A US PAYMENTS FORUM WHITE PAPER

Strengthening the Security of Consumer Authentication through Phishing-Resistant Multi-Factor Authentication

Version 1.0

June 2024

U.S. Payments Forum
544 Hillside Road
Redwood City, CA 94062

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body that brings stakeholders together on neutral ground to enable efficient, timely and effective implementation of emerging and existing payment technologies. This is achieved through education, guidance and alternative paths to adoption. The Forum is the only non-profit organization whose membership includes the whole payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on and have a voice in the future of the U.S. payments industry. The organization operates within the Secure Technology Alliance, an association that encompasses all aspects of secure digital technologies. Additional information can be found at http://www.uspaymentsforum.org.

Table of Contents

Executive Summary

This white paper highlights the challenges of traditional authentication methods, especially the vulnerabilities of passwords to phishing attacks. Phishing has become a major security threat in the U.S., reported as the number one fraud crime in 2022, and has prompted a requirement for all U.S. Federal agencies to implement phishing-resistant multi-factor authentication (MFA) by 2024.

While common MFA approaches (e.g., one-time passcodes) may thwart some phishing attacks, fraudsters use schemes to bypass MFA and gain access to user accounts. The white paper discusses various phishing-based MFA bypass schemes, such as social engineering, one-time-password (OTP) relay, and the use of bots and phishing kits, that payments industry stakeholders have experienced. Generative artificial intelligence (AI) is further altering the payments fraud landscape, providing new tools for fraud perpetrators.

Payments industry stakeholders are advised to implement countermeasures that can detect fraud, including monitoring user activity and educating customers. In addition, businesses are encouraged to implement some type of MFA in the short term – even if only OTP or push-based notifications – while developing a longer-term strategy. Mitigation tactics for financial institutions and merchants include monitoring customer activity, complying with the Payment Card Industry Data Security Standard (PCI DSS), educating the customer so that they maintain their vigilance to phishing, and using machine learning to identify suspicious actor behavior.

The ultimate goal is to support a phishing-resistant MFA solution, for example using FIDO2 specifications. These specifications use device-bound keys and eliminate the need for passwords, making authentication more secure. Standards and specifications that are being developed to promote global interoperability are at the forefront of emerging technologies that relate to the next generation of multi-factor authentication and identity in general.

The white paper concludes by highlighting the importance for all payments industry stakeholders to understand evolving authentication methods and implement emerging standards for improved security.

1. Introduction

Authentication is the process or action of verifying the identity of an end user and is critical when granting access to a given service. The most basic method of authentication is providing a username and password, which was invented in 1960 by MIT professor Fernando Corbató.

Many challenges exist with passwords today. The most secure passwords are those that are a complex set of capital and lower-case letters, numbers, and symbols; however, they are difficult to remember, creating an increased need for password reset, a costly and time-consuming process for both service providers and customers. In addition, the average person has 100 passwords to remember for all the sites and accounts they access. This leads users to create passwords that are easy to remember and sometimes include personal user references, such as a pet's name or place of birth, which can be easily identified by cybercriminals through social media accounts. In addition, people still use simple passwords like "123456" or "password", and often use these across multiple accounts. This practice makes it easier for cybercriminals to gain access to multiple accounts at once. Finally, many people maintain lists of their passwords in an unsecure manner and/or share their password and username with others, creating an even more likely scenario that they will be phished or stolen.

Password managers were introduced to create and store passwords in a safer and more efficient manner. While these prove to be a better alternative to memorization and handwritten notes, cybercriminals have found ways to hack into password managers as well, with at least two breaches reported in 2022.[1]

In an attempt to secure passwords, service providers created strong password policies to force users to create stronger unique passwords. Strong passwords are incrementally better but still leave users vulnerable: cybercriminals are constantly improving their tactics and data becomes available through breaches. As industries became more conscious of the inherent weakness in a password-only approach, multi-factor authentication (MFA) has become the next evolution in security.

Authentication factors used in MFA (Figure 1) include:

- Something you know: passwords, passphrases, personal identification numbers (PINs), passcodes.
- Something you have: USB token, mobile phone, email access.
- Something you are: face authentication, fingerprint, other types of biometrics.
- Something you do: behavioral biometrics such as typing speed, device orientation, touch pressure.

The most frequently used MFA technique is one-time passcode or OTP. With OTP the user is sent a unique code needed to complete authentication. The unique code is sent via email or SMS text messaging, neither of which are secure channels, making the whole second factor vulnerable.

