2017 STATE OF AUTHENTICATION REPORT

October 2017

Sponsored by:

fido alliance

Independently produced by:

JAVELIN

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

This study, sponsored by FIDO, explores the current state of authentication in the U.S., including the evolution and use of strong authentication to secure customer accounts and enterprise systems against unauthorized access.

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

OVERVIEW

Digital channels are becoming the go-to places where consumers interact with businesses and each other. To accommodate their customers and better manage their organizations in a digital world, businesses have become incredibly dependent on a web of systems both on and off their networks to manage, store, and transmit diverse information such as financial accounts, personally identifiable information, intellectual property, transaction records, etc. Authentication is central to the ability of these businesses to effectively secure access to consumer-facing digital channels and the systems that underpin their operations. This study examines how businesses are implementing authentication, their motivations for choosing authentication technologies and approaches, and how the evolving threat environment has given rise to new, more effective means of authenticating customers and employees in today's digital world. For additional context, this report includes real-world examples of organizations that are leveraging FIDO-compliant solutions to protect customers' accounts and the enterprise with strong authentication.

EXECUTIVE SUMMARY

Key Findings

Strong authentication is evolving. Strong authentication has traditionally been synonymous with multifactor authentication (MFA). Unfortunately, passwords are not only inherently broken, but also ubiquitous — so practically any current application of MFA is being undermined by their inclusion. A superior approach — high-assurance strong authentication — merges MFA with strong cryptography. In this model, in which two or more factors are in use, at least one leverages public key infrastructure (PKI) through a protocol such as FIDO to prevent replay attacks.

Traditional strong authentication is broadly available for customers, but adoption lags in the enterprise. Industry initiatives and regulations have resulted in broad availability of traditional strong authentication both for customers and within the enterprise. Fifty percent of businesses offer at least two factors when authenticating their customers, though within the enterprise only 35% of businesses use two or more factors to secure access to their data and systems.

A lack of high-assurance strong authentication is leaving businesses exposed. High-assurance strong authentication is rare — only 5% of businesses offer the capability to customers or leverage it within the enterprise. This represents a clear area of opportunity for criminals and other threat actors, who are increasingly able to circumvent different authentication solutions, regardless of how many they may encounter during a single session.

Mobile devices are a clear driver of traditional strong authentication. Facilitating both possession-based authentication (e.g., device fingerprinting, SMS-based one-time passwords (OTP), etc.) and inherence-based authentication (e.g., fingerprint scanning, voice recognition, etc.), mobile devices have increased the opportunity for businesses to leverage more than just passwords to authenticate their customers and employees.

Knowledge and possession factor solutions are the most common combination in a multifactor scheme. Passwords are supported by all businesses that provide access to customer accounts, and along with other knowledge factor solutions are the most popular for customer authentication. This is followed by those that are predicated on possession (e.g., security keys, hardware one-time password tokens, etc.), and solutions based on inherence (e.g., biometrics) are in a distant third place.

Accuracy and customer loyalty are key. To win support of businesses, authentication solutions must prove their effectiveness in both keeping bad actors out and ensuring a positive security perception for good ones. It is notable that, while customer loyalty tops the list, low customer friction falls to the bottom, indicating that many businesses see friction as not only unavoidable, but perhaps also beneficial in persuading customers that their site is secure.

A third of U.S. businesses have had customer information breached — including the very information businesses rely on to authenticate their customers**.** The mass compromise of passwords has contributed to increased risk of fraud on consumer accounts and network-level attacks from credential-stuffing botnet attacks.

Ease of integration and compliance with industry standards are seen as more important for employee authentication. While ease of use is perceived as an important factor in selecting employee authentication solutions, it ranks behind ease of integration with existing systems and certification to industry standards. No one attribute stood out as being of leading importance in employee authentication methods.

Responsibilities to clients aren't registering as a motivator to secure the enterprise. Despite an environment in which regulators and industry associations are leaning on businesses to ensure vendors and partners are using strong security, few businesses consider contractual obligations to clients for more stringent security when selecting authentication methods.

Unfortunately, more than half of U.S. companies protect IP and company financial information using only passwords. Although traditional strong authentication is widely used by businesses in the enterprise, this does not mean that all systems and data are secured with anything better than a password. Most aren't.

Businesses, especially retailers, are most concerned about third-party breaches. Sixty-five percent of businesses report being highly concerned with the threat posed to their business by third-party breaches, compared with 57% for employee fraud and abuse, and 52% for breaches by insiders such as employees, contractors, or vendors. While third-party breaches are undoubtedly concerning, this ranking raises the prospect that businesses are overlooking the threat posed by malicious actors entering through trusted channels.

When criminals breach a business and target the company's data, they most often go where the money is, but the company's competitive differentiators are also attractive. Among all types of enterprise data compromised, company financial data tops the list (46% of cases), followed closely by company intellectual property (44% of cases).

Recommendations

Make high-assurance strong authentication broadly available to reduce the risk from password breaches. High-profile data breaches continue to occur, compromising massive lists of passwords that criminals subsequently use to gain access to businesses in all industries. Making additional factors of authentication available, and ensuring that at least one leverages PKI, prevents criminals from easily being able to use compromised credentials.

Tout availability of high-assurance strong authentication to raise trust and deter criminals. Besides improving actual security, making customers aware that a business supports high-assurance strong authentication can also bolster the public perception of that business's security. In addition, criminals may have less incentive to attempt to compromise credentials belonging to customers of a certain business if they know the credentials cannot be reused without a secure additional authentication factor.

Bolster authentication after a breach, supplementing and possibly replacing knowledge factor solutions. Compromised information, even if something other than traditional login credentials, has been used with great effect by criminals. In the event of a breach, businesses would do well to layer additional, high-assurance authentication solutions simultaneously with their remediation plan.

Balance customer experience and security by ascertaining the risk of a transaction before deploying customer-facing authentication methods. Risk-based authentication allows businesses to optimize their use of authentication methods that could introduce additional friction into a customer interaction by limiting their use to only those situations that present a higher likelihood that an unauthorized user has initiated the transaction.

To reduce the risk that an individual channel may be compromised, use multiple channels — or out-of-band authentication — to further reduce customer authentication risk during login with strong authentication or during step-up. Out-of-band authentication, a practice promoted by financial industry regulators, further raises the bar for criminals by forcing them to gain control of multiple access channels and, ostensibly, different types of devices simultaneously.

Use high-assurance strong authentication where it counts within the enterprise. Certain systems are higher-profile targets for criminals than others. This includes anything Internet-facing and internal systems that could present attractive targets for insider threats, such as treasury management systems or data warehouses. High-assurance 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.

Make high-assurance strong authentication a differentiator when emphasizing the value proposition with prospective clients. In the current threat environment, in which businesses are being compromised by proxy when a vendor suffers a breach that exposes their clients' data or networks, using high-assurance strong authentication is both an effective preventative measure and a message to prospects and clients that they are safe doing business with a vendor.

STRENGTHENING AUTHENTICATION

Authentication is the means by which users prove they are who they say they are, making it central to securing nearly every part of our digital world, whether that be access to enterprise applications or consumer websites. Today's authentication solutions are being trusted to protect a diverse range of information and other assets, such as financial accounts, personally identifiable information, intellectual property, etc. These solutions fall into one of three categories or factors:

- Knowledge: something the user knows (e.g., passwords, answers to security questions, etc.)
- Possession: something the user has (e.g., a hard token, a mobile device, etc.)
- Inherence: something the user is (e.g., a fingerprint, their behavior, etc.)

Every Factor is Vulnerable on its Own

The introduction of every new authentication solution practically invites criminals and researchers alike to probe

No Single Authentication Solution is Bulletproof

Figure 1: Authentication Solution Table

Authentication Technology	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 elicit 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, e-mail, browser, etc.) that provides a single use code	Can be intercepted and replayed, or device 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, 2017

for vulnerabilities. Circumventing or fooling different authentication methods may require different degrees of technical sophistication, but despite the introduction of increasingly sophisticated solutions, none has eliminated vulnerability.

Knowledge Factor Vulnerabilities

The most common authentication solution is also the weakest. Knowledge factor authentication, including passwords, PINs, and even answers to security questions, is vulnerable to transcription. That opens the door to numerous compromise methods. Anything known is potentially at risk of being inadvertently shared or stolen. This can play out as something as ordinary as the theft of a laptop computer in which a user stores passwords for various sites or systems. Or it could involve attempts to brute force an answer, leverage social media, or use other public information to render a series of guesses, or even cracking encrypted password lists with programs such as Hashcat or John the Ripper. This last scenario has contributed to a recent phenomenon known as credential stuffing, in which criminals rely on the habitual reuse of passwords among users, taking entire lists of stolen passwords and testing variations of those passwords against different sites.

Possession Factor Vulnerabilities

It can be argued that as digital delivery of goods and services has become a bigger part of our everyday lives that some of us and our digital devices have become inseparable. That said, leveraging a user's device in authentication is no guarantee that it is in their possession, or that how it is used doesn't subsequently expose the user to compromise. Device fingerprinting, by use of JavaScript inspection, cookies, and Flash Shared Objects, or other methods, can be used to discern whether a device is known. This can even include information on the device's reputation from other interactions. Yet whether that device is a laptop or smartphone, it can be accessed without the knowledge of the legitimate user, such as through theft or remote access, rendering device fingerprinting ineffective.

