SECRET DOUBLE OCTOPUS

June 2026

2026 State of Identity Security in Financial Organizations

Table of Contents

Introduction and Key Findings

Introduction & Methodology

Identity remains one of the most targeted attack surfaces in cybersecurity and a major source of data breach and account takeover risks for organizations. For decades, authentication revolved around passwords, but passwords are notoriously vulnerable and easy to steal, share, and brute-force. This includes strong passwords, which can also be stolen through sophisticated phishing campaigns that cause serious distress and damage to individuals and organizations alike, by compromising identities and stealing data and funds. Even multi-factor authentication (MFA), while helpful, is not immune, especially when one of those factors is still a vulnerable password. In short, passwords have become a liability.

The rise of AI has fueled an increase in credential abuse by making it even easier for cyber criminals to scale their efforts, since rather than requiring specialized skills to launch phishing attacks, they can simply leverage AI-powered tools instead. Indeed, IDC predicts that by 2027, 80% of organizations will experience phishing attacks from criminals using synthetic identities, mixing real information with AI-generated data to create fabricated identities that appear legitimate.

AI has also created new identity risks around legacy systems, which are still widely used by a significant portion of financial organizations. When environments lack modern integrations, users may work around those gaps by sharing credentials in prompts and hardcoding them into agents. In doing so, they dramatically increase the risk of credential exposure, theft, and misuse. This is particularly worrisome for banks and financial institutions, which are heavily regulated to address rising breaches and data theft. To satisfy these stringent requirements, some of the regulations have been specifically developed to create more resistant measures for workforces accessing systems within their organizations, such as phishing-resistant MFA and passwordless authentication, which are now regarded as the baseline for strong authentication.

With the identity security landscape evolving so rapidly, we were keen to capture a snapshot of the market and explore the level of MFA coverage within the finance space. Our aim with this survey was to provide benchmarks for financial organizations to see how their efforts measure up compared with others in the industry, as well as insights on what they can do to reduce risk of phishing attacks and improve their overall identity security posture and compliance. This report should be of particular interest to identity security or IAM managers and leaders within financial organizations, as well as relevant stakeholders in IT, cybersecurity, compliance, and other relevant fields.

Methodology

To get more insight into the state of identity security in financial organizations, we commissioned a survey of 200 IAM leaders and stakeholders to shed light on current trends, challenges, gaps, and priorities in the finance industry.

All respondents hail from companies in the Financial Services industry (including banks, credit unions, investment firms and loan providers) across the US (80%) and Canada (20%), split evenly based on company size (25% in each of 100-500, 501-1000, 1001-5000, and 5001+ employees). The survey is based on responses from influencers and decision makers in the areas of Information Technology, cybersecurity, and identity security, who are responsible for IT security procurement in their departments.

This report was administered online by Global Surveyz Research, an independent global research firm. The respondents were recruited through a global B2B research panel and invited via email to complete the survey, with all responses collected during April 2026. The average amount of time spent on the survey was 6 minutes and 14 seconds. The answers to most of the non-numerical questions were randomized to prevent order bias in the answers.

Key Findings

01 IAM leaders are surprisingly confident, despite major identity security gaps

94% of respondents reported that phishing attacks have increased compared to the previous year (Figure 12), and only 28% of MFA used for workforce authentication is phishing-resistant (Figure 8). And yet, a staggering 82% say they are confident their current controls can mitigate account takeover risk (Figure 13). This reveals a major dissonance, and a wakeup call to assess whether that confidence is justified.

82%
are confident despite the gaps

02 MFA coverage in the finance space is partial and fragmented

Many companies run a mix of strong and weak authentication methods at once (Figure 1), which masks gaps and gives a false sense of security. While SaaS coverage is relatively high (74% on average, Figure 4), the low MFA coverage of legacy apps is of particular concern, with only 50% protected by MFA (Figure 5). Clearly there is a lot of room for improvement.

50%
of legacy apps are MFA-protected

03 Only 15% of workforce authentication flows are passwordless

Companies that do not adopt passwordless authentication essentially make it harder for themselves to prevent potential phishing attacks. The fact that only 15% of MFA workflows in financial services organizations are passwordless (Figure 9) is therefore a missed opportunity that requires attention. Many methods give only the illusion of being passwordless: the password still exists behind the scenes and can be stolen, whereas a true passwordless solution removes it from the flow entirely.

15%
of flows are passwordless

04 Financial organizations struggle to modernize a large legacy footprint

Most organizations (54%) report that 50-74% of their apps and infrastructure are legacy (Figure 6). This is concerning given only 50% of legacy apps have MFA (Figure 5), and 51% cite the inability to support legacy apps as a top obstacle (Figure 10). The legacy footprint is highest where compliance is a top driver (79%, Figure 7), since these systems were never built for modern authentication.

54%
are mostly legacy

Chapter 1: Current Status of Identity Security in Finance

Authentication Methods Currently Utilized for Workforce Access

Banks and financial organizations are currently using a wide range of authentication methods, with password + OTP (77%), password + push notification (76%) and hardware security keys / FIDO2 (72%) topping the list (Figure 1).

