AFTER SMS ONE-TIME PASSWORDS:
MEETING THE AUTHENTICATION NEEDS OF BANKS AND THEIR CUSTOMERS

March 2018

Independently produced by:

JAVELIN

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

This original report, sponsored by Boloro, examines the use and degradation of SMS one-time passwords, along with the qualities that made it so pervasive, and charts a path forward for institutions in search of a viable replacement.

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

OVERVIEW

SMS one-time passwords (OTPs) have permeated nearly all authentication experiences in financial services, but because of an increasing number of vulnerabilities, their ability to provide robust security against fraud is failing. Fraud has become prevalent. It is time for financial institutions and others who require identity verification to plan for the next generation of authentication. To be effective, an authentication solution must be secure, user-friendly, instantaneous, and cost-effective, taking the context into account in analyzing the cost and inconvenience of the process and the benefit of its use.

EXECUTIVE SUMMARY

Key Findings

The end of the SMS OTP era is approaching. SMS one-time passwords are beginning to crack under the growing weight of vulnerabilities. Although attacks against SMS OTPs are typically still limited to targeted schemes against high-value victims, fraudsters' technology and sophistication are growing, and these attacks will become more widespread.

SMS one-time passwords are nearly ubiquitous at banks. More than a third of top financial institutions (FIs) offer SMS one-time passwords as a method for authenticating a customer at login. Roughly half of FIs use SMS OTPs as step-up authentication for large transactions, changes of contact information, or other high-risk events.

Emerging channels pose authentication challenges. The proliferation of banking and payment channels — such as chat bots, voice assistants, and other aspects of the "Internet of things" — create new cases in which FIs need to apply high-assurance authentication. Unfortunately, many of these interactions do not lend themselves well to traditional authentication methods such as passwords or even biometrics.

Familiarity is key to consumers' comfort with SMS OTP. This authentication method provides a familiar experience that is easily accessible to nearly all consumers. Any technology that replaces SMS OTP will need to bring a similar level of accessibility and familiarity for consumers to transition comfortably.

Fraudsters have a variety of ways to intercept SMS messages. They include phone porting, mobile malware, browser interception, and social engineering. Nearly all of these derive from the fact that SMS messages offer only a loose second factor: possession of a phone number rather than a physical device.

One-time passwords don't inspire the confidence of consumers. Compared to most biometric modalities, consumers view one-time passwords unfavorably. Consumers have a loose but intuitive grasp of multifactor authentication and tend to trust authentication methods that require them to be present physically in order to authenticate or to have specific knowledge. This results in greater trust in biometrics and even in knowledge-based authentication.

No single-factor authentication solution is flawless. One-time passwords have increasingly revealed themselves to be vulnerable to attackers, but even smartcards and security keys can be physically compromised; various biometric solutions can be stolen, replayed, or emulated; and device fingerprinting can be obscured. And once a biometric solution has been compromised, it can never be relied on again.

Recommendations

Begin planning for the end of SMS OTPs. Replacing an authentication method as ubiquitous as SMS OTPs will require detailed planning, both in the integration with other systems within the financial institution and in how to build awareness and confidence among accountholders.

Think holistically about the costs of authentication methods. The cost of an authentication method is not determined just by the upfront investment but also by the costs of developing new integrations and supporting ongoing maintenance and optimization of the system, as well as the costs of adoption among users.

Aim for a consistent experience across channels and use cases. Expanding solutions spur volume discounts and create a consistent customer experience. That consistency is key both for ensuring that customers always rely on an authentication experience they trust and feel comfortable with and for minimizing disruptions in service due to authentication failure.

Prioritize multichannel authentication to eliminate the single point of failure. Multichannel authentication, also known as "out-of-band" authentication, asks customers to authenticate themselves through a different channel than the one used to initiate the action. A process that separately prompts the authentication request eliminates the single point of failure and dramatically increases the complexity required by a fraudster to simultaneously compromise multiple aspects of the victim's life, e.g., both her browser session and mobile phone.

Streamline the user experience by collecting multiple factors within the same authentication event. Authentication methods that collect multiple factors simultaneously minimize the number of hurdles that legitimate users must overcome while requiring fraudsters to impersonate multiple characteristics of the victim at the same time.

There is no single-factor replacement for SMS one-time passwords. Any type of strong authentication scheme must rely on multiple factors, each filling in the gaps of another's weaknesses. That suggests a risk-based model that employs behaviometrics, device fingerprinting, and third-party authentication software and processes, among other tools. Ideally, in addition to being multifactor, the authentication would be multichannel.

A CASE OF CONVENIENCE: SMS ONE-TIME-PASSWORDS

At login and at step-up authentication, the argument around online and mobile authentication can be broken down into three parts:

- Usernames and passwords are insufficient.
- Multifactor authentication is a stark improvement.
- But, first, customer service must be considered.

