yubico

Modern strong authentication and compliance for Financial Services

How the YubiKey meets global Financial Services regulations with phishing-resistant MFA

Contents

Authentication in Financial Services

Digital transformation and consumer expectations

Are you ready for regulatory change?

Financial regulations grow from need: from changing technology or from crises, including scandals and cyber attacks. The Enron and Worldcom scandals of the early 2000s triggered the creation of the Sarbanes-Oxley Act to provide greater financial oversight for public companies, including data security.

As the industry responds to new crises, including the COVID-19 pandemic, regulatory oversight is never far behind. Today, those changes include revisions to PCI DSS and the draft DORA regulation in the EU.

An evolution has been occurring in financial services, caused by a combination of new technologies and changing customer demographics. Commercial and retail banks, credit unions, brokerage and trading firms, investment banks, and other financial services organizations are being challenged to modernize both the front and back ends of their business to remain competitive with rising costs and the expectations of the financial customers of today and tomorrow.

This digital transformation has been accelerated by the growing cyber attack landscape and the demands of employees and customers amidst the global COVID-19 pandemic–namely broadening digital presence (online and mobile) and improving security across these channels. But without the right solutions in place to ensure secure access controls, financial services organizations face an increased risk of cyber attack and potential non-compliance with PCI DSS, SOX, and GDPR.[1]

Financial services institutions have been disproportionately targeted by cyber attacks since the start of the COVID-19 pandemic, representing 25.3% of all attacks.[2] "There is a strong link between the prevalence of WFH (work from home) arrangements… And the incidence of cyber attacks," notes a Bank for International Settlements Bulletin on COVID-19 and cyber risk in the financial sector.[3]

New regulations and standards for the protection of financial data and consumer privacy are keeping pace with the digital transformation and changing risk landscape. With each new regulation, greater clarity and specification around access controls are being introduced. While these regulations and frameworks are moving toward stronger authentication requirements, the secondary driver for strong authentication is the end customer.

Customer acquisition and loyalty hinge on concepts such as trust, security, convenience, and personalization. A cyber attack, while costly from a regulatory and recovery standpoint, can be devastating for customer churn: often the largest indirect cost associated with a data breach.[4] Fear of fraud is increasing across the board, with phishing and supply chain scams among the top concerns.[5]

Evolving cyber attack landscape

$5.97 Million

average cost of data breach in financial services[6]

27%

of all cyber attacks target the financial and healthcare sectors[7]

238%

increase in global cyber attacks against banks during COVID-19[8]

~60%

of financial services have 500+ passwords that never expire[9]

The financial services industry is under constant cyber attack due to its massive store of financial and personally identifiable information (PII) and the potential for large payouts. The COVID-19 crisis increased both the volume and type of attacks, with 80% of surveyed financial institutions reporting an increase in cyber attacks.[10] Coupled with this increase in attacks, remote work introduced new vulnerabilities such as unsecured home networks, unpatched devices, shared devices, and weak/reused passwords.

Financial services employees that perform high-risk, high-value transactions on a daily basis are often the target of cybercriminals. Credentials are the most sought after type of data in the initial phase of a cyber attack, with threat actors moving laterally to find data or compromise systems. Approximately 61% of data breaches can be traced back to credentials in some way.[11] In financial services, the average employee has access to nearly 11 million files the day they walk in the door and for large financial organizations, the number is double: 20 million files open to all employees.[12]

The consequences of cyber attacks can be devastating, including borrow rate changes, IT failures and business disruptions, reputational losses, regulatory and legal costs, ransomware recovery costs, and the loss of intellectual property.

While financial institutions were early adopters of two-factor authentication (2FA) solutions such as SMS codes, OTP, and push notifications, mobile-based authentication doesn't offer the best security and is vulnerable to account takeovers, phishing, malware, SIM swapping, and man-in-the-middle attacks.