These results indicate that many companies are using a combination of both strong and weak authentication methods simultaneously, such as phishing-resistant methods like FIDO2 or biometrics, and weak methods like SMS and OTP, which are easy to attack. This diversification of authentication methods can sometimes mask gaps and risks, giving these companies a false sense of security, because although they have MFA in place, the presence of weaker authentication methods at the same time degrades the efficacy of their overall coverage.

Interestingly, when looking more closely at the top response (Password + OTP) based on company size, we see that usage of this weak, phishable MFA method is more prevalent among small companies with 100-500 employees (90%), than among large enterprises with 5000+ employees (66%), as seen in Figure 2. This suggests that the bigger the company, the less likely it is to use weak MFA methods.

Only 2% of respondents reported they are using single-factor passwords or magic links, suggesting that virtually everyone understands the importance of MFA. That said, as this finding demonstrates, many companies are not using MFA in an optimal way.

TAKEAWAY Consolidating and standardizing authentication methods within the organization can help close gaps, minimize compliance risk, and improve identity security posture.

Figure 1: Authentication Methods Currently Utilized for Workforce Access

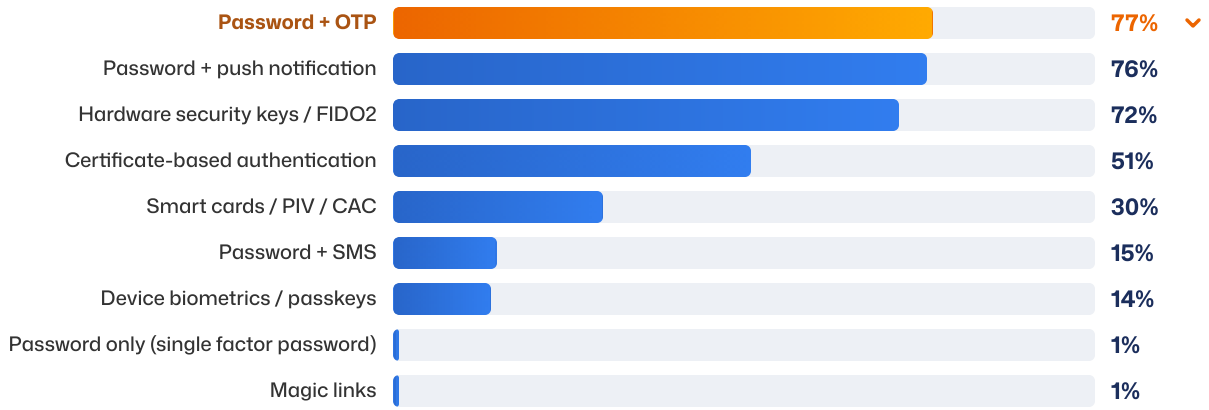
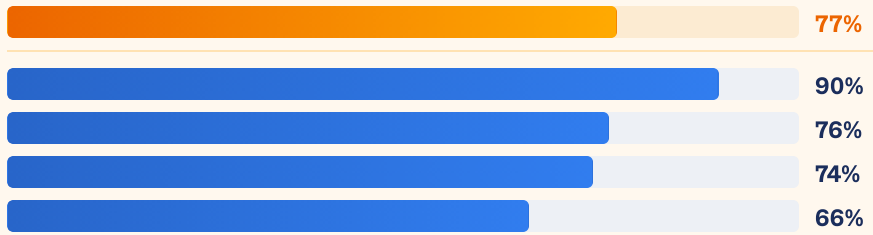


Figure 2: Password + OTP by Company Size



**Question allowed more than one answer and as a result, percentages add up to more than 100%*

Top Motivations for Modernizing the Workforce MFA

When respondents were asked what motivates them when considering modernizing their workforce MFA, their responses revealed five dominant motivations: reducing risk of phishing and credential-based attacks (64%), standardizing authentication across systems and environments (49%), improving overall security posture / moving toward Zero Trust (43%), closing MFA coverage gaps across legacy or on-prem systems (41%) and meeting regulatory or compliance requirements (37%).

While there were many other motivations to choose from besides the top five, the majority of the remaining options were selected only by a small portion of respondents.

TAKEAWAY The top factors that motivate companies in the finance industry to modernize their workforce MFA revolve around reducing risk, improving security posture, closing coverage gaps and complying with regulation. Other factors that are not directly related to security, such as reducing user friction and helpdesk-related costs, are not particularly motivating when considering modernization.

Figure 3: Top Motivations for Modernizing the Workforce MFA

**Question allowed more than one answer and as a result, percentages add up to more than 100%*

Chapter 2: Gaps in MFA Coverage, Including Phishing-Resistant and Passwordless Authentication

MFA Coverage in SaaS Apps vs Legacy* Apps

On average, MFA coverage of SaaS applications in the finance space is relatively high (74%), as seen in Figure 4. That said, it is somewhat surprising that this figure isn't closer to 100%, because most SaaS apps already offer simple, built-in MFA capabilities either directly or through SSO support, so they should be easy to implement if companies decide to enable them.