By comparison, combining reliance on a device with a unique text value for each authentication instance would appear to provide tokens with a greater security value, but that introduces additional complications. Hard tokens that generate one-time passwords can be physically stolen. Software tokens face similar risks, as the devices on which they are installed can be stolen or the codes they provide as output can be intercepted when entered into browsers or right from the device. Even one-time passwords sent via SMS text can be forwarded to another mobile device under a criminal's control.

Inherence Factor Vulnerabilities

Biometric authentication has captured the imagination of the public for decades thanks to its popularity in movies and television. But it has only been in the past few years that we have experienced a renaissance in the use of biometrics and behavior to authenticate users. Although these types of solutions represent a significant advancement from a technological perspective when compared with passwords or even device-oriented solutions, they are not without risk. Assessing and rendering a decision on user behavior is often done on a sliding scale, and efficacy requires a training period in which the software can learn about what constitutes the user's typical behavior over time.

Biometrics depends on the measurement and comparison of physiological features, but collection circumstances can be inconsistent, so neither is it a perfect solution. With

biometrics, fingerprints can be lifted, voices recorded or imitated, and faces photographed — prompting solution providers to seek ways to detect these and other spoofing behaviors. Criminals may also target the biometric data itself if it is exposed in storage or transmission, in an attempt to compromise and misuse that information to facilitate fraud. This has led to the storage of mathematical extrapolations of biometric patterns, rather than the pattern itself, and local secure storage of biometric data.

Vulnerability Mitigation Strategies

Criminals and other malicious actors can be incredibly creative and determined when it comes to gaining access to consumer's accounts or an enterprise's data. Effective authentication is among the first lines of defense against their efforts. Absent a security silver bullet among any authentication factors, a number of tactics and strategies to bolster authentication have been developed by private industry and the public sector, including:

- **Risk-based authentication**
  Implementing authentication based on the degree of risk, which typically involves analyzing any number of inputs to determine the best type of authentication to leverage given the determined degree of risk in a transaction or interaction.
- **Continuous authentication**
  A variation of risk-based authentication in which a user's actions through and across sessions is considered when deciding the degree of access a user has, or whether certain types of authentication are needed.
- **Out-of-band authentication**
  Leveraging authentication through an alternate channel, which can mitigate the risk that exists when the initiating channel is compromised or simply too insecure for the level of risk in the transaction.

Defining Strong Authentication

Security definitions are evolving in response to the growing sophistication of criminals and other malicious actors. In particular, strong authentication is an example of where the definition no longer aligns with the premise. Traditionally, strong authentication was synonymous with multifactor authentication (MFA). This interpretation is still broadly in use, but a variation that is more true to the spirit of the term has evolved over the past few years.

Multifactor authentication involves the use of two or more factors of authentication for a transaction so that if any one factor is compromised, a supplemental factor can be relied upon to reduce the risk of unauthorized access. This variation of strong authentication has found adherents across a variety of organizations.

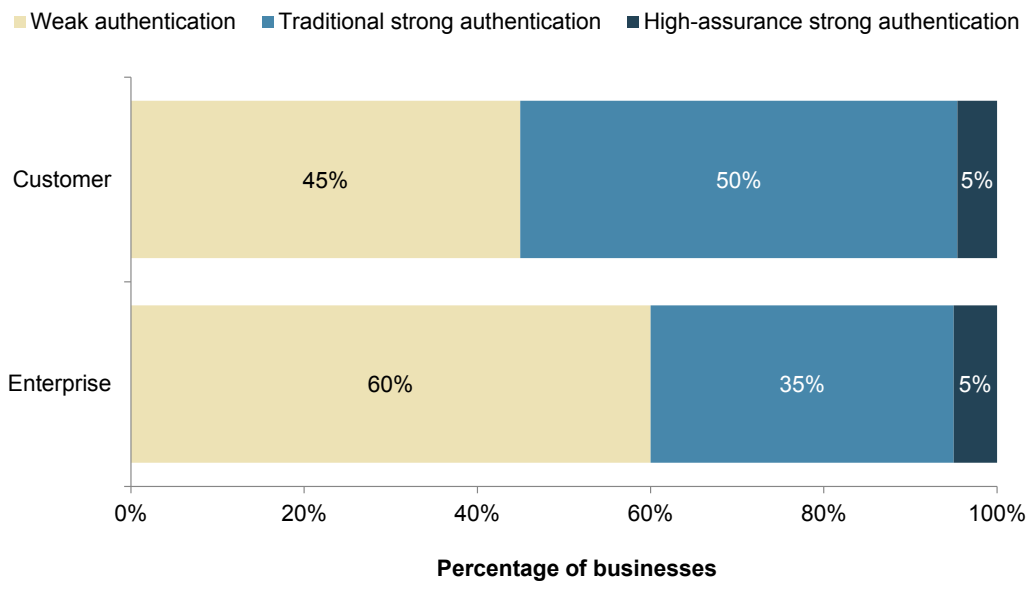
- **Financial services:** For financial institutions under the purview of the Federal Financial Institutions Examination Council (FFIEC), leveraging multiple authentication factors is an expectation when engaging in high-risk transactions.
- **Retailers:** Within the payments industry, the PCI Data Security Standards (DSS) evolved following high-profile retailer breaches to require the use of at least two factors of authentication for access to remote systems.
- **Consumer services:** There is a push to encourage adoption of two-factor (2FA) authentication among consumers when using online services such as email and social networking, with the National Cybersecurity Alliance's "Lock Down Your Login" campaign highlighting steps consumers can take to better secure their accounts.
- **Government:** The National Institute of Standards and Technology (NIST), which sets security guidelines for federal business, has called out the use of strong MFA as a best practice.[1]

Passwords are everywhere, but provide little security so practically any current application of MFA is undermined by their inclusion. A superior approach to strong authentication merges MFA with strong cryptography, the latter also advocated by NIST.[2] It is this idea that instead of sharing secrets to certify the identity of a user, that only the user's ownership of the secret is confirmed through public key cryptography, which helps to mitigate the most common authentication vulnerability — the chance that a secret is intercepted or stolen and subsequently replayed (see Figure X). This high-assurance form of authentication uses multiple factors in which at least one of those factors involves the use of PKI. Such individual solutions would include smart cards, security keys, and FIDO-enabled biometric authenticators.

The aforementioned MFA-oriented initiatives have resulted in broad availability of traditional strong authentication both for customers and within the enterprise. Fifty percent of businesses offer at least two factors when authenticating their customers, compared with only 35% of businesses that leverage at least two factors of authentication to secure access to their data and systems (see Figure 2). By comparison, high-assurance strong authentication is rare, with only 5% of businesses offering the capability to customers or leveraging it within the enterprise. This represents a clear area of opportunity for criminals and other malicious actors, who are increasingly able to defeat different authentication solutions, regardless of how many they may encounter during a single session.

Businesses Much More Likely to Exceed Strong Authentication When Protecting Customers

Figure 2: Strength of Authentication Available for Customers and Enterprise Users



Source: Javelin Strategy & Research, 2017

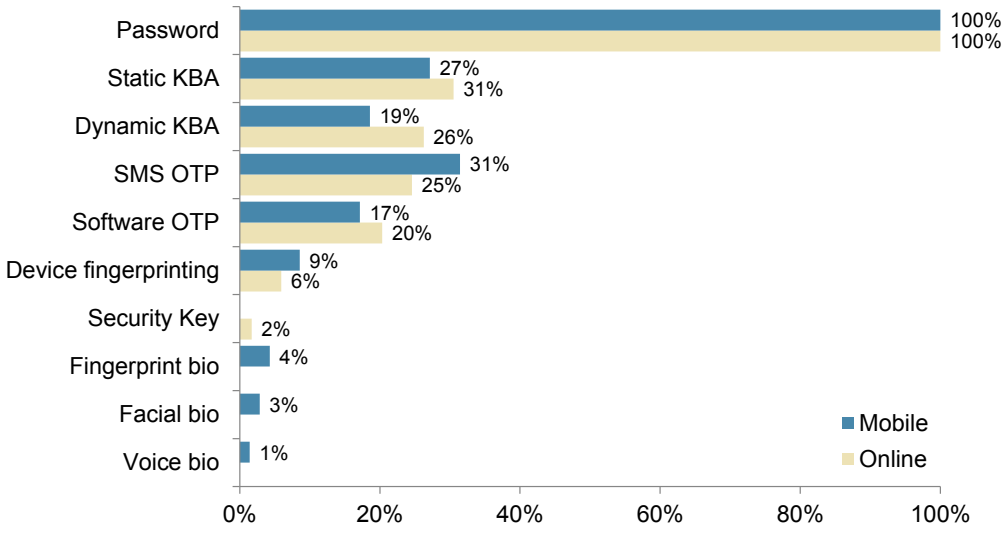
THE STATE OF CUSTOMER AUTHENTICATION

Digital channels are becoming the go-to places where consumers interact with businesses and each other. Over the past five years alone, the number of Facebook and Twitter users has more than doubled, the number of online banking users has grown by 50%, and mobile banking users have almost tripled (see Figure 3). To simultaneously ensure access for their good customers and protect their virtual storefronts from criminals, digitally oriented businesses are leveraging authentication. Much of this access has traditionally been facilitated by simple knowledge factor authentication — specifically, usernames and passwords. But criminals have become more sophisticated and consumers more demanding. This in turn has motivated another movement, one geared to strongly authenticating customers to reduce fraud, improve customer experience, and protect reputations.

