yubico

WHITE PAPER

A Secure Passwordless Future for Financial Services

Defeat AI threats with proactive, passwordless security using device-bound passkeys

Table of contents

$6.08 million

cost of data breach[1]

68%

of data breaches tied to the **human element** social attacks, errors, misuse, credential theft[2]

65%

of financial services hit by **ransomware**[3]

$2 million

cost of ransom payout[4]

AI Driving a Critical Need for Proactive Security

Cybersecurity has never been more critical in protecting the integrity of financial institutions and the trust of their customers. With the largest store of financial and personal data, financial services organizations are one of the highest value targets for malicious actors—from cybercriminals and hacktivists to nation-state adversaries, and have the second highest costs per data breach ($6.08 million USD on average). The impact of such breaches goes beyond the immediate financial loss, affecting everything from the institution's reputation to customer trust, regulatory compliance, and operational stability.

As technology evolves, so do the tactics, tools, and strategies used by cyber attackers, resulting in an even more complex and sophisticated cyber threat landscape. One of the latest and most concerning developments is the use of weaponized artificial intelligence (AI) to carry out cyberattacks. AI-powered cyberattacks can take various forms, such as phishing emails, malware, ransomware, or even social engineering techniques. What makes them dangerous is their ability to adapt and evolve based on the data they collect and learn from their targets. AI-powered tools like ChatGPT have given threat actors the ability to quickly craft convincing and targeted phishing emails that used to require considerable sophistication and resources.

In response to risk, financial services organizations today are subject to various standards and regulations that reinforce the need to securely authenticate employees, third parties, and customers to protect information systems, accounts and data and to support secure system-to-system communications. While many regulators and cyber insurers now require the use of multi-factor authentication (MFA), more often than not, the guidance often stops there — there usually is no mention of the merits and drawbacks of different forms of MFA, because not all forms of MFA are created equal.

- U.S. White House Executive Order 14028
- PCI DSS v4.0
- GLBA
- FFIEC
- PSD2
- eIDAS
- SOX & SOC2
- GDPR

The revised Payment Card Industry Data Security Standard (PCI DSS v4.0) became the first (and likely not last) financial standard to require phishing-resistant MFA for all access to the cardholder data environment which is relevant for financial services institutions.[5] For financial services institutions that work with government agencies, this requirement aligns with U.S. Executive Order 14028 and OMB Memo M-22-09, which mandates the use of phishing-resistant MFA as part of deploying a Zero Trust Architecture.[6] In March 2023, CISA and the NSA jointly released a new Identity and Access Management Best Practice Guide for Administrators in critical infrastructure sectors, including financial services, that recommends phishing-resistant MFA for many authentication scenarios.[7]

Additionally, in October 2024, the New York State Department of Financial Services issued guidance advising financial firms to assess and address cybersecurity risks arising from the use of AI.[8] The guidance, which imposes no new rules or regulations, highlights four AI-related risks that financial sector workers need to be aware of, including social engineering, cyberattacks, theft of nonpublic information, and increased vulnerabilities due to supply chain dependencies.

The Building Blocks for a Secure Passwordless Future

Most attackers don't break in—they log in using user credentials and codes such as SMS and OTP that are easily intercepted and stolen. Companies pour billions into sophisticated network security and breach detection, but are still relying on legacy passwords and mobile-based authenticator apps such as SMS, OTP and push notification apps which are easily bypassed by regular phishing scams and even more so by modern AI-powered hackers, creating a false sense of security.