The low MFA coverage of legacy apps is of particular concern, with an average of only 50% of legacy apps protected by MFA (Figure 5). This essentially means that the large legacy footprint of financial services organizations makes them especially prone to credential-based attacks (as seen next, in Figure 6), which is quite worrisome.

** Note: For this survey, "legacy" refers to systems and environments that are not primarily cloud/SaaS-based, such as on-premises applications, AD-joined Windows or Mac devices, VPNs, virtualization tools, RDPs, and shared-accounts.*

TAKEAWAY IAM leaders in financial services can reduce their susceptibility to risk and improve their overall identity security posture by mapping gaps in MFA coverage within their organization and creating a plan with both short- and long-term priorities to close those gaps.

Figure 4: MFA Coverage in SaaS Applications

Average: 74% of SaaS apps are protected by MFA

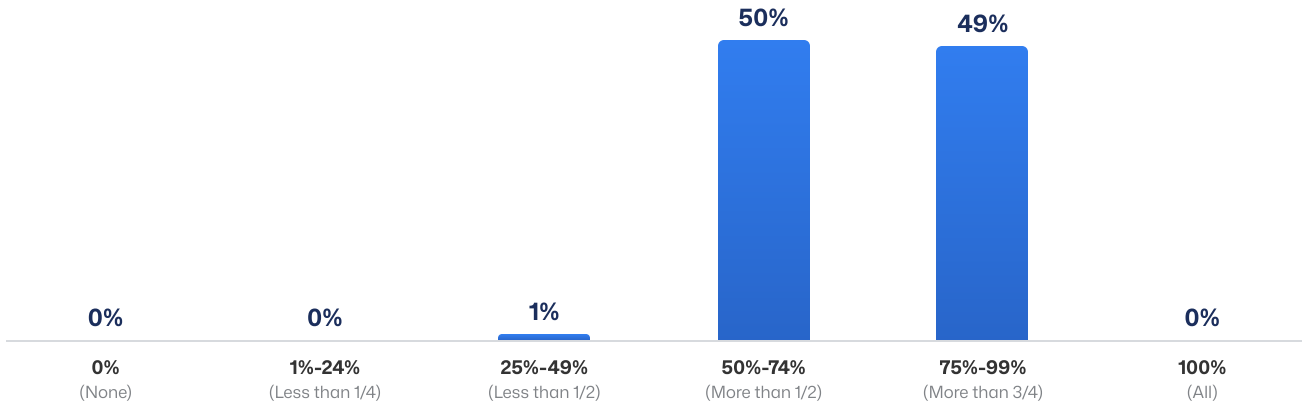
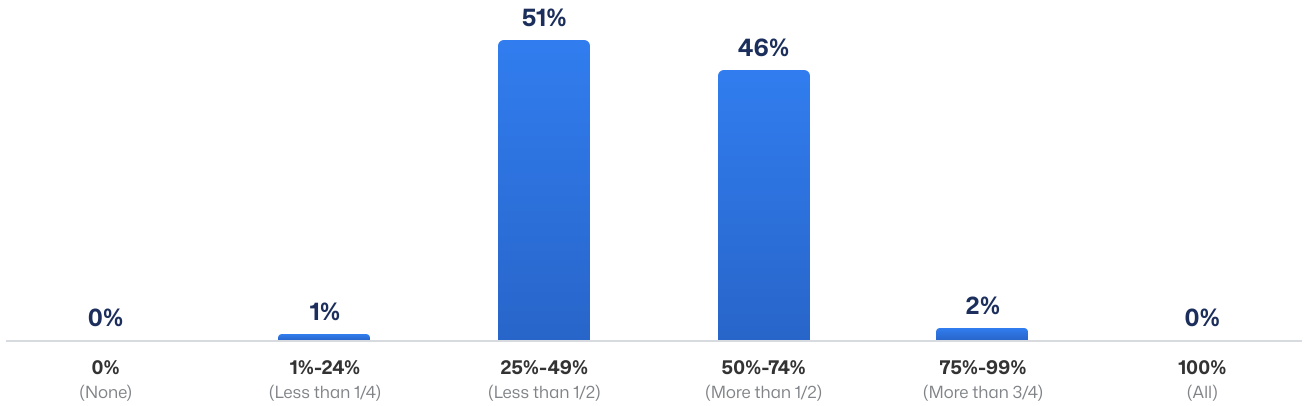


Figure 5: MFA Coverage in Legacy Systems and Applications

Average: 50% of Legacy apps are protected by MFA



Footprint of Legacy Apps and Infrastructure in Financial Organizations

Since only 50% of legacy apps are protected by MFA, as seen in Figure 5, the fact that on average, more than half (52%) of financial organizations' applications and infrastructure are legacy (Figure 6), indicates a fairly concerning gap.

