yubico

WHITE PAPER

Drive competitive advantage with modern strong authentication for Online and Mobile Banking

Contents

Authentication in Mobile and Online Banking

Meeting the demands of today's shifting risk and competitive landscape

The digitization of financial services accelerated since 2020. Driven by the COVID-19 global pandemic, mobile banking penetration grew across all demographics, up to at least 85% for all consumers under age 55.[1] However, while mobile and online banking adoption have been on the rise, so too have consumer fears about fraud and cyber crime. Between 30% and 40% of mobile banking users consider themselves "very" concerned about fraudulent activities, including identity theft, credential theft, or loss of funds.[2]

Combined with economic unrest, the global pandemic, increased competition, and the accelerated shift to digital channels, financial institutions are being challenged to create frictionless and secure digital experiences in order to attract—and retain—customers.

Most financial institutions today rely on a combination of username and password, security questions, or two-factor authentication one-time passcodes or one-time passwords (OTP and TOTP) sent by email, SMS or authenticator app for online and mobile banking authentication. While these options get progressively more secure, each is still vulnerable to cyber attacks—and each is a contributor to friction in the customer experience.

Different types of banking lend different risks to customers if strong authentication for online and mobile banking isn't deployed:

Commercial banking

Commercial banking customers, large or small, are typically dealing with credit products and investment services. While U.S. federal law requires banks to refund customers if someone takes money from their account without authorization and they notify the bank within 60 days of the transactions appearing on their bank statement, business accounts, however, have fewer protections and could be subject to greater losses.

Retail banking

For retail banking accounts, the Federal Deposit Insurance Coverage (FDIC) is automatic whenever a deposit account is opened at an FDIC-insured bank or financial institution but is only restricted to $250,000 per depositor, per insured bank, for account ownership categories. If a checking or savings account is hacked, banks typically cover those losses. Still, customers may have to jump through some hoops to get their money back. A bank could claim that a customer failed to take proper precautions, giving out their password or clicking on a phishing email, for example, and the customer may not be reimbursed.[3]

Investment banking

The FDIC doesn't insure investments like mutual funds, annuities, stocks, bonds or securities that banks may offer, making high security a must for these types of customer accounts. Additionally many customers don't login to their investment and retirement accounts as frequently as their checking and savings accounts, making it difficult to spot and stop any fraudulent activity.

Many of the worlds' largest financial institutions, including Vanguard and Morgan Stanley, are already making the switch to FIDO-based authentication for increased security, resilience against attacks, and a modern seamless customer experience.

The growing cyber crime threat, and the drawbacks of legacy authentication

$5.97 Million

cost of a data breach in financial services

The average cost of a data breach in financial services is $5.97 million in 2022, up from $5.72 million in 2021, and increase of 4.4%.[4]

Following the increased adoption of mobile banking, the FBI issued a consumer warning about an increase in malicious attacks targeting mobile banking apps.[5] The pandemic also triggered a significant rise in phishing and malware attacks that can inadvertently lead to fraud.[6] Consumer fear of fraud is increasing across the board, with phishing and supply chain scams among the top concerns.[7]

While the FDIC covers a certain level of fraud protection, the true cost of these rising attacks and data breaches is the loss of consumer trust. And that trust has a direct link to customer acquisition and retention—important figures when we are considering the lifetime value of each potential financial services customer. In fact, 76% of consumers report the most important factor when choosing a financial services account is security and privacy.[8]

Meeting the CX demands of today

The adoption of mobile and online banking has accelerated during the pandemic, reaching 95% of Gen Z (18-25), 91% of Millenials (26-40), 85% of Gen X (42-55) and 60% of Baby Boomers (56-75), whose adoption jumped by from 42% just one year prior.[9]

Percentage adoption by generation

95%

of Gen Z (18-25)

91 %

of Millenials (26-40)