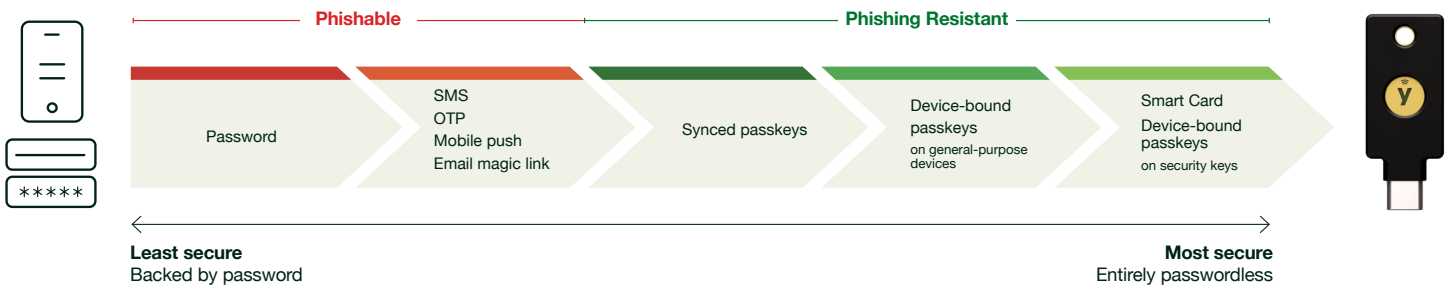
Pitfalls of Legacy Methods

- Compliance Gaps
- Partial Protection
- Burdened Users

It is critical that financial services organizations rethink their cybersecurity readiness postures because the world has changed. It is time to move past reactive security to proactive and phishing-resistant passwordless authentication, eliminating usernames and passwords altogether as well as removing reliance on mobile-based authenticator apps that are not phishing resistant. Device-bound passkeys such as the YubiKey offer the highly regulated financial services industry the most secure and simple way to adopt phishing-resistant authentication to secure user access to critical systems and data, and ensure cyber resiliency and business continuity across the enterprise.

What is phishing-resistant authentication?

Phishing-resistant authentication processes rely on cryptographic verification between devices or between the device and a domain, making them immune to attempts to compromise or subvert the authentication process. According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, only two forms of authentication meet the phishing-resistant mark: PIV/Smart Card and the modern FIDO2/WebAuthn authentication standard.



What are Passkeys?

Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are different passkey implementations:

Synced passkeys live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.

Device-bound passkeys offer enterprises greater control of their FIDO credentials compared to synced passkeys. However, there are different types of device-bound passkeys—those that reside in general purpose devices such as smartphones, laptops and tablets, and those that reside in hardware security keys purpose built for strong security. Device-bound passkeys in modern FIDO security keys offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach enterprises can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent compliance regulations.

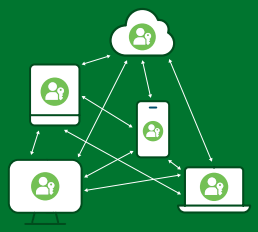
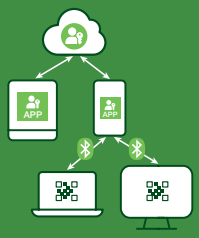
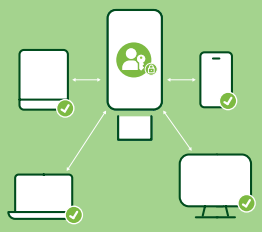
Which Passkey Approach is Right for You?

FIDO standards and passkeys have been embraced by all leading Identity and access management (IAM) platforms, identity provider (IDP) solutions and privileged access management (PAM) solutions to make it possible to support FIDO2 passwordless experiences at scale for business critical applications and services.

Syncable passkeys are great solutions for many low-risk consumers and low-risk applications as they are considered lower assurance, but are not suitable for high risk individuals or the enterprise, increasing the difficulty to:

- Audit and prove how passkeys are being synced or shared and to know which copy is being used
- Manage the lifecycle of the passkey after it has been created, since cloned passkeys that are shared are indistinguishable from the original.
- Support users that can't sign-in with their passkey or when they need help with recovery.
- Cover all use cases, since syncable passkeys rely on mobile connectivity, making them unsuitable for mobile-restricted environments, air-gapped or isolated networks, shared workstations. Furthermore, not all computers and phones support passkeys.

Device-bound passkeys do not sync or get copied to other devices. In a synced passkey scenario where passkeys can move between multiple devices, the factor that is used to unlock the authenticator could be from a different user as all factors don't travel with the passkey. With a device-bound passkey, there is a higher assurance that the user who is controlling the device is the one who is supposed to be using the passkey, eliminating the risk that the factor used to unlock the authenticator could be from a different user. A device-bound passkey offers higher assurance because the passkey lives on FIDO2 security keys or are created on a platform and persisted into a trusted platform module (TPM), which is how Windows Hello works. Device-bound passkeys provide the best enterprise-level controls that organizations need to properly manage and secure the lifecycle of a passkey, leveraging public key cryptography for high security, where the private keys never leave the authenticator.

