



BEST PRACTICES GUIDE

# How to get started with phishing-resistant MFA to secure financial services

Six deployment best practices to accelerate adoption at scale



\$5.97 Million



average cost of data breach in financial services<sup>1</sup>

82%



of cyber threats can be traced back to stolen credentials<sup>2</sup>

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, two forms of authentication currently meet the mark for phishing-resistant MFA: PIV/Smart Card and the modern FIDO2/WebAuthn authentication standard.

## Choosing the right MFA approach for financial services

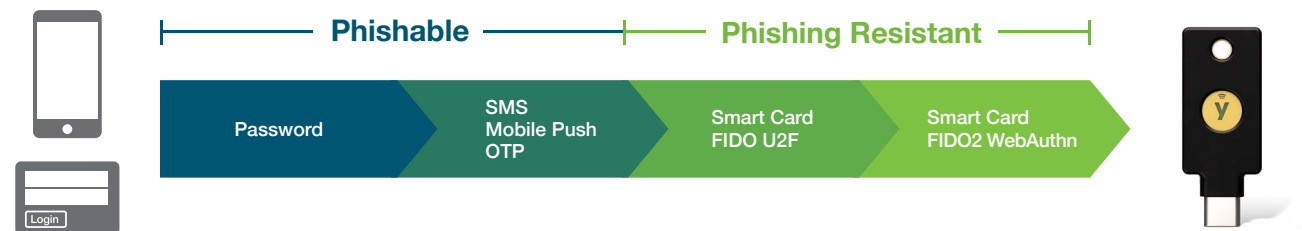
Financial organizations face mounting pressure to strengthen authentication in response to cyber threats, which are not only costly (\$5.97 million USD average data breach cost<sup>1</sup>) and undermine consumer trust, but the majority of which (82%) can be traced back to stolen credentials. It makes sense then why financial organizations are looking to harden cybersecurity defenses with multi-factor authentication (MFA) and why regulators and cyber insurers are also mandating the use of MFA.

In 2021, the Federal Trade Commission updated the “Safeguards Rule” (16 CFR 314)<sup>3</sup> of the Gramm-Leach-Bliley Act (GLBA) to require MFA for employees, third parties and customers. This rule helped bring the US financial regulations in alignment with EU requirements for MFA under the 2nd European Payment Services Directive (PSD2) and eIDAS (Electronic identification, Authentication and Trust Services).<sup>4</sup> In 2022, a Consumer Financial Protection Bureau (CFPB) circular clarified that the lack of MFA could trigger liability under CFPB regulations and the Dodd-Frank Act, even in the absence of a data breach.<sup>5</sup> All of this points to the requirement for MFA as part of a move away from flimsy passwords—but still not which form of MFA to choose.

Today, the regulatory environment is beginning to acknowledge that **not all forms of MFA are created equal**. Most basic authentication methods, including SMS, mobile authentication and one-time passcodes, are susceptible to account takeovers from phishing, social engineering and attacker-in-the-middle attacks. Acknowledging this, the revised Payment Card Industry Data Security Standard (PCI DSS v4.0) became the first financial standard to require **phishing-resistant MFA** for all access to the cardholder data environment.<sup>6</sup>

## What is phishing-resistant MFA?

**Phishing-resistant MFA** 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.





## YubiKey offers phishing-resistant MFA

The YubiKey is a multi-protocol key, supporting both Smart Card and FIDO2/WebAuthn standards along with OTP and OpenPGP, integrating seamlessly into both legacy and modern environments, and helping financial organizations **bridge to a passwordless future**. YubiKeys work with [hundreds of products, services and applications](#) including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and hundreds of cloud services.

Hardware security keys such as the YubiKey are an ideal option for strong phishing-resistant MFA because they don't require external power or batteries, or a network connection—a user can use a single key to secure hundreds of applications and services with the secrets never shared between services. The YubiKey is proven to [reduce risk by 99.9%](#) while delivering a great user experience, letting users securely log in with a single tap or touch:



### Strongest security

Reduce risk  
by 99.9%



### High return

Experience ROI  
of 203%



### More value

Reduce support  
tickets by 75%



### Faster

Decrease time to  
authenticate by >4x

“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.”