The second most common method of second-factor authentication, time-based one-time password (TOTP), has its own challenges, since the generated code or originating secret used to set up a TOTP can be compromised.

In short, as technology has advanced and cybercriminals have become savvier, MFA has begun to experience weaknesses.

[1] "Password Manager Industry Report and Market Outlook (2023-2024)," Security.org, September 13, 2023, https://www.security.org/digital-safety/password-manager-annual-report/.

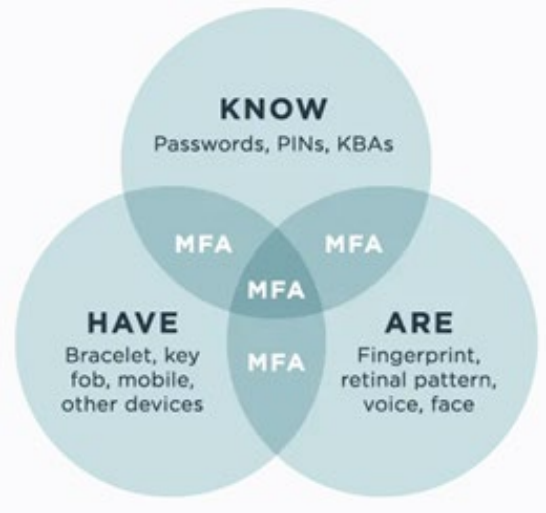

Figure 1. Multi-Factor Authentication[2]

Beyond technology challenges to authentication is a practice known as "phishing."

Phishing is an attempt by criminals to trick users into sharing information or taking an action that gives the fraudster access to accounts, computers, or even networks. It is no coincidence the name of these types of attacks sounds like "fishing." The attack will lure the user in, using some kind of bait to fool them into making a mistake. Phishing attacks may strike using email, text messages, or websites to trick users by posing as a trusted person or organization. A user might get a text or email from someone they know or an organization they trust, requesting them to click a link or download a file. Usually there is a sense of urgency or a problem that needs to be resolved.

And phishing works. In fact, according to the FBI's Internet Crime Complaint Center, "phishing schemes (which involve malicious attempts to gain data by threat actors) were the number one crime type"[3] last year, far outpacing other types of fraud (Figure 2). Some security firms have reported an increase of over 500% in malicious phishing emails over the past year alone. Phishing has become such a security threat that U.S. Federal agencies are required to implement phishing-resistant multi-factor authentication by 2024 under the direction of the White House/Office of Management and Budget (OMB), which released its Federal Zero Trust Strategy in January 2022.[4] As noted in this document, "Users can be fooled into providing a one-time code or responding to a security prompt that grants the attacker account access. These attacks can be fully automated and operate cheaply at significant scale."

Phishing-resistant multi-factor authentication eliminates the use of shared secrets at any point and is based on public/private key cryptography. While the "something you know," such as a password, PIN, or security question, does produce the majority of attacks, the vulnerabilities of "something you have," such as SMS or OTP are very susceptible to man-in-the-middle attacks.

---

2 "The One-time Password (OTP) Ultimate Guide," Ping Identity, November 10, 2023, https://www.pingidentity.com/en/resources/blog/post/one-time-password-ultimate-guide.html.

3 "Federal Bureau of Investigation Internet Crime Report 2022," https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

4 Office of Management and Budget, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," OMB-22-09, January 26, 2022, https://zerotrust.cyber.gov/federal-zero-trust-strategy/.