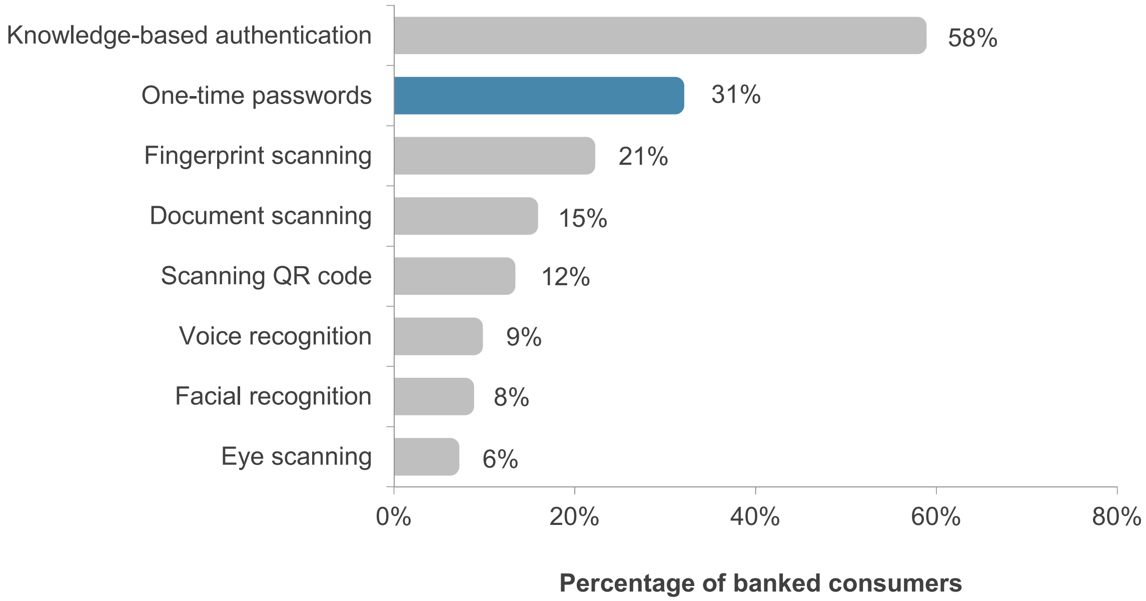
Around conference room tables, and over email and phone calls, nearly all firms operating online services —banking, retail, transportation, or healthcare, among others — have had the talk about authentication and fraud prevention. Each is considering its options.

The balance, some argue, should always shift toward convenience. The priority, others push back, is protecting customer information. For both reasons, the middle ground has traditionally been found in two-factor passwords sent over SMS text message (SMS one-time passwords).

Consequently, it should be no surprise that one -time passwords are one of the most familiar forms of authentication for consumers to see regularly. Just under a third (31%) of banked consumers have used one-time passwords to authenticate themselves; that's second only to knowledge-based authentication as the most widespread authentication method and even surpasses fingerprint scanning (Figure 1).

Nearly a Third of Bank Customers Have Used One-Time Passwords

Figure 1: Percentage of Consumers Who Have Used Each Authentication Method at an FI



Source: Javelin Strategy & Research, 2018

While the ease of delivery of SMS OTPs has propelled them to near-ubiquity, without additional factors, those four- to six-digit numeric codes delivered by text message have their own set of flaws. Criminals can target victims several ways: phone porting, browser interception, and mobile malware.

Without a doubt, stronger methods of authentication exist: sign-in tools that offer both accessibility and safety, without the specter of social engineering. They involve a mix of in-app login alerts, push notifications, and risk-based techniques that take advantage of mobile carrier technologies and device characteristics.

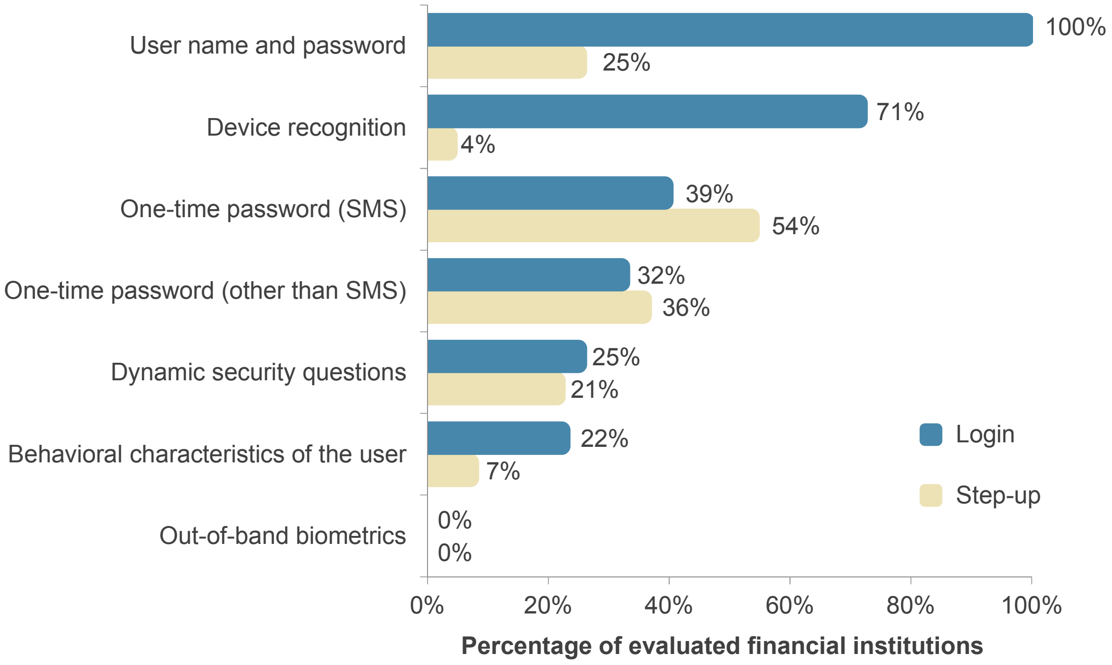
Bank Adoption of SMS OTPs

Banks have been among the most prominent companies to use text messages to send customers such one-time passwords to securely log into their web and online portals.