Most of the organizations surveyed (54%) reported that 50-74% of their apps are legacy. The footprint of legacy apps in these organizations is much higher among those for whom compliance with regulation is a top motivation to modernize their workforce MFA (79%), as seen in Figure 7. This is unsurprising given that legacy applications and infrastructure are typically very old and were not designed with advanced authentication capabilities in mind, making it more difficult for companies with a large footprint of legacy apps to comply with today's increasingly stringent security regulations. This finding therefore suggests a link between legacy-heavy organizations and compliance concerns.

TAKEAWAY Implementation of MFA should be prioritized for legacy apps to address risk and comply with regulations.

Figure 6: Legacy vs SaaS Applications and Infrastructure in Financial Organizations

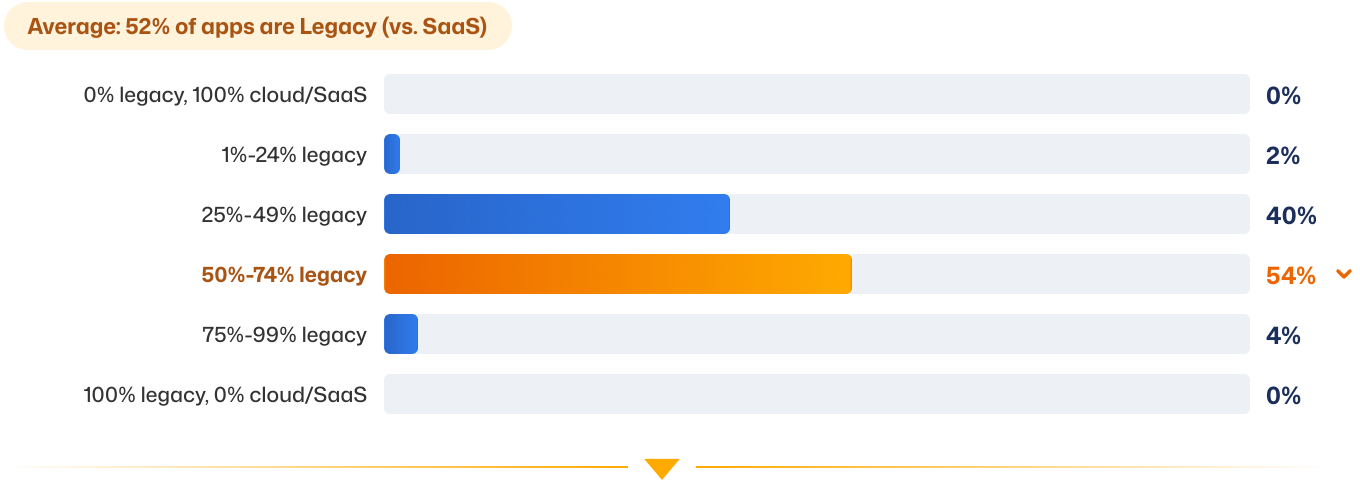
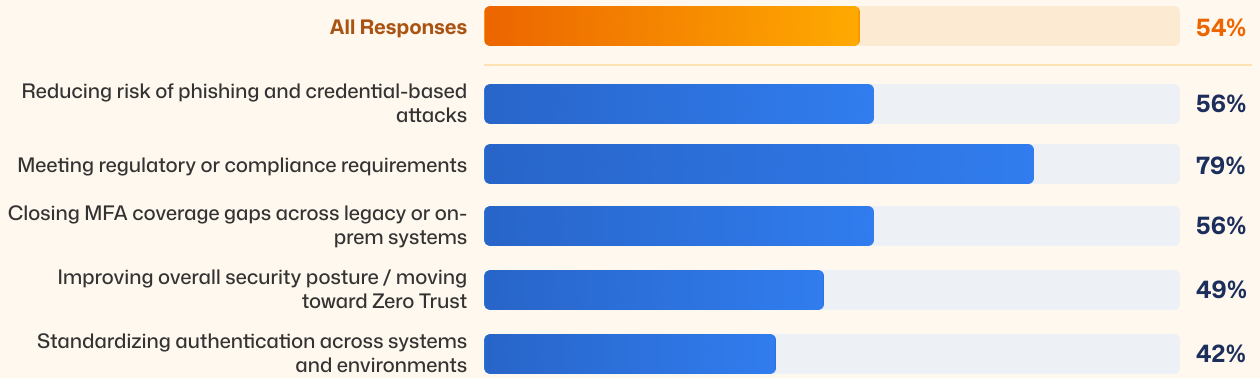


Figure 7: "50%-74% Legacy" by Top Motivations for Modernizing the Workforce MFA



Percentage of Utilized MFA Which Is Phishing-Resistant

On average, only 28% of MFA used for workforce authentication in financial organizations is phishing-resistant.