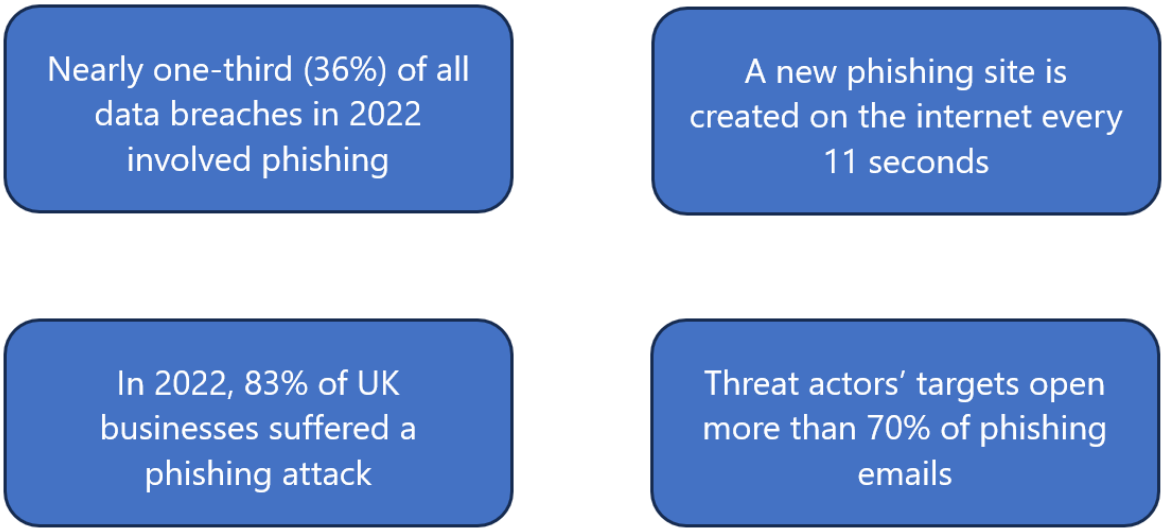

Figure 2. Trends in Phishing[5]

[5] "Phishing Statistics & How to Avoid Taking the Bait," DataProt, July 14, 2023, https://dataprot.net/statisics/phishing-statistics/.

2. Phishing-based MFA Bypass Schemes

While MFA can thwart phishing attacks, fraudsters use schemes to bypass MFA and gain access to user information or accounts. Common MFA bypass methods include:

- Standard social engineering.
- OTP relay schemes.
- Bots, phishing kits, and gummy browsers.
- MFA push spam/MFA fatigue.
- Generative AI-based approaches.

While these attacks may be seen in many industries, the discussion in this section focuses on use cases relevant to the payments industry.

2.1 Standard Social Engineering to Obtain OTP

Social engineering attacks are those where threat actors contact cardholders and attempt to trick them into providing sensitive information. Two methods are commonly used in this type of attack. The first is where the threat actor calls the cardholder, or sends an SMS text, claiming to be the cardholder's financial institution and alleging that the cardholder's account was involved in fraud. The cybercriminal convinces the cardholder to provide sensitive information (e.g., OTP, login credentials) that enable the cybercriminal's high-risk transaction to be completed.

The second commonly used social engineering attack method is where a threat actor contacts the cardholder through phone calls and pretends to be an employee at the cardholder's issuing bank. During these calls, the threat actor requests sensitive personally identifiable information (PII) that is then used to provision the primary account numbers (PANs) to threat-actor-controlled mobile devices or to access the cardholder's bank accounts. The threat actor also requests the OTP that was sent to the legitimate cardholder, which enables the threat actor to successfully complete authentication and access the victim's account.

2.2 OTP Relay Schemes

Threat actors create phishing websites, often using SMS phishing text messages, malicious advertising, or other search engine optimization tactics on retail or service websites, to entice victims to visit the site. These spoofed or phishing websites often mimic legitimate retail, services, government, or banking websites. When the victim clicks the link, they are directed to a spoofed website imitating the legitimate site. When the victim attempts to make a purchase or enters their sensitive PII or account login details on the spoofed websites, the threat actor steals the victim's payment account details and/or login credentials and uses that information on another, legitimate website, which often requests an OTP to authenticate during the purchase. To bypass the authentication, the threat actors create OTP templates that are sent to the victims during the purchase/login on the phishing website; these templates appear to be associated with the purchase/login the victim is intentionally making. The victim enters the OTP into the phishing template and the threat actor then uses the OTP to complete their fraudulent purchase.

2.3 Bots, Phishing Kits, and Gummy Browsers

Cybercrime underground marketplace sales offer the use of bot services for intercepting OTPs. The bots impersonate financial institutions to contact victims and use social engineering techniques to obtain verification codes, PINs, or card verification values (CVVs) from the victims. Different bots offer various services, such as: the ability to spoof specific banks, digital wallet application companies, or cryptocurrency exchange merchants; the choice of various languages to use in calling victims; or the ability to target specific accounts on social media platforms.

Custom phishing kits that facilitate bypassing MFA are also available in cybercrime underground marketplaces. These phishing kits employ the use of reverse proxies in which the threat actors can create a situation whereby the cybercriminal acts as a man-in-the-middle (MiTM) between the legitimate consumer and the legitimate website. In these schemes, and with the use of phishing kits, the threat actors present the legitimate website to the consumer and operate as an invisible intermediary. Consumers are less suspicious since the legitimate website is presented, rather than a spoofed phishing website, as is often the case in phishing schemes. The threat actor is then able to harvest any information that is entered into the website by the consumer, which often includes OTPs as well as username, password, and even session cookies. Session cookies can be further used to thwart MFA as the cookie could represent a session in which the consumer already authenticated.

