SPOTLIGHT REPORT

HYPR

When Trust is Hacked:

Customer Identity Security in Finance in 2024

Introduction

In today's crowded and fast-paced technology environment, finance organizations must efficiently and securely manage access to an ever-increasing range of digital services and resources. This puts tremendous pressure on their IT and security teams to keep operations running smoothly and cyber defenses ironclad, even as their exposure to cyberthreats grows. At the core of this challenge is identity security, which ensures authorized individuals gain access to systems and that imposters and threats are shut out.

As the most targeted industry for cyberattacks, financial institutions have historically led the way in security innovation. Yet attacks continue to slip past their identity security defenses. Financial and risk advisory firm Kroll found that the finance sector was the most breached industry last year. Phishing, increasingly aided by AI, continues to top the threat list, targeting institutions and their customers alike. Deepfakes are the fastest growing threat to the fintech sector, increasing by 700% in 2023 according to a recent Sumsub report. These attacks impact the safety of customer data and financial institutions' bottom line. Fraud losses from gen AI hit US$12.3 billion in 2023 in the United States and are predicted to reach US$40 billion by 2027.

To better understand the impact of this rapidly changing technology and threat landscape, we interviewed a total of 548 individuals, in separate surveys of both financial services organizations and their customers. A telling picture emerges when looking at finance customer concerns in parallel with the industry's identity security approaches and priorities. Banking customers are increasingly uneasy about cybersecurity and the safety of their data when it comes to managing their finances. Moreover, they are demanding cybersecurity innovation to address these concerns faster than their financial institutions can provide it.

Key Findings

Finance Organizations...

86% 

experienced an identity-related cyberattack in the last 12 months

84% 

were the victim of identity fraud in the last 12 months

77% 

experienced at least one breach related to credential misuse or authentication weakness

Finance Customers...

80% 

would likely switch financial institutions if their data was compromised

77% 

would be more likely to choose a bank that offers passkeys

22% 

use the same password for their financial institution as another account

Financial Services Threat Landscape

Attackers Target Identity Processes

Given that financial services is the most attacked industry, it's not surprising that nearly all organizations in this sector (98%) were hit by cyberattacks in the last 12 months. Identity processes are the area of greatest vulnerability. The vast majority of financial services organizations — 86% — experienced an identity-related cyberattack in the last 12 months. This is notably higher than the average across industries (78%) reported in our 2024 State of Passwordless Identity Assurance report.

Phishing continues to be the most prevalent form of attack (42%). Other pervasive identity-focused attacks include credential stuffing (29%), identity impersonation (28%) and push notification attacks (27%). Rare just a few years ago, push notification attacks (also known as MFA prompt bombing), are now a favorite technique of hacking groups such as Scattered Spider, infamous for the $100 million attack on MGM Resorts.