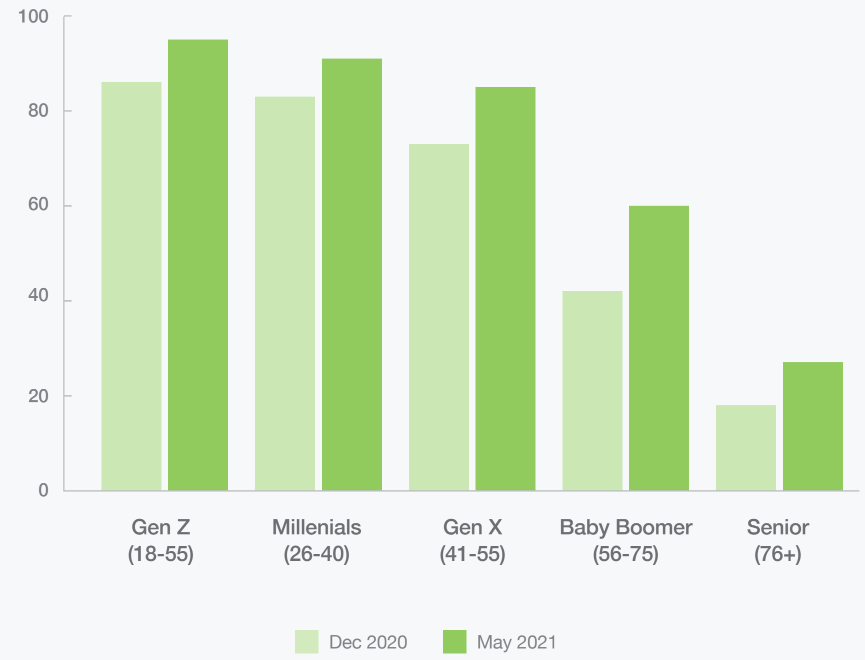
85%

of Gen X (42-55)

60%

of Baby Boomers (56-75)

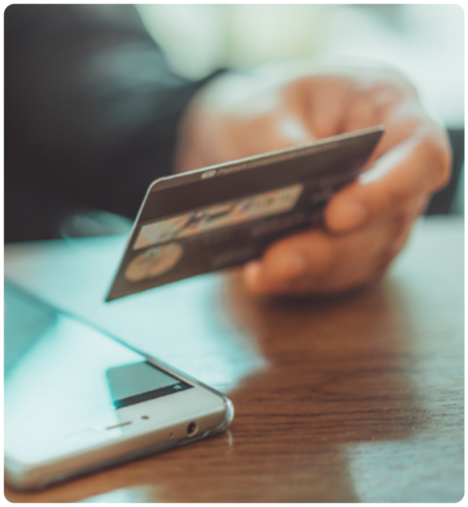
Mobile Banking adoption by generation



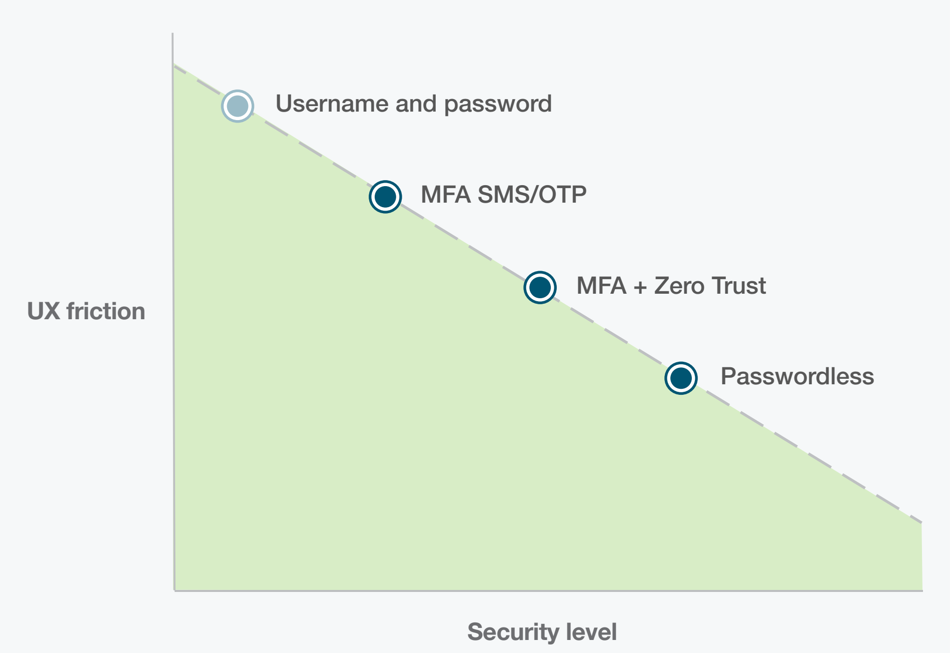
The high rates of online and mobile banking penetration are balanced against increasing competition from traditional and online-only financial service providers, as well as consumer expectations influenced by non-bank experiences. While financial customers have historically been slow to change financial service providers, new financial service options with a low barrier to entry are attracting away traditional banking customers. New battlegrounds on customer acquisition, relationship building, and retention are focusing on an understanding of consumer expectations and the customer experience CX.