Threat actors can also use “gummy browsers” to effectively capture a victim’s browser fingerprint (i.e., an online identifier for specific user devices, such as the browser type and version, device operating system, cookies, and device IP address, among other characteristics). These fingerprints are often used by websites to authenticate a user, track user activity for advertising purposes, and confirm the user is an actual person and not a bot. A gummy browser used by a threat actor requires a victim to visit an attacker-controlled website, which enables the capture of the browser fingerprint from the victim. The threat actor can then use this fingerprint to spoof the victim’s identity on websites that were previously visited by the victim. This attack can facilitate bypassing the MFA as the victim may have already authenticated through MFA to a website prior to visiting a gummy browser. The browser fingerprint for the victim could have been captured by malware, and the threat actor can use the victim’s browser fingerprint, once captured, to sign into the associated website without triggering an OTP or other MFA request.

2.4 MFA Push Spam/MFA Fatigue Schemes

MFA push spam or MFA fatigue is a relatively new OTP bypass scheme wherein a threat actor uses a script that attempts to login numerous times to a victim’s account or email using stolen login credentials. If the victim’s account is set up with MFA, the victim receives a push notification on their mobile device for each login attempt by the script. The threat actor runs the script continuously to overwhelm the victim with a torrent of MFA login push notifications with the goal of wearing the victim down to a point where the victim erroneously approves the false login attempt. If the victim does not ultimately authenticate the MFA prompt, the threat actor contacts the victim pretending to be IT support and tries to convince the victim to accept the MFA push notification, which ultimately allows the threat actor to access the victim’s account.

2.5 Impacts of Generative AI on Fraud

Generative AI is significantly altering the payment fraud landscape. Its impact is twofold, both as a tool for perpetrators and a defense mechanism for businesses. On one hand, malicious actors are harnessing the power of AI to:

- Generate convincing fake emails and websites.
- Automate spear-phishing campaigns (phishing that targets a specific individual).
- Evade detection.
- Personalize attacks at scale.
- Refine techniques to improve success rates.

On the other hand, AI can be used to defend against phishing, for example, by detecting AI-generated content. The two-sided impacts of generative AI are in their early stages.

3. Essential Strategies: Immediate Mitigation Tactics

Many authentication solutions support an MFA strategy, but these solutions vary greatly in terms of cost, complexity, usability, and security. Although there are standards[6] that define the architecture and usage of a proper authentication solution within an overarching strategy, the standards are not universal. Organizations with documented requirements often focus more on implementation and continued adherence. However, many other organizations operate without such directives and must rely on guidance from various sources and authorities, including their peers in industry.

Within payments, an MFA design can look very different for two similarly structured companies. And while selecting a proper long-term strategy can be quite difficult, it should not preclude businesses from starting with lower complexity solutions that can quickly deliver value with reduced expenditure, especially if the business is just starting on the authentication journey. SMS one-time passcodes are objectively less secure than other authentication methods; yet this method does provide a marked improvement over the traditional standalone password. Push notification-based authentication, when coupled with additional authentication event data elements, can provide a lower friction authentication event that leverages existing mobile app or browser services, all while enhancing confidence in the authentication and subsequent transaction.

The methods highlighted in this document have varying levels of effectiveness, especially when use cases are considered. These differences should certainly be considered but should not prevent a company from defining or improving their user authentication experience. Authentication challenges and solutions are continually being refined and all of these solutions provide value in some manner. It is ultimately up to the business leadership and their authentication teams to decide which is right for them now and then determine what is right for their future.

Examples of countermeasures include the following:

1. Banks and retailers should monitor customers' online activity and develop stronger authentication processes. Customers who have not registered or activated online storefront tools tend to be the most vulnerable to MFA bypass schemes, as cybercriminals are able to pose as businesses or impersonate customers using online/digital tools. Customers in some segments prefer non-digital channels (e.g., branch/retail locations and paper statements). Allowing these customers to disable digital channels at account origination if they prefer not to use them may decrease vulnerability to attacks. When customers call in about being blocked on high-risk items, organizations should have high-risk authentication procedures to ensure the call is not from a fraudster before approving these types of exceptions. Fraudsters are often adept at subverting controls, but by following industry best practices for strong authentication procedures, these types of issues can be mitigated.

