yubico

WHITE PAPER

Secure *customer access* to retail and commercial banking with phishing-resistant authentication

Stop account takeovers, mitigate risk and deliver frictionless customer experiences

Table of contents

Executive Summary

While digital banking has revolutionized the sector, retail and commercial banks face competing pressures: to create frictionless digital experiences while also protecting customers from cyberattacks, data breaches and fraud. In fact, an increasing number of consumer protections are mandating more secure forms of authentication for the end customer.

While any form of multi-factor authentication (MFA) is more secure than username and password alone, your consumer authentication strategy can have significant implications for both risk and the customer experience (CX). Too lax and the risk of fraud increases—this erodes trust and negatively impacts CX and loyalty. Conversely, if banks address security without understanding that not all forms of MFA are equal, they may fail to mitigate risk and/or make gains on CX goals.

This whitepaper will explore opportunities to align both security and CX goals and how banks can leverage scalable device-bound passkey solutions to build customer trust and loyalty while defeating stolen credential-driven fraud.

86%

of financial services organizations experienced an **identity-related cyberattack** in the last 12 months[1]

>50%

increase in **fraud attempts** on retail and commercial accounts in the US and UK in the past 12 months.[2]

$40bn

estimated **fraud losses from AI** in the US by 2027.[3]

Growing Cyber Threats Target Digital Banking Customers

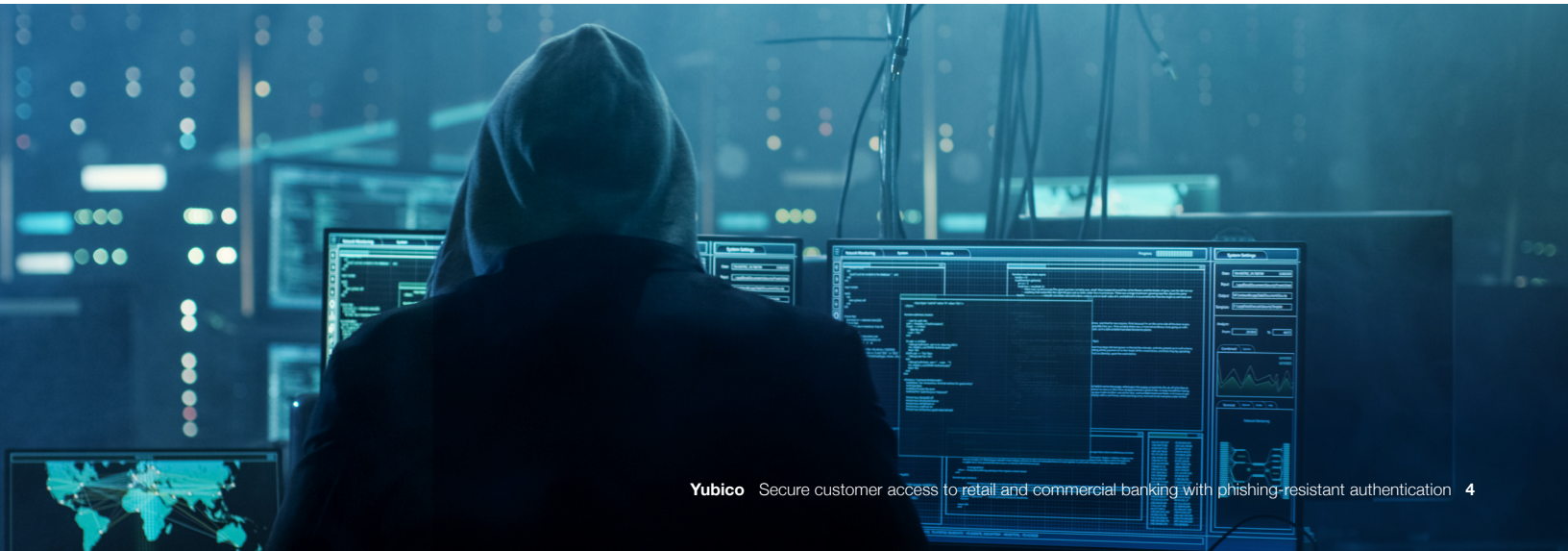
Globally, 57% of retail banking customers actively use digital channels for their banking needs.[4] Given the nature of operations, commercial services have traditionally favored human interaction, but a growing portion of commercial customers are looking for more digital self-service capabilities.[5] Overall, this increase in digital services has made banks—and banking customers—a growing target for cyber attacks, fraud, and other financial crimes.

In North America, 63% of financial institutions say fraud has increased 6% or more in the past 12 months.[6] In Europe, the Middle East and Asia (EMEA) and Asia Pacific (APAC), more than half of financial institutions report the same 6% or more increase in fraud, with 50% or more of that fraud originating from digital channels.[7]

Most cyber attacks and fraud at retail and commercial banks have one thing in common—compromised credentials.[8] Threat actors leverage common attack techniques such as phishing to gain access to credentials, opening the door to account takeovers and fraud.[9] Another technique is SIM swapping, when threat actors take control of a phone number to intercept one-time passcodes. Recently, SIM swapping resulted in a Bank of America customer reporting a loss of $21,000[10] and one Toronto couple over $160,000,[11] just two examples of the $50 million in reported SIM swap losses in the US in 2023.[12] Even more secure passkey implementations, leveraging FIDO2 credentials, are vulnerable to attacker-in-the-middle (AiTM) attacks if implementations fall back on passwords for account recovery.[13]

Advances in AI and low cost malicious toolkits have provided cyber criminals with increasingly sophisticated methods of targeting and deceiving bank customers. Since mid-2023, an operation called ‘Estate’ has logged more than 93,000 attacks, tricking victims into entering one-time passcodes (OTPs) for various accounts, including bank accounts and digital wallets.[14] AI is also being used to impersonate customers, with these ‘deepfakes’ capable of bypassing voice, photo and video Know Your Client (KYC) identity verification systems.[15]

For fraud related to credential theft, retail and commercial banks face financial and reputational losses, liabilities, and a loss of customer trust—losses more acutely felt in today’s highly competitive market. For commercial banking, the sheer scale and complexity of financial activities increases potential liabilities as the loss of corporate credentials could expose corporate accounts to fund manipulation, large-sum wire transfers, and other irrevocable transactions.