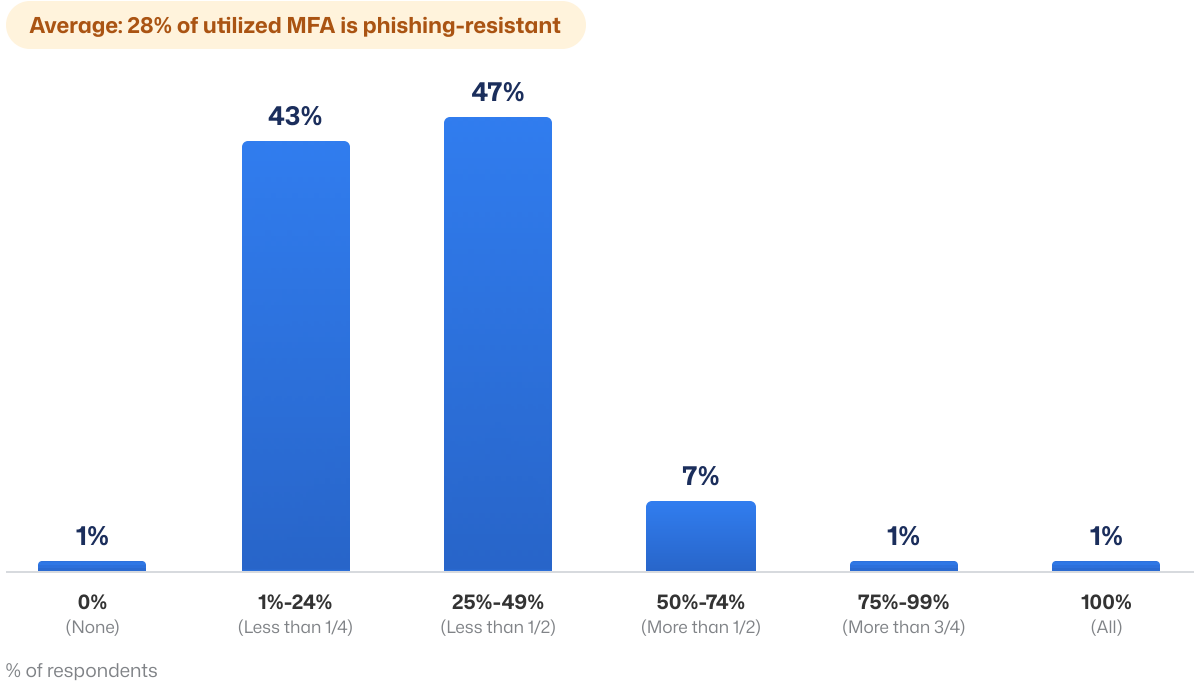
Phishing-resistant MFA typically relies on cryptographic devices or the elimination of phishable credentials. Methods such as SMS/email OTP (one-time password) or mobile push verifications are NOT considered phishing-resistant.

Given that on average, 74% of SaaS apps and only 50% of legacy apps are protected by MFA (as seen in Figures 4 & 5), the fact that on average only 28% of this MFA coverage is phishing-resistant suggests that actual protection against phishing attacks is very low. Most modern regulatory demands specifically mention the need for phishing-resistant MFA to protect sensitive data, so the fact that most organizations in the financial sector have very limited actual identity protection for their systems, and legacy systems in particular, which are sometimes more than a decade old, are quite concerning.

TAKEAWAY Financial organizations should identify weak authentication methods and consider upgrading to phishing-resistant ones to ensure compliance and minimize risk.

28% of utilized MFA is phishing-resistant, on average. Real protection against phishing is far lower than overall MFA coverage suggests.

Figure 8: Percentage of Utilized MFA Which Is Phishing-Resistant



Percentage of Workforce Authentication Flows That Are Passwordless

We asked respondents what percentage of workforce authentication flows at their organization are passwordless, i.e., where no user-managed password is required. Their responses revealed that on average, only 15% of their workforce authentication flows are passwordless.

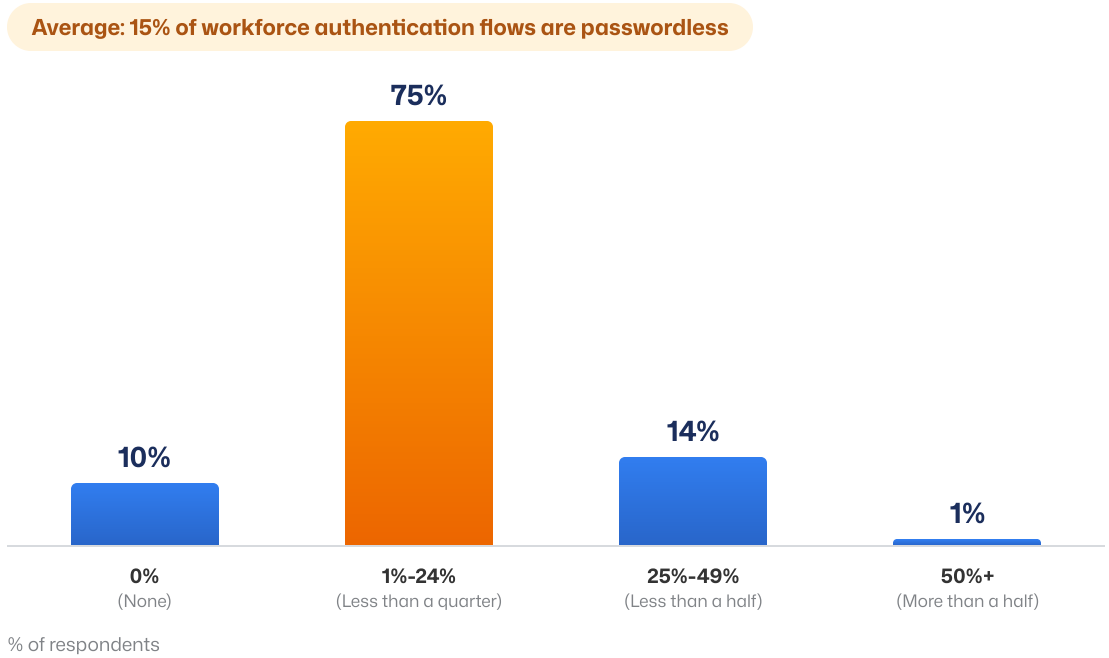
The low implementation of true passwordless solutions is likely due to the fact that it is limited by various technical challenges (as seen in figure 10). In addition, some stakeholders may perceive implementation as 'difficult' because they are not aware that it is possible to modernize authentication of legacy apps without the need to rearchitect or replace old systems.