   Organizations could consider having a velocity limit and service level for how long a push notification or SMS will take to reach a customer (typically, 5-10 seconds). Speed and velocity controls built into the risk solution design can add to success in defeating these types of problems.

[6] See the NIST publication, "Digital Identity Guidelines," SP 800-63, for more details: https://pages.nist.gov/800-63-3/sp800-63b.html.

2. Ensure the organization is compliant with the Payment Card Industry Data Security Standard (PCI DSS) for data transfers. For issuers, processors, acquirers, and merchants, security can be improved by ensuring that all confidential data is securely encrypted when it moves between approved organizations and that information security officers are aware of any data transfers into or out of the organization.

   The PCI Security Standards Council has extensive information on PCI DSS compliance.[7]

3. Communicate with customers to make them aware of best practices, security, and safety with their shopping habits.

   Issuers and merchants can employ various communication methods to warn customers about the risks of social engineering fraud, particularly phishing attempts. Methods can include email alerts, text messages, website notifications, mobile app alerts, and even phone calls to reach out to customers.

   These communications typically include guidance on recognizing and avoiding phishing scams and may provide contact information for reporting such incidents. Organizations also use social media platforms to share warnings and tips, while traditional mail can include printed materials. Additionally, educational content (e.g., videos, workshops, webinars, FAQs, and online resources) can be offered to inform customers about the dangers of phishing and methods to protect themselves.

   These efforts aim to maintain customer vigilance and promote a proactive approach to safeguarding personal and financial information against social engineering fraud.

4. Use machine learning/pattern recognition to identify the healthy habits of regular customers and to identify the behaviors of suspicious actors more effectively. Machine-learning approaches drive stronger outcomes as long as models are properly tuned and leveraged in both payment and authentication solutions.

[7] See "PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard," Version 3.2.1, July 2018, https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

4. The Goal: Phishing-Resistant Multi-Factor Authentication

Creating a phishing-resistant MFA solution can be challenging, but at its heart is one very important component. The true key or secret used for authentication must not be accessible to the authorized end user. The use of passwords or OTPs as part of MFA is inconsistent, as the secret (i.e. the password or OTP) is known to the end user and therefore can be phished by a cybercriminal. Push notifications are an important improvement; by removing knowledge of the actual secret, no information is available to share with a cybercriminal. Unfortunately, push notifications still have phishable attack vectors. A cybercriminal can enroll additional devices using phishable OTPs, clone elements of a device remotely, or convince a user to press "Yes." Worse yet, the user may simply be push-notification complacent and acknowledge the notification without even reading it.

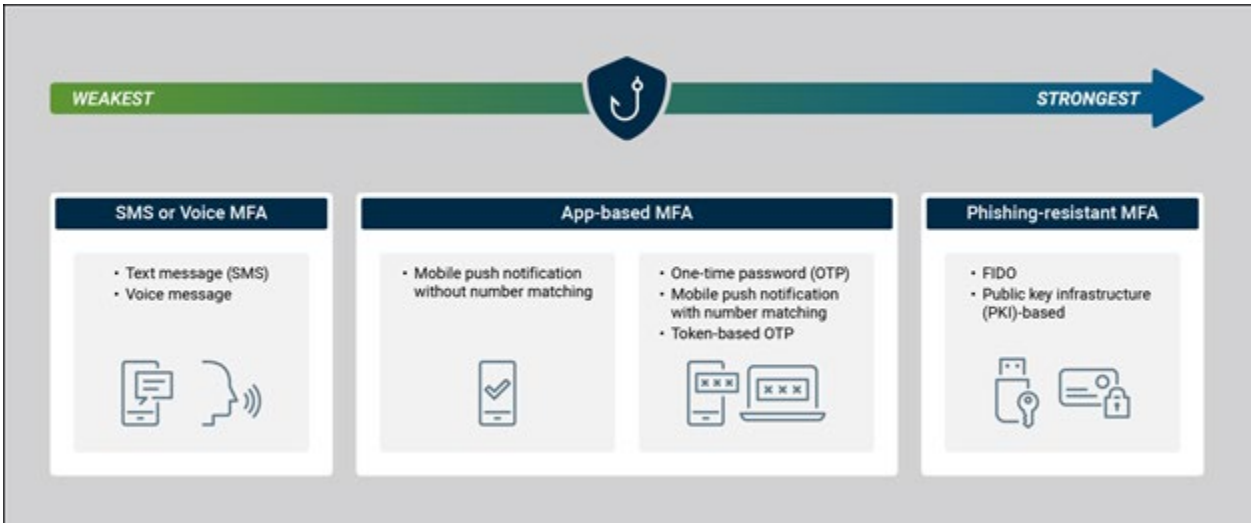

Figure 3. Effectiveness of MFA Methods for Combatting Phishing[8]