In 2017, more than a third of the top 30 financial institutions (FIs) enabled users to request one-time passwords delivered through SMS as additional authentication when logging into the bank's website, making it the third-most-prevalent form of login authentication, behind user names/passwords and device recognition (Figure 2). For step-up authentication, SMS OTPs are even more prevalent: More than half of FIs use it as a method of enhanced authentication for high-risk events such as password resets, changes of contact information, or high-value transactions.

One-Time Passwords Dominate Online Step-Up Authentication

Figure 2: Prevalence of Online Banking Login and Step-Up Authentication Methods



Source: Javelin Strategy & Research, 2018

SMS OTPs have been widely used outside of online banking channels to help verify that the user controls both the device and phone number she is enrolling. This can provide some anti-fraud assurance when an existing user is setting up mobile banking for the first time. More than a third of FIs lean on text messages during banking sessions both at mobile login and step-up authentication.[1]

> *"We are all gung-ho with the online channel, but how do you pull together the other channels? How are you getting the authentication correct on all sides there? … I can't believe that in the branch and call centers that we will still keep using the same forms of authentication."*
>
> Fraud executive,
> Regional financial institution

Banking and payment channels have proliferated, and SMS one-time codes been used in nearly all of them.

- Authentication in the call center: During customer service calls, some FIs send customers a one-time code over text to make sure those on the phone have access to the phone numbers registered to their accounts.
- Cardless cash: Banks like Wells Fargo, which support withdrawals from ATMs without the use of debit cards, give customers the option of sending a one-time password to a registered phone number.[2] This code is then entered at the ATM to authorize the withdrawal without the need to use a card.
- Transaction verification: For high-risk or out -of-pattern transactions, some banks require customers to respond to text messages, allowing the bank to approve or cancel the transaction.[3]

Understanding the Success of SMS

The widespread acceptance of SMS one-time codes among consumers can be attributed to three characteristics:

First, their use is straightforward. The user is already familiar with sending and receiving SMS messages, so there is no need for them to learn to use a new app. The codes are delivered on-demand, making authentication invisible until it is needed. Moreover, the experience is consistent: After the user has entered a code once, she will walk through a nearly identical process each time she needs to authenticate herself. This compares favorably even against biometric modalities, which can be sensitive to environmental conditions or the quality of the sensors on a user's device.

Second, they are device-agnostic. Assuming he owns any mobile phone, a user can enroll in SMS one-time passwords as soon as he enrolls in online banking without needing to download additional apps or learn new processes.

> *"The one thing I like is that everyone finally understands it, after all these years of making it available. Call it customer adoptability. It is commonplace. It is easy enough to use, although it can be a pain for some customers, depending on whether or not the carrier can deliver them in a timely way."*
>
> Fraud executive,
> Top 10 financial institution

Finally, one-time codes provide users with intuitive reasons to trust the security of the system. Users are already accustomed to a single phone number reliably being associated with a single person and, while they are unlikely to know the term “shared secret,” consumers have been trained to trust the effectiveness of codes and phrases to prove their identity online.

What Consumers Really Want

Three elements are essential in an authentication solution: ease of use, efficacy, and consistency. Unsurprisingly, consumers score one-time passwords high in convenience but comparatively low in perceived security.

