veins, with new scans captured optically	Image can be stolen and replayed
Facial Recognition	Inherence	Compares characteristics of a face on record with new scans captured optically	Image can be stolen and replayed
Voice Recognition	Inherence	Compares characteristics of a voice on record with new audio samples, either actively or passively	Sample can be stolen and replayed, or emulated

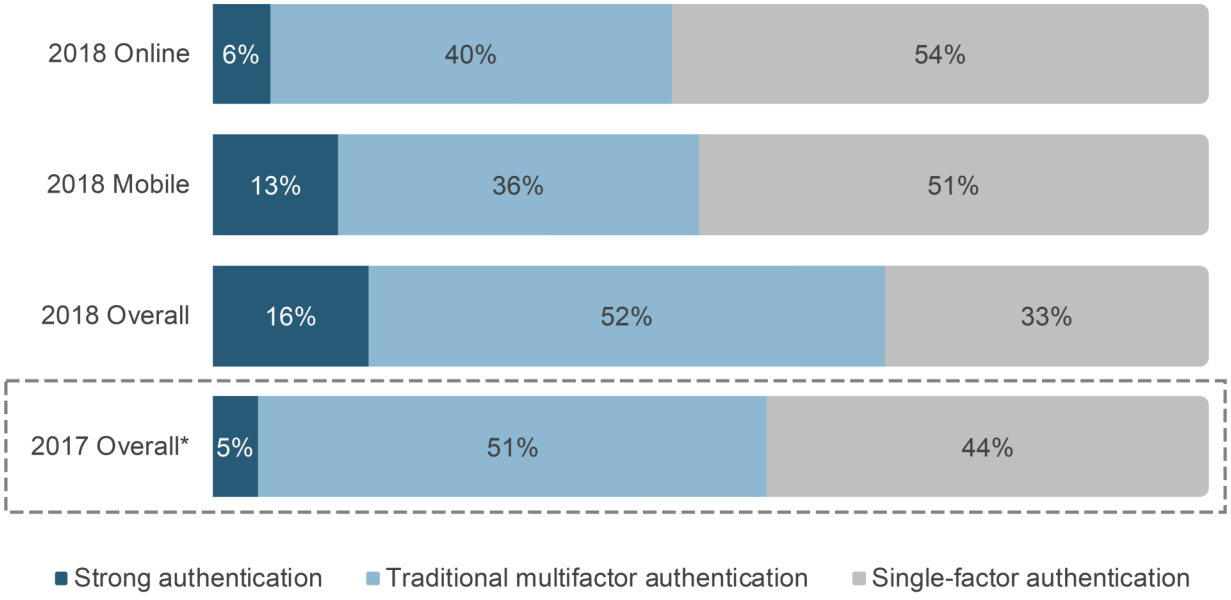
Source: Javelin Strategy & Research, 2018

Consumer Authentication

Since 2017, adoption of strong authentication for consumer authentication has risen sharply, principally due to availability of cryptographically backed authentication methods on mobile devices, although a somewhat smaller number of businesses are using strong authentication online as well. Overall, the percentage of businesses that use strong authentication in some portion of their enterprise tripled from 5% in 2017 to 16% in 2018 (Figure 3).

Adoption of Strong Authentication in Consumer Applications Triples From 2017

Figure 3: Adoption of Strong Authentication for Consumer Applications



* 2017 responses calibrated for longitudinality with 2018 data set
**Bars may not add to precisely 100% due to rounding

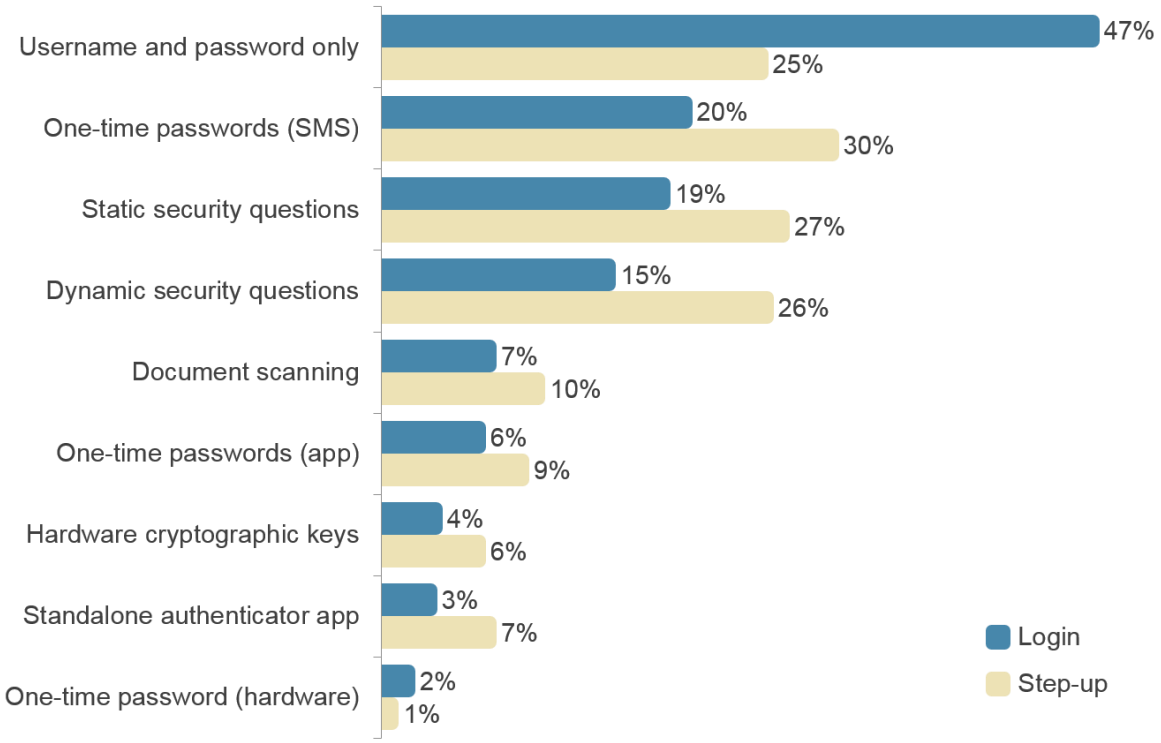
Source: Javelin Strategy & Research, 2018

Strong authentication methods are still somewhat limited for online authentication, with most organizations that use strong authentication for users' online logins turning to out-of-band authentication methods such as stand-alone mobile authenticator apps. Hardware cryptographic keys (aka security keys), such as the ones offered by Google, Feitian, OneSpan, and Yubico, are one of the only strong authenticators that natively function on laptop or desktop computers, but they are supported by only 3% of businesses for customer login (Figure 4).