Consumer Protection Regulations Require Strong MFA

The banking sector has been subject to a growing number of regulations that require the use of strong and phishing-resistant MFA, but emerging consumer protections are extending those requirements to the end-customer.

North America	United States	The **Gramm-Leach-Bliley Act (GLBA)** Safeguards Rule (16 CFR 314) requires MFA customer access to systems.
		The **Federal Financial Institutions Examination Council (FFIEC)** suggests that MFA be prioritized for digital banking consumers engaging in high-risk transactions and that hardware-based MFA be prioritized for high-risk users.
		A 2022 **Consumer Financial Protection Bureau (CFPB)** circular suggests that a failure to offer MFA to consumers—with an emphasis on MFA solutions that protect against credential phishing—could trigger liability under CFPB regulations or the Dodd-Frank Act.
		Customer Due Diligence (CDD) Rule requires banks to verify the identity of customers to protect against fraud.
Europe & the UK	All EU countries and European Free Trade Association (EFTA) States	The **Payment Services Directive 2 (PSD2)** requires banks to implement strong customer authentication (SCA) for access to digital services—and to evolve the method of SCA in response to the threat landscape. The draft PSD3 amends SCA rules to limit the risks of spoofing and phishing and to address accessibility concerns by prohibiting a "mobile-only" approach to authentication. PSD3 also introduces a requirement for banks to establish a method to "unambiguously identify the payee."
		The EU is also laying the groundwork for a digital identity framework with **eIDAS, the regulation on Electronic Identification, Authentication and Trust Services.** Once applied, eIDAS provides a framework for a common structure for electronic credentials based on digital identity wallets and the authentication of users to public and private services, including banking. Several European countries are now in the process of deploying device-bound passkeys in hardware security keys as part of an eID solution to securely and easily access government and banking services.
Asia Pacific	Singapore	The **Monetary Authority of Singapore (MAS)** has been strengthening consumer protections for mobile banking and payments, first with MFA and passwordless authentication, and most recently by phasing out the use of OTPs for customer logins to better protect customers from phishing.
	Australia	Although not an enforceable requirement, Australia's **Essential Eight Maturity Model (E8MM)** suggests that phishing-resistant MFA should be used for all online services, including customer services.

>1/3 of Gen Xers

would switch financial service organizations for a better experience.[26]

Satisfied customers **6x more likely** to remain with a bank and purchase more of its products.[27]

77%

of financial consumers would favor a bank offering **passkeys**.[28]

> "Frictionless digital experiences have now often become synonymous with trust, and banks cannot risk delivering subpar experiences."
>
> **Deloitte Center for Financial Services[29]**

The Interplay Between Security and Customer Experience in Digital Banking

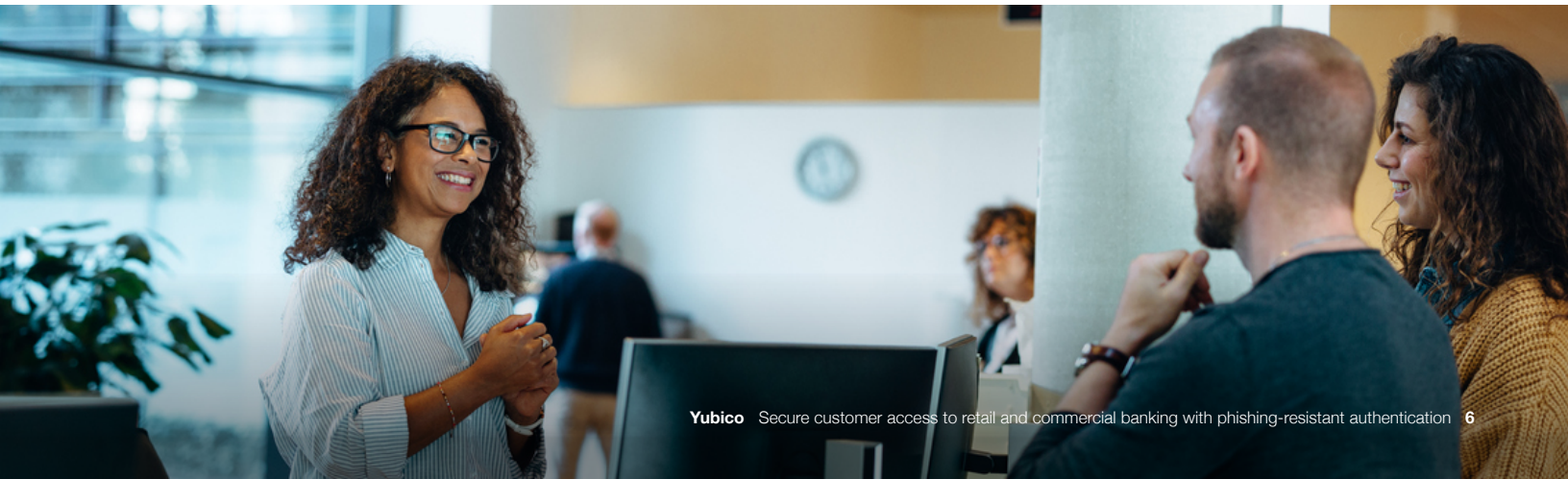
As digital banking has amplified consumer exposure to financial crimes, trust in financial institutions has become precarious.[30] Customers aged 25-78 say security and fraud are their biggest frustrations with digital banking.[31] Another survey suggests that 80% of banking customers would be willing to switch financial institutions if their data was compromised.[32]