For businesses that facilitate online access to their customers' accounts, a password is nearly always the minimum requirement to gain access. Other forms of authentication are far less commonly available. While passwords are recognized for a wide range of vulnerabilities, the most common alternatives have come under considerable scrutiny over the past few years. In particular, static security questions, which are offered by 31% of businesses to customers online and 27% in mobile channels, have answers that can easily be gleaned from consumers' social media accounts, for example. And SMS one-time passwords, offered by 25% of businesses that allow customers to access their accounts online and 31% in mobile, are at risk of interception during transmission or when entered (see Figure 3). The risk of interception is one of the weaknesses behind NIST's deprecation of SMS one-time passwords as a second factor of authentication in August 2016.

Adoption of Other Authentication Methods Pales in Comparison With Passwords

Figure 3: Customer Authentication Solutions Used, by Channel

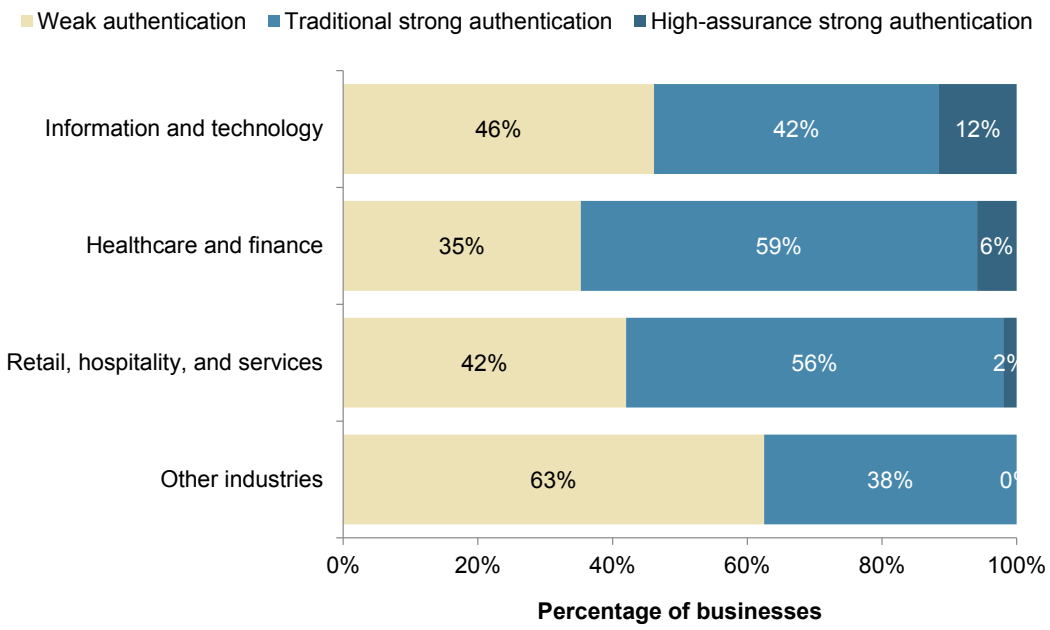


Source: Javelin Strategy & Research, 2017

In fact, vulnerabilities exist among practically every form of customer authentication, which has motivated both industry and government to devise approaches to better leverage authentication technology (see Strengthening Authentication section, pg. 8). And with different industries facing differing degrees of risk and regulation, the availability of strong authentication across these industries differs. Finance and healthcare are heavily regulated, high-profile targets for cybercriminals; as a result they are the most likely to offer traditional strong authentication to their customers (59%), but they are second to information and technology companies in offering high-assurance strong authentication. By comparison, 56% of retail and hospitality businesses offer traditional strong authentication, while only 2% offer high-assurance strong authentication (see Figure 4). Historically, these adoption rates of traditional strong authentication would have meant that businesses in a broad range of industries were providing strong protections for customers' accounts. But considering today's threats and the lackluster adoption of high-assurance authentication, there remain significant security gaps for criminals to exploit.

Heavily Regulated Finance and Healthcare Industries are Strong Authentication Leaders

Figure 4: Strength of Authentication Available, Customer Authentication

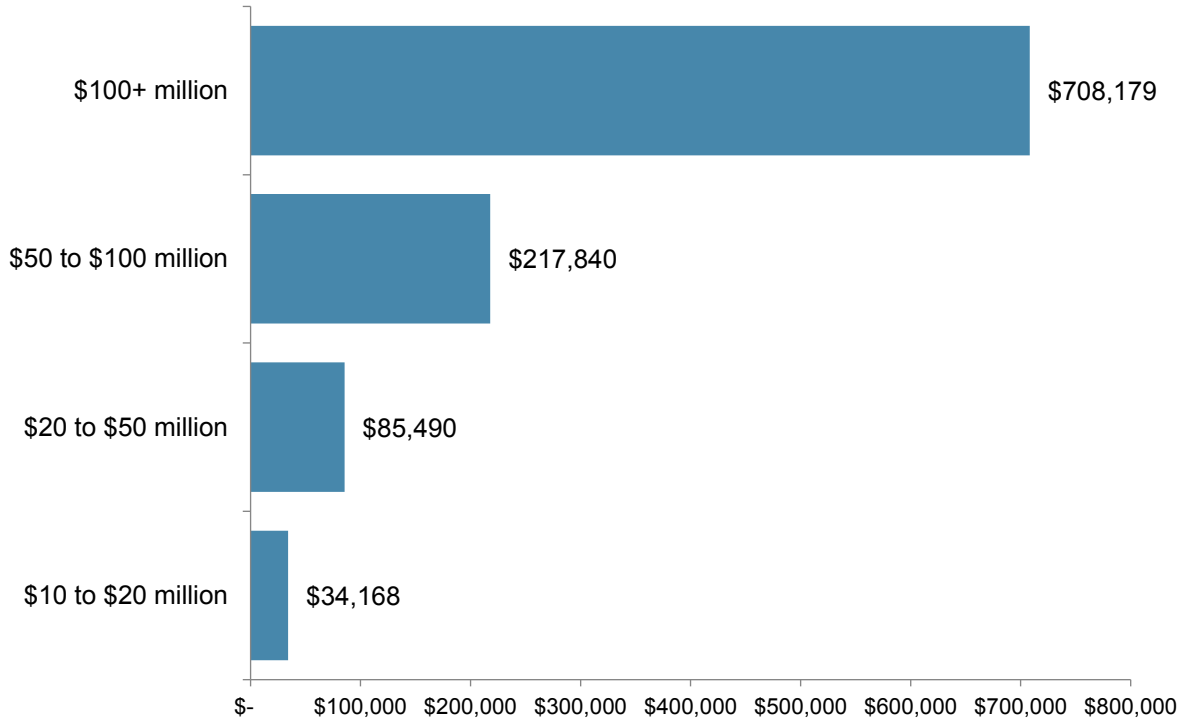


Source: Javelin Strategy & Research, 2017

The cost to authenticate customers is significant for many businesses, but the rise of the mobile device has benefitted both costs and security. Thanks to a wider array of authentication solutions than is generally available with desktop or laptop computers, including a range of biometric solutions, smartphones and tablets have helped enable better protection for consumer accounts. Even with some of the costs related to authentication hardware being shifted from the business to the consumer, thanks to the rise of smartphones and tablets, businesses that authenticate their customers spend $307,000 on average annually to do so. And for the largest businesses, this cost can be even higher — exceeding $700,000 for businesses with more than $100 million in revenue (see Figure 5). Understandably, these businesses likely have more accounts to protect, more at risk financially, and a greater ability to invest in authentication solutions than their smaller peers.

Investments in Authentication Grow by Orders of Magnitude Among Different Revenue Tiers

Figure 5: Annual Average Expenditures on Customer Authentication, by Annual Revenue



Source: Javelin Strategy & Research, 2017

Businesses should only expect to pay more as the nature of fraud continues to evolve. With the growing use of digital channels by consumers has come increased focus by criminals, who can operate more anonymously and efficiently digitally than they ever did in the physical world. In fact, identity fraud involving consumers reached a record high in 2016, creating 15.4 million victims. In the context of how fraud is evolving, it behooves businesses to leverage every reasonable tool at their disposal to protect their customers — especially authentication, with fraud reduction being the top benefit enjoyed by businesses that have employed a new authentication solution (70% — see Figure 6). With fraud on the rise, businesses will seek to replicate this success with further new solutions at a cost that ultimately is passed on to their customers.