Unfortunately, the comparatively low support for strong authenticators for in-browser authentication highlights a major gap. Consumers still tend to use businesses' websites to conduct higher-risk activities than they do through mobile apps. Within financial services, this includes online account opening, and the use of online banking for initiating outbound transfers.

One-Time Passwords, KBA Are Dominant for Consumer Authentication

Figure 4: Adoption of Online Authentication Methods (Consumer)



Source: Javelin Strategy & Research, 2018

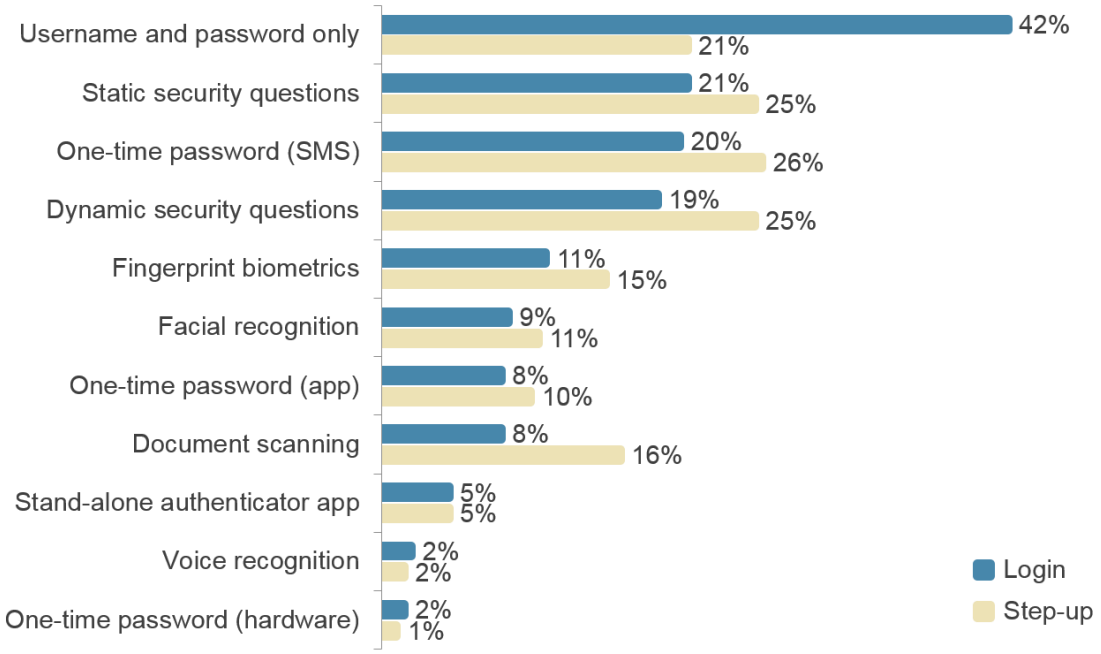
Fortunately, with the release of FIDO2, which includes the W3C's WebAuthn standard, enterprises now have more options for authenticating users on laptop and desktop computers. This standard establishes an API that offers organizations a framework to eliminate the need for passwords in customer authentication. Under WebAuthn, the site authenticating the user is able to directly interface with an authenticator, such as a stand-alone security key, on-device authentication with an integrated trusted execution environment, on-device biometric sensors, or out-of-band authentication on a mobile device.

Regulatory pressure is accentuating the need for businesses to switch to strong authentication methods. PSD2 and GDPR in Europe are having ripple effects even outside of their direct areas of influence. The two areas where these regulations have the greatest impact on authentication are related to specifications around the relative strength of authentication used and the privacy of a user's information. For PSD2, organizations are required to leverage so-called strong customer authentication or traditional multifactor authentication for online transactions above a certain threshold and access to their online payment accounts. With GDPR, citizens need to be afforded not only better protection of the data they share with organizations but better control over that data — including the ability to request its deletion.

More than half of businesses believe the authentication methods they currently employ will be rendered obsolete and insufficient to meet regulatory standards within the next few years (Figure 6). Some of this is simply due to

Vulnerable Authenticators Abound in Consumer Login and Step-up

Figure 5: Adoption of Mobile Authentication Methods (Consumer)



Source: Javelin Strategy & Research, 2018

the rapidly changing nature of cybersecurity. As identification and authentication methods become widespread, cyber criminals gain experience with compromising those methods, leading to the development of tools that get sold across criminal marketplaces to help other criminals overcome these barriers. This creates something of an arms race in which businesses and regulators are forced to keep escalating their defenses against ever more sophisticated threats.

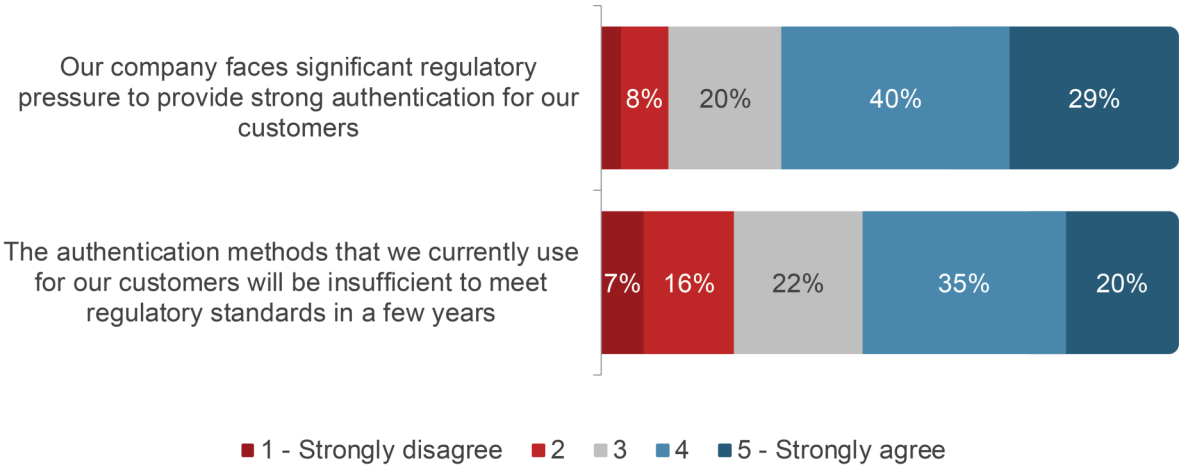
However, businesses that are reactive to regulation – applying authentication measures that meet only a basic standard for compliance – rather than looking ahead to what solutions provide the most longevity against emerging fraud schemes leave themselves with rip-and-replace options, and are perpetually trying to catch up to changing needs. Taking half-measures to upgrade authentication to meet the lowest regulatory pressure may reduce immediate costs, but they force businesses to constantly revise their infrastructure and strategies as regulatory standards, industry best practices, and criminal tactics advance with improving technology.