Acquisition and loyalty in financial services hinge on concepts such as trust, security, convenience, and personalization. Before you even get to the bells and whistles of digital experiences associated with online and mobile banking (AI, real-time alerts), every experience starts in the same place: with authentication.

Current mobile and online banking authentication creates friction in the user experience. Passwords and answers to security questions can be forgotten, and SMS/OTP codes can be delayed or missed. In addition to offering low security, these can add considerable friction (both time and frustration) to the customer experience.

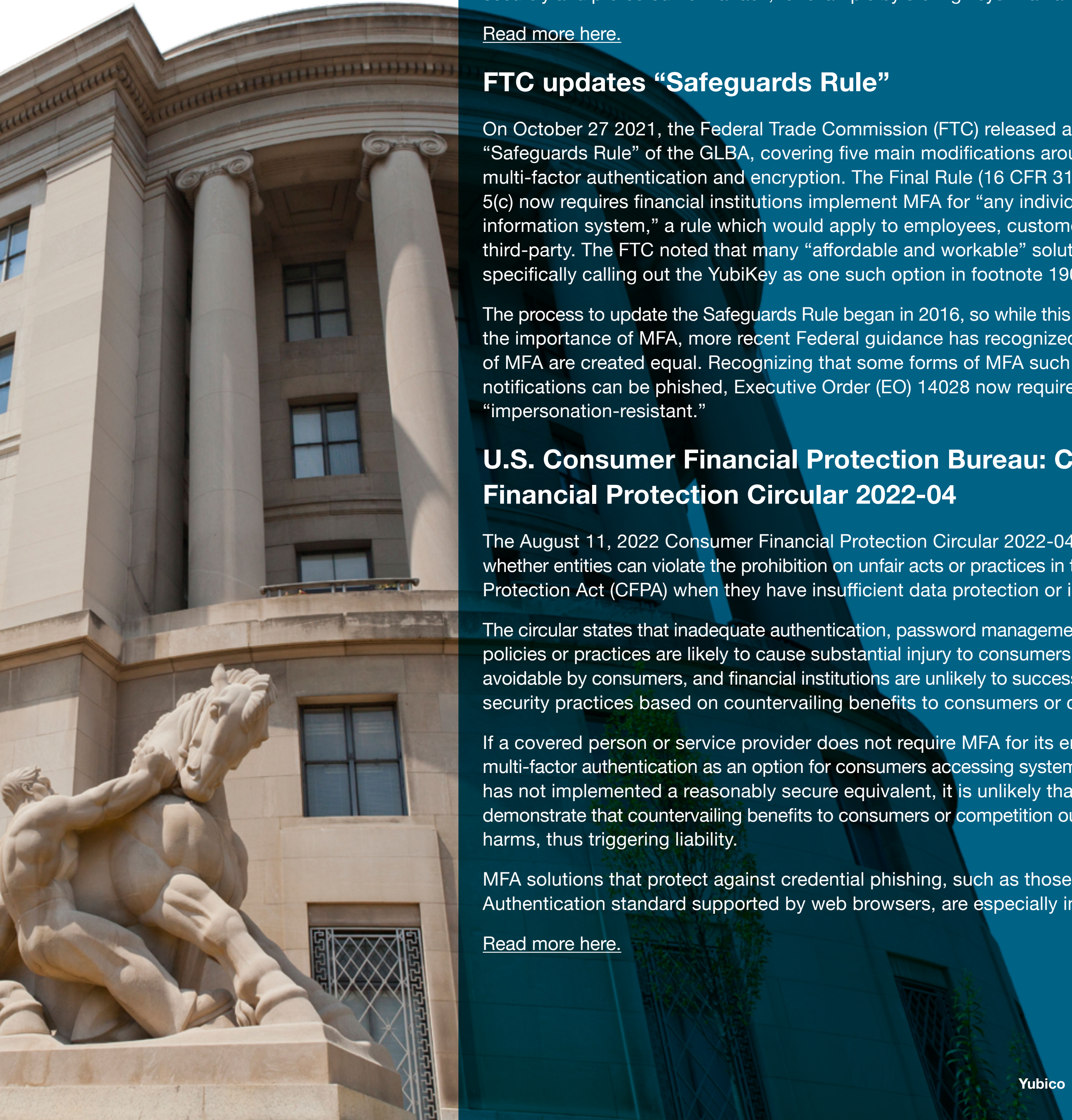


Road to FIDO passwordless



Financial institutions investing in digital transformation have historically seen a high ROI, particularly when those investments have focused on customer experience and efficiency. FIDO-based authentication can replace the friction associated with passwords, including the option for a tap-and-go passwordless experience with the highest levels of security protection against account takeovers.

For today’s financial consumers, strong multi-factor and passwordless authentication is not just a nice-to-have element to prevent fraud or to convey trust, it is an essential part of the customer experience.



EVOLVING REGULATORY LANDSCAPE

FFIEC issues guidance on authentication and access to financial institution services and systems

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 factors 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.

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. 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. The FTC noted that many “affordable and workable” solutions to MFA exist, specifically calling out the YubiKey as one such option in footnote 190.

The process to update the Safeguards Rule began in 2016, so 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 some forms of MFA such as OTP and push notifications can be phished, Executive Order (EO) 14028 now requires MFA that is “impersonation-resistant.”

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.

Read more here.