A recent VICE article, "The Booming Underground Market for Bots That Steal Your 2FA Codes," showcased the use of inexpensive phishing bots to bypass MFA.[13] These bots leverage stolen credentials, relying on pervasive password reuse practices to breach the first step in 2FA. The bots then automate scripted calls, triggering an OTP text to capture and bypass MFA. Previously, such scams required real people to make these calls - now, bots are automating the process, relying on consumer trust in MFA, "a security measure that many members of the public may assume is largely secure."[14]

> MFA is critical, but not all MFA methods are created equal. Twitter used application-based MFA, which sent a request for authentication to an employee's smart phone. This is a common form of MFA, but it can be circumvented. During the Twitter Hack, the Hackers got past MFA by convincing the Twitter employees to authenticate the application-based MFA during the login. The most secure form of MFA is a physical security key, or hardware MFA, involving a USB key that is plugged into a computer to authenticate users. This type of hardware MFA would have stopped the Hackers, and Twitter is now implementing it in place of application-based MFA.
>
> **–New York Department of Financial Services, Twitter Investigation Report, October 2020**

SolarWinds attack underscores supply chain risk

> As SolarWinds has shown, the supply chain threat is increasing as the cyber security landscape diversifies. Taking this into account, financial institutions need to be more aware of their supplier security posture and make sure stringent checks are in place.
>
> **– Neal Semikin, CISO 324 Consultancy, previous CISO of the Bank of England[15]**

In 2020, a major threat actor backed by the Russian government penetrated thousands of organizations, including creating a backdoor in the SolarWinds Orion Software, which in turn installed malware to spy on over 18,000 product customers.[16]

The attack went undetected for months, in part due to the supply chain attack method used to move laterally between systems and gain additional privileges. Of note is the supposed misuse of Identity and Access Management (IAM) systems like single sign on, network logon systems, SAML/OAuth/OIDC federation systems, and the like.

In the past 12 months, 33% of surveyed financial institutions said they've encountered an attack leveraging island hopping: an attack on a supply chain or partner to then target the primary financial institution.[17]

With SolarWinds, and almost every breach, you'll find credentials, keys, and secrets abused anywhere they can be. Once the attacker has initial access to the victim's environment, they diversify their access to help maintain a persistent foothold.

Financial services companies typically have large supply chains, all the way from application and services vendors to functions that are outsourced to third party vendors and partners such as call centers. In these scenarios large amounts of potentially sensitive data are handed over to third parties, and utmost case needs to be taken with respect to securing this data against cyber attacks.

Today's financial institutions are looking to strong authentication to prepare for a more stringent regulatory environment, but also to be more competitive in the fight to acquire and retain customers looking to grow their wealth in the long term.

Modern, phishing-resistant authentication with the YubiKey

The solution

YubiKey is the **only** solution that is proven to stop 100% of account takeovers in independent research.[18]

Smart Card/PIV

Out-of-the-box native integration for the Microsoft environment using Smart Card/PIV functionality based on the NIST SP 800-73 specification.

FIDO2 & FIDO U2F

Strong two-factor, multi-factor and passwordless authentication public key crypto to protect against phishing, session hijacking, man-in-the-middle, and malware attacks.

One time passcodes

Integrate Yubico OTP natively with the free YubiCloud authentication service or program unique TOTP or HOTP secrets.

Legacy multi-factor authentication solutions including mobile authentication such as SMS, OTP, and push notifications are better than just username and passwords, but are still not 100% effective against mitigating risks from evolving cyber risk vectors. In comparison, hardware security keys based on modern FIDO protocols are proven to stop successfull phishing attacks and and account takeovers in their tracks.

The YubiKey is a hardware security key manufactured by Yubico, that offers easy-to-use two-factor, multi-factor, and passwordless authentication at scale, helping financial services be compliant to MFA requirements across various regulations, certifications, and frameworks. Organizations receive a choice of FIPS 140-2 validated keys Overall Level 1 (Certificate #3907) and Level 2 (Certificate #3914), Physical Security Level 3. Organizations can also avail of the YubiKey Bio Series, a gold standard in biometric authentication.

With the YubiKey, financial institutions can:

- Stop account takeovers and prevent man-in-the-middle attacks with superior hardware cryptographic security
- Provide unmatched simplicity for users with 4x faster logins that ensure proof of presence and possession
- Comply with existing and emerging regulations such as FFIEC, SOX, PSD2, PCI, FIPS, and GDPR
- Bridge to passwordless authentication
- Reduce IT support costs related to password resets
- Deliver trust to users and gain peace of mind with a trusted solution from an industry leader pioneering global authentication standards

A single YubiKey supports multiple authentication protocols including Smart Card, One Time Password, OpenPGP, FIDO U2F, and FIDO2/WebAuthn, ensuring a single key can be used across both legacy and modern infrastructures and applications. To authenticate, users simply tap/touch their security key to any kind of device, including mobile phones and tablets.