**Mike Schwermin** | CIO | Afni

### What are passkeys?

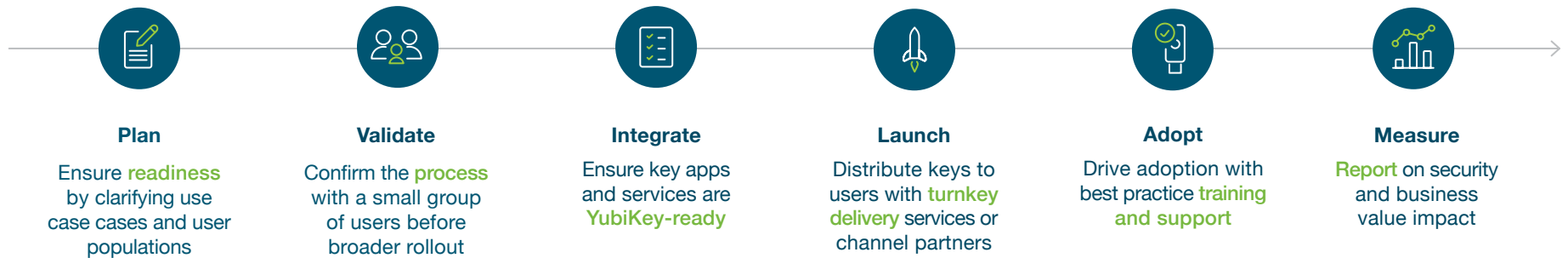
Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are different passkey implementations:

- **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 requirements across industries.

Given the threat landscape, the need for modern phishing-resistant MFA gets clearer on a daily basis. **But how do you start the journey?**

# Six key best practices to accelerate the adoption of phishing-resistant MFA

**Getting started is easy.** Based on Yubico's experience assisting hundreds of customers to deploy phishing-resistant MFA, including 4 of the top 10 U.S. banks, we have created a six step deployment process to plan for and accelerate adoption of phishing-resistant MFA at scale.



## 01. Plan

### Clarify use cases and ensure readiness

**A phased approach** is the best way to ensure a frictionless deployment. Put your **high value users and data first**, then expand. Rank use cases and user populations based on risk, workforce location, business impact and ease of technical integration.

## Determine use cases

There are many use cases across financial services where phishing-resistant MFA is essential. Your priority should be to address use cases and user populations based on risk and business impact, then expand to other use cases and populations. Some organizations choose to deploy phishing-resistant MFA to employee

user groups first due to security concerns or compliance regulations, while other organizations may choose to deploy phishing-resistant MFA to end-customer populations (commercial and/or retail) using online and mobile banking.

### Top scenarios for modern, phishing-resistant authentication



#### Privileged access

Protect sensitive data and targeted employees who have elevated access to systems or data.



#### Shared workstations

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, and IdP platforms.



#### High-risk transactions

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



#### Software supply chain

Protect code access and implement trusted code-signing.

### User groups



#### Office workers

Sophisticated attacks and lateral escalations make every user a privileged user.



#### Call center

Verify call center agent identity to provide access to key systems and shared workstations, in mobile-restricted environments.



#### Retail finance

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



#### Third Party

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



#### End customers

Protect customer accounts from fraud and build loyalty and trust with deployments to key customer segments.

## Assemble key stakeholders

While the number of resources on the project can vary based on the size and breadth of the YubiKey deployment, key stakeholders within the following departments can

positively influence the implementation of phishing-resistant MFA across the organization. It's important to have buy-in across all teams to ensure a smooth rollout:







## Engage Yubico experts as needed

Yubico, building on its years of helping secure some of the most security conscious organizations in the world, is focused on helping organizations easily access security products and services in a flexible and cost-effective way to heighten security across the business and free up productivity.

Organizations can benefit highly from a YubiKeys as a Service model and our Professional Services team offers best-in-class technical and operational guidance in support of your YubiKey implementation and rollout.



YubiEnterprise Services*		Yubico Professional Services	
 <b>YubiEnterprise Subscription</b>	 <b>YubiEnterprise Delivery</b>	 <b>Deployment 360</b>	 <b>Deployment planning</b>
Simplifies how businesses procure, upgrade and support <b>YubiKeys</b>	Global turnkey <b>YubiKey distribution</b> through YubiEnterprise Delivery or local channel partners	<b>Turnkey</b> planning, technical integration and deployment support	Jump start with workshops and <b>projects</b> to review use cases or develop a customized strategy

\* YubiEnterprise Services are available for organizations of 500 or more users.