FIDO authentication for Financial Services

What is the difference between FIDO U2F and FIDO2?

U2F was developed by Yubico and Google, and contributed to the FIDO Alliance after it was successfully deployed for Google employees. The protocol is designed to act as a second factor to strengthen existing username/password-based login flows. It's built on Yubico's invention of a scalable public-key model in which a new key pair is generated for each service and an unlimited number of services can be supported, all while maintaining full separation between them to preserve privacy.

Essentially, FIDO2 is the passwordless evolution of FIDO U2F. The overall objective for FIDO2 is to provide an extended set of functionality to cover additional use-cases, with the main driver being passwordless login flows. The U2F model is still the basis for FIDO2 and compatibility for existing U2F deployments is provided in the FIDO2 specs.

FIDO (Fast IDentity Online) is a modern authentication standard that replaces traditional username and password with strong two-factor, multi-factor, and passwordless authentication. The FIDO standard was created by the FIDO Alliance, an open industry association whose mission is to reduce the reliance on passwords.

To date, the FIDO Alliance has released three sets of specifications for stronger authentication including FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF), and FIDO2, which includes the W3C's Web Authentication (WebAuthn) specification and FIDO Client to Authenticator Protocol (CTAP).

WebAuthn

WebAuthn is an API that makes it easy for a relying party (web service, mobile app) to integrate strong authentication into applications using support built into all leading browsers and platforms.

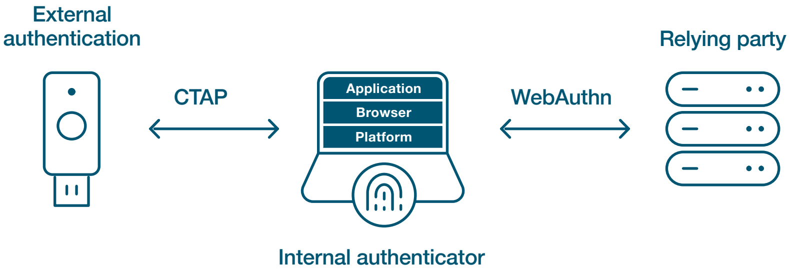
Leveraging WebAuthn, web services can offer their users strong authentication with a choice of authenticators, including internal device authenticators (PIN, biometric, voice recognition) and external authenticators (hardware security keys). Users can register multiple authenticators, with WebAuthn making it easy to recover access to accounts when devices are lost or stolen.