Another reason for low implementation is that many passwordless authentication methods only give the illusion of a "passwordless user experience", in the sense that users are asked to provide their passwords far less frequently, like when using facial recognition or a fingerprint to unlock a device. Behind the scenes, however, the password still exists and is still known to the user who may be prompted to provide it in certain circumstances, which means it can be stolen or compromised. A true passwordless solution eliminates the password from the authentication flow completely, which is the ultimate way to fight phishing.

TAKEAWAY It's time for organizations in the financial services industry to join the passwordless revolution that's already being led by all the big-tech companies. By reducing their reliance on passwords in workforce authentication flows, they can substantially improve their identity security posture.

15% of workforce authentication flows are passwordless, on average. The vast majority still depend on phishable passwords.

Figure 9: Percentage of Workforce Authentication Flows That Are Passwordless



Chapter 3: Key Challenges and Trends in Adoption of Phishing-Resistant MFA

Key Challenges Preventing Universal Implementation of Phishing-Resistant MFA

We asked respondents what they consider to be the biggest obstacles preventing their company from implementing universal phishing-resistant MFA across all workforce applications and services (Figure 10). The top challenges are: technical or architectural complexity (79%), cost and budget constraints (53%), the inability to support legacy apps and infrastructure (51%) and multiple IAM solutions (51%).

As we saw earlier, most of the organizations surveyed (54%) reported that 50-74% of their applications and infrastructure are legacy (Figure 6), and that only 50% of legacy apps are protected by MFA (Figure 5). Given the seriousness of these findings, we looked further into the responses of those who said that the inability to support legacy apps is their top challenge (51%), and analyzed them based on job seniority (Figure 11). Interestingly, the results showed that among first-level team leads and managers, a substantial 62% list this as a top challenge, compared to Directors (56%) and VP/C-Suite level executives (19%). This reveals a trend, where the more senior the stakeholder, the less they regard the inability to support legacy apps as a top challenge, possibly because executives have less visibility into the legacy challenge than first-line managers do, or because they have a broader list of priorities than IT managers whose primary focus is on actually managing identity security.

TAKEAWAY IAM leaders and senior management should align on the importance of securing legacy applications and infrastructure, as well as the challenges involved. The sooner organizations bridge this gap, the faster they can strengthen their overall identity security posture.

Figure 10: Key Challenges Preventing Universal Implementation of Phishing-Resistant MFA

