yubico

Strong authentication to mitigate cybersecurity risk in the financial services industry

The financial services industry is constantly under cyber attack

The financial services industry is highly targeted by cyber attackers, with the cost of a data breach across financial services averaging $5.97 million.[1] Financial services organizations face cybersecurity challenges on two fronts—on the workforce side they face identity phishing threats against employees, while their customers face account takeover threats related to online and mobile banking.

The long-term rise in remote and hybrid work extended the security perimeter and exacerbated the problem of enterprise-wide phishing attacks. With every home, unsecured network, and even personal devices connecting to enterprise networks, attackers have a much larger target.

The financial services industry was an early adopter of mobile-based authentication such as SMS, OTP, and push notifications, but these forms of authentication are similar to username and password authentication—they cannot prevent phishing and account takeovers. Passwords are easily breached and 2FA in the form of security questions, SMS codes, OTP, and push notifications are susceptible to phishing attacks, SIM swaps, and man-in-the-middle (MitM) attacks. Passwords and mobile authentication are also burdensome for users.

Strong authentication can be a powerful first line of defense for financial services organizations—whether protecting organizational or customer assets.

Strong authentication has two main qualities:

- It does not rely solely on shared secrets process or protocol (symmetric keys) at any point. This includes passwords, OTP, SMS codes, and recovery questions.
- It robustly repels credential phishing, MitM and impersonation. Strong authentication assumes some attacks will reach the end user and the authentication mechanism will prevent the attack from being successful.

Among the varied authentication protocols, only smart cards, modern FIDO U2F, and FIDO2/WebAuthn protocols are strong authentication.

In addition to security, it's also important to consider usability, portability, and scalability. Poor user experiences, low portability, and lack of scalability of authentication solutions can result in low adoption and drive up costs.

Better security and usability with the YubiKey

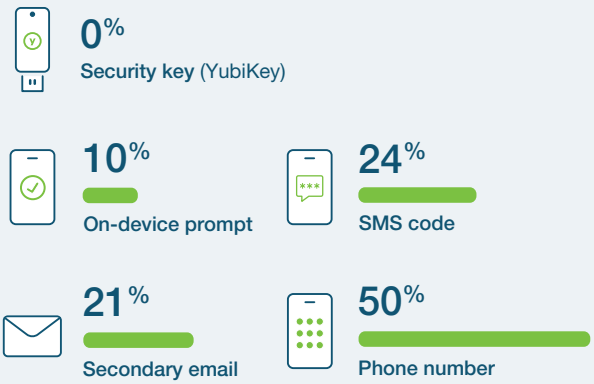
To reduce enterprise-wide identity phishing and customer-facing account takeovers, Yubico offers the YubiKey, for affordable and easy to use two-factor, multi-factor, and passwordless authentication.

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 SOX, PSD2, PCI, FIPS, GDPR, and CFPB Circular 2022-04.
- 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.

YubiKeys are proven to offer the highest levels of security against account takeovers in independent research, preventing targeted attacks.

Risk of account takeovers



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

Common use cases the YubiKey solves for the financial sector

1. Secure remote and hybrid workers

Strong multi-factor authentication (MFA) should be one of the top requirements for remote and hybrid work policies. YubiKeys provide highest-assurance MFA, and are easily integrated into existing systems and infrastructure including identity and access management systems such as Microsoft, Okta, Duo, and Ping. With the YubiKey, financial services organizations can ensure remote and hybrid workers have secure access to computers, VPN, and password managers—no matter where they work. YubiKeys can even be used to securely generate one-time time-based passcodes.

2. Secure high-risk, high-value transactions

Employees that perform high-risk, high-value transactions on a daily basis are often the target of cybercriminals. Access to high-risk systems can be strengthened by requiring strong and modern MFA using YubiKeys, ensuring only authorized account access and authorized high-value transactions.

3. Secure privileged users

Privileged users are prime targets for cybercriminals as they have greater access to sensitive company and customer information. Financial services organizations can strengthen privileged access management and stop targeted attacks by ensuring that authentication security best practices are followed by requiring privileged users to authenticate with phishingresistant hardware security keys such as the YubiKey.

4. Secure call center workers

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. YubiKeys offer strong 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. And unlike mobile phones that can capture images of customer and financial data, YubiKeys offers a much more secure authentication solution.

5. Secure shared workstations/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 with higher turnover and may have minimal commitment to the organization, increasing the insider threat. The YubiKey ensures strong authentication across shared access terminals and shared workstations to help prevent unauthorized access to high-value systems and resources.

6. Secure high net-worth customers

Compared to username and passwords, SMS, and OTP codes, YubiKeys offer the strongest security to protect online and mobile banking accounts of high net-worth clients against account takeovers. Providing customers with easy to use strong authentication can help financial services organizations drive new customer acquisition and help with customer retention. Integrating support for YubiKeys into online and mobile banking is simple. Financial services organizations such as Vanguard and Morgan Stanley offer clients strong authentication solutions, with support for hardware security keys.

Easily procure and distribute YubiKey authentication solutions at scale

Yubico offers flexible and cost-effective enterprise plans that help organizations with 500 users or more move away from legacy and broken MFA and accelerate towards phishing-resistant authentication at scale.

With YubiEnterprise Subscription, organizations can benefit from a predictable OPEX model, the flexibility to meet user preferences with choice of any YubiKey, upgrades to the latest YubiKeys, and faster rollouts with easy access to Deployment Services, Priority Support and a dedicated Customer Success Manager.

Subscription customers are also eligible to purchase additional services and product offerings, such as YubiEnterprise Delivery, a global turnkey hardware key distribution service to residential and office locations across 49 countries.

Trusted authentication leader

Yubico is the principal inventor of the WebAuthn/FIDO2 and U2F authentication standards adopted by the FIDO alliance and is the first company to produce the U2F security key and a multiprotocol FIDO2 authenticator.

YubiKeys are produced in the USA and Sweden, maintaining security and quality control over the entire manufacturing process.

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

[1] IBM Cost of a Data Breach Report 2022

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054, USA
844-205-6787 (toll free)
650-285-0088