By replacing passwords with strong authentication based on public key cryptography, in which the private key never leaves the user's device, WebAuthn makes authentication both easier to use and more secure, benefitting users and service providers alike.

WebAuthn was developed under the umbrella of the World Wide Web Consortium (W3C). Yubico, along with Microsoft and Google, is a leading contributor to WebAuthn and the W3C.

CTAP

The FIDO2 Client to Authenticator Protocol (CTAP) is a standard that defines how the client communicates with an external and portable authenticator (hardware security key, mobile device).



Mobile & online use cases for FIDO authentication

FIDO2 and WebAuthn open the door to a streamlined, more secure experience with a broad range of choices for authentication—everything from scanning a fingerprint to tapping a button on a hardware security key for a truly passwordless experience across a variety of use cases.

User registration

In this example, our user Sarah wants to create an account for an online banking website. Instead of entering both a username and password, she simply enters a username. In response, she is offered a choice of WebAuthn standard strong authentication methods including:

- Using an internal authenticator and either entering a PIN, a fingerprint scan, a facial scan, or voice recognition
- Using an external authenticator by inserting and tapping a hardware security key. The hardware security key can be protected with a PIN so that the user will have to enter a PIN while authenticating rather than simply tapping the key.

Taking any of these actions creates an authentication credential, which Sarah's WebAuthn-compliant browser or platform then submits to the website, where it will be bound to her newly created account. Best practice would suggest that Sarah register her hardware security key first, ensuring a portable root of trust in case her device used with an internal authenticator is ever lost or stolen.

Sarah creates her secure account in less than a minute with no friction over password length or complexity, security questions, or delayed OTP/SMS codes.

Sarah creates her secure account in less than a minute with no friction over password length or complexity, security questions, or delayed OTP/SMS codes.

User authentication

The next day Sarah wants to check her bank balance, so she simply enters her username and is prompted to insert and tap her security key, proving the login comes directly from her. The authentication process is frictionless and secure, with no delays, multiple screens, password errors, or resets.

Step-up authentication

Sarah's online banking website has a policy that re

quires users to re-authenticate when performing high-value, sensitive transactions. For added security, many similar financial institutions require customers to use an external security key for high value transactions.

In this case, Sarah logs into her account to transfer $5,000. During transfer initiation, Sarah is prompted for her external security key, which she connects and taps. The transaction proceeds.

Account recovery

By enabling users to register multiple authenticators for each website, service or application, WebAuthn makes it easy for users to recover access to accounts when devices are lost or stolen. With WebAuthn, a user can choose to use an internal device authentication and an external authenticator or account access in case the primary device is not available. Additionally the user can also set up two external authenticators such as hardware security keys, a primary and a backup.

FIDO2 strong authentication with YubiKey

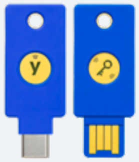
The solution

YubiKey is the **only** solution that is proven to stop 100% of account takeovers in independent research.[10]

The YubiKey 5 Series

Multi-protocol support for FIDO2, U2F, Smart card, OTP, and OpenPGP

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



The Security Key Series

Multi-protocol support for FIDO2, U2F, Smart card, OTP, and OpenPGP

From left to right: Security Key C NFC, Security Key NFC.

The YubiKey is a hardware security key, manufactured by Yubico, that offers easy-to-use two-factor, multi-factor, and passwordless authentication at scale. Available in a variety of options, the YubiKey offers a portable root of trust that can be used across a variety of devices.

Single Factor (Passwordless)

Use of the security key on its own as a strong first factor of authentication, requiring only the possession of the device, allowing for a tap and go passwordless experience

Two Factor (Password + Authenticator)

Use of the security key as a second factor in a two-factor authentication solution

Multi-Factor (Passwordless + PIN or Biometric)

Use of the security key for multi-factor authentication requiring possession of the device AND a PIN or Biometric, to solve high assurance requirements

A single YubiKey supports multiple authentication protocols including Smart Card, One Time Passcode, FIDO U2F, and FIDO2, 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.