Types of Cyberattacks Faced in the Last 12 Months

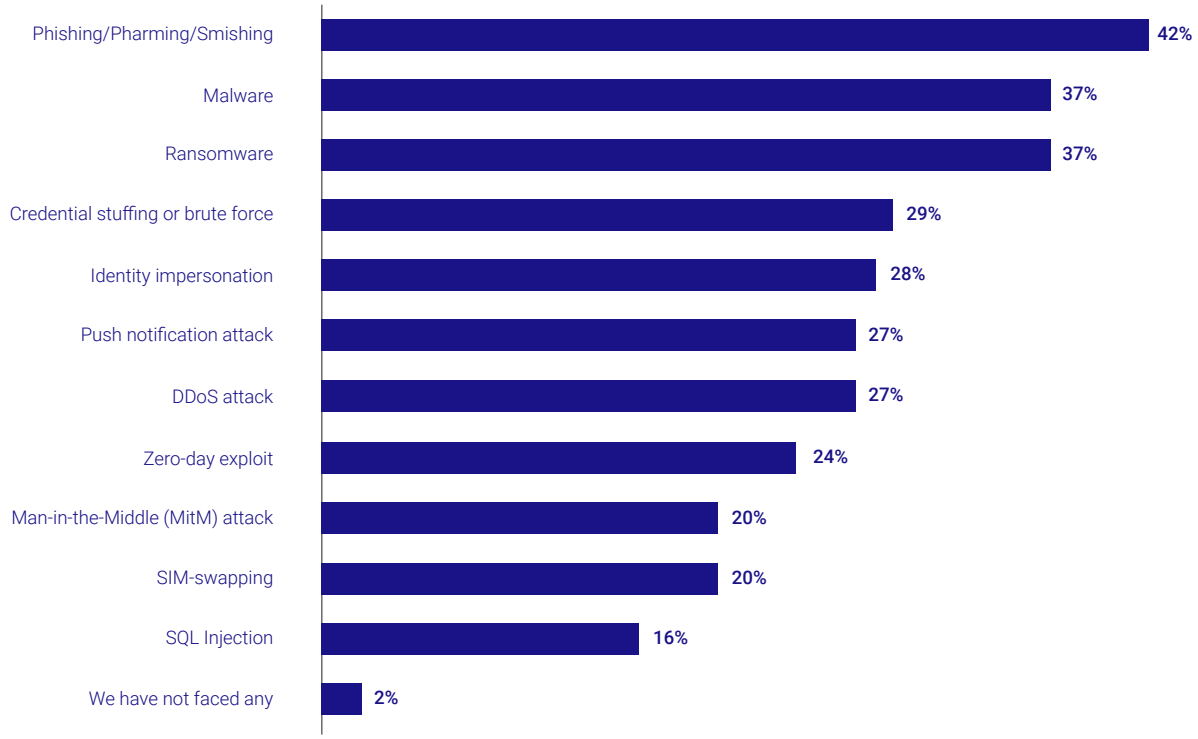


Figure 1: What, if any, types of cyber-attack has your organization faced in the last 12 months?

Identity Security Is Failing

Of those organizations hit by a cyberattack, 84% went on to experience at least one breach. When looking at root causes, 94% of organizations that were breached named credential misuse or authentication vulnerabilities as a factor in at least one breach. Doing the math, this means that **77% of all financial services organizations experienced at least one breach related to a weakness in authentication.**

Cyber Breaches Related to Credential Misuse or Authentication Vulnerabilities

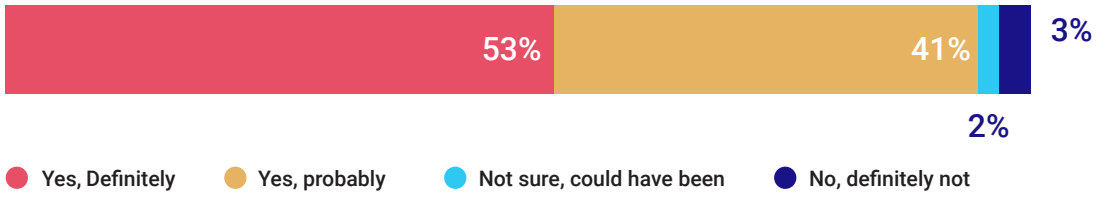


Figure 2: Were any of the cyber-breaches that your organization experienced related to credential misuse or authentication vulnerabilities? Only asked to respondents whose organizations have been the victim of a cyber-breach as a result of a cyber attack in the past 12 months

The impact on financial organizations of these identity security failures are far-reaching, from regulatory fines to loss of customers. Although determining the precise cost of a breach can be tricky, financial organizations state that, on average, breaches caused by insecure authentication caused losses of $4.57 million in the last 12 months — more than double the $2.19 million reported two years ago in the 2022 State of Finance Authentication report.

This sum doesn't include the impact of identity fraud. It's become so widespread that the vast majority of financial services organizations (84%) were the victim of identity fraud in the past year, with 59% hit multiple times, racking up an additional $2.77 million in costs on average.

$4.57M

average cost of authentication-related breaches in financial services organizations in the last 12 months

> Finance organizations are under pressure to strengthen identity security as they are increasingly targeted by threats like phishing, credential misuse and deepfakes. To stay ahead, banks must prioritize innovative, customer-centric security measures like passkeys or risk losing both revenue and trust.
>
> **— Gehan Dabare**
>
> IAM Leader at companies such as JPMC, Citi, CVS Health

Cybersecurity Directly Impacts Client Loyalty

Cybersecurity and breaches are a major concern for these organizations' customers. Consumers today expect the financial institutions they do business with to prioritize data security, holding them accountable for any gaps in their cyber defenses.