While account takeovers and fraud negatively impact the customer experience and lead to high levels of attrition, the inverse is also true: the right approach to account security can increase confidence and trust, and thus encourage customer loyalty. For commercial banking, where competition has resulted in one-third of companies with US$1 billion or more in revenues to bank with 10 or more institutions,[33] communicating strong security measures can help re-establish a closer relationship between commercial banks and their customers. Furthermore, 69% of banking customers rank fraud protection as their top consideration when selecting a new financial service provider.[34]

Banks not only face challenges with trust, a critical factor of a client's experience, but declining levels of CX quality overall—US banking CX quality dipped for the third year and EU banking CX quality declined significantly from 2023.[35] To meet the evolving needs of customers and modern companies, and to recapture CX quality, banks need to innovate across products and services and deliver frictionless, efficient digital experiences. This need extends to your MFA strategy.

As regulations require higher assurance methods of authentication to protect consumers and organizational resources, some forms of MFA may introduce friction into the authentication process, negatively impacting CX and leading to low usage and potential churn. On the flip side, eliminating pain points in the authentication process—both friction and the risk of fraud—can curate more positive experiences.

In the next section, we will further illustrate how not all types of MFA are created equal, in terms of risk and CX, and how leading banks are deploying hardware-bound passkeys to commercial and high-value retail consumers to stop account takeovers, mitigate risk, and deliver frictionless customer experiences.



> 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 key that is plugged into a computer to authenticate users."
>
> **New York Department of Financial Services, Twitter Investigation Report, October 2020**

Not all MFA is Created Equal

Consumer protections have made clear that not all MFA is created equal, with Singapore going so far as to entirely phase out OTPs from consumer authentication. This is because legacy MFA such as SMS, mobile authentication, email 'magic links,' and OTPs can all be easily bypassed by malicious actors, vulnerable to account takeovers (e.g. phishing) at a rate of 10-24%.[36]

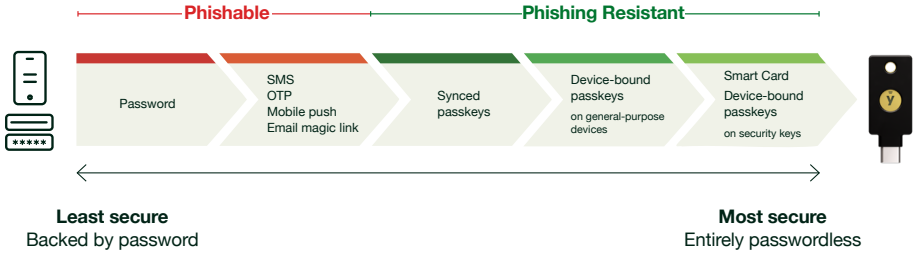
Hard-to-remember passwords and multi-step authentication processes are a huge source of friction and inefficiency in the digital banking experience, particularly when passwords are forgotten, there are OTP delays, or if there are accessibility challenges.

While many leading financial institutions are solving these security and experience challenges internally by adopting phishing-resistant MFA with FIDO2/WebAuthn (passkeys), passkeys are also a scalable solution for consumer authentication.

An Introduction to Phishing-resistant MFA and Passkeys

National Institute of Standards and Technology (NIST), globally recognized for promoting equitable standards, defines phishing-resistance in Special Publication (SP) 800-63 and Draft 800-63-4[37] as "the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party without reliance on the vigilance of the subscriber."

Phishing-resistant MFA processes rely on cryptographic verification between devices or between the device and a domain, making them immune to attempts to compromise or subvert the authentication process. The most secure forms of phishing-resistant MFA are entirely passwordless, implemented with no fall-back passwords for onboarding, device registration and account recovery.



Passkeys have been introduced by the FIDO Alliance as a way to accelerate the shift away from insecure passwords for consumers and organizations alike. Passkeys are now available on every major platform including Google, Apple, Microsoft and web browsers.

A passkey is simply a FIDO2 credential, and it can live on a smartphone, or another general-purpose device, such as tablets or laptops. Alternatively, they can reside in portable devices which are authenticators purpose-built for security, such as FIDO hardware security keys.

A passkey is the credential itself, a digital file. An authenticator is where the passkey lives. For example, on a phone, laptop, hardware key, or other device.