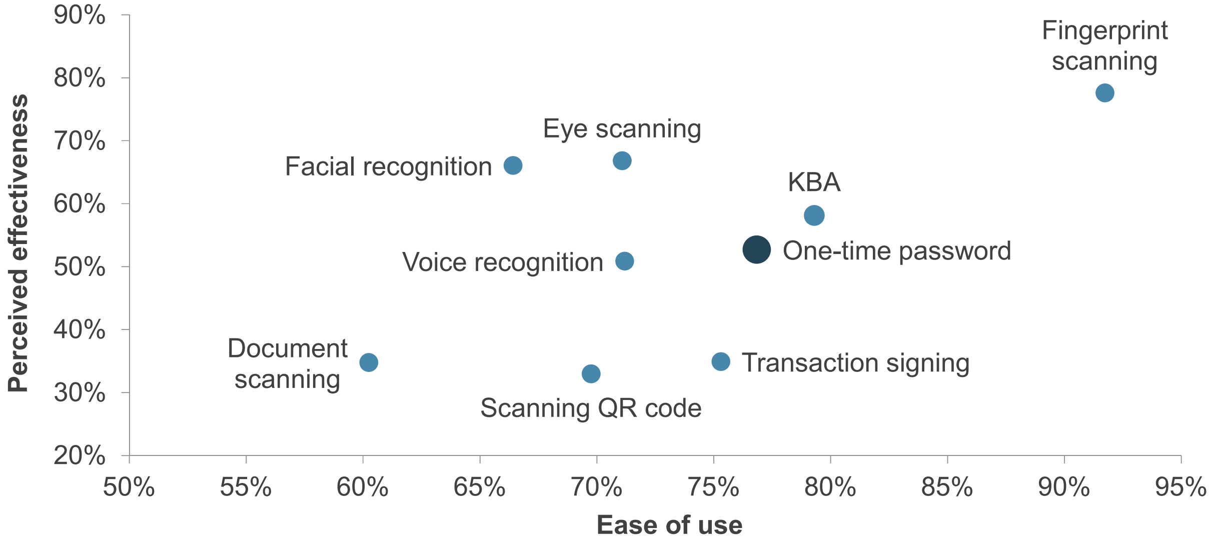
One-time passwords are seen as the third-easiest authentication method to use, behind fingerprint scanning and knowledge-based authentication, but ahead of face, eye, and voice biometrics (Figure 3). The familiar experience, easy enrollment, and lack of friction involved in receiving a password directly on a consumer’s phone pays dividends in this category.

Meanwhile, the trust that consumers place in one-time passwords is far less impressive. The authentication mechanism scores in the middle of the pack among its peers, which include facial recognition and transaction signing. This should be no surprise, either.

In a sense, consumers have a loose but intuitive grasp of the importance of two-factor authentication. It takes little security acumen to know that if a one-time code is delivered to your phone, anyone with access to the device can impersonate you. Conversely, more than a century of detective fiction has cemented fingerprints as immutable personal identifiers in consumers’ minds. If your device requires you to authenticate with a physical attribute — or secondarily, something only you know, such as a memorized PIN — consumers perceive much less risk of impersonation.

OTPs Get High Marks for Ease of Use But Not for Perceived Security

Figure 3: Consumers’ Perceived Effectiveness and Ease of Use for Authentication Methods



Source: Javelin Strategy & Research, 2018

AUTHENTICATION SHORTCOMINGS

The ubiquity of SMS OTPs — a once-simple fix for a complex problem — has attracted the attention of fraudsters, who have discovered a widening array of methods to intercept the codes:

- **Phone porting:** By calling the victims' phone carrier and providing basic personally identifiable information (PII) — often just a name, Social Security number, and phone number — fraudsters can deceive customer service personnel into transferring control of the line to a device under the fraudsters' control, claiming the old device has been lost, damaged, or stolen. Once the fraud scheme is complete, the fraudster can return control of the line to the victim.[4]

> *"If the fraudster goes through all the effort to get it (the phone porting) done at 2:00 in the afternoon, by 2:05 they are doing the transaction. The data better be very current, or it won't look like there is any issue."*
>
> Fraud executive,
> Regional financial institution

- **Social engineering:** Fraudsters can impersonate the victim's financial institution, under the guise of verifying a recent transaction or even addressing some fraudulent activity, and ask them to provide the one-time code as part of verifying their identity. The code is then provided to a fraudster who is trying to access the victim's banking portal while the call is underway.[5]
- **Mobile malware:** One of the earliest capabilities of mobile malware was intercepting SMS messages sent to the infected phone and forwarding them to a number under the control of the malware operator. Although mobile malware is less of a problem in the U.S., where Google and Apple exercise strong control over content in their app stores, it is a much greater threat in international markets where third-party app stores are more popular.
- **Flaws in Signaling System 7 (SS7):** Security vulnerabilities in the SS7 protocol underlying cellular networks can allow crooks to redirect a bank customer's text messages.[6]

This list could be expanded to include anecdotes about browser interception and call -forwarding techniques. The extent of the vulnerabilities in SMS delivery means that fraudsters who want to target a specific victim who is relying on SMS OTPs have plenty of tools at their disposal if one method fails.

The level of sophistication needed to exploit each of these vulnerabilities varies widely. Unfortunately, as has been demonstrated in other aspects of the criminal economy, once a skill or technology is discovered to be useful in perpetrating fraud, it quickly becomes repackaged into products that can be more widely used by less sophisticated fraudsters.

Currently, the level of targeting and investment required to successfully redirect SMS messages means that it is typically limited to high-value fraud schemes aimed at an established victim, rather than the kind of opportunistic fraud seen more broadly. This makes the vulnerabilities associated with SMS OTP particularly acute for financial institutions that serve high-net-worth clients, e.g., wealth managers. However, that does not mean that other financial institutions can afford to be complacent because, as fraudsters develop their skills and gain access to more sophisticated tools, the cost of targeting SMS messages will diminish and fraudsters will begin compromising them within progressively lower-value fraud schemes.

There is good reason to believe that this shift in the cybercrime market has already started. Over the past three years, the rate of mobile phone account takeover has risen dramatically, increasing more than fourfold from about 84,000 victims in 2015 to 380,000 in 2017 (Figure 4).