Fraud Reduction Key, but Reduced False Positives Another Major Benefit of New Authentication Tools

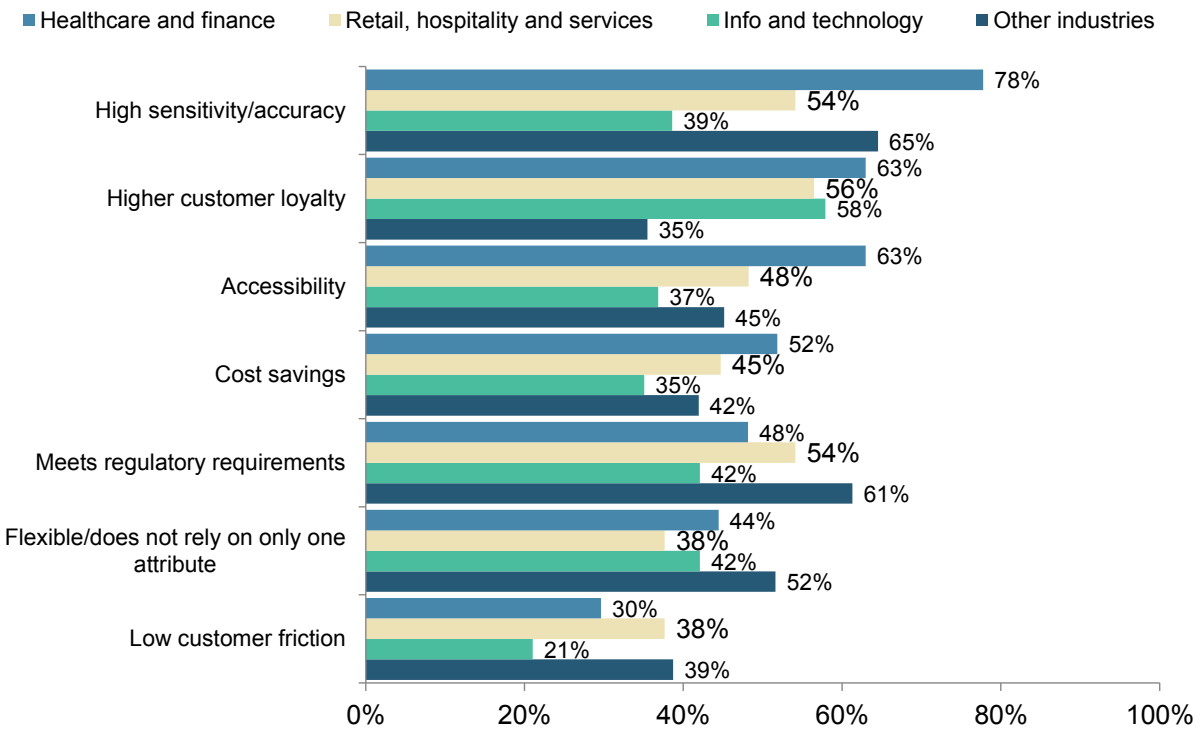
Figure 6: Benefits Experienced with Most Recent Authentication Implementation

Source: Javelin Strategy & Research, 2017

Efficacy alone, though, is not the sole or even most important driver for adopting an authentication solution for businesses in different industry verticals. Each industry vertical places an emphasis on specific qualities that best align with their risk profiles, customer expectations, and regulatory environment. For businesses that are frequent targets of fraudsters looking for a good payday, specifically those in the financial services and healthcare industries, accuracy is the top attribute they consider when selecting an authentication solution (78%). A favored quality is less clear among retailers, who instead have a more balanced set of desired benefits from their authentication solutions. Information and communication technology providers place as much value as retailers on how a solution can encourage customer loyalty (58%) but don't generally place much value on low-friction solutions (21%) — which can be viewed as a contradiction or as a willingness to trade friction for solutions that create a strong perception of security. This contrasts sharply, as can be expected, with services businesses, which place more of an emphasis on low friction when choosing an authentication solution (38%), (see Figure 7).

Accuracy is Most Important for Finance, While Retailers Have a More Balanced Set of Priorities

Figure 7: Most Important Attributes when Selecting an Authentication Solution, by Industry



Source: Javelin Strategy & Research, 2017

Regardless of the industry and the values common to businesses in those industries, businesses that store or transmit customer data are in possession of something frequently targeted by criminals. Criminals and other malicious actors have proven to be adept at identifying weak links in a business's security, or that of their partners, as evidenced by the 1 in 3 businesses that has experienced a breach of customers' data (see Figure 8). Besides the reputation damage that occurs after a breach, criminals add insult to injury by leveraging some of this same data to circumvent authentication.

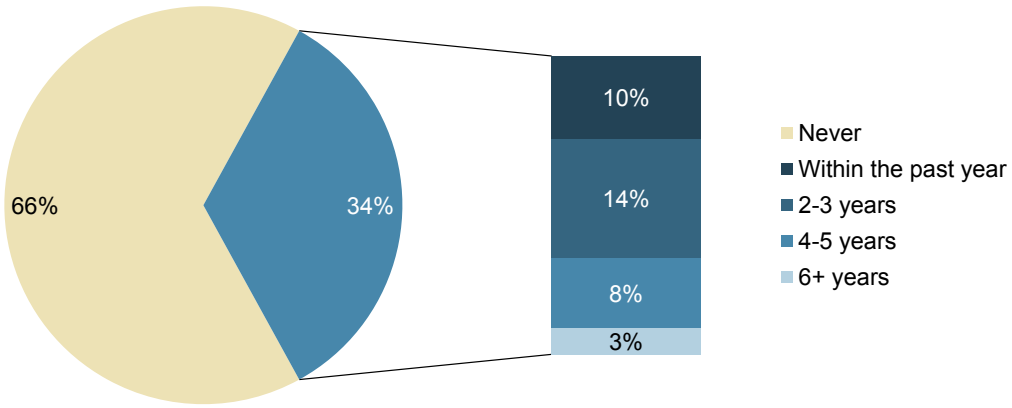
Examples include:

- The theft of password lists, which can be cracked and reused
- Compromised Social Security numbers, which many businesses leverage as an authenticator for the phone channel
- Mobile phone numbers, which criminals subsequently take over so as to have SMS OTP rerouted

Not all businesses are equal users of authentication, and some factors and solutions are more vulnerable than others. Facing the demands of the market and regulators, and at the same time seeking to repel attackers, those responsible for choosing and implementing customer authentication face a herculean task. High-assurance strong authentication and other effective mitigation strategies are needed now more than ever. This is true not only for securing access to customer accounts, though, as criminals seek access to the data within the enterprise — and that struggle has only just begun.

1 in 3 Companies Has Experienced a Customer Data Breach

Figure 8: Companies Aware of Experiencing a Breach of Customer Information



Source: Javelin Strategy & Research, 2017

THE STATE OF ENTERPRISE AUTHENTICATION

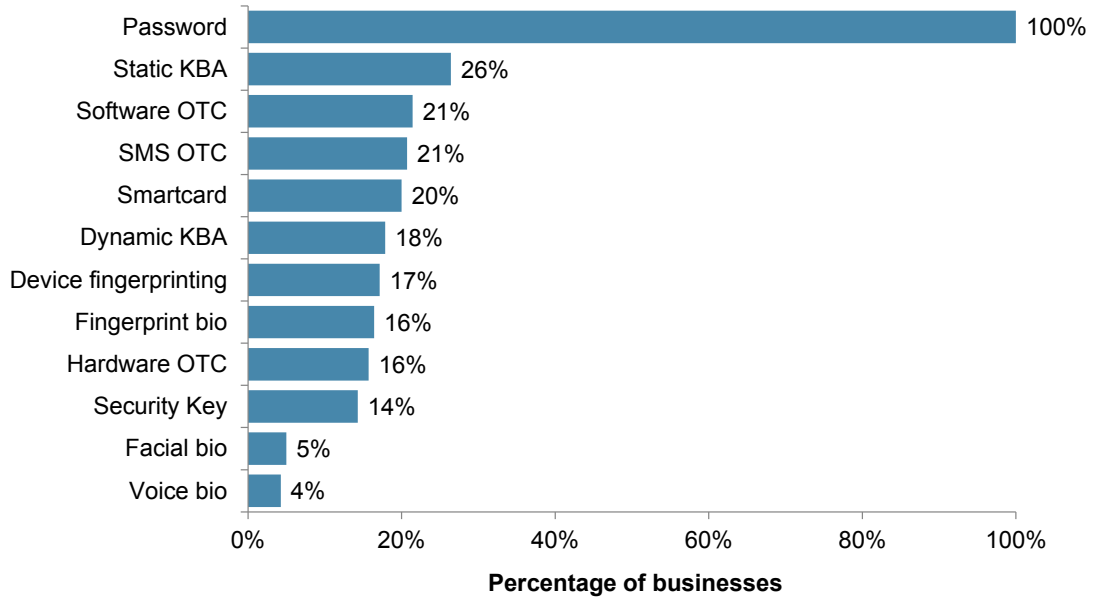
If targeting a business using stolen customer credentials and accounts is like death by a thousand cuts, then targeting sensitive information stored or transmitted on enterprise systems can be compared to a one-punch knockout. Enterprises in all industries regulate access to numerous systems housing intellectual property, customer and employee personal and financial credentials, and much more. Ensuring that only authorized personnel are granted access to sensitive information is paramount, but it can be daunting to decide how best to secure such a variety of systems with different numbers of users, risk quotients, and regulatory requirements.

Unsurprisingly, practically all businesses rely on passwords to authenticate users of some business functions. What is disappointing, however, is that the next most common authentication method is static security questions (26%). Because this method leverages user knowledge, it is still a weak method even when coupled with a password. Furthermore, it adds more friction to the login experience for employees compared with biometrics or device- or location-based solutions.

With 21% of businesses using software single-use tokens and SMS one-time passwords, and 16% leveraging hardware tokens for one-time password generation, the possession factor is the second most popular for employee authentication. Inherence has a foothold, with 16% of businesses using fingerprints to authenticate access to some system or other, but other biometrics still see low utilization, with adoption at or under 5% (see Figure 9).

