yubico

WHITE PAPER

Securing financial services with phishing-resistant MFA

Choosing the right MFA approach to protect against modern cyber threats

Contents

$5.97 million

average cost of data breach in financial service[1]

82%

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

55%

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

62%

of intrusions are from the **supply chain**[4]

The critical need for strong authentication in financial services

The financial services industry (FSI) is in the midst of a digital transformation, investing in technologies and strategic partnerships to create efficiencies, support flexible work models, and meet shifting competitive and consumer demands. However, as financial institutions become more digital and interconnected, cyber risk has reached critical levels.

The FSI is one of the highest value targets for cyber criminals, with the second highest costs per breach ($5.97 million USD on average), a figure which jumped 4.4% in a single year.[5] Additionally, financial services was the most breached sector in 2022, with 79 US FSIs reporting breaches of over 1000 or more consumers.[6] How are they gaining access? The vast majority—90% of the breaches—involved servers, with stolen credentials playing a key role in the attack.[7] Phishing, hacking and ransomware continue to be persistent threats in all attack types.

While increasing cyber risk exposes FSIs to potential loss of consumer trust, financial risk and threat of regulatory action, the Federal Reserve recognizes that this risk can have systemic ramifications, both as the consequence of an operational disruption or the use of shared technologies and third-party service providers.[8] In March 2023, the International Monetary Fund acknowledged that these risks are particularly acute with the growing interconnections across the world, including with countries that lack a cyber strategy, and that the "strength of cyber defenses depends on the weakest link."[9] The 2016 Lazarus attack on a Bangladesh Bank, for example, involved a compromise of SWIFT, the inter-banking messaging system used by every bank to confirm cross-border financial transactions—a compromise that thankfully did not extend to other institutions.[10]

In response to risk, FSIs 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 all the complex authentication scenarios and user groups within financial services, the merits and drawbacks of different forms of MFA, or how to get started.

This paper will explore these important considerations and how strong phishing-resistant and passwordless authentication can be deployed at scale to support strong security, efficiency and user experience.

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

Evolving regulations and the future of authentication in financial services

The fact that the majority of data breaches in financial services can be tied to credentials and phishing attacks points to continued reliance on legacy authentication. Legacy authentication methods such as flimsy passwords and mobile-based authenticators such as SMS, OTP and push notifications are highly susceptible to phishing, account takeovers, SIM swaps, and attacker-in-the-middle attacks.

A Google, NYU, and UCSD analysis of 350,000 real-world hijacking attempts revealed that a SMS-based OTP only blocked 76% of targeted attacks and a mobile push app only blocked 90% of targeted attacks.[11] In other words, the best case scenario was a 10% attack penetration rate. Knowing this, regulators are beginning to mandate not only the use of MFA, but to acknowledge that not all forms of MFA are created equal.

In 2021, the Federal Trade Commission updated the "Safeguards Rule" (16 CFR 314)[12] 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).[13] The FFIEC also suggests MFA be prioritized for digital banking consumers engaging in high-risk transactions and that hardware-based MFA be prioritized for high-risk users.[14]

A 2022 Consumer Financial Protection Bureau (CFPB) Circular places urgency under the transition to MFA for employees and as an option consumer accounts, stating that the lack of MFA could trigger liability under CFPB regulations or even the Dodd-Frank Act, even in the absence of a data breach.[15] Further, the CFPB has begun encouraging consumers to submit a complaint to the CFPB if a financial product or service lacks MFA.[16]

As regulators begin to mandate the use of MFA, they are now also drawing attention to the need for modern, phishing-resistant authentication to meet the authentication needs of today's FSIs. In its circular, the The CFPB Circular 2022-04 states that MFA solutions that protect against credential phishing are "especially important" and should be considered for consumer account protection.

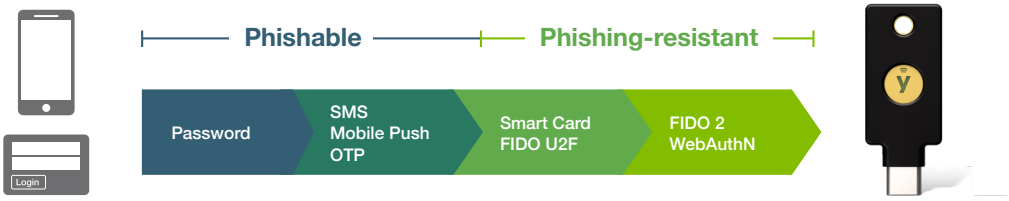
Regulations requiring phishing-resistant MFA

Although the CFPB Circular only stresses the importance of phishing-resistant MFA, other regulations are going one step further—they are requiring it.