One of the advantages of using a standards-based authentication framework is that it becomes quicker, easier, and less costly to integrate new authentication methods, either through improved hardware on consumer devices or through new software-based solutions. This enables a core authentication architecture that can remain constant, even while individual solutions are added or removed.

In addition to direct regulatory mandates for stronger authentication such as PSD2 and federal regulations within the U.S. such as the FFIEC's authentication guidance, strong authentication methods can reduce an enterprise's need to store customer data, such as biometric templates. This becomes increasingly important with the advent of GDPR and similar regulations such as California's recently passed privacy initiative.

Most Companies Face Strong Regulatory Pressure to Modernize Authentication

Figure 6: Impact of Regulatory Pressure on Current and Future Authentication Methods



Source: Javelin Strategy & Research, 2018

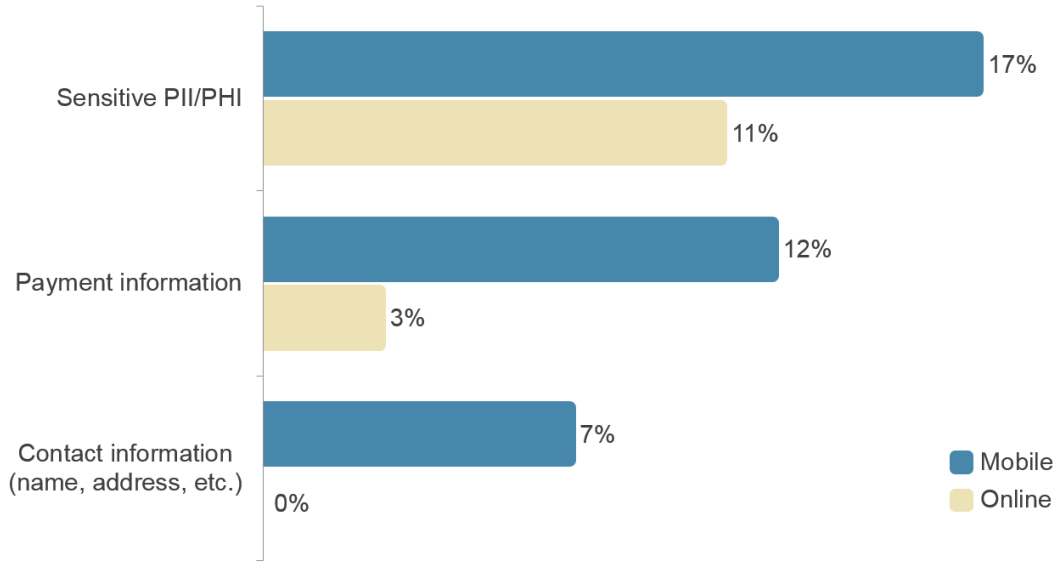
Beyond Security: The Other Benefits of Strong Authentication

Unsurprisingly, adoption of strong authentication tends to track closely with the sensitivity of data stored by the business. With the highest legal and regulatory pressure, companies that store sensitive personally identifiable information (PII), such as Social Security numbers or personal health information (PHI) tend to be the most aggressive adopters of strong authentication. These pressures are compounded by customer expectations that they will use what consumers see as the strongest authentication methods at the institutions that they trust with their most sensitive data. Organizations that process sensitive PII or PHI are more than twice as likely as organizations that handle only customer contact information to implement strong authentication in the mobile channel (Figure 7).

While it is easy for outside observers to say that even apparently "low-risk" consumer data like email lists and basic contact information has value to criminal organizations, it can be difficult for organizations that deal principally in this data to reconcile the apparent low risk of the data they handle with the cost of integrating strong authentication methods. However, there are good reasons why even businesses that store only what is seen as comparatively low-risk data should still make the move to strong authentication — including reduced regulatory pressure and improved customer experience.

Adoption of Strong Authentication Grows With Data Sensitivity

Figure 7: Adoption of Strong Authentication by Sensitivity of Data Processed



Source: Javelin Strategy & Research, 2018

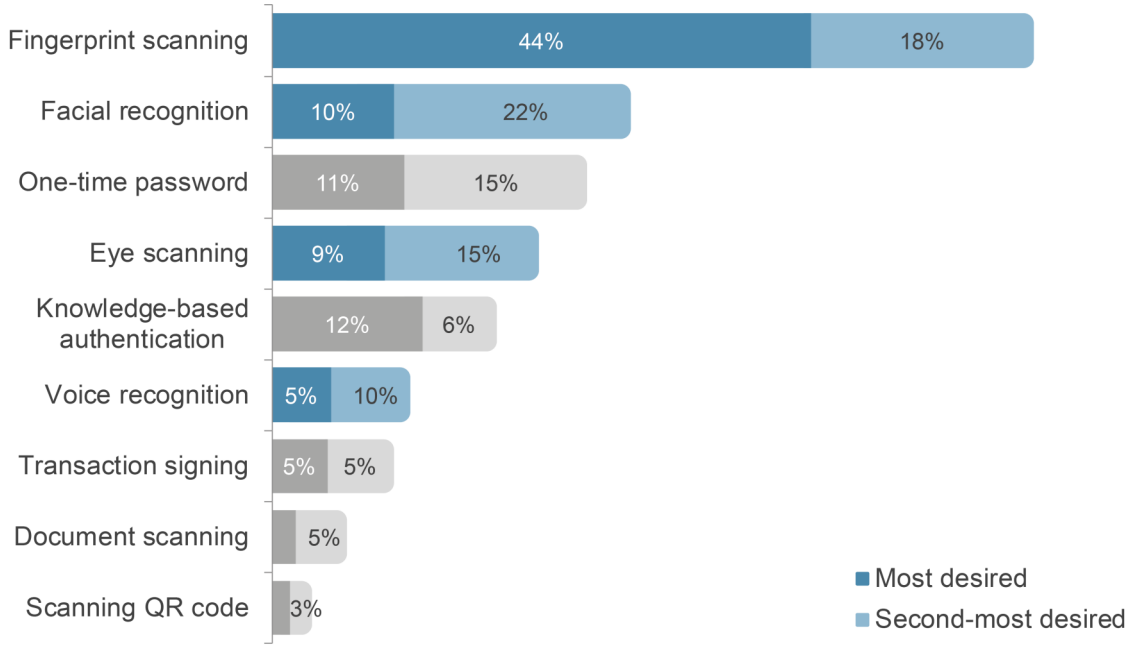
MEETING CUSTOMER EXPECTATIONS

Beyond the security benefits of strong authentication, businesses should consider upgrading their authentication methods to support a more positive customer experience as well. Biometric modalities in particular have strong support among consumer users, with biometrics and fingerprint far and away leading as consumers' favored means of identifying themselves.