To promote both security and broad adoption, an ideal phishing-resistant MFA solution would create an interaction that is both low friction for the consumer and yet highly secure. Such solutions currently include those based on (a) the FIDO2 standard, (b) public key infrastructure (PKI)-based authentication, and/or (c) advanced behavioral analytics.

a. FIDO2

The FIDO2 standard, created by the (Fast Identity Online) FIDO Alliance, are open and license-free and cover secure passwordless authentication over the internet for both consumer and enterprise use cases. The secret or key is stored and accessed locally on the consumer device and is not available, phishable, or enrollable to a remote cybercriminal. The critical component, the secret information, does not leave the device[9] and is only usable by the consumer, not directly accessible to them. Combining this with the seamless user experience of a biometric or PIN creates both a low friction and highly secure phishing-resistant solution.

[8] "More than a Password: Protecting Yourself from Malicious Hackers with Multifactor Authentication," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/MFA.

[9] Cloud-sharable passkeys are being considered by many service providers. This would allow all of, or a portion of, the secrets required for account access to be shared to eligible devices authorized by the user.

Elimination of the password/shared secret is an important component of phishing-resistant authentication. FIDO2/WebAuthn authentication and public key infrastructure (PKI)-based authentication are the most common methods of authentication which do not use passwords.

Two specifications make up FIDO2:

- The Web Authentication (WebAuthn) specification produced by the World Wide Web Consortium (W3C).[10]
- The Client-to-Authenticator Protocol (CTAP) developed by the FIDO Alliance.[11]

Together, these specifications allow for the creation of passkeys that work on device-bound and roaming authenticators. Passkeys are widely adopted by the major browsers as a password replacement solution. Usage is expected to continue to grow as passkeys are the authentication industry best practice according to CISA[12].

FIDO2 uses standard public key cryptography which matches a private key stored on a user's device with a public key stored on a service provider application/website. The public key is created when the user registers their device with the service provider application/website. FIDO2 eliminates the need for a password and replaces it with the FIDO2 login standard. WebAuthn is the browser-based application programming interface (API) that enables browser users to sign in with a cryptographic key pair that is stronger than a password.[13]

b. Public Key Infrastructure (PKI)-Based Authentication.

Some enterprises also choose to use PKI for employee authentication where each company-issued device or hardware token is set up with a unique client certificate. PKI authentication leverages a second factor, which is a time-based token, push notification, or OTP to verify the identity.[14] Users that authenticate with the device or hardware token can log in without a password. Depending on the value of the assets being protected, maintenance of client certificates and management of the certificate authority can be operationally expensive.

[10] "Web Authentication: An API for accessing Public Key Credentials Level 2," World Wide Web Consortium, April 8, 2021, https://www.w3.org/TR/webauthn-2/.

[11] "Client to Authenticator Protocol (CTAP)," Proposed Standard, FIDO Alliance, June 21, 2022, https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621.html.

[12] "Next Level MFA: FIDO Authentication," CISA, October 2022, https://www.cisa.gov/news-events/news/next-level-mfa-fido-authentication.

[13] "FIDO2: Web Authentication (WebAuthn)", FIDO Alliance, https://fidoalliance.org/fido2-2/fido2-web-authentication-webauthn/.

[14] "Implementing Phishing-Resistant MFA," CISA, October 2022, https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

c. Advanced Behavioral Analytics.

Another developing area is the use of advanced behavioral analytics deployed across the customer journey to provide an additional layer of passive authentication that is resistant to spoofing. The technology looks at network data, device, location, and behavioral intelligence, as well as behavioral biometric signals, to build up digital signatures of a user. The digital signatures are used to compare current transactions with past behaviors and can be layered with other more traditional types of authentication to augment risk assessments. The advantage of these passive authentication approaches is that they are virtually frictionless to trusted users, while offering real-time remediation steps for high-risk or fraudulent transactions. The approaches are also highly resistant to spoofing because the digital signatures are made up of hundreds of different pieces of intelligence relating to how a user typically transacts and interacts.[15]

Additional standards and specifications are continually being developed to promote global interoperability and are at the forefront of emerging technologies that relate to the next generation of multi-factor authentication and identity in general. See the Appendix for a list of various existing and emerging standards helping to shape the future of authentication.