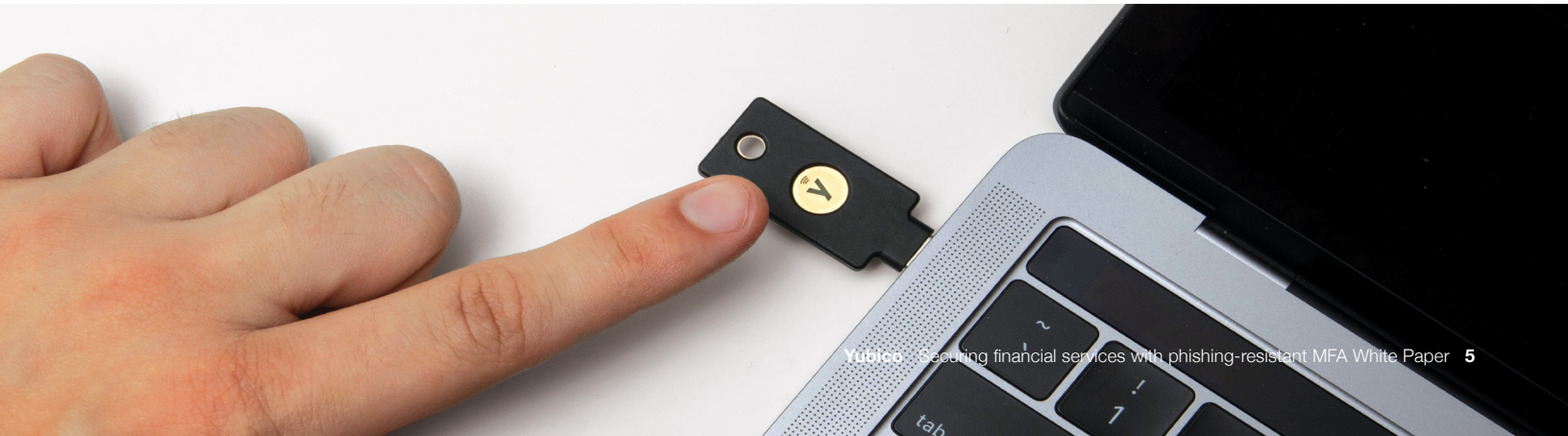
The revised Payment Card Industry Data Security Standard (PCI DSS v4.0) became the first (but likely not last) financial standard to require phishing-resistant MFA for all access to the cardholder data environment, which is relevant for the FSI.[17] For FSIs that work with government agencies, this requirement aligns with U.S. White House Executive Order 14028 on Improving the Nation's Cybersecurity and OMB Memo M-22-09, which mandates the use of phishing-resistant MFA as part of deploying a Zero Trust Architecture.[18] 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.[19]

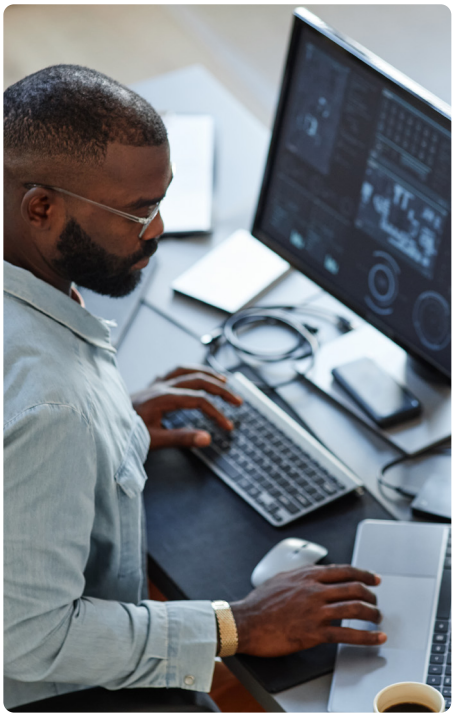
What is phishing-resistant MFA?

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.



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





Top authentication scenarios and user groups in financial services

As FSIs rush to comply with the requirements to extend MFA to all employees, third-parties and customers, their priority should be to address the highest priority use cases and user populations based on risk and business impact, then expand to other populations:

Top scenarios for phishing-resistant MFA

Privileged access
Targeted employees who have elevated access to systems or data.