YubiKeys can be used to stop phishing attacks and account takeovers for a variety of internal and end-customer use cases such as privileged users, call center workers, hybrid and remote workers, online/mobile banking, and for high-risk high-value transactions. YubiKeys can also be used for risk-based authentication requiring tap/touch of the security key for step-up authentication transactions.

Financial standards compliance

How the YubiKey for modern strong authentication addresses regulatory requirements

Only 54.7%

of financial services feel their security program is successfully meeting compliance regulations[19]

The financial services industry is subject to one of the highest levels of security requirements and regulatory burden. There are many compliance requirements to contend with, and in recent years there have been a number of wide-sweeping changes to financial benchmarks (LIBOR), new state and Global privacy laws (GDPR), executive orders, as well as indications of upcoming revisions to financial standards such as PCI DSS.

The YubiKey helps financial services organizations comply with existing and newly emerging regulations with modern, strong authentication, offering highest-assurance two-factor, multi-factor, and passwordless authentication. The following sections outline the various financial services regulations and the YubiKey capabilities that help organizations satisfy regulatory requirements related to authentication.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) officially took a stand on requiring MFA in its 2016 update, PCI DSS 3.2 and subsequent revisions.[20] In the information supplement related to MFA, which is mandated for Requirement 8.2 and 8.3, the PCI Security Standards Council sets forth the minimum requirements for authentication and cryptographic tokens (based on NIST SP 800-164 and NIST SP 800-157).[21] PCI DSS 4.0 goes further by expanding the scope of accounts that require MFA, and changing password and MFA policies to align with updated MFA and InfoSec Guidance.

PCI DSS requirement	PCI DSS v4.0	YubiKey capabilities
Protect cardholder data	3.5, 3.6, 3.7	• Hardware-backed MFA access controls • Centralized authorization policies to control access • Cryptographic module supports multiple protocols
Mechanisms to fight phishing attacks	5.4	• Hardware-backed MFA access controls • Centralized authorization policies to control access

PCI DSS requirement	PCI DSS v3.2.1	YubiKey capabilities
Develop and maintain secure systems and applications	6.1, 6.2, 6.5	• Hardware-backed MFA access controls • Centralized authorization policies to control access • MFA through multiple protocols - Something you know (FIDO2, PIV, CAC) - Something you have (Private key stored on the YubiKey) • Support password / PIN for MFA (FIDO U2F, FIDO2) • 100% protection from account takeovers • Replay attack resistant
Restrict access to cardholder data	7	• Hardware-backed MFA access controls • Centralized authorization policies to control access
8 Defines Strong MFA, lists factors and purpose 8.2 User Lifecycle 8.3 Strong authentication for users and administrators is established and managed. (requires MFA for all users excluding front line workers with extremely limited access to CDE) 8.4 MFA required for all CDE access (Excluding specific carve outs) 8.5 MFA is hardened against attacks	8	• Centralized authorization policies to control access • Portable for third-party remote access • Hardware-backed MFA access controls - Something you know (FIDO2, PIV, CAC) - Something you have (Private key stored on the YubiKey) • Support password / PIN for MFA (FIDO U2F, FIDO2) • YubiKey used as smart card
Restrict physical access to cardholder data	9.1, 9.2, 9.3	• YubiKey used as smart card
Track access to network resources and cardholder data	10.1, 10.2, 10.3	• Centralized authorization policies to control access • Capture access records in audit logs
Maintain and train users on security policies and acceptable use	12.1, 12.2, 12.3, 12.6, 12.9	YubiKeys are a demonstrable way to ensure MFA is in use. FIDO login workflows are faster and more secure than legacy methods – ease of use drives acceptance and avoids bad user habits common with other MFA methods that put critical and sensitive data at risk of being hacked

GLB Act / GLBA

The Gramm-Leach-Bliley Act (GLBA) requires financial organizations to implement "administrative, technical and physical safeguards" appropriate to the size, complexity, and scope of activities.[24]

GLBA requirement	Section	YubiKey capabilities
Protect non-public personal information with administrative, technical, and physical safeguards (Safeguards Rule)	501(b)	• Hardware-backed MFA access controls • YubiKey used as smart card • Centralized authorization policies to control access • Touch-button test of user presence
Detect and mitigate unauthorized access	521	• Hardware-backed MFA access controls • YubiKey used as smart card • Centralized authorization policies to control access

FTC updates "Safeguards Rule"

On October 27 2021, the Federal Trade Commission (FTC) released an update to the "Safeguards Rule" of the GLBA, covering five main modifications around access control, multi-factor authentication and encryption.[25]The Final Rule (16 CFR 314) section §314.4 5(c) now requires financial institutions implement MFA for "any individual accessing any information system," a rule which would apply to employees, customers, or any other third-party.[26] The FTC noted that many "affordable and workable" solutions to MFA exist, specifically calling out the YubiKey as one such option in footnote 190.