Passwords Are the Leading Form of Enterprise Authentication

Figure 9: Enterprise Authentication Methods Used

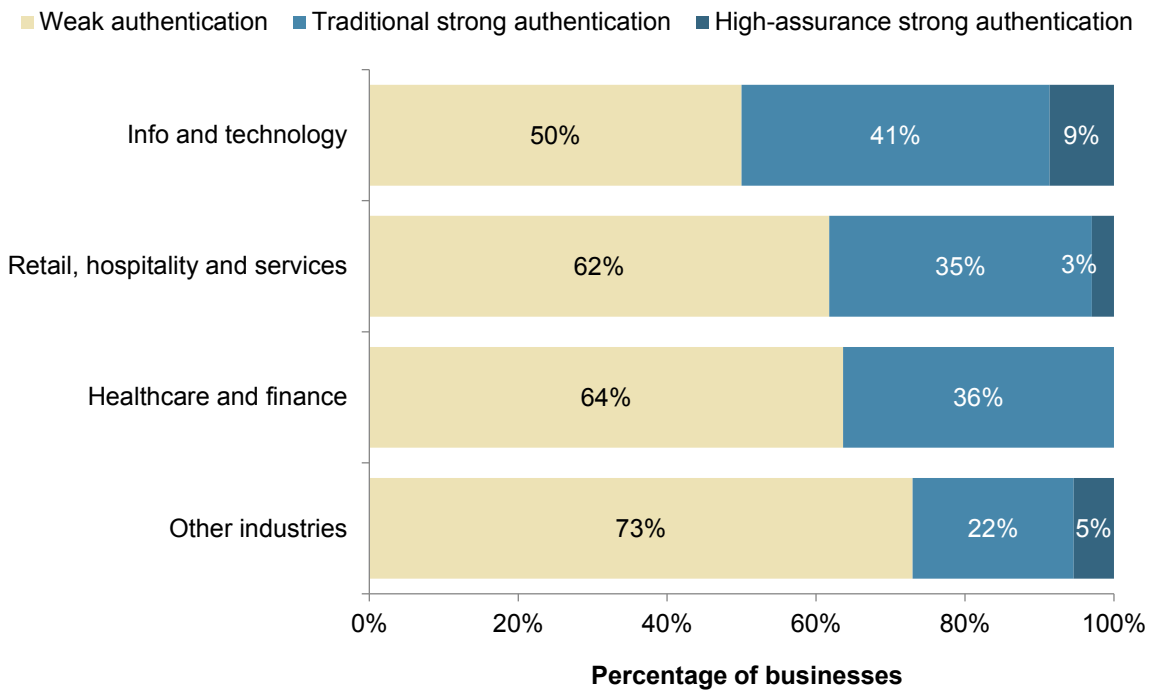


Source: Javelin Strategy & Research, 2017

Industries differ greatly in the strength of authentication they employ. Perhaps because of their technology orientation, information and technology companies tend to use strong authentication, with nearly half (41%) using strong authentication and 1 in 10 (9%) using high-assurance strong authentication. As an industry, healthcare is notorious for lagging behind other segments in implementing strong security measures. Adoption of high-assurance strong authentication is low enough not to register among surveyed healthcare or finance companies, and together the industries reported the second-highest adoption rate of traditional strong authentication, with 36% of these companies offering traditional multifactor authentication for employees (see Figure 10).

Finance and Healthcare Lead in the Adoption of Strong Authentication for the Enterprise

Figure 10: Strength of Authentication, Enterprise Authentication

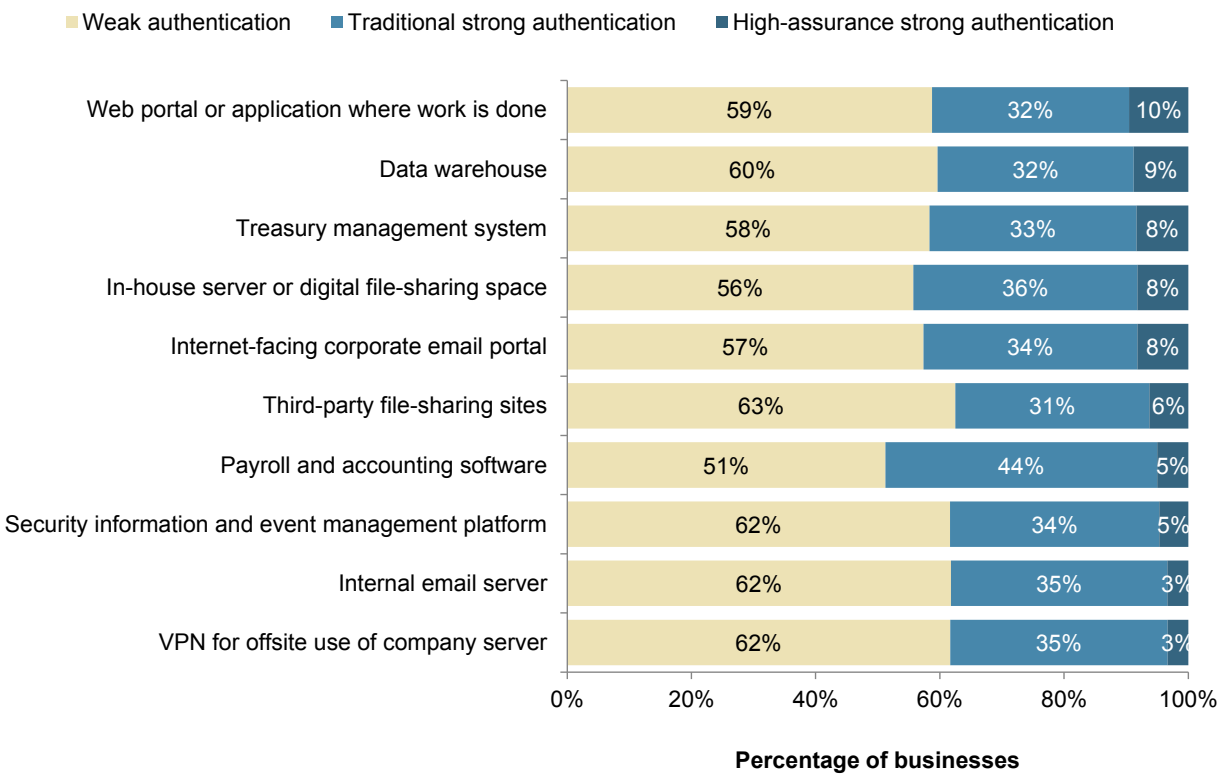


Source: Javelin Strategy & Research, 2017

Diving into the different systems in which authentication is employed, some emerge as higher protection priorities than others, and yet half or more of even the most important systems are still protected by weak authentication. Payroll systems are the most likely to require traditional strong authentication (44%), speaking to the sensitivity of the information they contain, but they have comparatively low adoption of high-assurance strong authentication (5%). Yet there are slight, but notable differences in the adoption rate of high-assurance strong authentication across different systems. Web portals or applications where work is done are the most likely to leverage this approach to authentication (10%), likely a function of the exposed nature of a system that anyone with a browser and a web address could attempt to access (see Figure 11).

Weak Authentication is Surprisingly Pervasive Across a Number of Systems

Figure 11: Strength of Authentication Used by Enterprises with Specific Data Systems

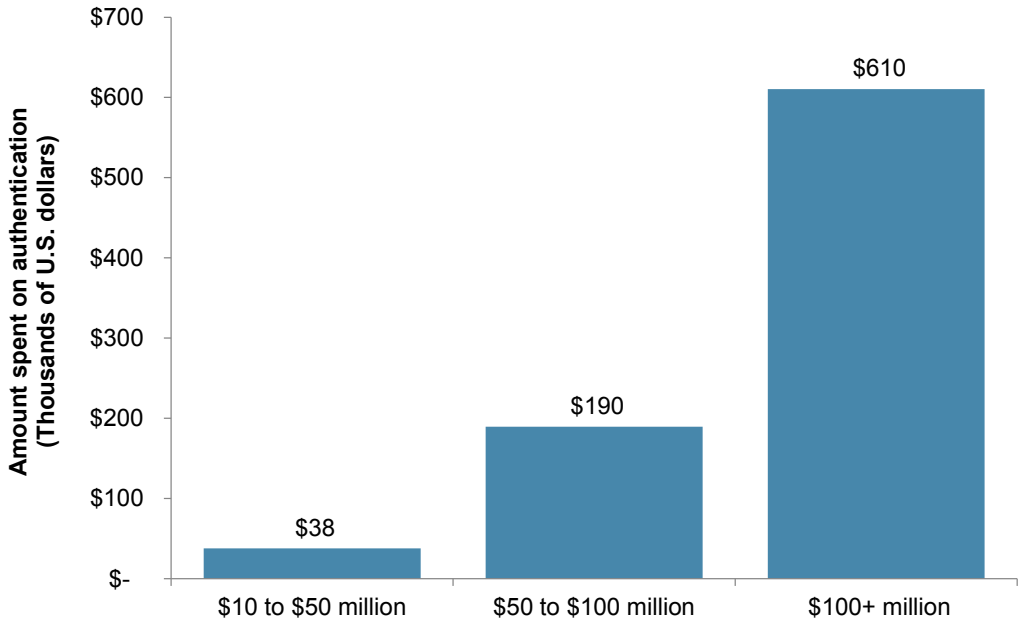


Source: Javelin Strategy & Research, 2017

Larger businesses spend more on authentication, which is makes sense on the face of it because they have more to spend and often have a greater volume of information to protect in the way of employee and customer data. However, businesses with $10 million to $50 million in revenue may in many cases have the same number of types of systems requiring authentication, or the same number of authorized users accessing the most sensitive company information, as a business 10 times that size. In these cases, spending on authentication solutions need not be directly proportionate to the size of the business. With relatively limited funds, smaller businesses may find themselves pressed to find an optimal balance between expenditure and securing the most data with the strongest combination of authentication solutions (see Figure 12).