> *"I would love to get to a point where we could have a PIN that doesn't leave the device. It would be just as secure as fingerprint or face. Keep it on the device. … User ID and password has become too convoluted for users. Some just reset it every time they use the site. Wouldn't it be great just to give them a four-digit PIN?"*
>
> Fraud executive,
> Top 10 financial institution

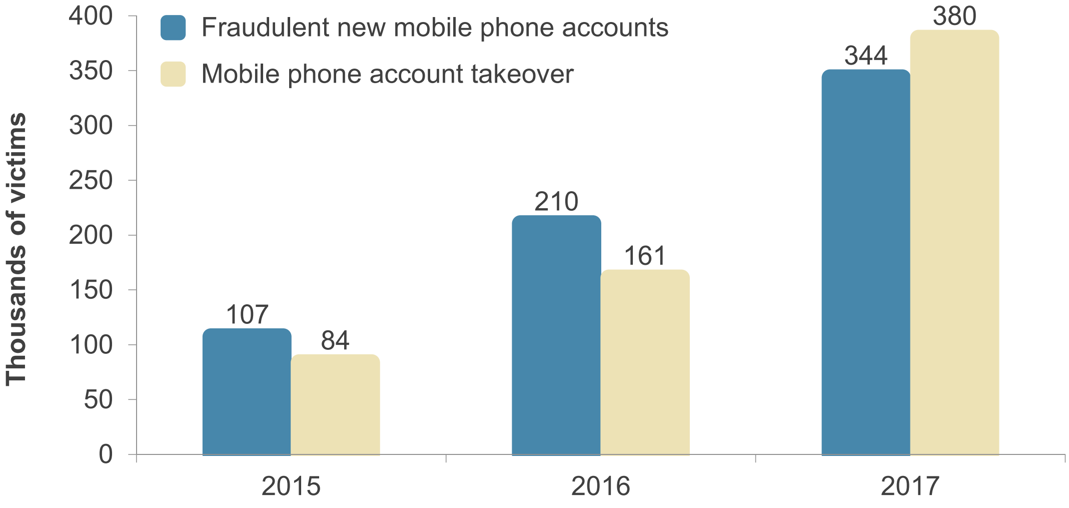
Because SMS one-time passwords must be entered into a browser where the user is initiating a login, they can only loosely be considered multichannel authentication. If the user's browser session is compromised, the one-time password can be collected at the same time as her other login credentials.

Compromising the user's browser can be accomplished several ways, ranging from a phishing campaign directing the user to a nearly identical version of their bank's login page or through malware that infects the victim's device, capturing the user's information as it is entered into the login page and relaying it to the fraudster.

Although the limited lifespan of an SMS OTP constrains fraudsters to using their victims' information almost as soon as it is entered, fraudsters who are able to capitalize on this access can gain nearly unlimited access to their victim's online banking portal. That's

Mobile Phone Takeover Is Rising Dramatically

Figure 4: New Fraudulent Mobile Phone Accounts and Account Takeovers



Source: Javelin Strategy & Research, 2018

because SMS OTPs are frequently used as step-up authentication in the event of an attempted login from an unfamiliar device or location.

The growing list of vulnerabilities in SMS OTP as a method of authentication led U.S. National Institute of Standards to deprecate two-factor authentication using SMS messages in July 2016. According to the agency, "Due to the risk that SMS messages or voice calls may be intercepted or redirected, implementers of new systems should carefully consider alternative authenticators."[7]

Regardless, no single-factor authentication scheme is flawless (Figure 5). One-time passwords have increasingly revealed themselves to be vulnerable to attackers, smartcards and security keys can be physically compromised; various biometric solutions can be stolen, replayed, or emulated; and device fingerprinting can be obscured.[8]

Even more sophisticated authentication methods have their shortcomings. For example, the use of biometric information to authenticate routine transactions might not be practical when the context of the transaction or other activity does not justify the potential risk of compromising biometric data. Once biometric data, such as a finger image, is compromised, it can never be relied on again. Biometric data is an individual's most personal information and answers the question, "Who are you?" Authentication is typically simply trying to answer the question, "Is this really you?" An authentication process that uses multiple factors (e.g., what you have and what you know), as well as multiple channels, with no potential compromising of personal data, can be the most effective way to verify a customer's identity and to allow the customer to validate a transaction in a user-friendly manner.

All of this points to a future of strong authentication, one in which multiple factors and metrics are used to authenticate consumers using online or mobile accounts. High-assurance, multiple factors of authentication reduce risk, making it more difficult for attackers to compromise a consumer's identity.

Mobile Network Security Working Group Looks for Answers

In light of the vulnerabilities with SMS one-time passwords, leading financial institutions have been meeting with mobile network operators (MNOs) to improve the security of SMS messages and related communication methods.

In particular, this working group has been pushing for more detail in the information provided by MNOs through third-party solutions and better identity-proofing before approving phone number porting to a new device. Being able to ascertain whether a phone number has been ported or is being forwarded is a crucial tool in reducing the risk of intercepted SMS messages, but timing is crucial. Fraudsters will frequently only port the number or establish call forwarding while the fraud scheme is in progress — often only a few hours. If data on the account's history is updated only every 24 hours, the data's value in preventing fraud is dramatically limited.