High-risk transactions
Employees supporting high risk service or high value transactions.

Shared workstation
Employees who need access to shared computers and devices (e.g. banks and call centers).

Software supply chain
Access and data exchange associated with third party software and code.

Hybrid and remote work
Employees who require remote access to VPN, IAP, IAM, & IdP platforms.

User groups

Office workers
Office workers who can be targets of elaborate credential phishing schemes.

Third party
Third-parties who need access to systems and data (e.g. BPO call centers, fintech partners).

Call center
Agents who need verified access to sensitive and personal client data and shared workstations.

End customers
Commercial and retail customer segments for secure online and mobile account access.

Retail finance
Employees who move between workstations to service customers or authorize transactions.

82%

Verizon estimates that 82% of data breaches have a connection to the human element, including the use of stolen credentials[20]

Priviledged users

Privileged users have special access or capabilities beyond regular users such as network and data administrators, security and systems administrators, application developers, C-suite employees or employees with elevated access to personally identifiable information (PII). Verizon estimates that **82% of data breaches have a connection to the human element, including the use of stolen credentials.**[20] FFIEC guidance suggests least privilege access controls and hardware-backed MFA for privileged users.[21]

Shared workstation

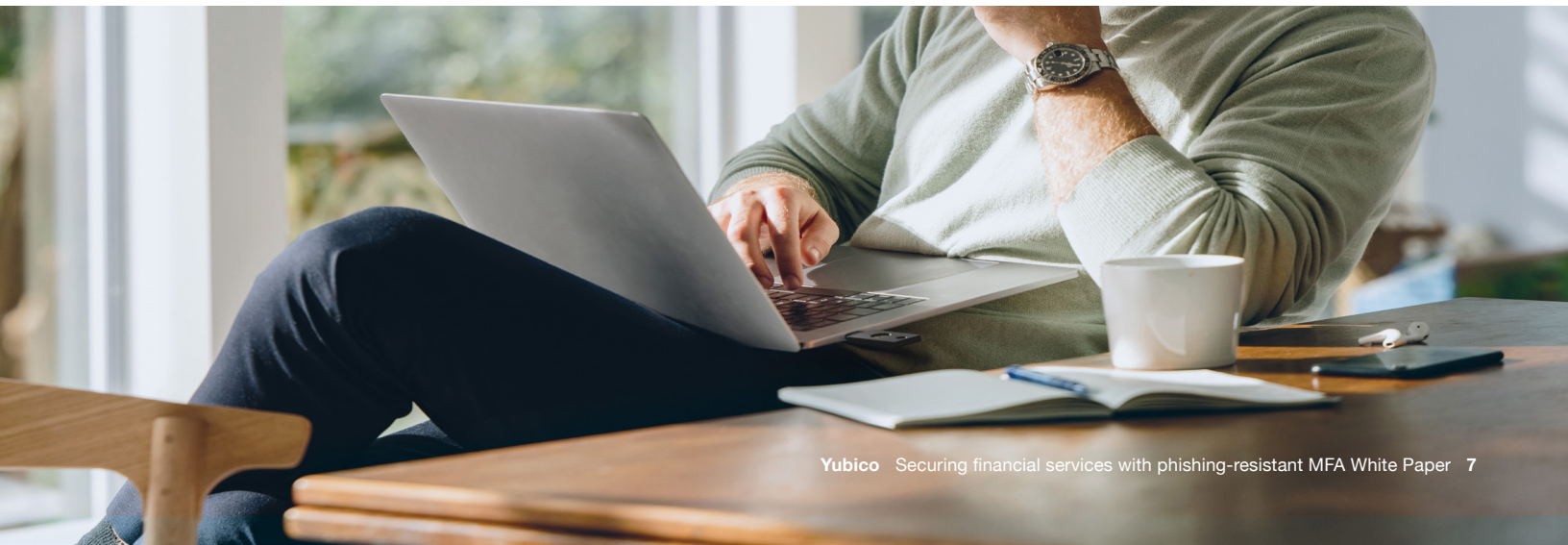
Customer support in both call center and retail banking environments depends on granting access to sensitive account information and supporting financial transactions in a shared workstation environment, with devices used by multiple users throughout the day. In these environments, users should have least privilege access to systems and data and an authentication process that reflects the need to support response time SLAs with fast authentication (or step-up authentication for high-risk transactions). The new CISA and NSA guidance suggests that portable authenticators be considered over software authenticators tied to a specific device.[22]