Consumer demand for biometric authentication is far outstripping companies' adoption rates, with biometric modalities constituting 3 of the 4 authentication features consumers would most like to see at their primary bank or credit union. With broad availability of biometric authentication methods on mobile devices, consumers have become accustomed to using their physical characteristics to unlock their phones and broadly expect the organizations that hold their accounts to offer the same functionality (Figure 8).

Consumers Demand Biometric Authentication

Figure 8: Most Desired Authentication Features Among Consumers



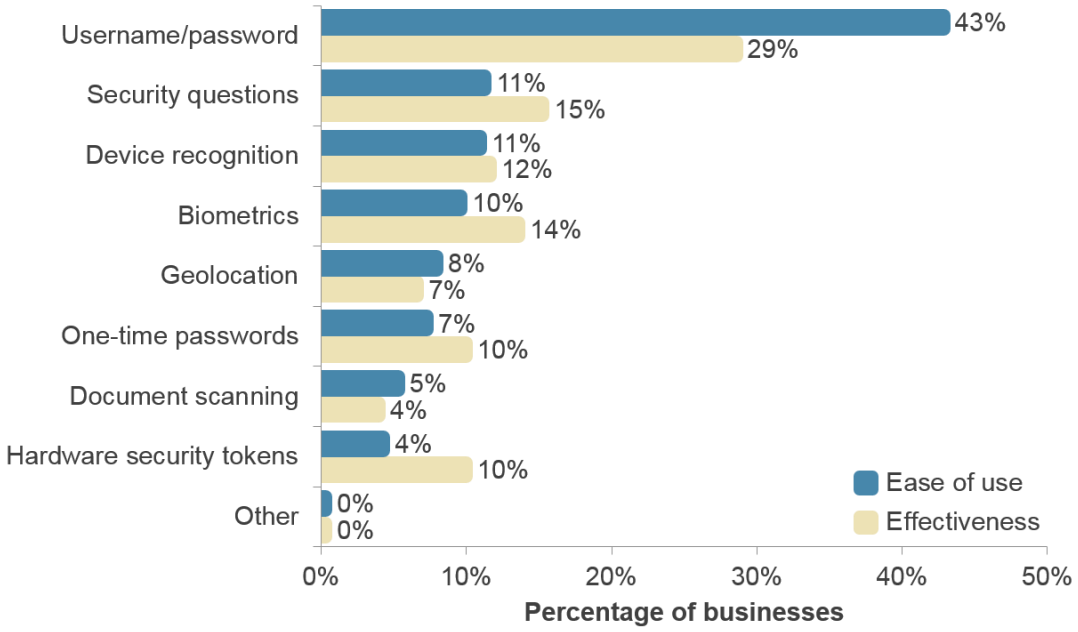
Source: Javelin Strategy & Research, 2018

However, this stands in marked contrast to the attitudes of the decision-makers at businesses responsible for rolling out authentication methods. Not only are businesses lagging in adopting the biometric modalities their customers favor, they tend to be pessimistic about the benefits of adopting these authentication methods. Just less than a third of business decision-makers believe passwords are the most effective of the authentication methods listed in Figure 9, and 43% believe passwords are the easiest authentication method to use.

Crucially, implementing a strong authentication framework enables businesses to shift the conversation away from authentication methods and rules they may need to implement to block fraud schemes to which methods are best suited to meeting and exceeding their customers' expectations.

Business Decision-Makers Are Optimistic About Passwords

Figure 9: Perceived Effectiveness and Ease of Use of Customer Authentication Solutions

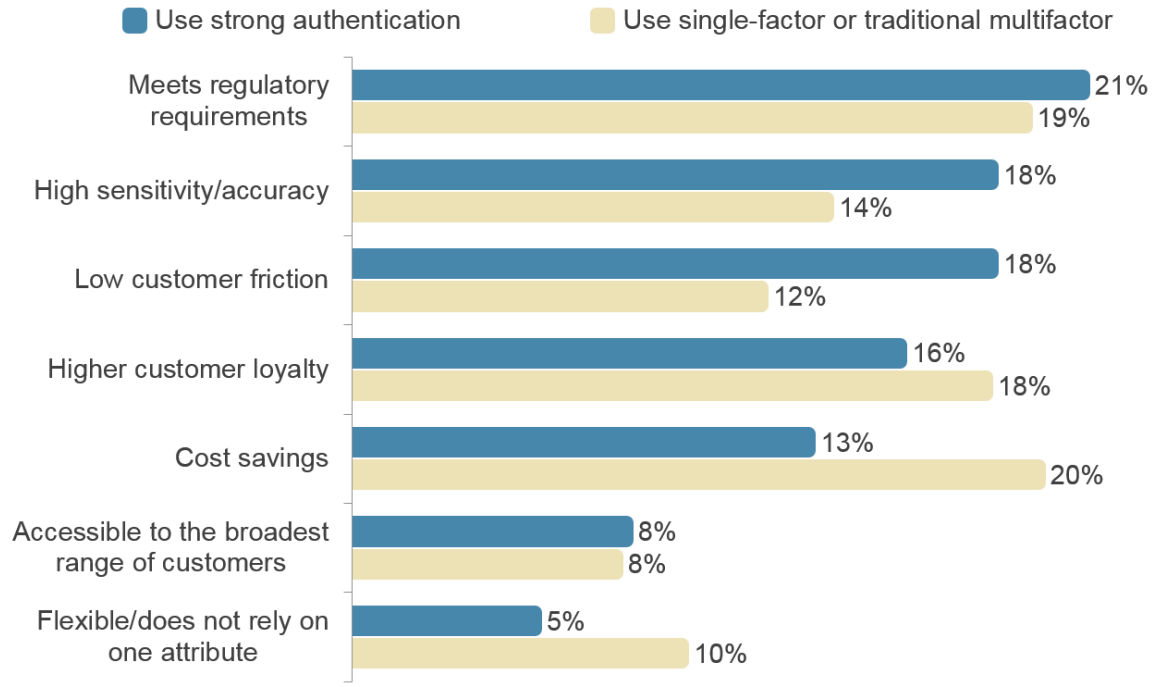


Source: Javelin Strategy & Research, 2018

While meeting regulatory requirements is quite reasonably the top priority for both enterprises that use strong authentication and those that do not, businesses that already use strong authentication are much more likely to say lower customer friction is the most important attribute they consider when evaluating an authentication method (18% vs. 12%) (Figure 10).

