yubico

OCTOBER 2021

Getting started with strong authentication in financial services

Best practices for implementing the YubiKey for fast, easy and strong authentication

Introduction

The financial services industry is one of the highest value targets for cyber criminals due to its massive store of financial and personally identifiable information (PII), and the potential for quick payoffs through fraudulent money transfers. The 2019 Financial Breach Report: The Financial Matrix found that while financial services organizations accounted for just 6% of breaches in 2019, more than 60% of all leaked records in 2019 were exposed by this industry[1].

As passwords are easily breached, financial services organizations can no longer rely on username and passwords for employee authentication to systems and applications. Stronger authentication in the form of two-factor authentication (2FA) or multi-factor authentication (MFA) is required to stop account takeovers and to help eliminate cyber-attack driven fraud.

Usernames and passwords create security risks

Passwords were the most commonly used form of authentication today, but were also the weakest link in enterprise security as they are susceptible to an array of attack vectors: phishing and social engineering, password spray, brute force, credential stuffing, key logging, etc. Financial services organizations relying on passwords expose a large and easy-to-exploit threat surface. According to the 2019 Forrester Analytics Global Business Technographics® Security Survey, 27% of breaches are carried out using lost or stolen credentials and 18% are carried out as phishing attacks[2].

Password fatigue leads to data breaches

Users grow tired of creating new passwords for different services and changing passwords every few months. Many users end up relying on simplistic passwords which are easy to crack, or reuse passwords across personal and professional accounts, where breach of one account results in breach of another. The 2020 State of Password and Authentication Security Behaviors Report found that individuals reuse passwords across an average of 16 workplace accounts and IT security respondents reuse passwords across an average of 12 workplace accounts[3].

Phishing attacks target credential theft

Phishing continues to be a massive security problem as attack techniques continue to evolve. The 2019 Verizon Data Breach Investigations Report states that 32% of breaches involved phishing, and email was the primary delivery phishing method, 96.8%, in the finance industry[4]. Cyber criminals send fake email messages urging users to re-enter credentials which are then harvested for account takeovers. Many phishing attacks also lead to the installation of malware, to help perpetrate a breach. Even if users set up complex passwords, hackers can easily gain access to them through phishing attacks.

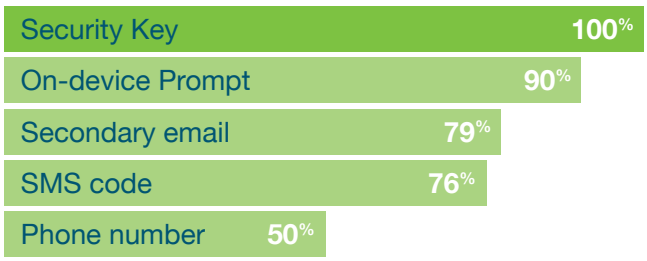
Not all MFA is equal

Many strong authentication tools and techniques exist to augment or replace passwords. While replacing passwords (going passwordless) should be the end goal for all organizations, financial services organizations can get started by strengthening authentication security to 2FA or MFA.

While MFA in the form of security questions, SMS codes, and OTP are prevalent, these methods offer little to no protection against account takeovers, phishing, malware, and man-in-the-middle attacks. Requiring mobile-based authentication can also make companies liable for employee mobile related costs.

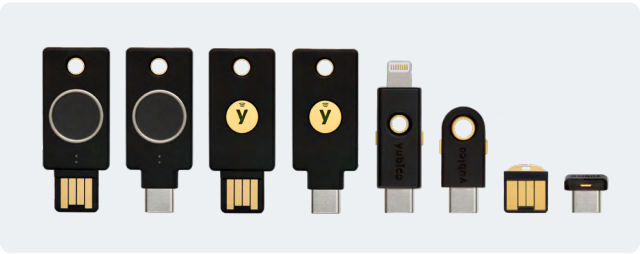
Hardware security keys such as the YubiKey, offer a modern, secure, and cost-effective alternative for protecting digital accounts against phishing and account takeovers. YubiKeys have been proven to offer the highest levels of security against account takeovers in independent research, preventing targeted attacks, and many of the worlds' largest financial institutions use YubiKeys to secure their most important information, accounts, and applications.

Account Takeover Prevention Rates



Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks.

YubiKey Bio Series - FIDO Edition and YubiKey 5 Series



From left to right: YubiKey Bio USB-A, YubiKey Bio USB-C, YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano.

Benefits of the YubiKey for MFA

YubiKeys can be used for single factor authentication, 2FA, or MFA depending on the requirements of the organization. As a single factor (passwordless) YubiKeys can be used as a strong first factor of authentication, requiring only the possession of the key and allowing a tap and go passwordless experience. For second factor authentication (2FA), YubiKeys are used as a second factor in addition to a username and password combination, and for MFA, organizations can use YubiKeys for MFA requiring possession of the key and a PIN or biometric.

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

YubiKeys offer several benefits as a MFA solution:

Strong security

The YubiKey's open architecture and broad set of protocols (OTP, FIDO U2F, FIDO2, PIV) allow for rapid integration with new and existing systems—supporting over 1,000 apps out-of-the-box. By leveraging these modern authentication protocols, the YubiKey provides very strong multi-factor authentication. Additionally, the YubiKey stores a user's credential securely on the hardware form factor, ensuring it cannot be exfiltrated.

Ease of use

YubiKeys offer a frictionless user experience. Users login with a single touch or tap, which is 4 times faster than receiving and typing a code delivered by SMS, so less time is wasted logging into systems. Google did an extensive study and found that using YubiKeys decreased login time by nearly 50 percent compared to a mobile authenticator[5]. The more applications a user needs to log into, the more important this becomes.