Hybrid and remote work

Many FSIs and call centers have adopted a hybrid and remote work approach that moves security from a perimeter-based approach to a per user and per device approach. Remote work introduces new vulnerabilities such as unsecured home networks, unpatched devices, shared devices, and weak/reused passwords—vulnerabilities that persist when connecting to Virtual Private Networks (VPN), Identity-Aware IdentityProxies (IAP), IAM and Identity Provider (IdP) platforms.

High-risk transactions and activities

FFIEC guidance suggests identifying high-risk transactions by the potential for financial loss or breach of information, both of which would require enhanced authentication controls.[23] Stronger MFA and/or step-up authentication or secondary authentication could be extended to transactions that are high dollar amount, in volume or for account changes (such as password resets) regardless of the user segment (employee, third party, customer).



Software supply chain

Increasingly sophisticated attacks are targeting software supply chains as an entry point to compromise financial systems and data, with 82% of CIOs stating their organizations are vulnerable to software supply chain attacks.[24] For example, in 2021, developer auditing tool maker Codecov suffered a compromise of its Bash uploader script that could export information stored in user environments—and some of its users were banks.[25] With regulators such as the FDIC now holding FSIs responsible for third-party weaknesses, organizations need solutions to manage source code and secure code signing.[26]

Office workers

While it may seem obvious to protect privileged users first, in today's modern cyber threat landscape, every user can be considered a privileged user. Today's sophisticated threat actors leverage stolen credentials to move laterally on the network to search for or phish for credentials that ultimately escalate privileged access to high-value data assets and systems. Further, 90% of organizations feel vulnerable to insider attacks, either directly against confidential business information (57%) or against privileged account information (52%).[27]

Call centers

FSI call centers and contact centers are fast paced, managing large and/or high-risk transaction volumes on a daily basis. They typically operate 24/7, with customer service agents logging in and out of key systems and across shared workstations, with authentication methods limited by mobile-restriction policies. A 2019 Aite Group interview of 25 executives at 18 of the top 40 largest U.S. financial organizations found that 61% of fraud can be traced back to the contact center.[28] As call center activities are increasingly outsourced to third-parties and/or include remote and hybrid work, these risks have only increased.

Retail finance workers

Employees at banks, brokerage firms and insurance companies constantly move from one workstation to another to service customers and support and authorize transactions. Unfortunately, despite access to PII and customer account details, many organizations are still relying on username and password based authentication or legacy mobile-based MFA, which can easily open up vectors for attack and costly non-compliance.

Third-party

FSIs have extensive third-party relationships with Business Process Outsourcing (BPOs), vendors, contractors, fintech partners and support ongoing exchanges of data and communications between banks all around the world. This exchange of data also introduces additional data privacy considerations in order to comply with the General Data Protection Regulation (GDPR) and similar legislation. Although the health of the FSI and the financial system as a whole hinges on the weakest link, FSIs can reduce third-party risk by implementing stronger access and authentication controls.

End customers

Between 30% and 40% of mobile banking users consider themselves “very” concerned about fraudulent activities, including identity theft, credential theft, or loss of funds.[29] However, many online banking providers still use legacy authentication methods that combine passwords with security questions or push authentication (SMS or email), which doesn’t keep customers safe against phishing attacks or account takeovers and introduces frustrating delays in the authentication experience. In fact, 75% of fraud volume occurs when customers have been tricked into performing a fraudulent transaction.[30]

Phishing-resistant multi-factor and passwordless authentication with the YubiKey

The concept of “not all forms of MFA are created equal” is about more than security. Phishing-resistant authentication protocols (e.g. FIDO2 and WebAuthn) address the security concerns with legacy mobile-based authentication, but a modern authentication solution must also consider usability and ROI—establishing a streamlined authentication process for all users, across all authentication scenarios, without costly readers or support costs.

Modern authentication begins with the hardware security key—a critical combination of highest-assurance security along with an optimized user experience. That’s why Yubico created the YubiKey, a hardware security key that delivers modern authentication alongside an optimized user experience to enable phishing-resistant two-factor, MFA and passwordless authentication at scale. 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 to help financial organizations bridge to a passwordless future.