With the YubiKey, financial institutions can:

- Stop account takeovers and SIM swapping and prevent man-in-the-middle (MitM) attacks with superior hardware cryptographic security
- Provide unmatched simplicity for users with 4x faster logins that ensure proof of presence and possession
- Reduce customer 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
- Comply with existing and emerging regulations such as FFIEC, SOX, PSD2, PCI, FIPS, and GDPR

The YubiKey enables strong verification of users before providing access to sensitive and PII data, keeping financial services organizations compliant with existing and emerging regulations. YubiKeys are FIPS 140-2 certified (Certificate #3517) Overall Level 2, Physical Security Level 3.

How financial services institutions can get started

> MFA is critical, but not all MFA methods are created equal. The most secure form of MFA is a physical security key, or hardware MFA, involving a USB keythat is plugged into a computer to authenticate users.
>
> **–New York Department of Financial Services, *Twitter Investigation Report*, October 2020**

Recognizing the challenges of digital transformation for financial services, including legacy technology and outsourced services, Yubico has worked with leading financial institutions on a phased approach to deployment that offers flexibility regardless of where organizations are in their strong authentication and passwordless journey.

If you outsource any of these services, talk to your financial services provider about what options you have for strong authentication with YubiKey.

Phased approach to YubiKey deployment

Step 1. Enterprise

Strengthen authentication internally enterprise-wide. A risk-based approach often begins with call centers, privileged users, users that perform high-risk, high-value transactions, and remote or hybrid workers.

Step 2. Hardware-backed TOTP

Strengthen existing TOTP processes by replacing insecure SMS authentication with the Yubico hardware-backed authenticator to generate the TOTP.

Step 3. Online & mobile banking customers

Provision and deploy YubiKeys to customer segments in a phased approach: commercial customers, high net-worth customers, investment customers, frequent mobile customers, then all retail mobile and online customers.

Enterprise deployment

A good place to start on enterprise deployment within financial institutions is within call centers, followed by other risk-based deployments to remote, privileged users, or to support high-risk, high-value transactions.

- **Call centers** can deploy YubiKeys to deliver stronger security that can securely verify the identity of call center agents before they are given access to PII and other sensitive data, or make any changes to a customer account, such as raising a credit limit. For additional details, read the white paper: Essentials for enabling strong authentication in financial services call centers.
- Requiring **privileged users** (network and database administrators, security and systems administrators, application developers, and C-suite employees) and employees that provide **high-risk, high-value transactions** to authenticate or step-up authenticate with phishing-resistant hardware security keys to securely access services and applications will help stop targeted attacks and prevent account takeovers
- Minimize the risk of **remote work** and **shared access terminals** or workstations with a hardware security key like the YubiKey, which is both faster and more secure than traditional authentication.

Deployment of YubiKeys to employees is very quick and cost-effective: YubiKeys can be sent to a central branch or office location, or even directly to each employee, including remote employees. To learn more, read our whitepaper: Getting started with strong authentication in financial services.

OTP—One-time password

Passwords or passcodes that are valid for only one login session or transaction. OTP can be accessed through an app, SMS message, email, or hardware key.

TOTP—Time based one-time password

A OTP where time is a part of the uniqueness. The TOTP must be used within the given timeframe.

TOTP-based hardware-backed authentication

For financial services organizations already on the road to passwordless by using TOTP-based authentication, the next step is replacing insecure mobile-based authentication methods such as SMS or authenticator apps.

OTP and TOTP codes sent via email and SMS are vulnerable to cyber attack and are a source of CX friction. Many common authenticator apps store credentials within the mobile device app, introducing another element of risk.

Similar to other authenticator apps, the Yubico Authenticator generates a one-time code used to verify identity to log into various services. However, unlike other authenticator apps, the secrets are stored in the YubiKey rather than in the app itself, making it necessary for a user's YubiKey to be physically present to receive the time-based codes. Secrets cannot be stolen from the hardware key.

The Yubico Authenticator can secure all services currently compatible with other authenticator apps, including Google Authenticator.