Laying Strong Authentication Groundwork Enables a Focus on the Customer

Figure 10: Most Important Factors when Choosing an Authentication Solution



Source: Javelin Strategy & Research, 2018

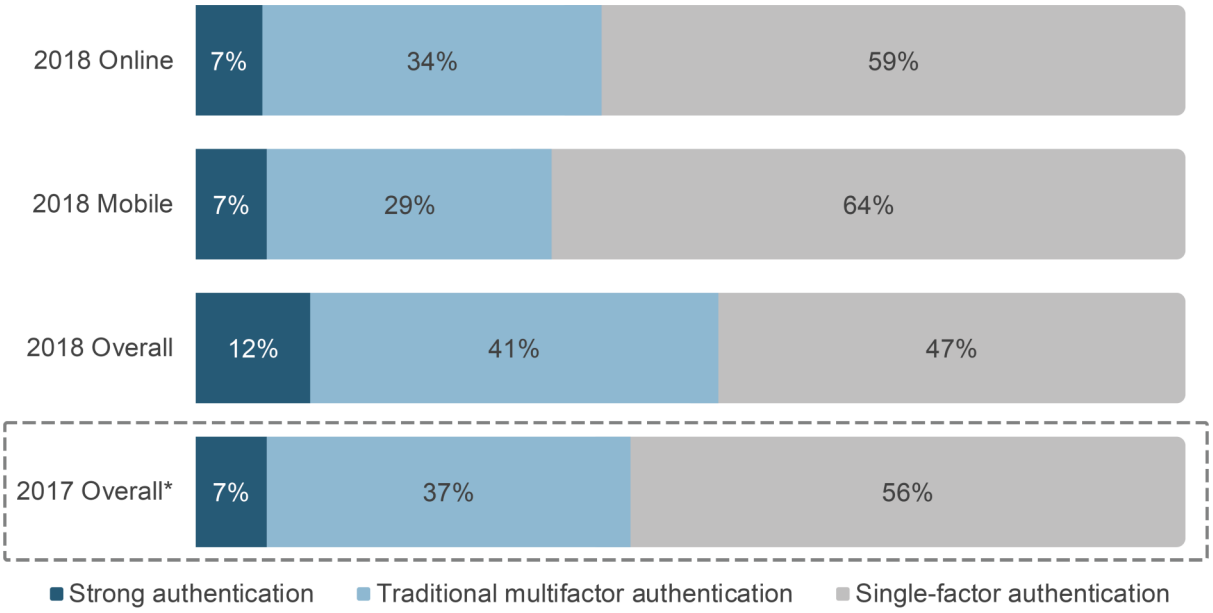
ENTERPRISE AUTHENTICATION

Since 2017, adoption of strong authentication within the enterprise has risen quickly, but somewhat more modestly than for consumer authentication, increasing from 7% of businesses to 12%. Unlike for customer authentication, use of non-password authenticators is somewhat more prevalent online for enterprises than on mobile devices.

Similar to customer authentication, around half of enterprises report using only usernames and passwords to authenticate their users at login, with one in five (22%) also solely relying on passwords for secondary authentication for high risk events. However, unlike consumer authentication, no single authentication method stands out as the primary supplement for passwords within enterprise authentication.

Enterprise Adoption of Strong Authentication Grows From 2017

Figure 11: Adoption of Strong Authentication within the Enterprise



*2017 responses calibrated for longitudinality with 2018 data set
Source: Javelin Strategy & Research, 2018

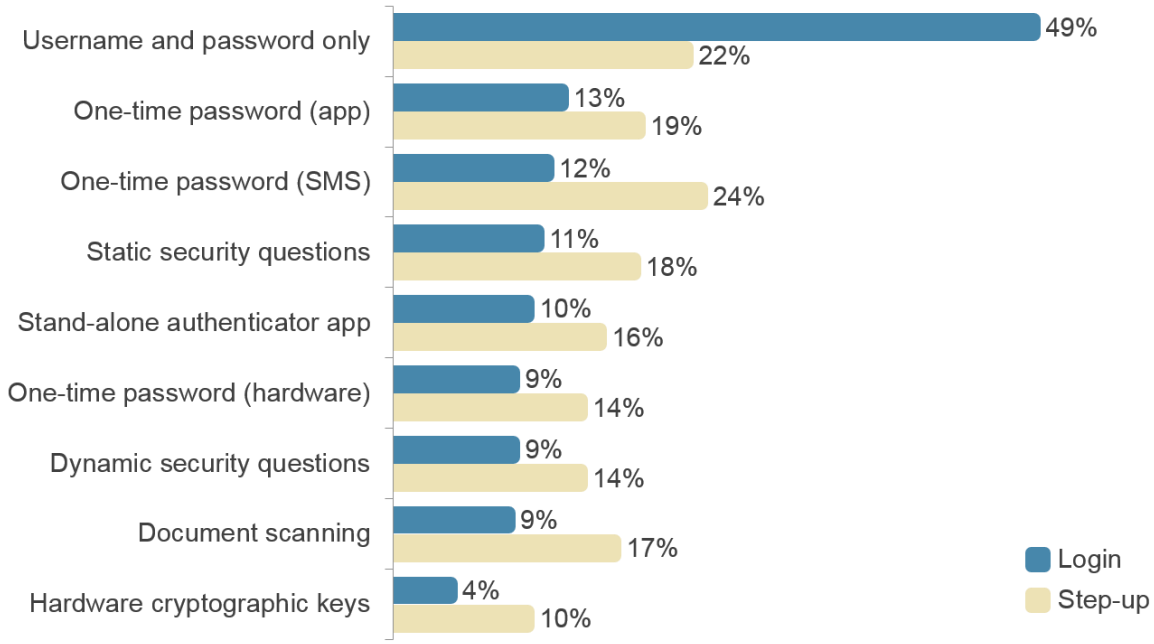
The next two most prevalent authentication methods are one-time passwords delivered through a standalone app, which are used by 13% of businesses to authenticate users at login, and one-time passwords delivered by SMS. While both have very similar adoption rates for use at login, looking at step-up authentication, reliance focuses on SMS one-time passwords with just under a quarter of businesses (24%) using this method to authenticate their employees and contractors post-login (Figure 12).

The growth in enterprise use of strong authentication can likely be attributed to the increased availability of cryptographically backed authentication methods within enterprise identity management platforms. Most frequently, this is done through stand-alone authenticator apps, which are the most widely adopted phishing- and interception-resistant authentication method for enterprises.

Unlike for stand-alone OTP generator apps, when the user attempts to log in or perform another activity that requires authentication, these services prompt the user to approve the activity from his mobile device. Unlike with one-time passwords, the response sent by the

Half of Enterprises Use Only Passwords to Authenticate Users at Login

Figure 12: Adoption of Online Authentication (Enterprise)



Source: Javelin Strategy & Research, 2018

authenticator app is specific to the instance and site requesting authentication, ensuring that even if the data is intercepted in transit, it cannot be reused.