The security around phone porting, call forwarding, and other changes of account information are another key area of discussion. An authentication method is only as strong as its fallback solution, and when SMS OTPs fall back to rely on basic pieces of static personal information, comparatively little protection against fraud is offered.

No Single-Factor Authentication Method Offers Complete Protection

Figure 5: Authentication Methods and Their Vulnerabilities

Authentication Technology	Factor	Description	Key Vulnerabilities
Password, PIN, and Password	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 characterstics 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 charcteristics 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

BANKING PERSPECTIVES

Regardless of how financial institutions and mobile networks are able to shore up gaps in the security surrounding SMS one-time passwords, financial service providers who currently rely on this authentication method need to begin planning for the authentication method that will replace it.

In addition to meeting the needs of consumers, any new authentication must also be able to effectively meet business objectives at financial institutions. SMS one-time passwords have become so prevalent because they addressed several major needs at financial institutions, and any solution designed to replace them must be able to provide the same value.

Security Assurance

To provide sufficiently strong assurance of security to warrant use in financial services, any authentication method used to replace SMS OTPs must provide additional authentication factors beyond knowledge. SMS OTPs provide only a loose second factor (possession) because receipt is tied to the possession of a phone number rather than of a particular device. This loose connection enables many of the vulnerabilities that are currently plaguing this authentication method.

Obviously, no single solution offers an absolute answer for every conceivable instance of fraud, so whatever method financial institutions implement to replace SMS OTPs will require support from other solutions to provide appropriate levels of assurance. But the more assurance an authentication method is able to provide on its own, the less effort financial institutions will have to expend in shoring up gaps.

The strength of the assurance is tied closely to the regulatory environment the institution operates in. Regulatory programs like the Payment Services Directive 2 (PSD2) in Europe and Federal Financial Institutions Examination Council (FFIEC) authentication guidance in the U.S. are pushing financial institutions toward broader use of multifactor authentication in all channels.

Branding/Control of Technology

Unlike standalone code generators, financial institutions can exert greater control of branding within the authentication experience. Rather than visually ceding the process of securing accounts to Duo, Authy, Google, or some other provider, a financial institution can provide one-time codes from a consistent phone number with the financial institution's name included in the message. Of course, the plain-text nature of SMS messages also dictates that the financial institution is unable to include any visual branding within the message.

Satisfying the Customer Base

Of course, satisfying customers is a tremendous consideration for financial institution executives. In an industry built to protect customers' finances, usability and perceived security are core factors in evaluating any authentication method.

Technological accessibility is obviously a major concern and probably the primary reason that SMS became the default delivery method for one-time passwords rather than stand-alone apps or in-app notifications.

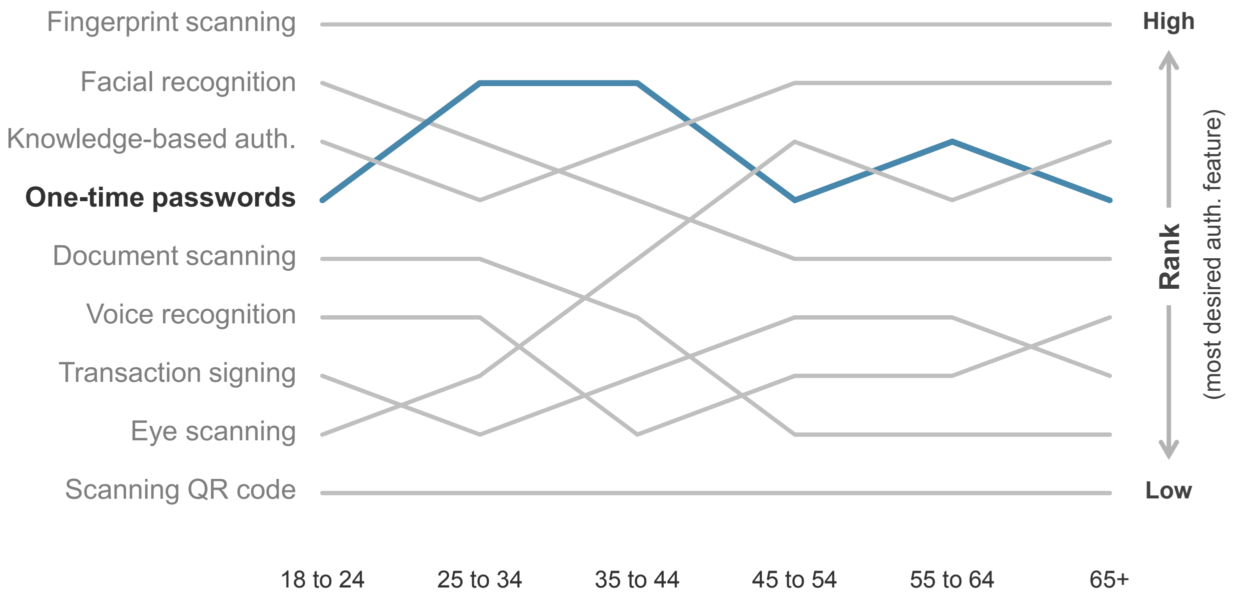
There is also an element of security theater to the choice of authentication solutions. In addition to the real fraud protections that come with implementing a particular security feature, the financial institution must offer anti-fraud measures that provide tangible assurance of security to their customers. Typically, this requires two things: First, there must be a visible, participatory element to the authentication method; second, the customer must be able to understand how the authentication method links back to them.