Passkey

Authenticators

Security keys

Device-bound credentials with Attestation

Platform authenticators

Authenticators built into your devices

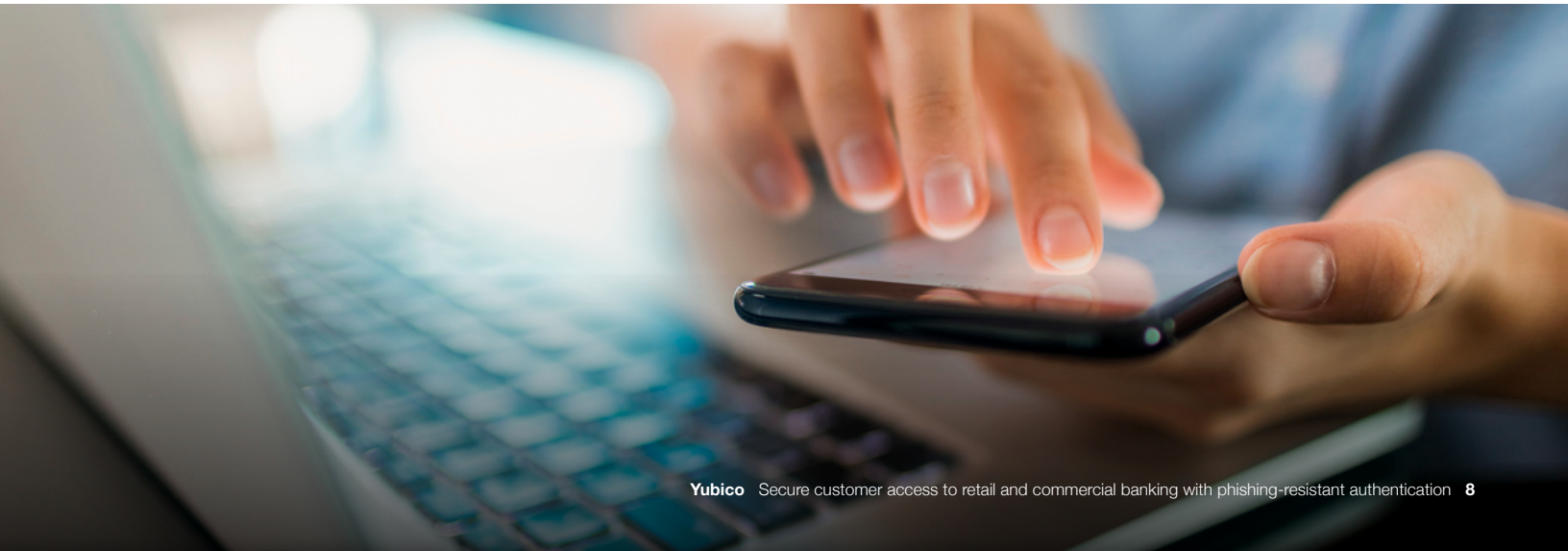
3rd party authenticator apps

Applications that provide user authentication solutions

- **Synced passkeys** live on a smartphone, tablet or laptop where it can be copied and shared across many devices. Synced passkeys are easy to use, but can still be circumvented by malicious threat actors using AiTM attack or if the passkey is exposed by a breach of a third-party passkey provider service
- **Device-bound passkeys** reside in general purpose devices such as smartphones, laptops and tablets or in hardware security keys. Those that live in hardware security keys are known to offer the highest security assurance and attestation that can provide the security of the credentials.

Phishing-resistance and passkeys sound complicated, so you may think that passkeys are hard to use. In reality, passkeys are very simple and fast to use: once set up, customers simply verify their sign-in with biometrics, local PIN or by touching their FIDO security key.

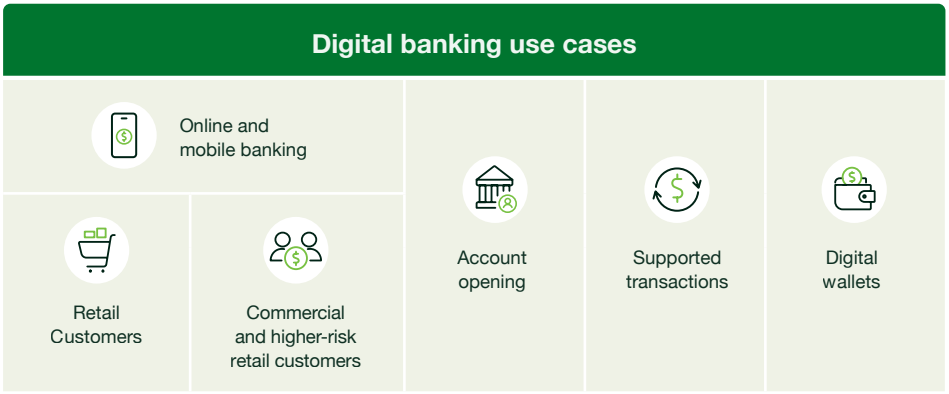
You may also think your customers don't know about passkeys, but the opposite is true: 62% of people surveyed in the US and UK are aware of passkeys—and 53% already enable passkeys on at least one of their accounts.[38] Further, 61% of those familiar with passkeys say they are more convenient than passwords—a clear CX win.[39]



How to Choose the Right Passkeys

All passkeys may be phishing-resistant, but not all are ideal for some digital banking use cases

The passkey approach you choose for your customers will depend on what level of security assurance you need and the risk tolerance and CX goals you have for each customer segment.

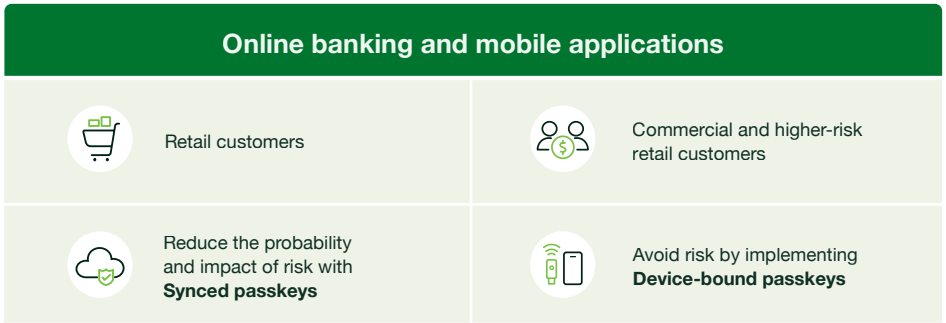


Online and Mobile Banking

Online banking websites, portals and applications fall into a broad category of high-risk customer-facing applications. While the compromise of credentials has the potential to be devastating for any customer, most banks have a higher risk tolerance for general retail customers and a lower risk tolerance for commercial customers.