Larger Businesses Spend Proportionately More on Enterprise Authentication

Figure 12: Dollars Spent on Authentication by Revenue, in Thousands

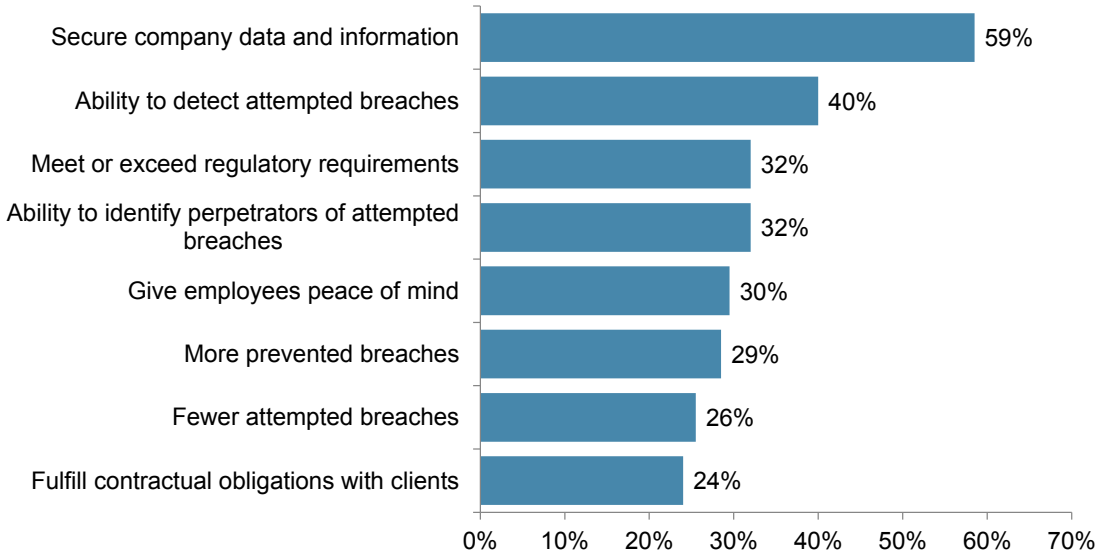


Source: Javelin Strategy & Research, 2017

When businesses select enterprise authentication solutions, their top priority is the actual security — or preventive power — the solution affords them. Three in five businesses say they choose methods to implement with security in mind, weighing this highly compared with the ability to detect breaches (40%) or identify perpetrators (32%), underscoring that businesses prefer to stop pilfering and fraud before it occurs, rather than swiftly detecting or resolving it. Meeting or exceeding regulatory requirements is a top priority for nearly a third of businesses, as is giving employees peace of mind (30%), (see Figure 13). Specific scenarios such as an increase in prevented or altogether-deterred breach attempts take a back seat to the more general measure of security, and few businesses consider contractual obligations to clients for more stringent security when selecting authentication methods.

General Security Benefits Top of Mind

Figure 13: Top Benefits Considered when Choosing Internal Authentication Methods



Source: Javelin Strategy & Research, 2017

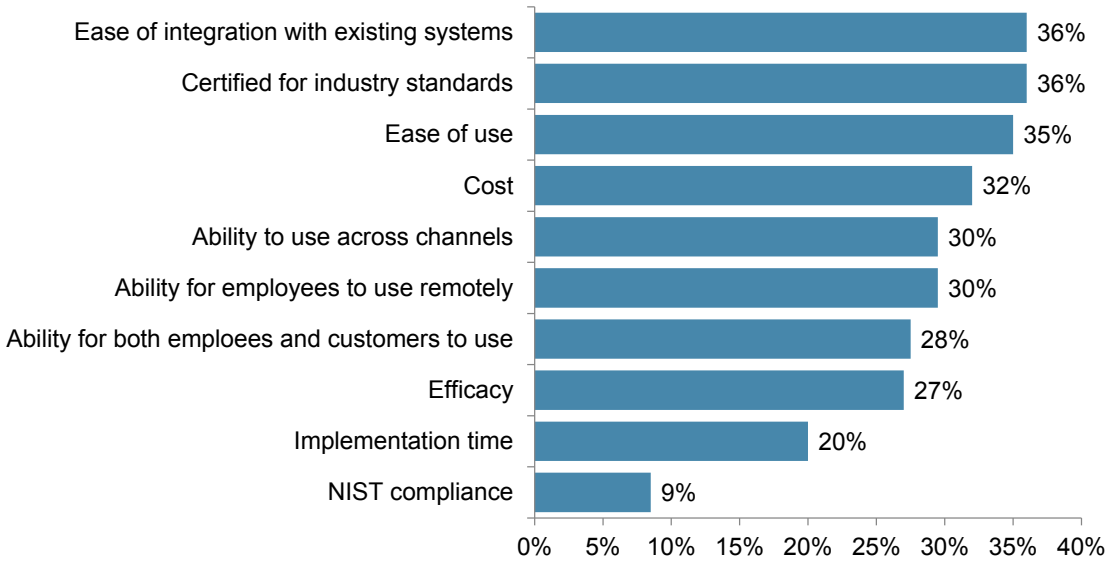
While businesses seek to meet certain ideals around security when they select an authentication solution, logistical considerations can prove just as critical. Many businesses seeking to increase the security of their internal systems are not assembling an authentication scheme from scratch but rather layering on additional solutions to an existing framework. Accordingly, ease of integration with existing systems is one of the two most frequently cited priorities for implementing new employee authentication solutions (36%). Sharing the lead in priorities is that the solution is certified to industry standards. This certification is a way for businesses to ensure the interoperability and quality of the products they purchase, and also importantly meets the need to prove their compliance to regulators.

Ease of use is a top priority for 35% of merchants, followed by cost (32%). Considerations related to versatility and scalability are of key importance to just under a third (28-30%) of businesses.

Perhaps in contrast to stated ideals, efficacy trailed many implementation considerations, cited by 27% of businesses. However, it could be that this is a lesser consideration due to a perception that solutions tend to be equally effective, rather than lower import given to this attribute. Implementation time and NIST compliance are the least-considered factors, with 20% and 9%, respectively, holding these as top considerations (see Figure 14).

Ease of Integration, Industry Standards Important for Employee Authentication

Figure 14: Most Important Attributes when Considering New Employee Authentication System



Source: Javelin Strategy & Research, 2017

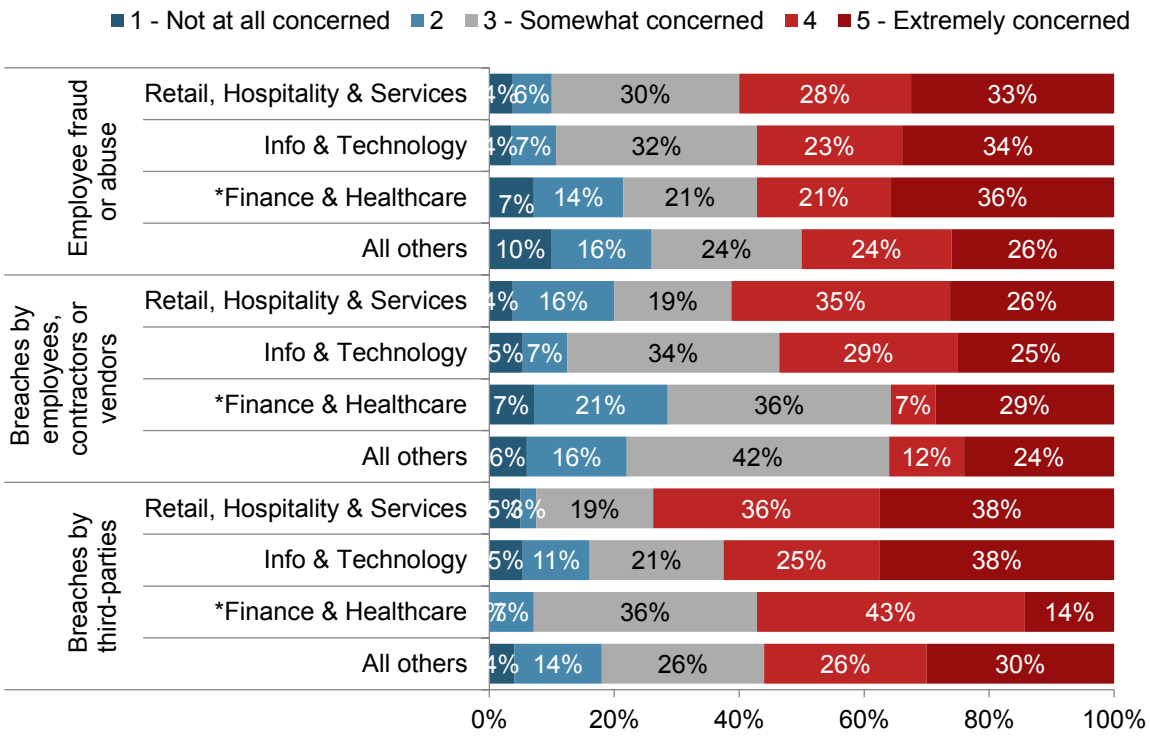
When businesses secure their sensitive information, they are protecting themselves from threats both from inside and outside the business. Third-party breaches may be at the top of the public consciousness, but many breaches are facilitated by insiders, and the greatest opportunity for fraud and embezzlement is in the hands of current employees. The internal threat (or the threat of employee-assisted breaches or hijackings of legitimate authenticated sessions) underscores the need for strong authentication, as businesses must verify that the person requesting access to highly sensitive data is the same person who initially entered the session or has the necessary permission.