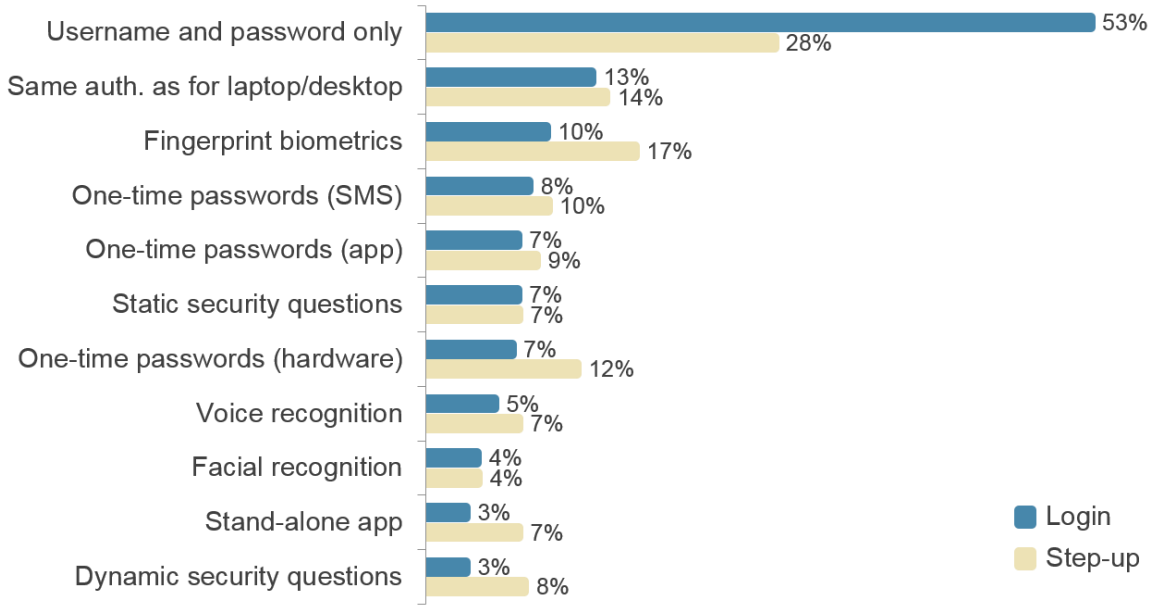
For mobile authentication of employees and contractors, enterprises tend to be even more reliant on passwords than when authenticating consumers. Just more than half (53%) of enterprises solely use passwords when authenticating users' access to company assets through their mobile device (Figure 13).

Fortunately, fingerprint biometrics is the next most prevalent authentication method for both login and step-up mobile authentication. This provides an opportunity for phishing-resilient authentication over employee mobile devices. In addition to greater availability of strong authentication factors, increased awareness of the value of data assets is another apparent driver of adoption of authentication that does not rely on passwords. For nearly every major type of data and network assets, companies' use of non-password authentication increased from 2017.

Company financial data appears to be the highest priority for authentication investment, with the highest rate of use of non-password authentication (44%), which showed the fastest growth from 2017 (increasing by eight percentage points). Intellectual property (40%) and human resources (HR) records (39%) come just behind financial data for adoption of non-password authentication. Not only is the value associated with these types of data widely recognized, they also tend to be accessed by comparatively small numbers of

Adoption of Alternatives to User Name and Password Trail Significantly

Figure 13: Adoption of Mobile Authentication Methods (Enterprise)



Source: Javelin Strategy & Research, 2018

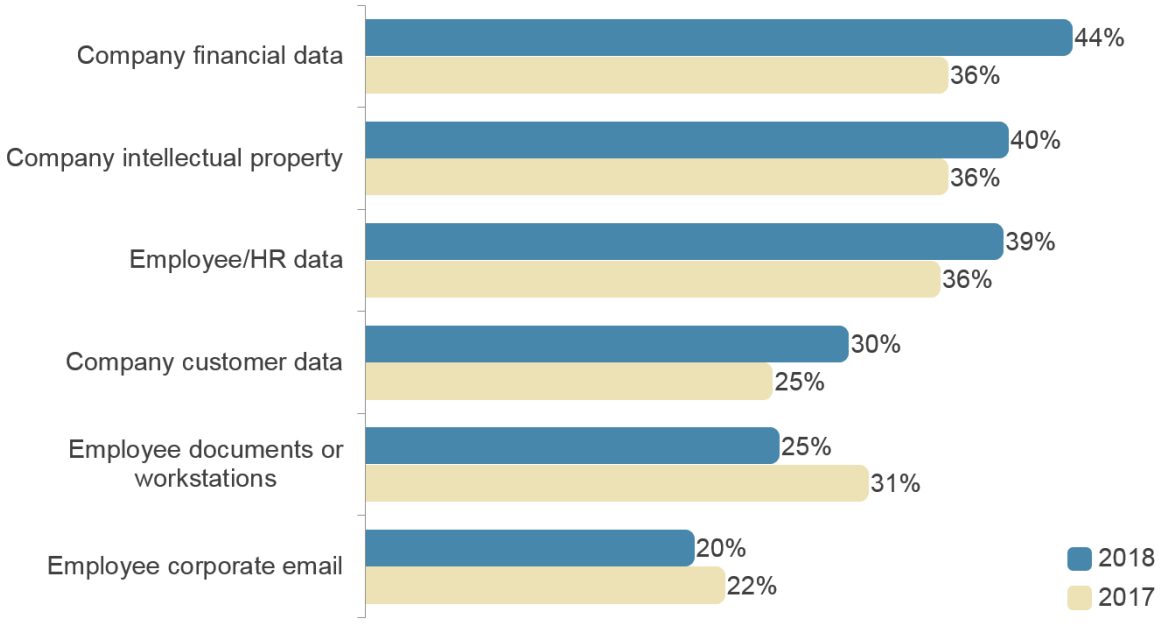
employees, reducing the potential disruption from higher-friction authentication methods. In contrast, data types and devices that are more generally accessed across the enterprise still tend to be protected solely by passwords. Employee documents/workstations and corporate email portals are the areas of worst offense in this regard, with only a quarter of enterprises protecting these assets with non-password authentication (Figure 14).

While it is understandable that companies would want to minimize the impact on employees' ability to conduct their day-to-day tasks, insecure access to both employee workstations and corporate email can undermine the security measures in place in other portions of the enterprise.