While this update underscores the importance of MFA, more recent Federal guidance has recognized that not all forms of MFA are created equal. Recognizing that mobile-based authentication can be phished, Executive Order (EO) 14028 now requires MFA that is "impersonation-resistant."

FFIEC

The Federal Financial Institutions Examination Council (FFIEC) provides information security guidance with five banking regulators: the FDIC, FRB, NCUA, OCC, and the CFPB.[27] In a guidance entitled *Authentication in an Electronic Banking Environment,* the FFIEC stated that "single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information."[28] The guide further stated that MFA of appropriate strength should be implemented and regularly audited.

FFIEC issues new guidance on authentication

On August 11, 2021 the Federal Financial Institutions Examination Council (FFIEC) issued guidance that provides financial institutions with examples of effective authentication and access risk management principles and practices for customers, employees, and third parties accessing digital banking services and information systems. FFIEC states that the attributes, including usability, convenience, and strength, of various authentication actors can differ and each may exhibit different vulnerabilities which may be exploited. For example, certain MFA factors may be susceptible to MiTM attacks, such as when a hacker intercepts a one-time security code sent to a customer. FFIEC offers guidance that for high-risk users, strong authentication, such as MFA solutions using hardware and cryptographic factors, can mitigate risks associated with unauthorized access to information systems, because when cryptographic MFA solutions are used, cryptographic keys are stored securely and protected from attack, for example by storing keys in a hardware security module. Read more here.

FFIEC requirement	Section	YubiKey capabilities
Preventative risk mitigation	II.C.3	• Multi-factor cryptographic device • Hardware-backed MFA access controls • Centralized authorization policies to control access • 100% protection from account takeovers
Control implementation	II.C.4	• AAL3 certified NIST SP 800-63
User security controls	II.C.7	• Hardware-backed MFA access controls • YubiKey used as smart card • Centralized authorization policies to control access
Physical security	II.C.8	• YubiKey used as smart card
Network controls	II.C.9	• Hardware-backed MFA access controls • YubiKey used as smart card • Centralized authorization policies to control access

FFIEC audit topics vary from year to year, but priorities have been known to change.[29] It is likely that examiners, regulators and auditors will be shifting priorities to address the risks of remote work in the financial sector.

PSD2

The EU financial sector is regulated by the EU Payment Services Directive 2 (PSD2) coupled with the related Regulatory Technical Standard. The directive includes the concept of dynamic linking (Article 97), which requires that the payment amount and the payee of the transaction be linked to the user through strong authentication of at least two factors.[30] The European Banking Authority confirmed that SMS OTP verification alone is no longer sufficient.[31]

The FIDO Alliance, where Yubico is a contributing member, created FIDO solutions to offer the best end user experience to fulfill PSD2 requirements. FIDO compliant PKI devices, like the YubiKey, support both authentication and digital signatures with a streamlined user experience. FIDO2 can also be used with 3D Secure, an additional protection for card authentication that is PSD2 compliant, and will also play an important role in the upcoming W3C standard on Secure Payment Confirmation. Read the White Paper, FIDO2 & PSD2- Providing a satisfactory customer journey, to learn more.

eIDAS

In the EU, eIDAS (Electronic identification, Authentication and Trust Services) is a standard for electronic transactions in the EU market, specifically covering topics such as signatures and authentication.[32] In June 2021, the Commission proposed a framework for a EU Digital Identity Wallet (a mobile-based wallet), provided to all EU citizens, residents, and businesses, that will be used to authenticate users.[33]

eIDAS requirement	Section	YubiKey capabilities
Remote electronic signatures should include security procedures, systems, and products	52	• Hardware-backed MFA access controls • YubiKey with SmartCard or FIDO2 • Centralized authorization policies to control access v Touch-button test of user presence
Support common identification and authentication measures	10-12 / Directive 2011/24/EU	• Hardware-backed MFA access controls • YubiKey used as smart card • Centralized authorization policies to control access
Assurance levels of electronic identification schemes. "Substantial" requires 2FA, "High" adds the requirement of tamper-proof authentication devices and dynamic cryptographic schemes.[34]	Chapter II Article 8	• Hardware-backed MFA access controls • Centralized authorization policies to control access • Cryptographic module supports multiple protocols • FIDO2 support

SOX & SOC 2

SOX requires formal data security policies, communication of data security policies, and consistent enforcement of data security policies. Companies should develop and implement a comprehensive data security strategy that protects and secures all financial data stored and utilized during normal operations.