This is why methods such as one-time passwords and fingerprint biometrics have conventionally been received well by consumers but largely invisible methods like device recognition and geolocation are often viewed with greater suspicion. In fact, despite younger consumers' reputation for preferring frictionless, high-tech solutions, one-time passwords are second only to fingerprint scanning as the most desired authentication feature among consumers age 25 to 44 (Figure 6). This also highlights one of the major challenges for financial institutions in designing an authentication strategy: Different sets of users have different needs and priorities.

In addition, frictionless, high-tech solutions provide only partial protection against fraud, and not absolute protection, because they do not capture all issues. They are also susceptible to false positives that block legitimate activity, inconveniencing the customer and resulting in a loss of business.

OTP Codes Are Second Only to Fingerprints Among Young Consumers

Figure 6: Most Desired Authentication Features, by Age



Source: Javelin Strategy & Research, 2018

Budget

The cost of implementing a solution and its return on investment over time are inevitably major considerations in pitching a new authentication solution to non-fraud parts of the business.

The authentication method's ability to provide an immediate, measurable improvement in the financial institution's ability to address an ongoing fraud threat is obviously important. This provides the initial impetus to justify the effort and expense of implementing a wholly new system or expanding a tool that is currently in limited use.

Ease of integration is a major factor in determining the cost of implementing a new authentication system. For instance, can the new system interface with existing anti-fraud and rule-management systems at the financial institution without requiring the FI to build new connections? This can be especially important for smaller institutions that lack the personnel to renovate their internal systems to implement a new authentication method.

The ongoing cost of maintaining and optimizing any solution will affect the long-term return on investment and provides a difficult balance for solution providers. Black-box solutions that rely on proprietary processes require comparatively little involvement from personnel at client companies, but they also make it more challenging for the client to adjust parameters to optimize fraud controls as criminal schemes and legitimate customer behavior change.

Being able to use a given solution in more than one use case or channel can help ease budget considerations. For financial institutions, expanding use of the solution to better secure online, mobile, and call center channels enables them to replace other solutions, create volume discounts, and create a consistent customer experience.

Future-Proofing

Although an authentication solution might be cost-efficient when initially implemented, the evolving nature of fraud can force institutions to add additional controls — and by extension additional costs — to maintain effectiveness over time. SMS OTPs provide a perfect example of this because financial institutions must also supplement an OTP system with data from mobile network operators to detect phone porting and malware detection to prevent interception and forwarding.

FUTURE-PROOFING AUTHENTICATION

With the growing sophistication of fraudsters and the proliferation of tools and services on criminal marketplaces, financial institutions must critically assess the gaps in their authentication strategy in all banking channels. To have longevity against evolving fraud threats, any authentication scheme must be: reliable, multichannel, and multifactor.

Reliable

Providing a consistent customer experience that is easily accessible, regardless of device type or installed software, is tremendously important on several levels. First, as has been discussed, providing users with security solutions that have low barriers to use is crucial for quickly establishing a wide user base and transitioning from older, less secure methods of authentication.

Reliability also provides security benefits, in addition to its impact on customer relationships. Fallback authentication poses a significant problem in that the secondary authentication method used — frequently knowledge-based authentication like security questions or details of recent account activity — is often less robust than the primary authentication method. This offers fraudsters an opportunity to force the targeted organization to use an authentication method they know they can overcome.

Multichannel

Requiring customers to authenticate themselves through a different channel than the one used to initiate the action that prompted the authentication request dramatically increases the complexity of fraud. By requiring fraudsters to simultaneously compromise multiple aspects of the victim's life, both their laptop and mobile phone, for instance, multichannel authentication makes all but the most lucrative fraud schemes cost-prohibitive.

A secondary advantage of multichannel authentication is that an authentication request that is not connected to their activity alerts accountholders to fraudulent login attempts. Not only does this prevent fraudsters from successfully accessing their victims' accounts, it can enable victims and their financial institutions to be on high alert for additional suspicious activity.

For users, out-of-band authentication can ensure a consistent authentication experience even on emerging financial and payment channels. As tools such as chat bots, voice assistants, and the "Internet of things" expand in financial services, consumers will expect a similar security experience wherever they manage their money. Out-of-band authentication can ensure that users walk through a familiar authentication process whenever they need to verify their identity.

Multifactor

Much like multichannel authentication, multifactor authentication increases the complexity of fraud by requiring the fraudster to impersonate multiple characteristics of the accountholder. While it is often feasible to obtain the information or access necessary to impersonate one aspect of the victim fairly easily, combining multiple characteristics of the victim to overcome a multifactor authentication challenge is much more difficult.