[15] Explanation courtesy of Darwinium, a provider of the described approach to digital security and fraud prevention.

5. Conclusion

While multi-factor authentication is the gold standard for authenticating an individual, it too has vulnerabilities, namely phishing attacks.

Phishing attacks manifest in different ways, but in the end, they all work by exploiting human behavior to compromise the “something you know” authentication factor. The success of phishing is evidence of how difficult it is to change behavior.

Mitigation tools do exist, ranging from easy-to-implement, basic security hygiene, to newer tools, such as FIDO2-based solutions, PKI- based authentication, and the use of advanced behavioral analytics, which can eliminate the need for passwords and, thereby, a chief vulnerability of current authentication methods. Such tools require more effort to implement but can provide much more robust protection than passwords or OTPs against the never-ending efforts of cybercriminals.

6. Sources

Federal Bureau of Investigation, “Federal Bureau of Investigation Internet Crime Report 2021,” https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

Federal Bureau of Investigation, “Federal Bureau of Investigation Internet Crime Report 2022,” https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

Office of Management and Budget, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,” OMB-22-09, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

7. Appendix: Emerging and Established Standards

FIDO (Fast Identity Online) Alliance. Created in 2013 to solve the world's reliance on (and facilitate the elimination of) passwords, FIDO has gained mass adoption by all major browsers, including macOS®/ Safari®, Windows®/Edge®, Chrome OS™/Android™ and Firefox™. The FIDO specification relies on public/private key cryptography to create an authenticator that can be used for login, eliminating the need for knowledge-based authentication. The credentials can be bound to a platform or security key or synchronized across devices. Additional information can be found at https://fidoalliance.org/.

OpenID Foundation (OIDF). Created in 2007 to help people assert their identity wherever they choose, OIDF's mission is to lead the global community in creating identity standards that are secure, interoperable and privacy preserving. The OpenID Connect Specification, the Financial-grade API (FAPI) Specification, and the Client Initiated Backchannel Authentication (CIBA) Specification, all examples of technical standards produced by OIDF, are used by over three billion people worldwide across millions of applications. OIDF has produced over 45 web standards with wide adoption in various ways, such as "Sign in with Google." Additional information can be found at https://openid.net/.

ISO/IEC 18013-5 (Mobile Driver's License [mDL] and Mobile ID [mID]). Completed in 2021, this ISO specification created the foundation for a mobile driver's license and mobile ID for universal use and acceptance. It specifies interoperable technical mechanisms to obtain and trust the data from an mDL/mID for in-person transactions. Data transfer is only initiated by the mDL holder after giving affirmative consent and pivotal privacy technologies are designed into the standard. Using the standard can reduce verifier liability concerns associated with storing personal data and expand use cases beyond the physical ID card. Additional information can be found at https://www.iso.org/standard/69084.html.

World Wide Web Consortium (W3C) Verifiable Credentials Data Model. Published in 2022, verifiable credentials can represent information found in physical credentials, like a badge or a license, or things that have no physical equivalent, such as ownership of a bank account. They have numerous advantages over physical credentials, most notably, they are digitally signed, which makes them tamper-resistant and instantaneously verifiable. Verifiable credentials can be proof of something you are, know, have, or own. They can also represent an event, such as a vaccination. More information can be found at https://www.w3.org/2022/06/verifiable-credentials-wg-charter.html.

National Institute of Standards and Technology (NIST) SP 800-63, **Digital Identity Guidelines**. NIST, under the umbrella of the U.S. Department of Commerce, exists to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve the quality of life. As part of that mission, NIST developed a set of digital identity guidelines (Special Publication 800-63) to provide an overview of general identity frameworks, using authenticators, credentials, and assertions together in a digital system, and a risk-based process of selecting assurance levels. To respond to the changing digital landscape that has emerged since publication of the last revision of SP 800-63 (2017), an updated version is underway. This version enhances fraud prevention measures by updating risk and threat models to account for new attacks, providing new options for phishing-resistant authentication, and introducing requirements to prevent automated attacks against enrollment processes. It also opens the door to new technology, such as mobile driver's licenses and verifiable credentials. Additional information on the updated specification can be found at https://csrc.nist.gov/pubs/sp/800/63/4/ipd#NoteToReviewers.