For all online and mobile banking scenarios, **synced passkeys** provide an easy, phishing-resistant workflow for customers, building off the security controls of the devices they already use—an important first step on the journey to higher assurance security with device-bound passkeys.

Where the risk tolerance is lowest, banks want to avoid all opportunities for identity-based attack. To do this, banks can deploy and enforce the use of the highest assurance passkey protection available—**device-bound passkeys in the form of FIDO hardware security keys**. Provisioning keys to commercial clients and other high-value clients is a competitive differentiator that can pay dividends in the form of stronger security, efficiency, confidence and CX quality.



With the option to deploy security keys as-a-service, banks incur a low monthly cost (OPEX) that represents a huge savings in potential liabilities. Over time, deployments can extend to retail customers who deal with high-risk transactions or who have multiple account holders, such as small-to-medium business customers.

Account Opening

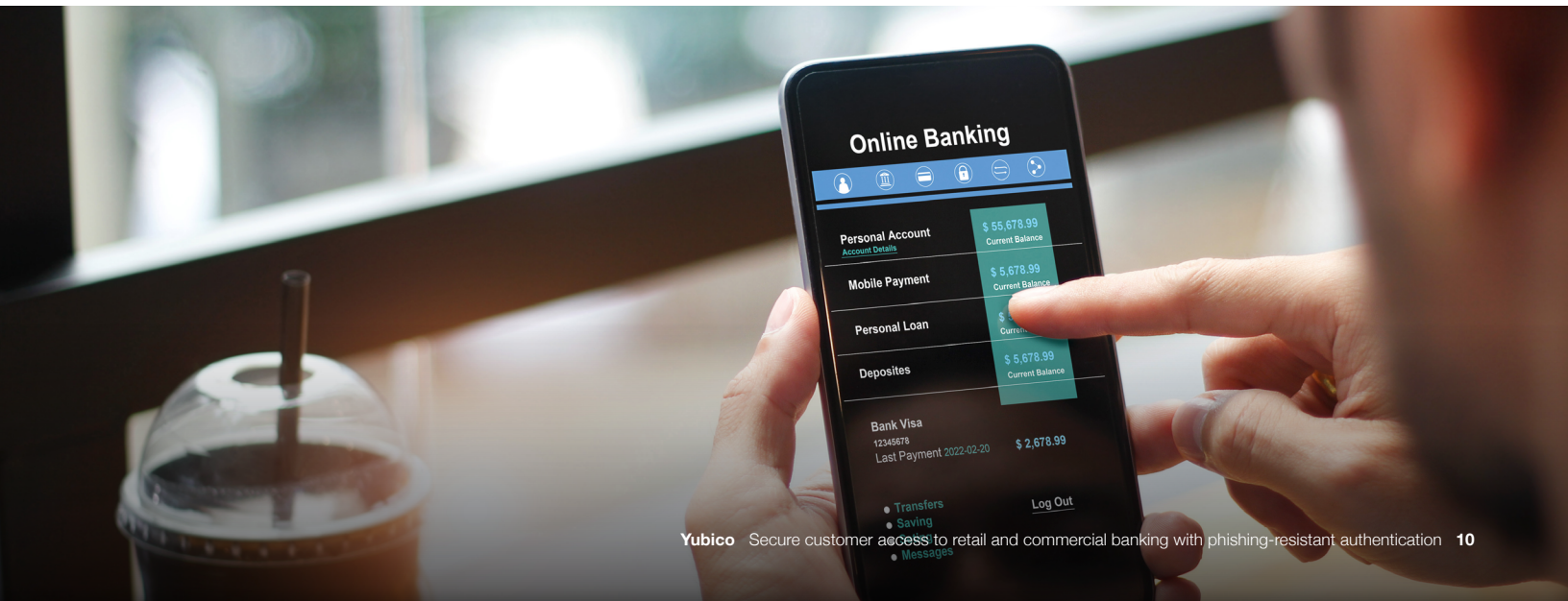
Regulatory requirements are increasingly focusing on the need for banks to unambiguously identify bank customers both at the point of account opening and for subsequent transactions, efforts made to combat growing rates of synthetic identity fraud. This all starts with strong identity proofing of the customer at time of account opening.

Passkey-based identity proofing can be built into an application or a web-page sent to end customers, or as part of a ceremony that is conducted during an in-person scenario. The passkey enrollment process involves creating an authentication credential that is bound to either a platform authenticator (synced passkey) or hardware security key (device-bound passkey). This trusted process will not involve setting fall-back passwords, security questions, or confirming OTP codes, making set-up a frictionless process.

Supported Transactions

Requirements from regulatory bodies require traceability and auditability of transactions conducted on behalf of end customers, which can occur in both in-person and call-center supported transactions. Traceability and auditability starts with strong **identity proofing** of both the customer requesting the transaction and the agent facilitating the transaction.

The consumer-side would require strong identity proofing at time of opening, which would bind users to passkeys and support streamlined authentication using either synced or device-bound passkeys. On the employee-side of the picture, passkey authentication unlocks the powers of strong cryptography to tie individual enterprise users to specific transactions and actions. For call-center supported transactions, device-bound passkeys provide employees with a simple and highly-assurant identification process that does not break end-customer interactions and functions within mobile-restricted environments.