The YubiKey is proven to reduce risk by 99.9% while delivering a great user experience, letting users securely log into leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and hundreds of cloud services—all with a single tap or touch.

More value
Reduce support tickets by 75%

Strongest security
Reduce risk by 99.9%

High return
Experience ROI of 203%

Faster
Decrease time to authenticate by >4x

Forrester Consulting Total Economic Impact™ study, September 2022, metrics based on a composite organization

Financial services use cases supported by the YubiKey

Four out of 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.

Hybrid and 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**

YubiKeys as a Service to accelerate deployment of phishing-resistant MFA 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.

The Yubico Best Practice Deployment Guide will walk you through 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.

YubiEnterprise Services*		Yubico Professional Services		
YubiEnterprise Subscription	**YubiEnterprise Delivery**	**Deployment 360**	**Workshops**	**Implementation projects**
Simplifies how businesses procure, upgrade and support YubiKeys	Global distribution to remote and in-office locations	Service hour bundles	Custom engagements	Technical projects to aid in your YubiKey integration

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**

Summary

Financial organizations face mounting pressure to strengthen authentication in response to cyber threats. While risk appears to come from all fronts — legacy infrastructure, the tech and software supply chain, mobile banking, remote and hybrid work — leading FSIs are looking to phishing-resistant MFA and passwordless not just to protect data and comply with regulations, but to create a better user experience for employees, third-parties and customers.

In a world where not all forms of MFA are created equal, the YubiKey accelerates the adoption and scale of phishing-resistant MFA 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, 2022 Cost of Data Breach Report, (July 27, 2022)

2 Verizon, 2022 Data Breach Investigations Report, (2022)

3 Sophos, The State of ransomware in Financial Services 2022, (August 2022)

4 Verizon, 2022 Data Breach Investigations Report, (2022)

5 IBM, 2022 Cost of Data Breach Report, (Accessed August 12, 2022),

6 Carter Pape, Breach data from Maine shows scope of bank, credit union exposures, (August 24, 2022)

7 Verizon, 2022 Data Breach Investigations Report, (2022)

8 Danny Brando, et al., Implications of Cyber Risk for Financial Stability, (May 12, 2022)

9 Tobias Adrian, Caio Ferreira, Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards, (March 2, 2023)

10 Michael Corkery, Once Again, THieves Enter Swift Financial Network and Steal, (May 12, 2016)

11 Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019)

12 FTC, Agency updates Safeguards Rule to better protect the American public from breaches and cyberattacks that lead to identity theft and other financial losses, (October 27, 2021)

13 European Parliament and the Council of the EU, Directive 2015/2366, (November 25, 2015)

14 FFIEC, Authentication and Access to Financial Institution Services and Systems Guidance, (August 11, 2021)

15 CFPB, Consumer Financial Protection Circular 2022-04 (August 11, 2022)

16 CFPB, Tweet, (September 30, 2022)

17 PCI SSC, PCI DSS v4.0, (March 2022)

18 Shalanda D. Young, Office of Management and Budget, M-22-09, (January 26, 2022),

19 CISA and the NSA, Identity and Access Management: Recommended Best Practices for Administrators, (March 2023)

20 Verizon, 2022 Data Breach Investigations Report, (Accessed March 1, 2023)

21 FFIEC, Authentication and Access to Financial Institution Services and Systems Guidance, (August 11, 2021)

22 CISA and the NSA, Identity and Access Management: Recommended Best Practices for Administrators, (March 2023)

23 FFIEC, Authentication and Access to Financial Institution Services and Systems Guidance, (August 11, 2021)

24 Venafi, CIO Study: Software Build Pipelines Attack Surface Expanding, (June 2022)

25 Ax Sharma, Hundreds of networks reportedly hacked in Codecov supply-chain attack, (April 20, 2021)

26 FDIC, Third-party arrangements: elevating risk awareness, (2007)

27 Crowd Research partners, Insider Threat (2018)

28 Pindrop, Fraud in the Contact Center, (2019)

29 Cornerstone Advisors, Accessed on Forbes.com: Mobile Banking Adoption in the United States Has Skyrocketed (But So Have Fraud Concerns), (July 29, 2021)

30 Outseer, 1H 2022 Outseer Fraud & Payments Report, (September 21, 2022)

yubico

About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico is privately held, with a presence around the globe. For more information, please visit: www.yubico.com.