Although institutions can achieve multifactor authentication by requiring users to authenticate themselves through multiple methods, ideally both authentication factors are combined in the same authentication “event” for the user. This is an ideal that SMS one-time passwords have never been able to achieve because they could not accommodate user response. Consequently, the most assurance that SMS OTPs could offer was proof that the individual entering the code was in possession of a device associated with the user’s phone number.

Newer authentication methods enable financial institutions to authenticate users through multiple factors simultaneously: for instance, by collecting a password or PIN through a secondary device that is linked to the account. Other options include biometric authentication over formalized authentication protocols like the Fast Identity Online (FIDO) standard, which combines verification of physical attributes of the user with cryptographic assurance that the device sending the transmission is the same one that was previously enrolled.

> *“I love the idea of authenticating to the device with password or PIN. There is a movement in the industry to deputize the customer, to give them control — especially in the card space. I can get alerts, turn it off, etc. Why not take it the next step?”*
>
> Fraud executive,
> Regional financial institution

CONCLUSION

Successful authentication solutions will strike the right balance between security and user-friendliness, taking context into account in determining the levels of cost and inconvenience that are practical when measured against the risk and benefit involved.

Any potential solution will be subject to shelf-life limitations, even considering the value of enhancements that can be implemented over time. SMS one-time passwords have rightly grown ubiquitous across financial services, but they are starting to crack under the growing weight of vulnerabilities. As vulnerabilities become more easily exploited by fraudsters, attacks against SMS OTPs will shift from targeted attacks on high-value victims to more widespread attacks against consumers. Protecting accountholders means preparing a replacement solution before that occurs.

Convenience and the ability to be broadly accessed are essentials for any SMS OTP successor, which makes use of the authentication method across channels crucial. Compatibility with all mobile devices is essential. Accountholders use and trust SMS OTPs because they are straightforward, based on a familiar experience, and provide a consistent experience in all channels. As financial services and payments expand into new channels — chat bots, voice assistants, and the Internet of things — consumers will expect a similar security experience wherever they manage their money. Any solution that does not begin at parity with SMS OTPs in this regard will be fighting an uphill battle to gain acceptance among consumers.

Additionally, fraudsters have grown more sophisticated alongside advancements in anti-fraud tools. This means that any authentication event must take into account multiple factors — knowledge, ownership, and possession — as well as multiple channels in order to trust the individual on the other side of the computer. These multiple factors and channels dramatically increase the complexity of any fraud scheme, raising the cost of stealing accountholders funds high enough to deter cybercriminals.

METHODOLOGY

Consumer data was collected from an online survey of 5,000 U.S. adults over age 18; this sample is representative of the U.S. census demographics distribution. Data collection took place from November 1-16, 2017. Final data is weighted using 18+ U.S. Population Benchmarks on age, gender, race/ethnicity, education, census region, and metropolitan status from the most current CPS census. For questions answered by all 5,000 respondents, the maximum margin of sampling error is ±1.39 percentage points at the 95% confidence level.

Further data was taken from an online survey of 5,028 individuals fielded from November 5-21, 2016. For questions answered by all 5,028 respondents, the maximum margin of sampling error is ±1.40 percentage points at the 95% confidence level.

Data on bank adoption of authentication features was collected by Javelin with a two-stage process. Results from 28 of the largest depository financial institutions were initially collected through a network of mystery shoppers with at least one active account at each financial institution. Once the mystery shopping had been completed, each financial institution was contacted and given the opportunity to validate the results. Twenty-one financial institutions validated the results of the scorecard. Results for financial institutions that declined to validate results were confirmed by Javelin personnel who held at least one account at each financial institution.

Additionally, Javelin conducted interviews of senior financial industry executives responsible for authentication at U.S. retail banks.

ENDNOTES

1. **Account Safety in Banking Scorecard**, Javelin Strategy & Research, 2017.
2. https://www.wellsfargo.com/help/faqs/access-code/, accessed January 7, 2018.
3. https://www.usaa.com/inet/pages/security_watch_out_for_suspicious_account_activity, accessed January 7, 2018.
4. https://www.nbcchicago.com/news/local/Thieves-Able-to-Hack-Cell-Phones-Through-Porting-373934121.html, accessed February 8, 2018.
5. http://www.sfgate.com/business/article/Social-engineers-hack-people-not-computers-7991010.php, accessed February 8, 2018.
6. https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/, accessed February 8, 2018.
7. https://www.theregister.co.uk/2016/12/06/2fa_missed_warning/, accessed February 8, 2018.
8. https://www.fireeye.com/blog/threat-research/2018/02/reelphish-real-time-two-factor-phishing-tool.html, accessed February 8, 2018.

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

Contributors: Sean Sposito, Analyst, Cybersecurity

Publication Date: March 2018

ABOUT BOLORO

Boloro is a globally patented, multi-channel, multi-factor authentication and mobile payments system that allows users to authenticate any activity using their mobile phone. Boloro’s ATM-like approach uses what you have (your physical mobile phone) and what you know (your memorized PIN), and separates the authentication process from the actual transaction by using the secure, signaling layer of the mobile carrier. Boloro’s authentication process avoids the Internet and the Operating System, providing a separate, secure way to validate Internet-based transactions and other activity.