Corporate email portals in particular are incredibly valuable targets for cybercriminals, since successfully compromising a legitimate email account within a target business provides fraudsters a trusted cover to deceive other employees into aiding them. This kind of access is key to the aptly named "business email compromise" fraud scheme, in which fraudsters impersonate an executive within the company, prompting another employee to initiate an outbound transfer to an account controlled by the fraudster or to send sensitive data such as employee or customer records. Because the recipient of the deceptive email is typically operating within her standard job responsibilities, she can successfully overcome any additional authentication protecting financial accounts or sensitive data assets — inadvertently abetting the fraudster.

Email Portals Are the Weak Link in Securing Data Access

Figure 14: Use of Non-Password Authentication to Protect Corporate Data Assets



Source: Javelin Strategy & Research, 2018

Unfortunately, growing awareness of the value of corporate data is likely to bring shrinking returns over time. Among holdouts that rely solely on password authentication within the enterprise, two-thirds (66%) do so because they believe passwords provide enough security for the type of information their company needs to protect (Figure 15).

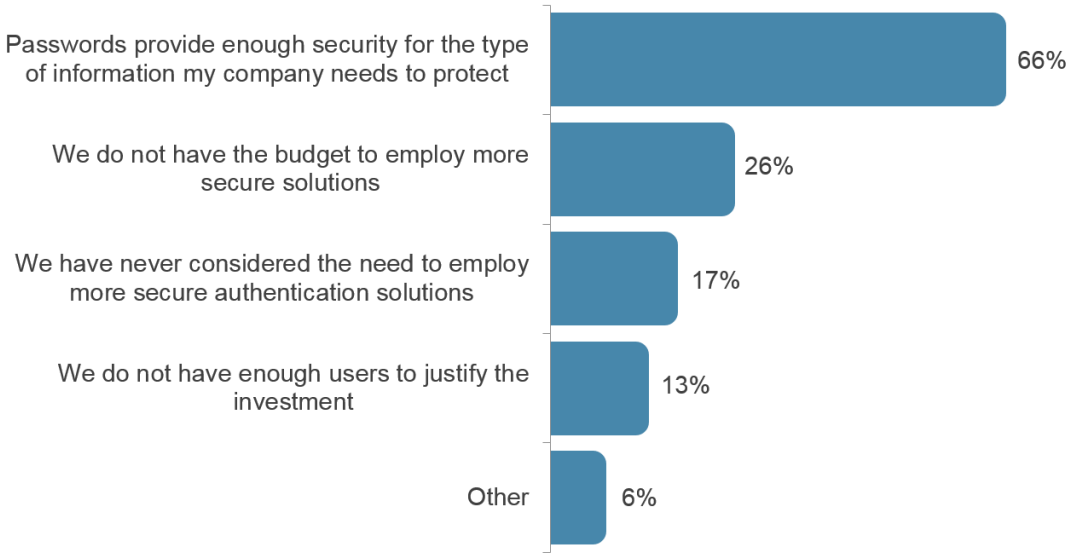
These holdouts are most likely to be persuaded by the operational benefits strong authentication can bring to the enterprise. As strong authentication solutions become more pervasive and baked into major identity and access management (IAM) systems, they become less expensive and time-intensive to implement, since the technology becomes standard across the solutions.

This is one of the crucial benefits for standards -based cryptographic authentication. With a common communication standard, subsequent integrations of new authenticators become much easier since they do not require building bespoke integrations for each new authentication method. This essentially futureproofs enterprise authentication, increasing the ease of regularly improving authentication to keep pace with innovation, regulatory requirements, and the growing sophistication of criminal tactics.

Moreover, just as businesses with a strong customer authentication framework are more effectively able to prioritize low-friction authentication flows, enterprises that can build in authentication flexibility can tailor authentication methods they implement to improve ease of use for employees. For enterprises where employees are regularly accessing sensitive systems and customer data, this can streamline frequent authentication events and minimize interruptions, including calls to the help desk for authentication-specific issues like password resets.

Most Holdouts Believe Passwords Are 'Good Enough'

Figure 15: Reasons for Using Only Passwords to Authenticate Employees and Contractors



Source: Javelin Strategy & Research, 2018

WHAT IS FIDO?

The FIDO Alliance is an open industry association with a focused mission: developing authentication standards to help reduce the world's over-reliance on passwords. Comprised of more than 200 leading global brands and technology providers, the Alliance is changing the nature of online authentication with technical standards that provide interoperable, frictionless strong authentication that is far more secure and easier to use than passwords and SMS OTPs. FIDO standards are based on public key cryptography where the user's private key lives on – and never leaves – the user's device, eliminating the risks associated with storing credentials in the cloud.

By enabling FIDO, any website or cloud application can interface with a broad variety of existing and future FIDO Certified devices that users can leverage for enhanced online security.

The FIDO Alliance currently has three sets of specifications for simpler, stronger authentication: FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (UAF) and FIDO2, which includes the W3C's Web Authentication (WebAuthn) specification and FIDO Client to Authenticator Protocols (CTAP). FIDO2 was recently released to enable expansion of FIDO authentication across web browsers and related web platform infrastructure.

- **FIDO UAF.** In this experience, the user registers their device to the online service by selecting a local authentication mechanism such as swiping a finger, looking at the camera, speaking into the mic, entering a PIN, etc. The UAF protocol allows the service to select which mechanisms are presented to the user. Once registered, the user simply repeats the local authentication action whenever they need to authenticate to the service. The user no longer needs to enter their password when authenticating from that device. UAF also allows experiences that combine multiple authentication mechanisms such as fingerprint + PIN.
- **FIDO U2F.** This experience allows online services to augment the security of their existing password infrastructure by adding a strong second factor to user login. The user logs in with a username and password as before. The service can also prompt the user to present a second factor device at any time it chooses. The strong second factor allows the service to simplify its passwords (e.g. 4–digit PIN) without compromising security. During registration and authentication, the user presents the second factor by simply pressing a button on a USB device or tapping over NFC. The user can use their FIDO U2F device across all online services that support the protocol on supported web browsers.

.

FIDO2 specifications:

- **W3C Web Authentication Specification.** The Web Authentication specification, based on three technical specifications submitted to the W3C by the FIDO Alliance last year, defines a standard web API that enables web applications to move beyond passwords and offer strong FIDO authentication across all web browsers and related web platform infrastructure. Native support in web browsers and platforms will expand FIDO's reach across PCs and mobile devices.
- **Client-to-Authenticator Protocols (CTAP1 and 2).** CTAP enables browsers and operating systems to talk to external authenticators like USB Security Keys, NFC - and Bluetooth-enabled devices. CTAP removes the requirement of registering a credential on every device. With this specification, a user could use their wearable or mobile device, for example, to log in to their computer, tablet, IoT device and more.CTAP 1 is the U2F protocol, while CTAP2 adds new capabilities like passwordless login.