No Tolerance For Breaches

Eight in ten consumers state that they would likely switch financial institutions if their data was compromised. Interestingly, those customers under 35 demonstrate the least tolerance for security failures — only 7% would probably stay with their current bank in the face of a data compromise. By contrast, 27% of customers aged 45 or older would likely stay with their financial institution despite a security breach.

Likelihood of Customers Switching Financial Institution After Data Breach

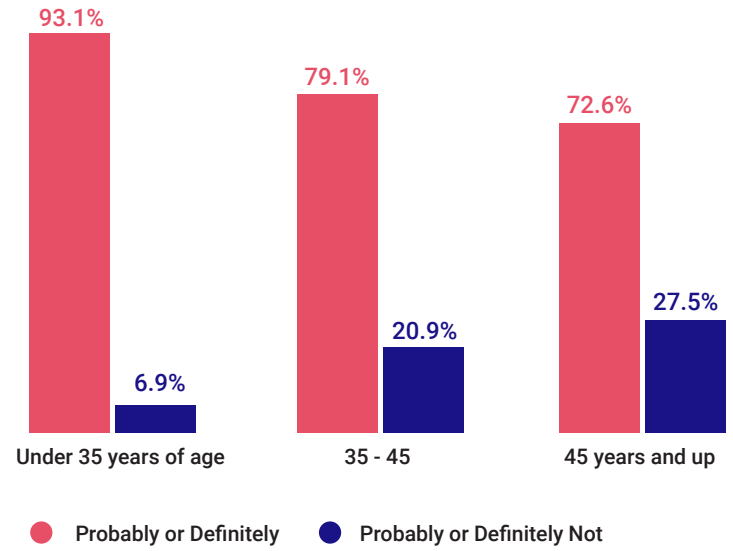


Figure 3: Would you switch financial institutions if your data was compromised?

We should note that customer loss due to breaches reported by financial institutions is far below this figure. When looking at breach impacts on financial organizations, only 40% state that they lost customers after a breach. This could indicate that customers are more reluctant to switch banks than they profess. Or, the more likely scenario, many customers remain ignorant of the extent of financial institution breaches.

The Breach Communication Gap

Despite financial customers' active interest in data security and cyber threats, our data reveals that they remain in the dark about the extent of the problem. Only 11% say that their financial institution has had a breach, 63% state that the financial institutions they use have not been breached, and the rest admit that they just don't know. The marked discrepancies between industry breach figures and customer awareness should make regulators take pause. Despite strict notification mandates, messages about potential data violations do not seem to be reaching their intended audience.

Finance Customers: Has Your Financial Institution Been Breached?

Figure 4: To your knowledge, has your financial institution been breached?

Customers Are Looking for Passkeys

Consumers today take a strong interest in cybersecurity innovations and expect their financial institutions to keep pace. This becomes especially evident in attitudes about passkeys. Although introduced to the public only two years ago, nearly all finance customers (95.5%) have heard of them. While around 30% admit that they don't understand the difference between passkeys and passwords, nearly two-thirds (65.7%) have at least some knowledge of how they are used.

Customer Passkey Knowedge Levels

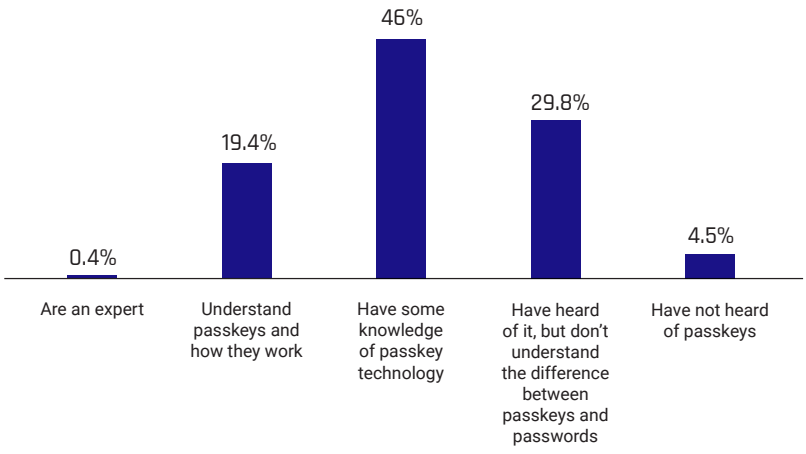


Figure 5: How familiar are you with passkey technology?