Digital Wallets

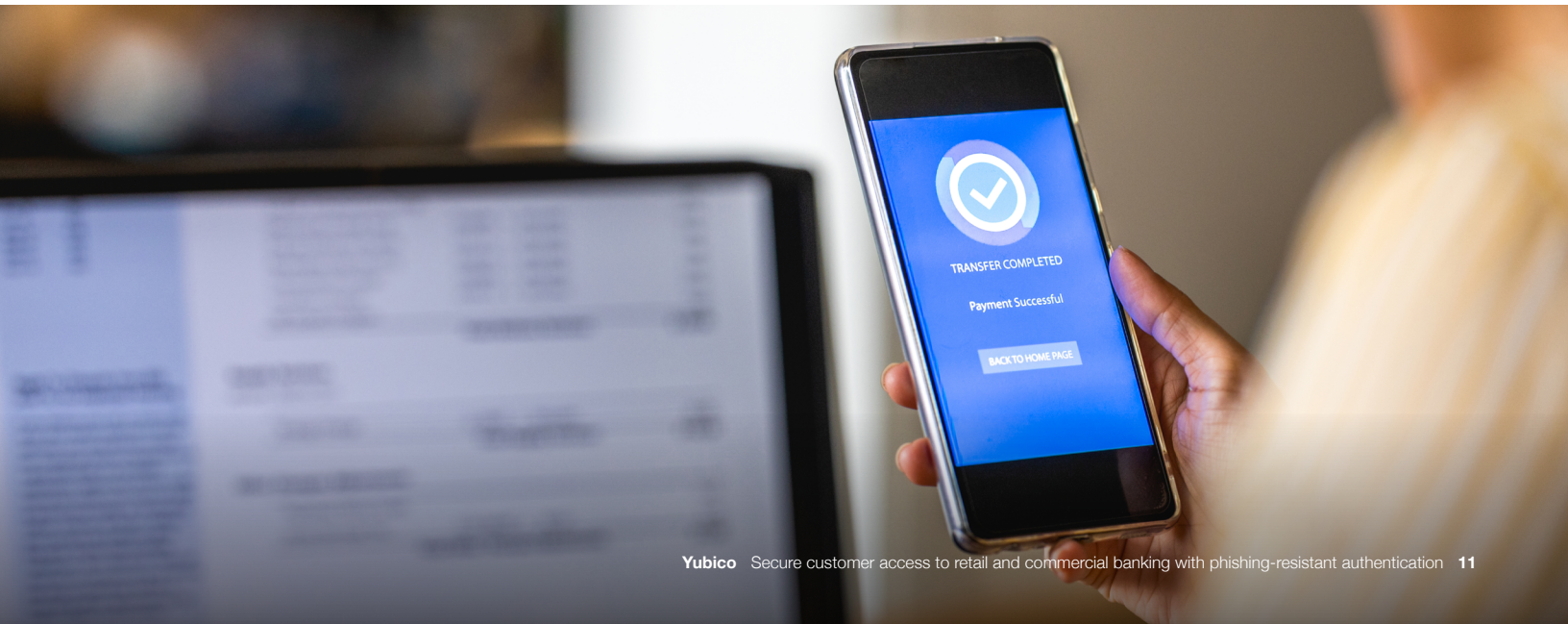
Digital wallets are an increasingly common solution to store financial information and facilitate secure payments, projected to support 5.8 billion global users by 2029,[40] and similar in concept to the EU Digital Identity (EUDI) wallets being rolled out as part of eIDAS. Unfortunately, attackers are able to exploit weaknesses in identity proofing and authentication to add consumer bank cards to an unauthorized wallet, particularly when authentication falls back on knowledge-based questions.[41]

Apart from user authentication, hardware security keys can play a crucial role in securing digital wallets. A wallet's contents can be encrypted and decrypted using cryptographic keys derived from secrets bound to the secure hardware of a FIDO security key. Additionally, the solution can be used for commercial and business accounts that involve shared control over an "organizational wallet."

Secure Onboarding and Recovery *is a Must* for All Users

Phishing-resistant MFA offers the lowest level of risk, reducing the threat of compromise and attack from phishing, but critical choices you make during deployment can contribute to gaps in coverage. Since passkeys typically rely on self-service registration, many implementations will fall back on passwords, shared secrets or legacy MFA for onboarding, device registration and account recovery procedures. But that just gives malicious actors a simple path to bypass the intended protection of phishing-resistant MFA.

FIDO security keys enable banks to build trusted account opening and onboarding processes when combined with strong identity proofing that secure the authentication lifecycle without falling back on phishable MFA. By closing the loop on the credential lifecycle, it's not only possible to adopt phishing-resistant authentication, but to actually create phishing-resistant customers that are protected across every authentication task.



YubiKey has you covered:

- ✓ Reduce risk of credential theft by 99.9%[42]
- ✓ Provide secure user access at scale on any device
- ✓ Does not need battery or cellular connectivity to function
- ✓ Reduce help desk calls for password resets
- ✓ Meets eIDAS 'high' assurance requirements

Move from Reactive to Proactive Security with the YubiKey

Retail and commercial banks looking to safeguard consumer access to digital banking are deploying the device-bound passkeys residing in FIDO hardware security keys.

Yubico offers the YubiKey, a FIDO hardware security key that contains the highest assurance passkeys to help banks meet evolving regulations and bridge to a more secure and efficient digital banking experience.

By safeguarding registration, authentication, and recovery across all devices, platforms, and processes with purpose-built, portable hardware security keys, such as YubiKeys, banks can support phishing-resistant clients who are protected from evolving identity-based threats and the risk of fraud.

The YubiKey can be deployed at scale to **reduce risk of credential theft by 99.9%,**[43] all while enabling a frictionless CX, letting users quickly and securely log in to their accounts with a single tap or touch.

To remove all the guesswork out of planning, purchasing and delivery, Yubico offers YubiKey as a Service, a service-based and affordable model to simplify how banks procure, upgrade and support YubiKeys for employees and end-customers alike, as well as streamlined global distribution to end-users in both domestic and international locations, including residential addresses, through YubiEnterprise Delivery and trusted channel partners.