Open Wallet Foundation. The Open Wallet Foundation was launched May 22, 2023, as an open-source code project under the Linux Foundation to drive collaboration and development of digital asset (e.g., money, credentials for identity, academic achievements, driver's licenses) custody and interoperability in the open-source community. Additional information can be found at https://openwallet.foundation/.

Regulatory Mitigation Recommendations/Resources

Cybersecurity and Infrastructure Security Agency (CISA). CISA leads the U.S. national effort to understand, manage, and reduce risk to our cyber and physical infrastructure by connecting stakeholders in industries and the government to offer resources, analyses, and tools to help them build their own cyber, communications and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people. In October 2022, CISA released two fact sheets to highlight threats against accounts and systems using certain forms of multi-factor authentication. CISA strongly urged all organizations to implement phishing-resistant MFA to protect against phishing and other known cyber threats. The guidance can be found at https://www.cisa.gov/news-events/alerts/2022/10/31/cisa-releases-guidance-phishing-resistant-and-numbers-matching.

Cyber Safety Review Board (CSRB). In 2022, the U.S. Department of Homeland Security set up the CSRB, which is tasked with investigating major cyber incidents and making recommendations on how to prevent them from being repeated. Their top recommendation calls for the U.S. government to develop a new "secure authentication roadmap" for the United States.

> *"The Board recommends that organizations urgently implement improved access controls and authentication methods and transition away from voice and SMS-based MFA; those methods are particularly vulnerable. Instead, organizations should adopt easy-to-use, secure-by-default, passwordless solutions such as Fast IDentity Online (FIDO)2-compliant, phishing-resistant MFA methods. Device and software manufacturers will need to innovate and deliver effective solutions that the global digital ecosystem can quickly adopt. To facilitate the transition to passwordless authentication, the Board recommends that the federal government develop and promote a secure authentication roadmap for the nation. The roadmap should include standards, frameworks, guidance, tools, and technology that can enable organizations to assess, progress, and implement leading practices for passwordless authentication."*

The report goes on to say:

> *"Web and mobile application developers should leverage Fast IDentity Online (FIDO)2-compliant, hardware backed solutions built into consumer devices by default. Use of these built-in tokens should have easy integration with applications and web-based services, leveraging standards such as WebAuthn and technologies such as Passkeys."*

The full report is located at https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf.

8. Acknowledgements

This white paper was developed by the U.S. Payments Forum to highlight the importance for all payments industry stakeholders to understand evolving authentication methods and implement emerging standards for improved security. Publication of this document by the U.S. Payments Forum does not imply the endorsement of any of the member organizations of the Forum.

The U.S. Payments Forum thanks **Marie Jordan** of Visa for leading this project, **David True** of PayGility Advisors**, Sue Koomen** of American Express**, Nathan Markiecki** of Discover Financial Services, and **Shailesh Agarkar** of Clover, for drafting the white paper, and Working Committee members for their contributions. Participants involved in the project team developing and reviewing this white paper included:

Participants	
Shailesh Agarkar, Clover	**Greg Aurre, FIS**
Gladys Calfas, Discover Financial Services	**David True, PayGility Advisors**
Nathan Markiecki, Discover Financial Services	**Tim Mansfield, Truist**
Andrew Patania, Elavon	**Marie Jordan, Visa**

9. Legal Notice

This document is provided solely as a convenience to its readers, as a high-level overview of multifactor authentication (MFA), phishing, and ways to improve the security of MFA against phishing attacks. While great effort has been made to ensure that the information provided in this document is accurate and current, this document does not constitute legal or technical advice and should not be relied upon for any legal or technical purpose; accordingly, all warranties of any kind, whether express or implied, relating to this document, the information herein, or the use thereof are expressly disclaimed, including but not limited to warranties as to the accuracy, completeness or adequacy of such information, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement. Any person that uses or otherwise relies on the information set forth herein does so at his or her sole risk. This document provides only a high-level description of the subject matter, and is not exhaustive; for example, there may be other methods of improving the security of MFA against phishing attacks than the examples discussed herein. Accordingly, readers interested in improving the efficacy of MFA against phishing attacks are strongly encouraged to consult with their respective security provider, subject matter experts and professional and legal advisors, as well as relevant payments industry stakeholders, such as payment networks, issuers, acquirers, and others, prior to any implementation decisions.