The Sarbanes-Oxley (SOX) Act of 2002 is a US law meant to protect investors from fraudulent accounting activities by corporations. The SOX Act is overseen by an annual audit in which financial institutions and all companies listed on the US stock exchange must prove they have kept data secure with "adequate" internal controls (Section 404).[35] While controls are not specified, it is up to management to attest to the effectiveness of controls and for auditors to agree, so the onus is on financial insitutitions to adopt the highest level of controls reflective of today's risk environment. Non-compliance with SOX can result in heavy fines or even jail time.

As a consequence of the SOX Act, the International Standard on Assurance Engagements 3402 (ISAE 3402) was developed to ensure compliance by means of Service Organizational Control (SOC) audits and compliance criteria. SOC 2 focuses specifically on the handling of data and five key trust services criteria (TSC), with a minimum focus on two-factor authentication similar to NIST 800-53 criteria for access controls.[36] As a 10-year old standard, it is possible that the events of the past year will trigger a revision of SOC 2 criteria.

Trust service criteria (CC6.2): logical and physical access control

The SOC 2 audit process includes 5 categories of Trust Services Criteria: Security, Availability, Confidentiality, Processing Integrity, and Privacy. These categories each cover a set of internal controls related to different aspects of your information security program.

Main Features

- Hardware-backed MFA access controls
- Centralized authorization policies to control access
- 2FA and MFA options
- YubiKey used as smart card

GDPR

The General Data Protection Regulation (GDPR) came into effect in 2018, mandating data protection and privacy standards for organizations that deliver goods or services (including financial services) to EU citizens. GDPR fines are among the most severe—4% of global annual turnover or €20 million, whichever is higher.[37]

GDPR requirement	Section	YubiKey capabilities
Data protection impact assessment	Article 35	• Hardware-backed MFA access controls • Centralized authorization policies to control access • Multi-factor cryptographic device
Security of processing	Article 32	
Data protection by design and by default	Article 25	

U.S. executive order on improving the Nation's cybersecurity (EO)

> Having strong authentication is a foundational security component of a Zero Trust architecture. Yubico and YubiKeys help fill the gap, for example, where weak passwords have been used, by providing validated, phishing-resistant security keys.
>
> **–John Kindervag, Creator of Zero Trust**

The recent number of attacks on critical systems has triggered increased regulatory pressure from the U.S. Federal government. On May 12 2021, the Biden administration issued an Executive Order 14028 on "Improving the Nation's Cybersecurity."[38]

This new order requires agencies and organizations in the public and private sector who work with the government, including financial services. The order includes the requirement to adopt Zero Trust frameworks within 60 days, as well as multi-factor authentication and encryption for data at rest and in flight within 180 days.[39] OMB Memo 21-30 further amended EO 14028 to require a phased integration of NIST standards, including impersonation-resistant MFA.[40] Any authenticator that involves manual entry of an authentication output is not considered impersonation resistant, according to NIST SP 800-63.

The Zero Trust emphasis in the order demonstrates the high priority status the government is placing on modernizing agencies' infrastructure. Strong, modern authenticators, like the YubiKey, will be essential to reaching Zero Trust goals while providing a low-friction and secure user experience.