Retailers express the most concern about third-party breaches, as their customers' financial data has proven a desirable target to hackers in recent years. Financial institutions, conversely, are most concerned about insider fraud, likely because a high number of employees at these institutions are able to access and initiate transactions from customer accounts (see Figure 15).

Breaches are shockingly common among large and mid-sized businesses. High-assurance strong authentication could play a key role in reversing this trend. Forty-four percent report that their business had ever been victimized, and 13% report that the breach occurred within the past 12

Retailers Are Understandably Most Concerned About Third-Party Breaches

Figure 15: Concern About Breaches and Insider Threats, by Industry



Source: Javelin Strategy & Research, 2017

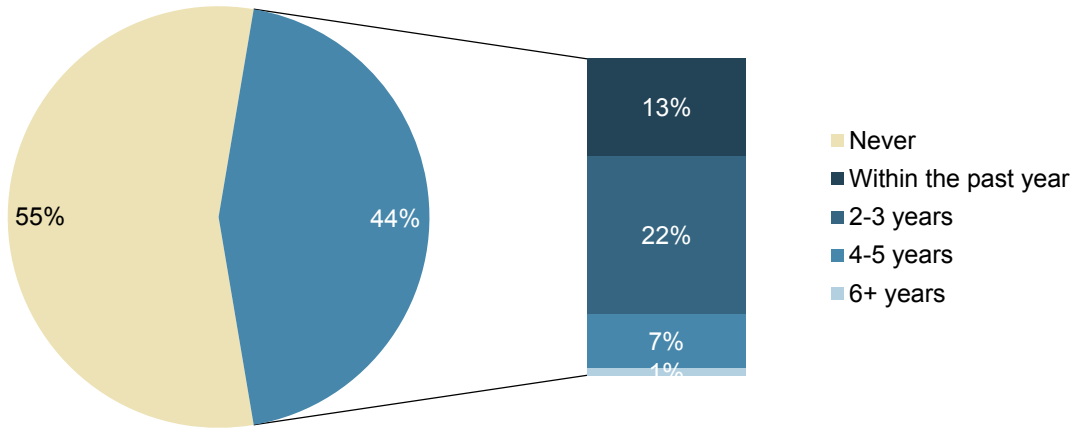
months (see Figure 16). These rates are likely skewed by underreporting, as some businesses may not have had the detection mechanisms in place to verify that a breach had occurred.

The overwhelming majority of executives of breached businesses were aware of the type of information that was pilfered during the breach. Among all breached businesses, company financial data was most likely to be targeted (46% of cases), followed by intellectual property (44% of cases).

However, almost as many breaches targeted employees' personal information (30%), which could be used to open new accounts in their name or misuse their existing accounts (see Appendix, Figure 18). Bearing in mind that 61% of treasury systems and 50% of payroll systems are protected only by weak authentication, and 56% of file-sharing spaces are weakly protected, the type of data most commonly breached may often prove low-hanging fruit to criminals.

More Than 4 in 10 Companies Have Experienced a Data Breach of Any Kind

Figure 16: Companies Aware of Experiencing a Breach of any Type of Information



Source: Javelin Strategy & Research, 2017

FIDO STRONG AUTHENTICATION EXAMPLES

What Is FIDO?

The FIDO (Fast IDentity Online) Alliance is a non-profit organization formed in July 2012 to address the lack of interoperability among strong authentication devices and the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance's goal is to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services.

FIDO standards utilize public key cryptography for enhanced online security and provide "single gesture" authentication experiences. To ensure interoperability among FIDO-enabled products and services in the market, the FIDO Alliance has rolled out a certification program and has certified approximately 360 products and services to date. This allows any FIDO-enabled website or cloud application to offer strong authentication to users leveraging a broad variety of existing and future FIDO Certified devices.

The FIDO Alliance currently has two sets of specifications for simpler, stronger authentication: Universal Second Factor (U2F) and Universal Authentication Framework (UAF).

- **FIDO UAF**. In this experience, users register their devices 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 FIDO 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 needed to authenticate to the service. The user no longer needs to enter a password when authenticating from that device. FIDO 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 at any time it chooses. The strong second factor allows the service to simplify its passwords (e.g. four-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 near-field communication (NFC). Users can use their FIDO U2F devices across all online services that support the protocol on supported web browsers.

FIDO is developing new specifications under the "FIDO 2 project" to be published this fall, which will enable expansion of FIDO authentication across web browsers and related web platform infrastructure: The Web Authentication (WebAuthn) specification in partnership with the World Wide Web Consortium (W3C) and the Client -to-Authenticator Protocol (CTAP):

- **W3C Web Authentication Specification.** The Web Authentication specification, based on three technical specifications submitted to the W3C by the FIDO Alliance last year, will define a standard web API to enable web applications to move beyond passwords and offer strong FIDO authentication across all web browsers and related web platform infrastructure.[3] Native support in web browsers and platforms is expected to expand FIDO's reach across PCs and mobile devices.[4]
- **FIDO Client-to-Authenticator Protocol (CTAP).** CTAP will enable browsers and operating systems to talk to external authenticators such as USB security keys and NFC- and Bluetooth-enabled devices and remove the requirement for users to re-register on every device they use. With this specification, a user could use a wearable or mobile device, for example, to log into a computer, tablet, IoT device, and more.

Google

Merging Security and Customer Experience with Security Keys

How is FIDO being used?

Google has been a pioneer in the digital space with innovative approaches to customer experience and product design, so it should be no surprise that it was one of the first businesses to make FIDO Universal 2nd Factor (U2F) authentication available to its employees and customers. In October 2014, Google announced it was offering support for security keys, FIDO U2F-compliant USB second factor devices.

Security keys are USB devices that supplement traditional password authentication for Google accounts by transmitting a cryptographic signature unique to each device. Since they are resilient against physical observation, interception, and phishing, security keys provide a significant increase over static passwords and even over many forms of secondary authentication, such as temporary passcodes delivered by SMS. This provides robust protection against account takeover attempts by dramatically increasing the complexity of fraud and minimizing the value associated with compromised user credentials.

What has been the impact?

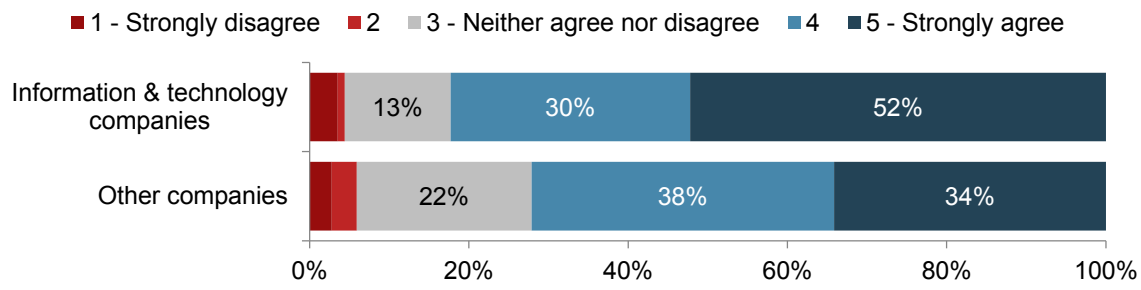
Security keys proved to be so successful that Google provided one security key for each employee device — averaging two per employee — across its more than 50,000 employees. In its preliminary analysis, Google found that authenticating with security keys outperformed one-time passwords on a variety of metrics. Employees authenticating with a security key were able to sign in twice as quickly as those using one-time passwords, and consumer users saw similar benefits.

At the same time, while there was an employee authentication failure rate of 3% with one-time passwords, security keys resulted in zero authentication failures during the studied time period.[5] With the lower failure rate, Google saw its second-factor-related support incidents consistently decline as users transitioned from one-time passwords to security keys. Google's Juan Lang reports, "For the deployment, we found the increased user productivity, and decreased support cost, were worth the increased hardware cost."[6]

More broadly, these types of benefits can explain why the FIDO Alliance's mission resonates particularly strongly with the information and technology industry, where 82% of businesses familiar with the FIDO Alliance report that they

FIDO Alliance's Mission Resonates Strongly with Information and Technology Companies

Figure 17: Perception of FIDO Alliance Among Information and Technology Companies, Other Companies



Source: Javelin Strategy & Research, 2017

believe what the FIDO Alliance does is innovative, compared with 72% of respondents in other industries (Figure 17).

BC Card

FIDO-Enabled Biometric Payment Authentication

BC Card is South Korea's largest payment processor and a subsidiary of the $7 billion telecom giant KT Corp.[7] As the first Asian financial services company represented on FIDO's board of directors, BC Card relies on FIDO for its biometric integrations into payment applications, such as Samsung Pay.

How is FIDO being used?