If you need	Synced passkeys	Device-bound passkeys on general-purpose devices	Device-bound passkeys on hardware security keys
			
Synced/shareable between devices	Unmanaged syncing	Managed syncing	No syncing between devices
Works across Apple/ Google/Microsoft	May not work	Works across all platforms	Works across all platforms
User registration/onboarding	Weak; backed by password	Weak; app backed by password	Most secure when used with Yubico FIDO Pre-reg, as then user registration not reliant on password
Credential recovery	Easy to recover	Time to replace phone and costly	Fastest with a backup key
Compliance and audit	Authenticator Assurance Level 2 (AAL2) No attestation; unsure if user controls passkey	Authenticator Assurance Level 2 (AAL2) Supports software attestation	Authenticator Assurance Level 3 (AAL3) Supports hardware attestation
Risk/Costs	Perceived as “free”; high IT/ helpdesk costs and higher risk exposure is costly	Perceived as cheaper than HW; but risk exposure gaps can be costly in long run	Perceived as higher cost upfront; but less costly due to lowered breach risk and reduced IT burden
Works across enterprise scenarios	Not in mobile-restricted, shared workstations	Not in mobile-restricted, shared workstations	Works across all enterprise scenarios

More Value
Reduced support tickets by 75%

High Return
Experience ROI of 203%

Strongest Security
Reduce risk by 99.9%

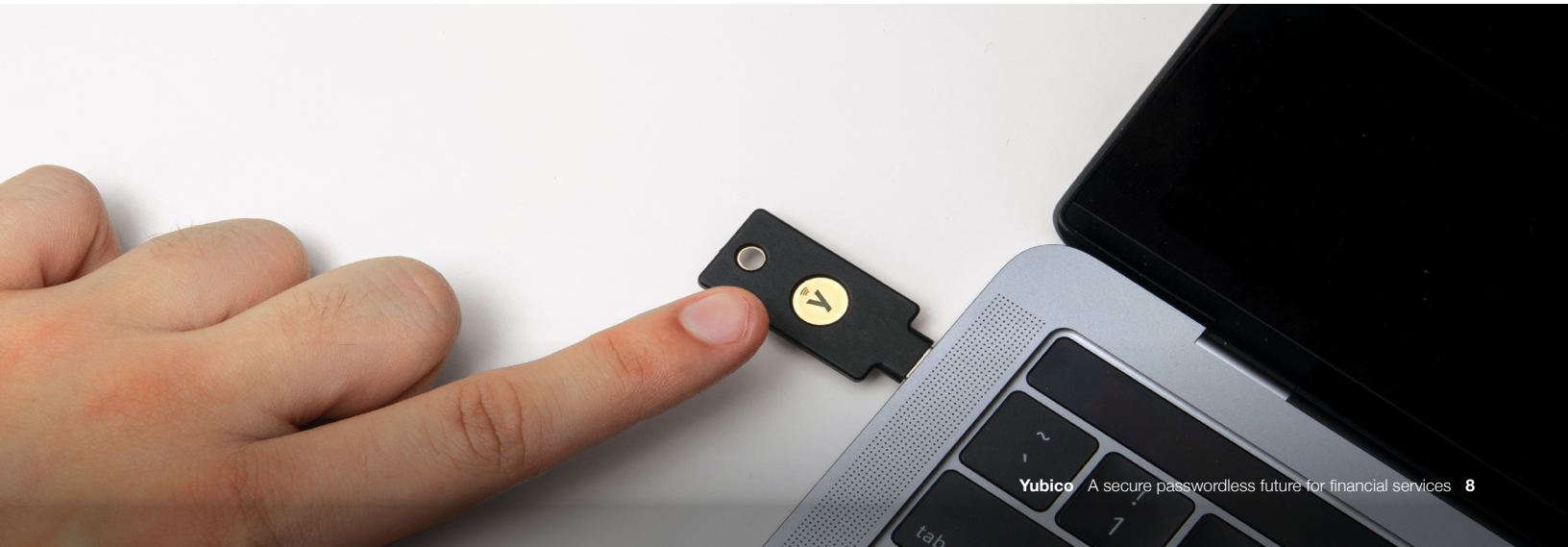
Faster
Decrease time to authenticate by >4x