Online & mobile banking customers

While many leading financial services organizations are adopting YubiKeys for enterprise MFA on their journey to passwordless, we recognize the external and internal hurdles to online and mobile-based deployment. As the growing industry competition and changing consumer expectations have demonstrated, it is no longer a question of if financial services customers will demand hardware-based security, it's a question of when. And with that question comes the opportunity for significant market advantage to those leaders provisioning and deploying YubiKeys to key customer segments, including:

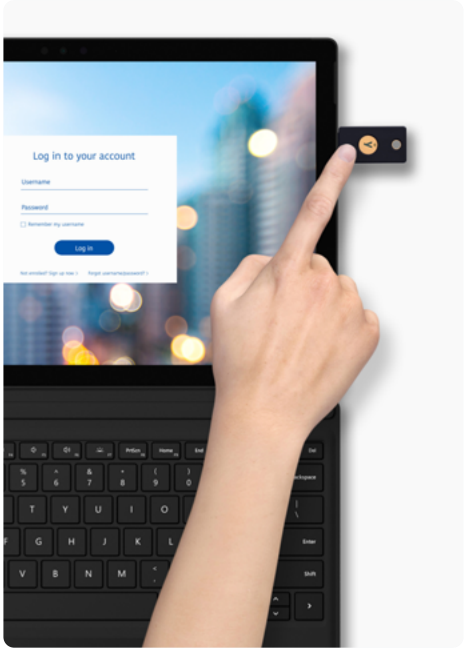
- Commercial banking customers
- High net-worth customers
- Tech savvy or frequent users of online and mobile banking
- Investment banking customers
- New users, to support conversion
- All online and mobile banking customers

Whether customers are interacting with online and mobile banking frequently, as is the case for commercial or retail customers, or are less frequent users such as investment banking customers, who want the benefit of impersonation-resistant MFA, YubiKeys offer a range of benefits.

YubiKeys can be customized with corporate branding to support marketing efforts, with streamlined enterprise delivery to over 30 countries across the USA, Canada and Europe.

Financial technology systems and platforms

Leading financial institutions rely on financial technology systems and platforms such as FiServe, FIS, Finastra and others, for many enterprise, banking and capital market solutions, including mobile and online banking. As leaders in customer and channel management, these partners are uniquely positioned to meet the growing demand for a secure omnichannel customer experience if inroads for security and CX are made with support for FIDO.



YubiKey rapid integration resources

Yubico provides open source code, developer tools, SDKs, and the Yubico Developer Program as resources for organizations implementing strong authentication. Visit the Developer site for more information on how to deliver rapid integration of hardware-based strong authentication.

Developers.yubico.com

Summary

The financial services industry is highly regulated and faced with the growing threat of targeted and costly cyber attacks. As a result, leading financial services organizations are already on the journey to implement FIDO2 passwordless across some or all enterprise use cases. And the growth of online and mobile banking, economic and competitive pressures, and the changing expectations of today's financial customer, has also created an urgent need for financial organizations to extend strong MFA and passwordless protections to downstream consumers.

Financial institutions offering retail, consumer, and investment banking services, and looking to grow and support their customer base, should work to fast track secure, easy-to-use authentication for digital banking and transactions As the passwordless ecosystem continues to expand, YubiKeys are perfectly designed to help financial organizations meet the regulatory and consumer demands of today—and tomorrow.

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

Sources

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

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

[3] USA Today, Jessica Menton, Banks, Bitcoin, bond funds: Where is your money safe in an era of cyberattacks?, (January 25, 2020)

[4] IBM Report, Cost of a data breach 2022

[5] FBI, Increased Use of Mobile Banking Apps Could Lead to Exploitation, (June 10, 2020)

[6] Kantor, Alice, Coronavirus triggers epidemic of cyber fraud, (April 14, 2021)

[7] BAI, BAI Banking Outlook: The Widespread Fear of Fraud, (Accessed June 7, 2021)

[8] TransUnion, TransUnion Global Fraud Solutions & Insights West survey, (Accessed August 4, 2021)

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

[10] BDO, Digital Transformation in Financial Services, (April 2019)

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.

© 2022 Yubico