This knowledge affects customer decision-making. Over three-quarters (76.5%) would be more likely to choose a bank that offers passkeys. Given that the latest Consumer Banking Report found that 30% of customers are considering switching new banks in the next 12 months, all finserv companies should have passkeys on their roadmap, if they don't already offer them.

77%

of customers would be more likely to choose a bank that offers passkeys

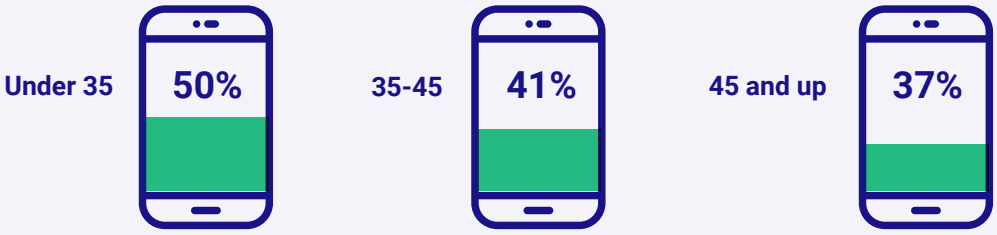
Insecure Habits Abound Despite Concerns

Ironically, although consumers have high security expectations of their banks, they do not always adhere to secure practices themselves. Nearly a quarter (22%) use the same password for their financial institution as another account. The worst offenders are the under 35 age group, with just about 3 in 10 (29%) sharing passwords between accounts.

Insecure MFA methods are rampant, although this likely reflects what their financial providers offer, rather than a deliberate choice by customers. The vast majority (89.6%) use OTP-based MFA — one-time codes sent by SMS, email or voice — for at least one of their accounts. A surprising number (7%) don't use any form of 2FA, relying on passwords alone for protection.

Authenticator Apps Are More Popular Among the Younger Set

When looking at the types of MFA finance customers use, authenticator app uptake appears to be directly correlated with age.



Question:
What type of two-factor / multi-factor authentication do you use to log in to your financial institution(s)

So Where's the Passkeys?

Customers may be clamoring for passkeys but it will be a while before their finserv providers make them available. Less than one-third (31.3%) plan to offer passwordless / passkey authentication to their customers within the next three years.The delay may stem from (real or perceived) implementation complexities. Over a third (37%) name deployment challenges as a barrier to adoption of passkeys and more than half (54%) are concerned about implementation costs.

Interestingly, passkey uptake is moving faster for employees of the same firms. A bit less than half (41.7%) plan to implement passwordless/ passkeys for their workforce within three years. This mirrors what we see in the industry — financial services organizations want to successfully deploy new technologies internally before bringing them to their customers.

Authentication Technologies for Customers In Use and Planned

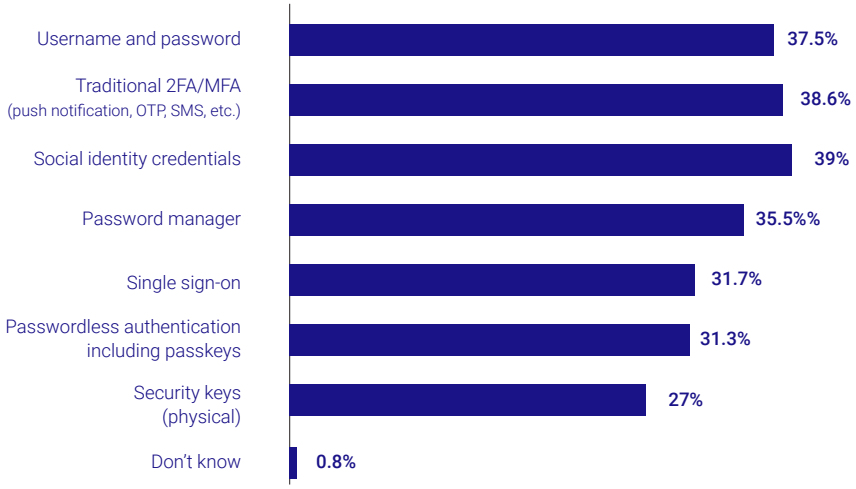


Figure 6: Which of the following authentication methods does your organization plan to adopt, or use/ continue to use in the next 1-3 years for customers? omitting some answer options

Most finance organizations will continue to employ a variety of less secure customer authentication options for the next three years. More than one-third (37.5%) will let customers log in using username and passwords, a similar number will offer legacy MFA methods, and nearly four in ten (39%) plan to offer login that uses social identity credentials.