Main Features

- Hardware-backed MFA access controls
- YubiKey used as smart card
- Centralized authorization policies to control access

CCPA, 23 NYCRR 500 & other state laws

The California Consumer Privacy Act (CCPA) was the first US-based data privacy bill to adopt stringent measures in line with the GDPR. Followed by the California Privacy Right Act (2023) amendment, which introduces even more requirements, other states are following suit, including the recent Virginia Consumer Data Protection Act (CDPA), which comes into effect January 1, 2023.[41]

These regulations require financial institutions to implement "appropriate" and "reasonable" precautions to protect and secure data.[42]

Main features

Hardware-backed MFA access controls

- Something you know PIN (FIDO2, PIV, CAC)
- Something you have (Private key stored on the YubiKey)

Support password / PIN for MFA (FIDO U2F, FIDO2 or OTP)

> Authentication is key to securing computer systems and is usually the very first step in using a remote service or facility, and performing access control.
>
> **–ENISA**[43]

EU Cybersecurity Act & framework (in development)

The EU Cybersecurity Act strengthens the EU Network and Information Systems Agency (ENISA), transitioning the agency to become the new EU Agency for Cybersecurity to establish a cybersecurity certification framework and to oversee assessment.[44] ENISA reports previously established 2FA as a base standard, with the new Act underscoring the importance of promoting "basic multi-factor authentication" (Section 40).[45]

"Authentication is key to securing computer systems and is usually the very first step in using a remote service or facility, and performing access control." –ENISA[46]

The Act requires ENISA to create an ICT framework to "protect the availability, authenticity, integrity and confidentiality" of data. The framework is still in development.

U.S. Consumer Financial Protection Bureau: Consumer Financial Protection Circular 2022-04

The August 11, 2022 Consumer Financial Protection Circular 2022-04 covers guidance on whether entities can violate the prohibition on unfair acts or practices in the Consumer Financial Protection Act (CFPA) when they have insufficient data protection or information security.

The circular states that inadequate authentication, password management, or software update policies or practices are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers, and financial institutions are unlikely to successfully justify weak data security practices based on countervailing benefits to consumers or competition.

If a covered person or service provider does not require MFA for its employees or offer multi-factor authentication as an option for consumers accessing systems and accounts, or has not implemented a reasonably secure equivalent, it is unlikely that the entity could demonstrate that countervailing benefits to consumers or competition outweigh the potential harms, thus triggering liability.

MFA solutions that protect against credential phishing, such as those using the Web Authentication standard supported by web browsers, are especially important.[47]

DORA (draft)

The Digital Operational Resilience Act (DORA) is a draft regulation in the EU to support digital finance with appropriate safeguards.[48] The proposed regulation proposes that financial entities adopt an ICT risk management framework that includes several requirements in Article 8, Protection and Prevention, including the following provision:

"Implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated controls systems to prevent access to cryptographic keys whereby data is encrypted based on results of approved data classification and risk assessment processes."[49]

DORA is most likely to refer to the elements of the NIST Cybersecurity Framework, which are:

Standard	NIST SP | FIPS	YubiKey capabilities	YubiKey certification level
Digital identity guidelines define authenticator assurance level (AAL)	SP 800-63	• Multiple-protocol support OTP, OATH, HOTP, U2F, PIV, Open PGP • 2FA and MFA options • Multi-factor cryptographic device • Hardware-based authenticator • Touch-button test of user presence	AAL3
Guidelines for the protection of controlled unclassified information	SP 800-171	• Hardware-backed MFA access controls • YubiKey used as smart card • Centralized authorization policies to control access	
Security and privacy controls for information systems and organizations	SP 800-53	• YubiKey used as smart card • Centralized authorization policies to control access	
Security requirements for cryptographic modules	FIPS 140-2	• Cryptographic module supports multiple protocols • YubiKey used as smart card • Touch-button test of user presence • Time or hash-based synchronous OTP • FIDO U2F	• Overall Level 1 #3907 • Overall Level 2 #3914 • Physical Security Level 3 #3517

YubiKeys offer a bridge to passwordless for Financial Services

With the YubiKey, financial services organizations can implement FIDO2 passwordless, smart card passwordless or a hybrid strategy, depending on the infrastructure and use cases that need to be addressed. As the passwordless ecosystem continues to expand, YubiKeys are perfectly designed to help financial organizations bridge the transitory period from legacy MFA to passwordless MFA. YubiKeys uniquely support a broad range of authentication protocols, enabling a single security key to work across a wide range of applications and services, regardless of where financial services organizations are in their strong authentication and passwordless journey.

Take a stand against cyber attacks and future-proof your compliance stance with the YubiKey.

The YubiKey 5 Series

From left to right: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano

The YubiKey 5 FIPS Series

From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS

YubiKey Bio Series - FIDO Edition

From left to right: YubiKey Bio - FIDO Edition, YubiKey C Bio - FIDO Edition

The YubiHSM 2 Series

From left to right: YubiHSM 2 and YubiHSM 2 FIPS

Summary

Today's financial institutions are faced with a consumer whose faith and commitment has been shaken by a global pandemic, social unrest, economic uncertainty, and rising fears about fraud. Faced with increasing cyber attacks, a solid bedrock of authentication provides much more than regulatory compliance–it provides a competitive advantage and peace of mind.