STRONG AUTHENTICATION INDUSTRY CASE STUDIES

Google

From Google's perspective, defending against phishing is the key to securing employees' and customers' accounts. With the prevalence of cloud-based services, both among consumers and within enterprises, usernames and passwords are frequently the only thing stopping malicious actors from compromising data. With authentication using FIDO protocols, the authenticator provides cryptographic proof that the user is interacting with the legitimate service, even if the authenticator's responses is captured in transit, it cannot be successfully replayed by malicious actors to impersonate the user.

Over two years ago, Google published the result of their internal implementation of FIDO U2F security keys, and reported impressive outcomes. According to the company, there has not been a successful phishing attack against their 85,000+ employees since requiring use of physical security keys. Since the publication of this report, Google has taken a number of other notable steps with integrating FIDO protocols into their consumer and enterprise authentication flows.

Most recently, Google has released their own U2F hardware security key, known as the Titan Security Key. Titan Security Keys provide both a familiar USB security key and a Bluetooth version, which enables the security key to authenticate via users' smartphones. While the Titan Security Key is available generally for purchase, it is intended largely for enterprise users, especially those who already use Google's cloud services.

With the release of Chrome 70, Chrome will support the credential management API specified in the W3C's recently released WebAuthn standard. This allows web applications to create and use cryptographically attested credentials to authenticate users. Crucially, this lays the foundation for fully passwordless authentication in the browser using a variety of strong credentials, ranging from U2F security keys such as Google's own Titan key or the one built into Google's Pixelbooks to local biometric authentication such as Apple's TouchID.

Ultimately, the goal is having as many users as possible on phishing-resistant authentication protocols, whether they utilize a security key, an on-device biometric authenticator, or a cryptographic handshake with the users' mobile device.

Tradelink

Established in 1998, Tradelink is a publicly traded company that acts as a gateway between the Hong Kong government and commercial businesses. Since its inception, Tradelink has been at the leading edge of online security — first in facilitating communications between the government and traders and since as a provider for security in the HK banking industry. One aspect that has been central to delivering these secure interactions since late 2016 has been the FIDO protocol.

The organization decided the Internet was going to be how it managed communications. It made security a priority and leveraged public key infrastructure (PKI). Originally used for communications between the HK government and traders, the technology was eventually opened up to the banking industry.

Since that time, Tradelink's approach to authentication has continued to evolve leading the organization to FIDO. At first there was a trend to move away from digital certificates and towards one-time passwords. And approximately four years ago, they began to explore biometrics as a solution in partnership with the banking industry, which helped fund the effort. After examining different technologies and standards worldwide, Tradelink decided to use FIDO-based authentication starting in 2016.

In their estimation, adoption by banks has been strong because no information about the user is sent from mobile devices. And whoever is the service provider, whether the banks or Tradelink, doesn't need to transmit or store the biometric data which is important to the stringent requirement on data privacy protection in Hong Kong. This together with the adoption of Public Key Cryptography as the backbone for the FIDO Standard were the other major factors driving banks to rapidly adopt the FIDO standard.

In fact, the appeal of this biometric approach has resonated extremely well in Hong Kong. As evidence, the Hong Kong Government will launch a new initiative for electronic ID in 2020 that will leverage FIDO to authenticate citizens online.

Visa

Visa recently released its ID Intelligence suite of services to help organizations better identify and authenticate users. Banks, card issuers, and even merchants are being confronted with the need to strengthen their authentication capabilities to mitigate risks and meet compliance rules under directives such as PSD2. Through this suite of services, these organizations can easily obtain the different authentication capabilities they need from a trusted provider with a single point of integration. Visa has chosen to make a FIDO-based implementation of biometrics one of these offerings as it aligns with their strategic approach to authentication.

With ID Intelligence, organizations work through a single source to integrate a select set of identification and authentication solutions. These solutions fall into four categories:

- Authenticate with biometrics
- Authenticate with a photo ID and selfie
- Authenticate the data provided by the user (PII validation)
- Authenticate the device data (trusted vs. suspicious)

There is a wide variety of biometric platform providers in the market today. For ID intelligence, Visa partnered with Daon to deliver FIDO-compliant biometrics capabilities. Daon offers both a FIDO-compliant and non-FIDO solution, but only the FIDO-compliant solution is part of the ID Intelligence suite. The appeal of the FIDO protocol came from its alignment with Visa's approach to authentication which prioritizes how best to protect user data, leverage available data to make better decisions, devaluing data when it is compromised and empowering the customer.

Implementation requires an integration of the SDK with the client's mobile application, which is typically a six to twelve month process, along with on premises hosting of the FIDO server. And while Visa is looking to extend the range of authentication solutions it offers as part of the ID Intelligence suite, the FIDO-compliant biometrics capability is available today.

METHODOLOGY

Enterprise data in this report was collected from a survey of 600 identity and authentication decision makers for businesses headquartered in the United States, with revenues of at least $20 million for the previous year. 301 respondents answered questions about their business' practices in authenticating customers and 299 answered questions about their business' practices in authenticating employees, vendors, and contractors.

When data was compared against 2017 responses, previous years' data was adjusted to exclude businesses with annual revenues under $20 million for more accurate comparisons against the 2018 respondent pool.

ABOUT JAVELIN STRATEGY & RESEARCH

Javelin Strategy & Research, a Greenwich Associates LLC company, is a research-based consulting firm that advises its clients to make smarter business decisions in a digital financial world. Our analysts offer unbiased, actionable insights and unearth opportunities that help financial institutions, government entities, payment companies, merchants and other technology providers sustainably increase profits.

Authors: Al Pascual, Senior Vice President, Research Director
Kyle Marchini, Senior Analyst, Fraud Management

Contributor: Ian Benton, Senior Analyst, Digital Banking & Payments
Crystal Mendoza, Production Manager

Publication Date: January 2019

ABOUT THE FIDO ALLIANCE

The FIDO Alliance is an open industry association with a focused mission: authentication standards to help reduce the world's over-reliance on passwords. Comprised of more than 200 leading global brands and technology providers, the Alliance is changing the nature of online authentication with technical standards that provide interoperable, frictionless strong authentication that is far more secure and easier to use than passwords and SMS OTPs. FIDO standards are based on public key cryptography where the user's private key lives on – and never leaves – the user's device, eliminating the risks associated with storing credentials in the cloud.

Today, FIDO Authentication is now supported by major mobile and desktop platforms and leading web browsers There are hundreds of FIDO Certified solutions and large global brands have made FIDO-based protection available for internal employee and consumer-facing applications .