Synced vs. Device-Bound Passkeys

Passkeys has become an umbrella term for passwordless authentication based on FIDO standards. Passkeys replace passwords with a cryptographic key pair and on-device authentication to make user login easier and more secure. There are two types of passkeys, synced and device-bound.

Synced Passkeys: A synced passkey is a digital credential for phishing-resistant login to websites or apps without a password. They are provided and managed by platforms such Apple, Microsoft, Google. They can be synced between the user's devices via cloud services like iCloud or Google Cloud, and are the type of passkey that consumers are most familiar with.

Device-Bound Passkeys: A device-bound passkey is generated and stored in dedicated hardware on a single device and cannot be shared across devices. This could be a security key (like a YubiKey) or a smartphone or computer.. They are provided and controlled by the enterprise and may support advanced protocols such as transaction signing. Financial institutions frequently choose to implement this type of passkey for their customers, integrated into their own app.

Conclusion

As the finance industry continues to evolve and modernize, organizations face increasing and fast-changing security threats. Generative AI has proven a boon and a risk to finserv companies; improving operational efficiency and services, yet opening up new avenues of attack. In this distributed, connected world, identity is the new security perimeter, and as these findings demonstrate, the greatest area of vulnerability.

Financial services customers, acutely aware of the growing risks, are setting a high security bar for their providers. They have a strong interest in modern security technologies like passkeys, and expect their financial institutions to be at the forefront of such innovations. Client loyalty hinges on how well finserv organizations can meet these expectations.

The good news is that these technologies are mature, enterprise deployable, and actually bring benefits beyond security — faster access, lower help desk costs, less user frustration. The sooner that this technology gets into the hands of consumers, the better off the industry as a whole will be.

How HYPR Can Help

HYPR is a pioneer in FIDO passkey-based authentication, and is deployed and battle-tested in some of the largest banking and financial institutions in the world. The HYPR Identity Assurance platform combines frictionless passwordless authentication, proactive risk controls and integrated identity verification to stop modern identity attacks while reducing customer frustration. Learn how HYPR can help secure your customers and business at https://www.hypr.com/demo.

Appendix: Approach and methodology

The insights in this report were derived from two separate surveys:

1) HYPR commissioned independent technology market research specialist Vanson Bourne to survey 750 IT security professionals in February and March of 2024 for its 2024 State of Passwordless Identity Assurance report, published May 2024. The survey included 259 respondents in the financial services sector. This report uses the financial services survey data to uncover findings specific to that sector. Interviews were conducted online using a rigorous multi-level screening process.

2) The customer research survey was conducted in June 2024 through Userlytics, a research panel company. The sample consisted of 289 US-based consumers. Respondents were invited to take the survey and informed that it was research on attitudes about online banking security. Participants were incentivized to participate via the platform's established compensation program.

Sources

[1] https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2024
[2] https://sumsub.com/fraud-report-2023/
[3] https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html
[4] https://www.epam.com/insights/research/2024-banking-report

See how HYPR helps secure your finance organization and customers

Visit: hypr.com/demo

HYPR
THE IDENTITY ASSURANCE COMPANY

www.hypr.com | hypr.com/contact

About HYPR

HYPR, the leader in passwordless identity assurance, delivers the industry's most comprehensive end-to-end identity security for your workforce and customers. By unifying phishing-resistant passwordless authentication, adaptive risk mitigation, and automated identity verification, HYPR ensures secure and seamless user experiences for everyone. Trusted by organizations worldwide, including two of the four largest US banks, leading manufacturers, and critical infrastructure companies, HYPR secures some of the most complex and demanding environments globally.