## 02. Validate

### Confirm the process with a small group of users

**Validate** with a small group of users across a priority use case for confirmation and feedback, leveraging Yubico best practice resource guides, videos and engagements. **Practice, learn and then move forward with expansion.**

## 03. Integrate

### Ensure your environment is YubiKey-ready

YubiKeys can work with any number of professional and personal services with no shared secrets between the services, enabling high security and privacy at scale. A single key can work across over 1000 applications and services and secure your users' work and personal digital lives. To ensure that YubiKeys are integrated

seamlessly with key applications and services you wish to secure, below are some **critical questions** to think about. It's a good best practice to first answer these questions for your pilot program, then circle around for each expanded deployment.



### Works with YubiKey

YubiKeys, the industry's #1 security keys, work with hundreds of products, services, and applications. To browse YubiKey compatibility go to [yubi.co/wwwk](https://yubi.co/wwwk).



#### Who

##### Who needs access?

Employees, contractors, third parties, supply chain



#### What

##### What authentication approach will you take?

MFA (password and strong second factor), passwordless



#### Where

##### Where in your environment do you require strong authentication?

Critical infrastructure elements, network, applications, developer tools.

##### How do you manage access?

IAM, IdP, PAM, SSO, VPN



#### How

##### How does location impact deployment?

Remote, hybrid, on-premise, multi-office





##### What types of devices need to be supported?

Owned, BYOD, desktop, laptop, smartphone

## Prepare to deploy

After ensuring that your environment is YubiKey ready, it's time to create a plan to deploy YubiKeys across your organization. Optimizing deployment involves

organizational change management through effective communication, training and support. Yubico offers a variety of Professional Services to help you deploy quickly:

Yubico Professional Services			
 <p><b>Deployment planning</b> Rollout plan development</p>	 <p><b>Integration services</b> Architecture and infrastructure review, vendor integration analysis</p>	 <p><b>Implementation projects</b> Technical engagements to implement YubiKeys in your environment</p>	 <p><b>Service bundles</b> Flexible consulting hours for when and how you need them</p>



### What?

#### Increase awareness

Build up user training and support materials



### Why?

#### Boost engagement

Demonstrate value to the organization and the user

## 04. Launch

### Get keys in hands and plan Go Live events

We want your deployment to be as frictionless as possible for all teams and all users. This includes simplifying deployment plans, helping you answer critical

questions about how you will distribute keys to users and how you will manage the YubiKey lifecycle:

Distribution	Key management
Self-service   Channel Partner   YubiEnterprise Delivery	Onboarding   Support   Offboarding



“ We’re going down the same path as the most advanced organizations in the world. And we’re all rolling out YubiKeys.”

**Mike Schwermin** | CIO | Afni

## YubiKey rollout best practice recommendations

Once your users have their YubiKeys, the next step involves registering the keys with the applications and devices they will use. We recommend that each user has a second YubiKey as a backup, and if users cannot locate a YubiKey, revoking and replacing keys

is the recommended next step. If a user leaves the organization, some organizations retrieve YubiKeys prior to their departure while others prefer to allow departing users to keep their YubiKeys and continue using it for their own personal accounts.



Offer **flexibility and choice** in YubiKey form factor



**Two YubiKeys per person** for backup



Future-proof with **extra keys** to cover for churn or lost/stolen keys



Encourage **security** with personal use policies



**Plan an event** to make the future of your organization's security exciting

## Go Live events

Support the launch with a series of kick-off communications that introduce the YubiKey to users—communicate early, often. The ideal Go Live communications make users excited about the modern features of the YubiKey.



## 05. Adopt

### Support adoption and boost engagement

At Yubico, we believe success should not be measured by how many YubiKeys you have, but by how many keys are being used.

While the Go Live communications educate users on the **'what YubiKeys are'** and the **'why they matter'**, support teams need to be prepared to explain the **how**, with FAQs available to help with any questions that may arise for onboarding and troubleshooting (e.g. what to do in case of a lost key).

Effective education and awareness is important during this phase in order to showcase to your user community why the company invested in the YubiKey, and the direct benefits to users. The YubiKey's simple user experience requires minimal training and on-going support for users.