Proactive Passwordless Security With the YubiKey

Start your proactive security journey with the YubiKey—a critical combination of highest-assurance security along with an optimized user experience, enabling phishing-resistant MFA and passwordless authentication at scale. The YubiKey is a device-bound passkey in a multi-protocol hardware security key form factor, supporting both Smart Card and FIDO2/WebAuthn standards along with FIDO U2F, OTP and OpenPGP, integrating seamlessly across legacy and modern environments to help financial organizations bridge to a secure passwordless future.

YubiKeys work with over 1,000 products, services and applications including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services. The YubiKey is proven to reduce risk by 99.9% and deliver significant business value to large enterprises at scale, delivering an ROI of 203%, all while delivering a frictionless user experience, letting users quickly and securely log in with a single tap or touch[9].

- Proactive prevention
- Passwordless security
- Purpose built
- Compliance built-in
- Protection for all
- User-friendly security



Financial Services Use Cases Supported by the YubiKey

Four out of the ten top ten U.S. banks have already deployed the YubiKey to solve for a growing list of use cases, starting with high risk user groups and scenarios, then extending outward to provide value with more streamlined authentication, reduced support costs, and to meet growing consumer demands for secure online and mobile banking experiences.

How the YubiKey addresses risk and delivers business value across the top financial services use cases:

Top scenarios for phishing-resistant MFA

Privileged access
The YubiKey design enables the authentication secret to be stored on a separate secure chip built into the YubiKey, so it cannot be copied, stolen or intercepted remotely.

Shared workstation
Enable secure and efficient access to shared computers in banks and call centers, including mobile-restricted areas.

Remote work
Add an extra layer of protection, providing secure access to VPN, IAP, IAM, & IdP platforms.

High-risk transactions
Provide step-up authentication to re-verify users for high risk service or high value transactions.

Software supply chain
Protect code access and implement trusted code-signing.

User groups

Office workers
Drive employee experience and productivity with a single key that works across devices, legacy and modern systems and data.

Call center
Verify call center agent identity to provide access to key systems, shared workstations or for remote workers.

Retail finance
Support seamless authentication between workstations to service customers or authorize transactions.

Third party
Protect third-party access to systems and data.

End Customers
Protect customer accounts from fraud & build loyalty and trust with deployments to key customer segments based on risk and value.

Call center protects its financial service clients with phishing-resistant MFA

Financial service organization Afni has been providing comprehensive inbound and outbound channel services to financial service organizations around the world, including services in collections and insurance subrogation. Despite having MFA for nearly all of its 10,000 employees, phishing remained a problem.

To tackle this, Afni's CISO prioritized getting to 100% adoption of MFA and replacing legacy authentication methods with phishing-resistant MFA. The YubiKey is natively supported by Afni's Microsoft environment, making it easy to roll out to office and call center workers — even those working remotely.

Deploying the YubiKey has helped reduce risk in the face of sophisticated attack, a protection that has been recognized by a 30% reduction in the organization's cyber insurance premiums.

> "With every user having a YubiKey, I don't have to worry about leakage of credentials. That's a very, very good place to be as a CISO."
>
> **Brent Deterding**
> CISO, Afni

YubiKey adds security layer for access control at TrueCode Capital

Hedge fund investment firm TrueCode Capital relies on YubiKey for phishing-resistant MFA authentication to verify employee identities for SSO access to its enterprise cloud services, reducing both startup and operating costs to the tune of hundreds of thousands of dollars. With the aim to help individuals protect their investments, every new investor is also sent a YubiKey as part of their welcome package.

> "People have lost more money out of bad passwords than they have from market draw-downs."
>
> **Joshua M. Peck**
> Chief Investment Officer, TrueCode Capital

Simple six step deployment at scale

Learn the six deployment best practices that can help your organization accelerate adoption of modern, phishing-resistant multi-factor and passwordless authentication at scale using the YubiKey.