Financial institutions looking to grow and support their customer base are working to fast track secure easy-to-use authentication to ensure that remote workers are securely connecting to networks and that cloud-hosted services do not leave open doorways for cyber criminals to exploit.

Customer trust and loyalty are the product of exceeding customer expectations at every interaction. YubiKeys can be extended to customers to provide strong 2FA and MFA authentication for digital transactions without the requirement for a smartphone or the risks associated with mobile authentication.

If you are a forward-thinking financial institution looking for a competitive differentiator, contact us.

Yubico Inc.

530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088

https://www.yubico.com

Sources

[1] Varonis, 2021 Data Risk Report: Financial Services, (Accessed May 13, 2021), https://info.varonis.com/hubfs/docs/research_reports/2021-Financial-Data-Risk-Report.pdf?utm_content=146358482&utm_medium=social&utm_source=twitter&hss_channel=tw-21672993

[2] BIS, Covid-19 and cyber risk in the financial sector, (January 14, 2021), https://www.bis.org/publ/bisbull37.pdf

[3] BIS, Covid-19 and cyber risk in the financial sector, (January 14, 2021), https://www.bis.org/publ/bisbull37.pdf

[4] ITRC, The Impact of Cybersecurity Incidents on Financial Institutions, (2018), https://cdn2.hubspot.net/hubfs/524149/Content%20Map%20Files/Whitepapers%20and%20Infographics/The%20Impact%20of%20Cyber-security%20Incidents%20on%20Financial%20Institutions%20Whitepaper.pdf

[5] BAI, BAI Banking Outlook: The Widespread Fear of Fraud, (Accessed June 7, 2021), https://www.bai.org/research/bai-banking-outlook/the-state-of-fraud-in-financial-services/

[6] IBM, 2022 Cost of Data Breach Report, https://www.ibm.com/security/data-breach

[7] VMware, Global Threat Report, (Accessed May 17, 2021), https://www.carbonblack.com/resources/global-threat-report-extended-enterprise-under-attack/

[8] VMware, Modern Bank Heists, (May 14, 2020), https://www.businesswire.com/news/home/20200514005258/en/

[9] Varonis, 2021 Data Risk Report: Financial Services, (Accessed May 13, 2021), https://info.varonis.com/hubfs/docs/research_reports/2021-Financial-Data-Risk-Report.pdf?utm_content=146358482&utm_medium=social&utm_source=twitter&hss_channel=tw-21672993

[10] VMware, Global Threat Report, (Accessed May 17, 2021), https://www.carbonblack.com/resources/global-threat-report-extended-enterprise-under-attack/

[11] Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

[12] Varonis, 2021 Data Risk Report: Financial Services, (Accessed May 13, 2021), https://info.varonis.com/hubfs/docs/research_reports/2021-Financial-Data-Risk-Report.pdf?utm_content=146358482&utm_medium=social&utm_source=twitter&hss_channel=tw-21672993

[13] Joseph Cox, The Booming Underground Market for Bots That Steal Your 2FA Codes, (November 2, 2021), https://www.vice.com/en/article/y3vz5k/booming-underground-market-bots-2fa-otp-paypal-amazon-bank-apple-venmo

[14] Joseph Cox, The Booming Underground Market for Bots That Steal Your 2FA Codes, (November 2, 2021), https://www.vice.com/en/article/y3vz5k/booming-underground-market-bots-2fa-otp-paypal-amazon-bank-apple-venmo

[15] Neal Semikin, What financial services should learn from the SolarWinds cyber attack, (February 18, 2021), https://www.consultancy.uk/news/26997/what-financial-services-should-learn-from-the-solarwinds-cyber-attack

[16] Jon Porter, White House now says 100 companies hit by SolarWinds hack, but more may be impacted, (February 18, 2021), https://www.theverge.com/2021/2/18/22288961/solarwinds-hack-100-companies-9-federal-agencies

[17] VMware, Global Threat Report, (Accessed May 17, 2021), https://www.carbonblack.com/resources/global-threat-report-extended-enterprise-under-attack/