Durable and reliable

YubiKeys are extremely durable. The keys do not require any batteries and work without cellular or internet access so they can be used in any environment—including internet and mobile-restricted environments. Additionally, unlike phones or authenticator apps, they do not need to be updated or charged.

Strong ROI

MFA setup can be done via self service and does not require an IT administrator. Deployment of keys to employees is very quick and cost-effective-keys can be sent to a central branch or office location, or even directly to each employee, including remote employees. YubiKeys are also proven to reduce password-reset related IT support calls by 92%, saving thousands of hours per year in help desk and support costs[6].

YubiKeys for MFA use cases

Meet compliance regulations and security audits

The financial services industry is highly regulated and several regulations mandate strong authentication including SOX, FIPS, GDPR, PCI and PSD2.

Financial services organizations can meet compliance regulations and security audits by deploying YubiKeys for strong MFA. 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. They are also FIPS 140-2 certified. Overall Level 1 (Certificate #3907) and Level 2 (Certificate #3914), Physical Security Level 3.

Protect privileged accounts

A privileged user is any employee that has higher authorization levels to access sensitive customer, company, or financial information. The vast majority of large security breaches involve the misuse or escalation of privileged credentials and gaining ready access to valuable information such as customer data, account numbers, credit card information and more—resulting in crippling consequences for the business.

Financial services organizations can strengthen privileged access management, and ensure MFA using YubiKeys for all privileged users including network and database administrators, security and systems administrators, application developers, C-suite employees, and employees in finance, accounting and human resources. Requiring privileged users to authenticate with phishing-resistant hardware security keys to securely access services and applications will help stop targeted attacks and prevent account takeovers.

Secure remote workers

Hackers are taking advantage of the rise in remote work with targeted phishing attacks. Advancements in technology make it possible for employees to work from anywhere, but also introduce a new set of challenges for IT. Unsecured wifi networks, unmanaged personal mobile devices, and phishing scams make it easy for cybercriminals to steal user credentials and difficult for IT teams to securely manage geographically dispersed teams.

Financial services organizations can develop business contingency plans that include protecting their remote workforces, so employees can securely access systems without introducing new risks and vulnerabilities. Enabling MFA should be one of the top requirements for a work from home policy. For highest-assurance MFA, hardware security keys like the YubiKey can be used with identity access management systems and identity providers to log into computers, secure VPN access, step up authentication for password managers, and even to securely generate one-time time-based passcodes. For additional details, read the white paper Strong Authentication to Support Remote and Hybrid Work in Financial Services.

Step-up authentication security for high-risk, high-value transactions

Employees that perform high-risk, high-value transactions on a daily basis are often the target of cybercriminals. MFA-resistant phishing, spear phishing, and business email compromise (BEC) use social engineering lures to trick employees to give up their account credentials, install malware or ransomware on their device, or pay a falsified but realistic invoice to the criminal's bank account.

Passwords are too easily guessed, brute-forced, breached, compromised, or even copied from a stick-ynote attached to a user's laptop/desktop. Access to high-risk systems can be strengthened by requiring strong and modern MFA using YubiKeys, to ensure only authorized account access and authorized high-value transactions.

Provide highest-assurance security for branch workers using shared access terminals

Employees who work on shared workstations are common in banks and call centers. Tellers move from one station to another and supervisors move to authorize transactions. Users in these environments are often part-time employees that are associated with high turnover and a minimal commitment to the organization, increasing the insider threat. Shared access terminals and workstations open up attack vectors to admin accounts through keystroke logging and pass-the-hash.

Financial services organizations can double down on security across shared access terminals and shared workstations, to prevent unauthorized access to high-value systems and resources. Authentication via usernames and passwords does not offer high security—passwords can be breached using keystroke logging. The YubiKey offers highest-assurance MFA security for shared terminals and workstations and offers a frictionless and easy user experience.

Protect confidential personal and financial information across call centers

In 2019, Aite Group interviewed 25 executives at 18 of the top 40 largest U.S. financial institutions, and found that 61% of fraud can be traced back to the contact center[7]. With high employee churn, seasonal peaks, and other challenging business dynamics, call center environments need a secure, yet simple approach to verify agent identities before providing access to critical systems and data.

Financial services 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. As mobile phones can capture images of customer and financial data such as account numbers, card expiration dates, and numerous other details that might violate customer privacy, YubiKeys offer a much more secure authentication solution. For additional details, read the white paper: Essentials for enabling strong authentication in financial services call centers.

Prevent fraud, account takeovers, and achieve strong authentication security with the YubiKey

The YubiKey offers a modern, highly secure, easy to use, and cost-effective approach to MFA to help financial services organizations prevent fraud and lost revenue. By providing only authorized MFA employee access to sensitive and PII data with the YubiKey, financial services organizations can stay compliant with existing and emerging regulations including SOX, PSD2, PCI, FIPS, and GDPR and mitigate cybersecurity risk and account takeover related fraud.

Learn more about how YubiKeys protect financial services organizations from cyber security threats.

1. 2019 Financial Breach Report: The Financial Matrix
2. 2019 Forrester Analytics Global Business Technographics® Security Survey
3. 2020 State of Password and Authentication Security Behaviors Report
4. 2019 Verizon Data Breach Investigations Report
5. Security Keys: Practical Cryptographic Second Factors for the Modern Web
6. Ibid
7. https://www.pindrop.com/blog/61-of-fraud-traced-back-to-the-contact-center/

yubico

About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.