Get the guide

Accelerate Deployment of Passwordless at Scale

There is no question that phishing-resistant MFA is the right solution to secure financial services against modern cyber threats. Though the path to phishing-resistant MFA and passwordless can seem daunting, it doesn't have to be.

To make it easy to deploy passwordless authentication at scale, Yubico offers YubiEnterprise Services consisting of YubiKey as a Service and YubiEnterprise Delivery for easy procurement and delivery of Yubikeys.

With YubiKey as a Service, organizations receive a service-based and affordable model for purchasing YubiKeys in a way that meets their technology and budget requirements. This service also provides priority customer support, ease of form factor selection, backup key discounts, and replacement stock benefits. With YubiEnterprise Delivery, organizations receive a cloud-based service that streamlines the distribution of YubiKeys to end-users, serving both domestic and international locations including residential addresses.

Yubico also offers the Yubico Enrollment Suite, delivering a complete registration experience for easy enrollment of YubiKeys on behalf of users, with support for Microsoft and Okta currently, and additional Identity Provider (IdP) support planned to come on board.

Yubico's Professional Services team can help you with a successful implementation. Yubico offers a wide variety of advisory services in support of your YubiKey implementation and deployment, including best practices workshops, technical implementation packages, on-demand consulting resources and custom engagements. Our Professional Services team is comprised of trained and accredited security professionals with experience gained from hundreds of customer implementations across a wide range of industries and the government sector. From standard implementations to complex enterprise rollouts, Professional Services has the skills and expertise to help guide you through all facets of your YubiKey implementation

We've also created a detailed Best Practice Deployment Guide to walk you through the six deployment best practices to accelerate adoption of MFA and YubiKeys at scale. To remove all the guesswork out of planning, purchasing and delivery, Yubico offers professional services and as a service options and works with many channel partners to make getting started easy.

Summary

Financial organizations face mounting pressure to strengthen authentication in response to evolving AI-driven cyber threats and new regulations. By understanding the complexities of modern cyber risks and implementing proactive security measures, financial institutions can better safeguard their assets, data, and customer trust in an increasingly hostile digital environment.

In a world where not all forms of MFA are created equal, the YubiKey accelerates the adoption and scale of phishing-resistant multi-factor and passwordless authentication so that financial services professionals have the freedom to do their jobs while knowing they're secure.

Further, with intense pressure to seek out solutions to manage risk with consumers, the YubiKey addresses an urgent need to meet consumer demand and create a competitive advantage. The YubiKey can be customized with corporate branding and extended to key customer segments based on risk and value.

Sources

[1] IBM, 20224 Cost of Data Breach Report, https://www.ibm.com/security/data-breach

[2] Verizon, 2024 Data Breach Investigations Report, https://www.verizon.com/business/resources/reports/dbir/

[3] Sophos, The State of ransomware in Financial Services 2024, https://news.sophos.com/en-us/2024/06/24/the-state-of-ransomware-in-financial-services-2024/

[4] Sophos, The State of ransomware in Financial Services 2024, https://news.sophos.com/en-us/2024/06/24/the-state-of-ransomware-in-financial-services-2024/

[5] PCI SSC, PCI DSS v4.0, (March 2022), https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

[6] Shalanda D. Young, Office of Management and Budget, M-22-09, (January 26, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[7] CISA and the NSA, Identity and Access Management: Recommended Best Practices for Administrators, https://www.cisa.gov/news-events/alerts/2023/03/21/cisa-and-nsa-release-enduring-security-framework-guidance-identity-and-access-management

[8] New York Department of Financial Services, Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks, https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies-combat-related-risks

[9] Forrester Study, Total Economic Impact of Yubico YubiKeys, https://www.yubico.com/resource/tei-forrester-report/

yubico

About Yubico

Yubico (Nasdaq Stockholm: YUBICO), the inventor of the YubiKey, offers the gold standard for phishing-resistant multi-factor authentication (MFA), stopping account takeovers in their tracks and making secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

Yubico's solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across hundreds of consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

As part of its mission to make the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. The company is headquartered in Stockholm and Santa Clara, CA. For more information on Yubico, visit us at www.yubico.com.