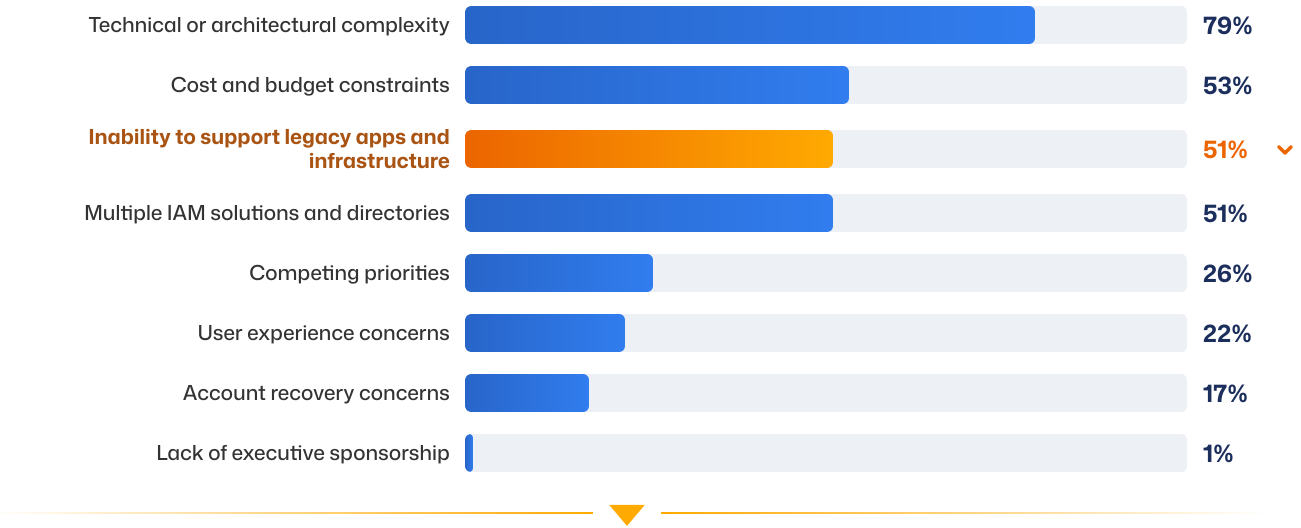
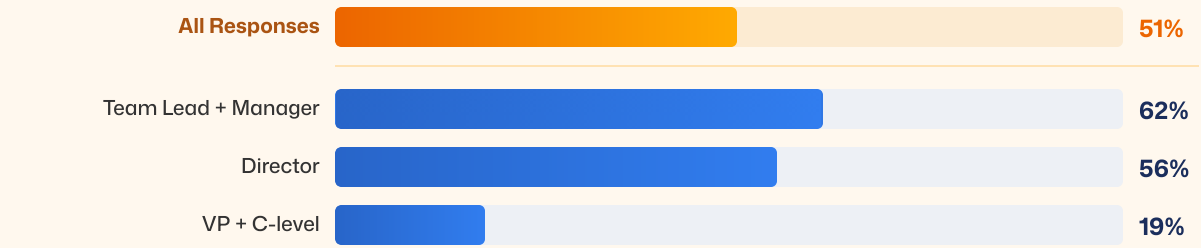


Figure 11: Inability to support legacy apps and infrastructure by Job Seniority



**Question allowed more than one answer and as a result, percentages add up to more than 100%*

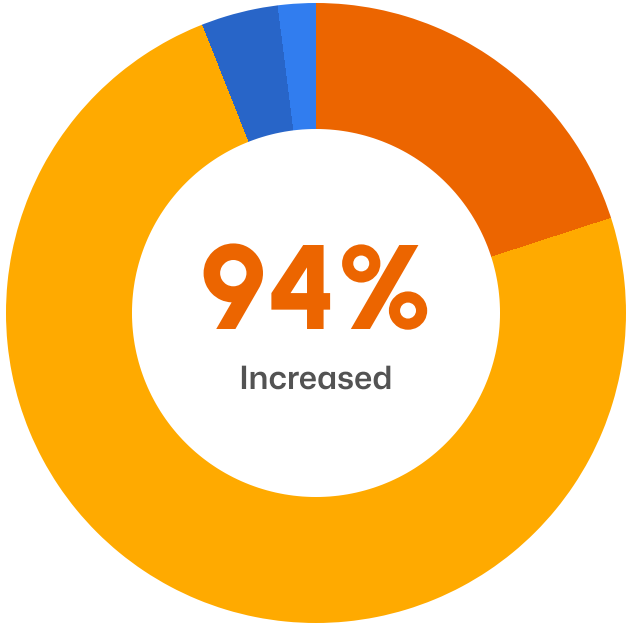
Phishing Attacks Over the Past 12 Months

When asked to what extent they have experienced phishing attempts against their organization in the past 12 months, a whopping 94% of respondents reported that phishing attacks have increased compared to the previous year, with 20% describing this increase as significant.

While it's likely of no surprise to anyone that the rate of phishing attacks has increased, the fact that such a high proportion of companies recognize this increase reinforces the severity of the problem.

TAKEAWAY Phishing activity has not plateaued; rather, it continues to grow and poses an ongoing threat. Given that phishing-resistant MFA protection is very limited at banks and financial institutions, as seen throughout this report, this means that a significant number of them are highly vulnerable to attacks, and therefore facing a race against time to upgrade their identity security posture.

Figure 12: Trends in Phishing Attempts Over the Past 12 Months



Significantly increased	20%
Increased	74%
Stayed about the same	4%
Decreased	2%
Significantly decreased	0%

Level of Confidence in Current Authentication Controls to Mitigate Account Takeover Risk