Yubico Enrollment Suite

YubiKey offers right-sized solutions to enroll YubiKeys on behalf of your customers. Yubico FIDO Pre-reg is a premium service that delivers factory enrolled pre-programmed keys to new or existing users or customers, while YubiEnroll is a client application that can help pre-enroll YubIKeys on behalf of new users or customers.

Credential registration

Sarah registers her synced or device-bound credentials to her account, with no friction over password length, complexity, or the need to confirm an OTP code.

Digital banking login

Sarah wants to check her account balances, so she enters her username and is prompted to tap her biometric reader on her laptop (synced passkey) or to enter and tap her YubiKey (device-bound passkey).

Step-up authentication

Sarah wants to make a large wire-transfer. To protect high-value, sensitive transactions, she's prompted to re-authenticate by simply tapping her YubiKey.

Self-service credential management

Sarah has lost her phone and needs to revoke the synced passkey. Thankfully, she first registered a YubiKey, so she can recover access to her account.

Account lockout

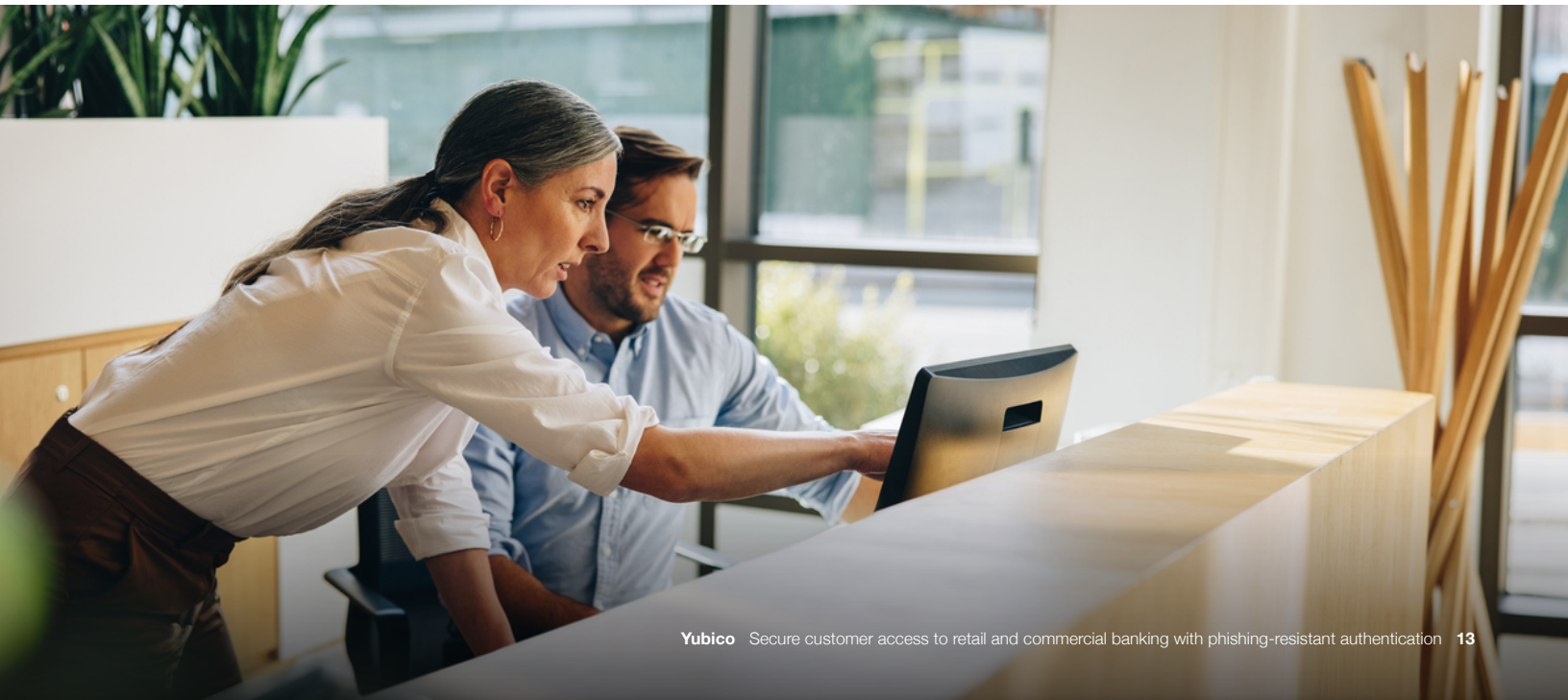
Sarah has lost access to all her devices and YubiKeys. She follows a secure process to get a new credential and YubiKey.

Designing the Right Approach

While regulatory bodies are starting to mandate more secure forms of authentication, retail and commercial banks must design an approach to consumer authentication that is commensurate with risk, supports CX quality, and can be deployed to support the large and complex ecosystem of devices used by the vast end-customer base to access digital services.

When designing your approach, consider the following:

- Impact to clients
- Opt-in or mandatory?
- Impact to contact center
- Define target customer segments
- Timeline for adoption
- Distribution and enrollment considerations
- Educating customers about how passkeys protect against fraud



Leading banks in the US and across the EU are rolling out synced and device-bound passkeys with multi-channel communications that leverage emails, banner ads, videos and help desk materials. Best practices emphasize a commitment to keeping digital banking secure and how simple it is to set up a platform authenticator or to order, set up, and use a YubiKey.

Taking the time to roll out passkeys in waves can allow your bank the opportunity to work through any challenges and ensure frontline support staff are able to effectively troubleshoot common onboarding questions. Once passkeys have been deployed at scale, your bank can begin the process of deprecating insecure parallel methods of MFA in favor of the exclusive use of synced and/or device-bound passkeys to provide the highest level of protection against risk and fraud.