Within the Samsung Pay architecture, when users attempt to make a transaction with their mobile wallet, they may use biometric authentication on their device, which provides the cryptographic signature to be verified against the FIDO server. Upon verification, Samsung Pay submits the token request to BC Card's server. Once BC Card's server receives the token request from Samsung Pay, it confirms the authentication validity against the FIDO server and provides the tokenized payment credentials to the merchant, enabling the transaction to be processed securely.[8]

In addition to providing the supporting infrastructure for Samsung Pay, BC Card utilizes FIDO's standard to integrate voice biometric authentication into its BC Pay services. This enables BC Card to securely replace PIN authentication for payment approval.

What has been the impact?

Throughout this process, the transaction is enabled without the transmission of the user's payment or biometric information, minimizing the risk of compromise. In addition to the added security associated with eliminating transmitted credentials, integrating biometric authentication into Samsung Pay enables a more streamlined user experience with mobile-oriented authentication. In fact, BC Card reports that almost 90% of Samsung Pay users in its network use biometric authentication, rather than passwords.

Aetna

Next Generation Authentication Initiative

As one of the leading health insurance providers in the United States, Aetna plays a crucial role in the lives of nearly 50 million consumers. Providing healthcare coverage that consumers can get the most out of is driving Aetna to evolve its authentication capabilities. As part of its "Next Generation Authentication Initiative," Aetna will be leveraging the FIDO standard to revolutionize a key administrative component of healthcare — consumers' accessing and managing their health insurance through digital channels.[9]

How is FIDO being used?

A primary goal of Aetna's initiative is to eliminate the use of passwords to protect customer accounts. Passwords have become an unwelcomed focal point for Aetna's customers in digital channels. That passwords are vulnerable to compromise and at the same time are a roadblock for good customers is not lost on the company. Protecting customer health and payment data ultimately required a different approach.

Aetna's new approach to authentication will evolve across multiple phases:

- Phase 1 (2017) — Fingerprint and PIN were introduced, enabled by the FIDO protocol, along with risk-based authentication

- Phase 2 (2017) — Browser fingerprinting is to be added, along with the ability to approve logins across channels (i.e., a customer attempts to log in via Aetna's website and subsequently approves the login attempt via a bound mobile device)
- Phase 3 (2018) — User behavior will be integrated into the risk-based authentication models, and biometric authentication will be enabled for browser-based interactions via the W3C/FIDO protocol.

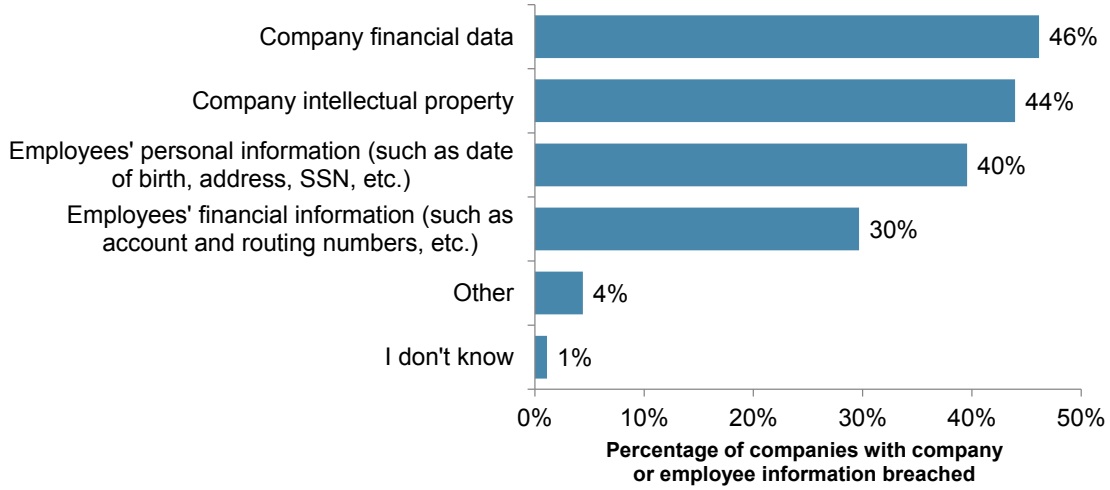
What has been the impact?

Implementation has only just begun, but Aetna expects to realize additional benefits to the company from the initiative. More specifically, leveraging the FIDO protocol is expected to allow Aetna to reduce the costs and complexity associated with integrating new authentication solutions. In an environment where businesses are leveraging new models and channels to better serve customers and new authentication solutions are regularly introduced, a flexible architecture is a logical approach to futureproofing Aetna's business.

APPENDIX

Criminals Go Where the Money Is, Preferring to Compromise Company Financial Data in a Breach

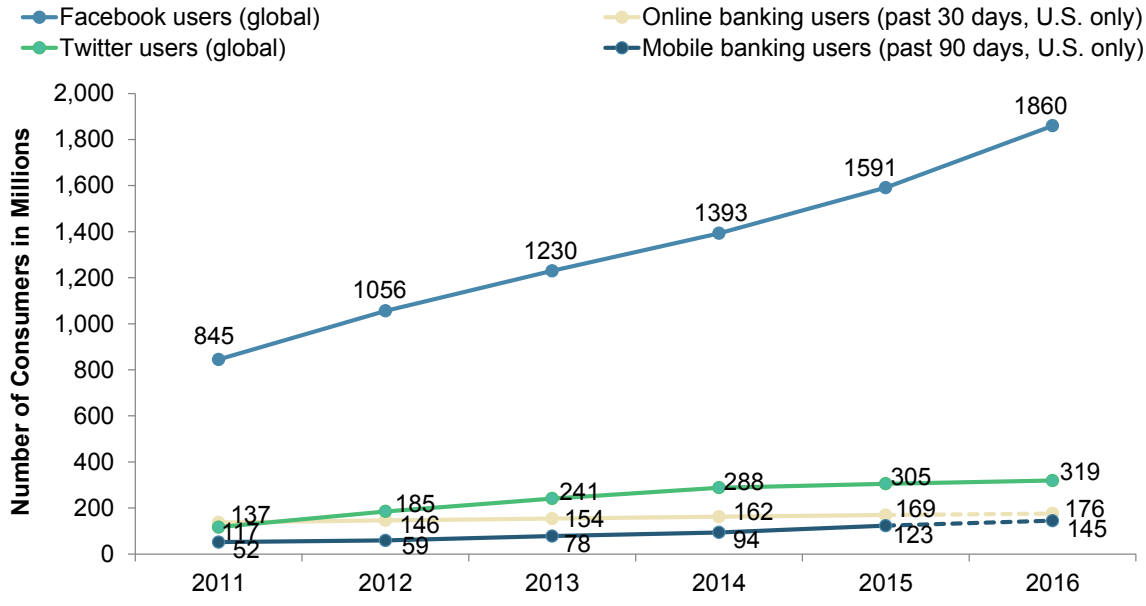
Figure 18: Type of Non-Customer Information Compromised in Breaches



Source: Javelin Strategy & Research, 2017

The Past Five Years Have Witnessed Explosive Growth of Digital Services

Figure 19: Strength of Authentication Available for Customers and Enterprise Users Number of Users, by Service and Channel (2011-16)



Source: Javelin Strategy & Research, 2017

METHODOLOGY

Merchant data in this report is based primarily on information collected in two surveys fielded in February 2017:

- An online survey of 200 businesses with authenticated customer online or mobile portals.
- An online survey of 200 businesses with authenticated employee portals.

Additionally, in-depth interviews were conducted with industry executives in roles influencing enterprise authentication policies.

ENDNOTES

1. https://pages.nist.gov/800-63-3/sp800-63-3.html, accessed July 3, 2017
2. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf, accessed July 3, 2017.
3. https://fidoalliance.org/w3c-launches-web-authentication-work-based-on-fido-specifications/, accessed August 1, 2017.
4. https://fidoalliance.org/google-launches-security-key-worlds-first-deployment-of-fast-identity-online-universal-second-factor-fido-u2f-authentication/, accessed July 31, 2017.
5. http://fc16.ifca.ai/preproceedings/25_Lang.pdf, accessed July 31, 2017.
6. Ibid.
7. https://www.forbes.com/companies/kt-corp/, accessed July 4, 2017.
8. https://www.slideshare.net/FIDOAlliance/bc-card-case-study-fido-biometric-authentication-for-payment-services, accessed July 31, 2017.
9. https://blogs.wsj.com/cio/2017/07/12/aetna-adds-behavior-based-security-to-customer-application/, accessed July 25, 2017.

ABOUT JAVELIN

Javelin Strategy & Research, a Greenwich Associates LLC company, is a research-based advisory 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 & Security
Sarah Miller, Research Manager – Custom Research & Operations

ABOUT THE FIDO ALLIANCE

The FIDO (Fast IDentity Online) Alliance is a non-profit organization formed in July 2012 to address the lack of interoperability among strong authentication devices and the problems users face with creating and remembering multiple usernames and passwords. Now made up of more than 250 leading global brands and technology providers, the alliance is dedicated to changing the nature of online authentication by establishing technical standards that will provide interoperable, frictionless strong authentication that is far more secure and easier to use than passwords. FIDO standards are based on public key cryptography in which 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, there are more than 350 FIDO Certified solutions, and deploying organizations have made FIDO-based protection available to more than 3 billion user accounts. FIDO-based solutions are available on the world's top five mobile platforms, the top four browser providers all have or are developing FIDO support, and Intel's newest chip platforms provide native support for FIDO-based authentication.