#### How to?

##### Educate users

Have clear calls to action on how to get started and how to get help



## 06. Measure



### Report on security and business impact

We know **the truth is in the numbers**. Validate the pilot against these metrics, then expand to other users to increase the overall business impact.



## Ready for scale

Yubico offers expert consulting services, including operational and technical workshops, implementation projects, on-demand resources and custom engagements, designed to jump-start and accelerate your YubiKey deployment at scale.

### Professional Services

Expert consulting services, including operational and technical workshops, implementation projects, on-demand resources and custom engagements, designed to jump-start and accelerate your YubiKey deployment.

**Services Offered**

- Deployment 360 Program**  
A turnkey program packaging all of the essential elements and expertise to ensure your successful YubiKey deployment.
- Workshops**  
Interactive sessions designed to help jump-start YubiKey integrations and deployments.
- Technical Implementation Projects**  
Tailored projects designed to facilitate your YubiKey implementation and rollout.

Yubico is leading the charge toward a more secure and riskless authentication future. Our team of experts provides technical and operational guidance to help streamline your YubiKey implementation and rollout.

To download the Professional Services Solution Brief go to [yubi.co/ps](https://yubi.co/ps)

YubiEnterprise Services*		Yubico Professional Services		
<b>YubiEnterprise Subscription</b>	<b>YubiEnterprise Delivery</b>	<b>Launch planning</b>	<b>Training and support</b>	<b>Analytics and reporting</b>
Cost effective and flexible <b>YubiKey procurement</b>	Global turnkey <b>YubiKey distribution</b> through YubiEnterprise Delivery or local channel partners	Create a marketing and <b>communication plan</b> tailored to your users	Best practice <b>training and support</b> materials and processes	Customized <b>metrics</b> and dashboard design

\* YubiEnterprise Services are available for organizations of 500 or more users.

“ I am used to subscription offerings in the cloud and YubiEnterprise Subscription has some helpful benefits that just made sense for our needs.”

**Mike Schwermin** | CIO | Afni



## YubiEnterprise Subscription

Gain leading, phishing-resistant authentication security for less than the price of a cup of coffee per user, per month. YubiKeys as a service, via subscription, delivers peace of mind in an uncertain world.

[Learn more yubi.co/yes](https://yubi.co/yes)



## YubiEnterprise Delivery

Yubico and trusted partners provide IT teams with powerful capabilities to manage delivery of hardware security keys to users globally and accelerate the adoption of strong authentication.

[Learn more yubi.co/delivery](https://yubi.co/delivery)

## Yubico Professional Services



### Deployment 360

Service hour bundles



### Workshops

Implementation projects



## Ready to get started?

There is no question that phishing-resistant MFA is the 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.

**Don't know where to start?** The good news is that you don't need to know all the answers upfront about how many keys to buy, what kind, how to integrate them into your environments and how to get them in the hands of employees.

Modern enterprises recognize that **security as a service** can take all the guesswork out of achieving success. When you choose YubiKeys as a service, you make decisions as you go with our insight and help, simplifying the process of scaling YubiKeys to wider circles of users as your business needs grow. We include success guides and priority support to help you be successful as quickly as possible.

If you want a closer partnership on any of the six steps of this plan, [Yubico's Professional Services](#) team is here to help.



**Contact us**  
[yubi.co/contact](https://yubi.co/contact)



**Learn more**  
[yubi.co/ps](https://yubi.co/ps)



## Sources

<sup>1</sup> Verizon, [2022 Data Breach Investigations Report](#), (Accessed August 22, 2022)

<sup>2</sup> Shalanda D. Young, Office of Management and Budget, [M-22-09](#), (January 26, 2022)

<sup>3</sup> National Security Memorandum/NSM-8, [Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems](#)

<sup>4</sup> NIST, [FIPS 201-3](#), (January 2022)

<sup>5</sup> CFPB, [Consumer Financial Protection Circular 2022-04](#), (August 11, 2022)

<sup>6</sup> PCI SSC, [PCI DSS v4.0](#), (March 2022))



## About Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering modern, hardware-based passkey authentication security at scale to customers in over 160 countries.

For more information, please visit: [www.yubico.com](http://www.yubico.com).