To help you on your journey to strong customer authentication, we offer a simple guide that details the six deployment best practices to accelerate adoption at scale, How to get started with phishing-resistant MFA.

Plan

Ensure **readiness** by clarifying use cases and user populations

Validate

Confirm the **process** with a small group of users before broader rollout

Integrate

Ensure key apps and services are **YubiKey-ready**

Launch

Distribute keys to users with **turnkey delivery** services or channel partners

Adopt

Drive adoption with best practice **training and support**

Measure

Report on security and business value impact

If you want a closer partnership on any of the six steps of this plan, Yubico's Professional Services team is here to help.

Sources

[1] HYPR, When Trust is Hacked: Customer Identity Security in Finance in 2024, (October 10, 2024),

[2] Alloy, 2024 State of Fraud Benchmark Report, (2024),

[3] Deloitte Center for Financial Services, Generative AI is expected to magnify the risk of deepfakes and other fraud in banking, (May 29, 2024),

[4] McKinsey & Company, The state of retail banking: Profitability and growth in the era of digital and AI, (October 10, 2024),

[5] Deloitte Center for Financial Services, Commercial Banking 2025: Finding a new compass to navigate the future, (October 13, 2024),

[6] LexisNexis Risk Solutions, 2023 True Cost of Fraud Study, (2024),

[7] LexisNexis Risk Solutions, 2023 True Cost of Fraud Study; 2023 True Cost of Fraud Study, (2024),

[8] IBM, 2024 Cost of Data Breach Report, (July 30, 2023); FDIC, Authentication in Internet Banking: A Lesson in Risk Management, (Accessed 2024),

[9] BAI, 2024 banking outlook, (December 2023),

[10] Roher, Christine and Johnson, Carolyn, Man lost $21,000 in SIM swap scam. Here's how to protect yourself, (April 16, 2024),

[11] O'Shea, Sean, 'A nightmare': SIM card swap scam hits Toronto-area couple for more than $140,000, (March 21, 2024),

[12] FBI, Internet Crime Report 2023, (2024),

[13] Seals, Tara, Passkey Redaction Attacks Subvert GitHub, Microsoft Authentication, (July 2, 2024),

[14] Whittaker, Zack, 'Got that boomer!': How cybercriminals steal one-time passcodes for SIM swap attacks and raiding bank accounts, (May 13, 2024),

[15] Titterington, Alanna, How fraudsters bypass customer identity verification using deepfakes, (August 15, 2024),

[16] 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),

[17] FFIEC, Authentication and Access to Financial Institution Services and Systems, (August 11, 2021),

[18] CFPB, Consumer Financial Protection Circular 2022-04, (August 11, 2022),

[19] Financial Crimes Enforcement Network, Information on Complying with the Customer Due Diligence (CDD) Final Rule, (2018),

[20] EU, Directive 2015/2366, (November 27, 2017),

[21] European Commission, Modernising payment services and opening financial services data: new opportunities for consumers and businesses, (Jun 27, 2023); European Commission, Proposal to amend Regulation No 1093/2010, (June 28, 2023),

[22] European Commission, eIDAS Levels of Assurance (LoA), (2014),

[23] MAS, MAS' Cyber Security Advisory Panel Proposes Ways to Tackle Mobile Malware Scams and Generative AI Risks for the Financial Sector, (October 30, 2023),

[24] MAS, Banks in Singapore to Strengthen Resilience Against Phishing Scams, (July 9, 2024),

[25] Australian Signals Directorate, Essential Eight Maturity Model, (November 23, 2023),

[26] BAI, Banking outlook for 2024 and beyond, (February 2024),

[27] Chheda, Shital et. al., Five ways to drive experience-led growth in banking, (May 2, 2023),

[28] HYPR, When Trust is Hacked: Customer Identity Security in Finance in 2024, (October 10, 2024),

[29] Deloitte Center for Financial Services, Commercial Banking 2025: Finding a new compass to navigate the future, (October 13, 2024),

[30] Edelman, 2024 Edelman Trust Barometer Supplemental Report: Insights for Financial Services, (May 7, 2024); Edelman, 2024 Edelman Trust Barometer, (May 7, 2024),

[31] BAI, Banking outlook for 2024 and beyond, (February 2024),

[32] HYPR, When Trust is Hacked: Customer Identity Security in Finance in 2024, (October 10, 2024),

[33] Deloitte Center for Financial Services, Commercial Banking 2025: Finding a new compass to navigate the future, (October 13, 2024),

[34] FICO, Fraud, Identity, and Digital Banking Consumer Survey 2023 - USA, (March 6, 2024),

Sources

[35] Forrester, Predictions 2025: Banks Must Innovate To Reverse The Double Whammy Of Declining CX And Profitability, (October 23, 2024),

[36] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019),

[37] NIST, NIST SP 800-63-4 Digital Identity Guidelines, (December 2022),

[38] FIDO Alliance, Consumer Password and Passkey Trends, (May 2, 2024),

[39] Ibid

[40] Juniper Research, Which Countries Are Leading Digital Wallet Adoption in 2024, (September 30, 2024),

[41] Anwar, Raja et al., In Wallet We Trust: Bypassing the Digital Wallets Payment Security for Free Shopping, (August 14, 2024),

[42] Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022),

[43] Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022),

yubico

About Yubico

Yubico (Nasdaq Stockholm: YUBICO), the inventor of the YubiKey, offers the gold standard for phishing-resistant multi-factor authentication (MFA), stopping account takeovers in their tracks and making secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

Yubico's solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across hundreds of consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

As part of its mission to make the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. The company is headquartered in Stockholm and Santa Clara, CA. For more information on Yubico, visit us at www.yubico.com.