[18] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019), https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[19] Cisco, Security Outcomes Study: Financial Services Sector (Accessed May 14, 2021), https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-outcomes-study-fs-industry-mini-report.pdf

[20] PCI SSC, PCI DSS v3.2.1 Quick Reference Guide, (July 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

[21] PCI SSC, Information Supplement Multi-Factor Authentication v1.0, (February 2017), https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf

[22] Lindsay Goodspeed, PCI DSS v4.0 Timeline Update to Support an Additional RFC, (February 27, 2021), https://blog.pcisecuritystandards.org/pci-dss-v4.0-timeline-updated-to-support-an-additional-rfc

[23] Ian Terry, PCI DSS 4.0: What Changes Can We Expect, (April 8, 2021), https://www.ispartnersllc.com/blog/pci-dss-version-4-0-launching-2020/

[24] US Government Printing Office, Gramm-Leach-Bliley Act, (Accessed June 7, 2021), https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm

[25] 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), https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial

[26] IFTC, 16 CFR Part 314 Final Rule, (Retrieved November 5, 2021), https://www.ftc.gov/system/files/documents/federal_register_notices/2021/10/safeguards_rule_final.pdf

[27] FFIEC, Information Security, (Accessed June 9, 2021), https://ithandbook.ffiec.gov/it-booklets/information-security.aspx

[28] FFIEC, Authentication in an Internet Banking Environment, (August 8, 2001), https://www.ffiec.gov/pdf/authentication_guidance.pdf

[29] FDIC, Consumer Compliance Examination Manual, (June 2019), https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/7/vii-4-1.pdf

[30] European Parliament and the Council of the EU, Directive 2015/2366, (November 25, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

[31] EBA, Opinion on the elements of strong customer authentication under PSD2, (June 21, 2019), https://eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2

[32] Official Journal of the European Union, Regulation (EU) No 910/2014, (July 23, 2014), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[33] European Commission, Commission proposes a trusted and secure Digital Identity for all Europeans, (June 3, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

[34] FIDO Alliance, Using FIDO with eIDAS Services, (April 2020), https://fidoalliance.org/wp-content/uploads/2020/04/FIDO-deploying-FIDO2-eIDAS-QTSPs-eID-schemes-white-paper.pdf

[35] Public Law 107-204, Sarbanes Oxley Act of 2002, (July 30, 2002), https://pcaobus.org/About/History/Documents/PDFs/Sarbanes_Oxley_Act_of_2002.pdf

[36] AICPA, Trust Services Criteria, (Accessed June 8, 2021), https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

[37] European Commission, Data Protection, (Accessed June 10, 2021), https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

[38] The White House, Executive order on Improving the Nation's Cybersecurity, (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[39] David Treece, Quick Take: Executive Order on Improving the Nation's Cybersecurity, (May 13, 2021), https://www.yubico.com/blog/quick-take-executive-order-on-improving-the-nations-cybersecurity/

[40] NIST, Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028, (July 19, 2021), https://www.nist.gov/system/files/documents/2021/07/09/Critical%20Software%20Use%20Security%20Measures%20Guidance.pdf

[41] Moritt Hock & Hamroff LLP, Virginia Becomes the Second State to Pass a Comprehensive Privacy Law, (March 24, 2021), https://www.jdsupra.com/legalnews/virginia-becomes-the-second-state-to-2607391/

[42] Intersoft Consulting, General Data Protection Regulation, (Accessed May 19, 2021), https://gdpr-info.eu/art-32-gdpr/; National Law Review, CPRA Security Risk Assessments & Privacy Compliance, (November 6, 2020), https://www.natlawreview.com/article/cpra-security-risk-assessments-privacy-compliance

[43] ENISA, Privacy and Data Protection by Design - from policy to engineering, (December 2014), https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

[44] European Commission, The EU Cybersecurity Act, (Accessed June 9, 2021), https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[45] ENISA, Authentication Methods, (Accessed May 20, 2021), https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods; European Commission, The EU Cybersecurity Act, (Accessed June 9, 2021), https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[46] ENISA, Privacy and Data Protection by Design - from policy to engineering, (December 2014), https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

[47] Consumer Financial Protection Bureau, Consumer Financial Protection Circular 2022-04, https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/

[48] European Commission, Proposal for a Regulation of the European Parliament and of the Council, (2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&rid=10

[49] European Commission, Proposal for a Regulation of the European Parliament and of the Council, (2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&rid=10

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.