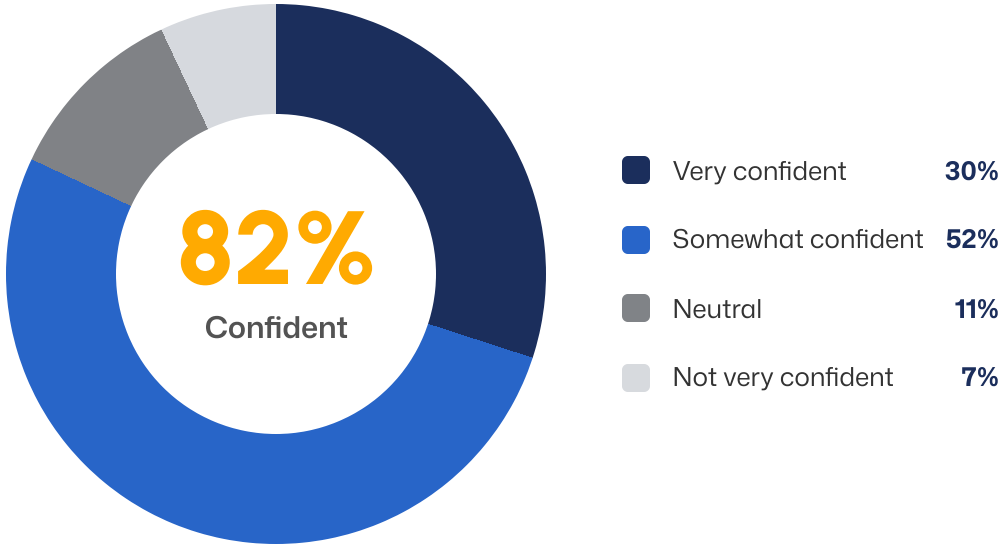
In stark contrast to the previous findings, a staggering 82% of organizations report they are either "somewhat" confident (52%) or "very" confident (30%) that their current authentication controls can effectively mitigate account takeover risk. This is highly surprising.

This finding reveals a major dissonance between the actual risk facing organizations in the finance space, and how they feel about it. Given that most of their responses throughout the report indicate that their MFA coverage is partial, their phishing resistance is extremely limited, and phishing attacks are on the rise. It is odd that most respondents feel such a strong level of confidence in their ability to mitigate the increasing onslaught of identity security threats with their current authentication controls. It is even more baffling, considering that half of the organizations in the industry are still heavily reliant on legacy apps that were not built with modern identity security measures in mind.

This dissonance may also point to a potential blind spot, in that many finance companies that have some form of MFA in place feel a false sense of protection, because they are unaware that MFA is not effective if coverage is only partial (because it still leaves critical systems unprotected) or if it isn't phishing-resistant. Moreover, they may be unaware that their current MFA gaps are actually solvable, by upgrading to more modern, and more regulation-compliant authentication methods.

TAKEAWAY This finding is akin to a major wakeup call for companies to assess whether their confidence in their current authentication controls is justified. They can do this by mapping their identity security measures, identifying apps that are not covered by MFA (or where passwords are still used), and creating both a short- and long-term plan to migrate to universal phishing-resistant MFA protection.

Figure 13: Level of Confidence in Current Authentication Controls to Effectively Mitigate Account Takeover Risk



Demographics

Country, Industry, Company Size, Department, Job Seniority and Role

Figure 14: Country

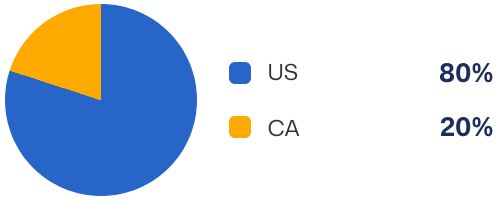


Figure 15: Industry

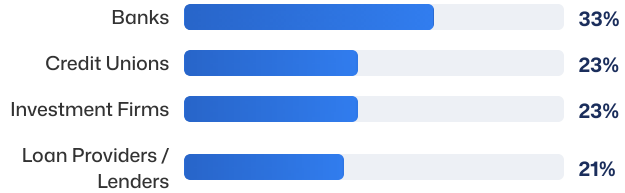


Figure 16: Company Size

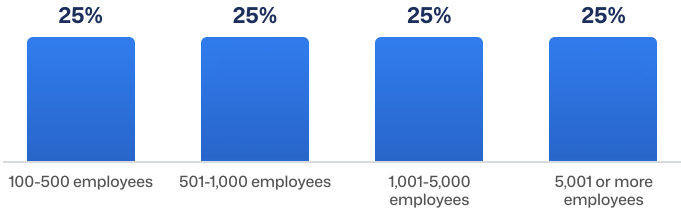


Figure 17: Department

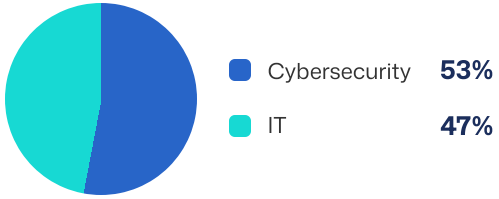


Figure 18: Job Seniority

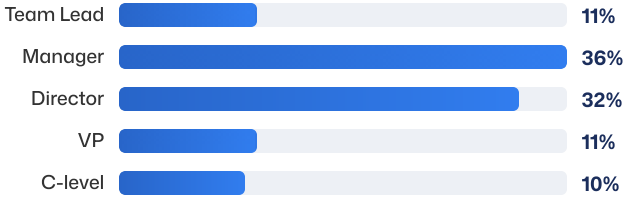


Figure 19: Role

SECRET DOUBLE OCTOPUS

About Secret Double Octopus

At Secret Double Octopus, we believe authentication should be stronger, simpler, and completely password-free.

Our patented ZeroPassword™ technology eliminates passwords even from legacy and on-prem systems, delivering unmatched security and user experience.

Our platform integrates seamlessly into any infrastructure, supporting any system, use-case, or authentication method.

Trusted by SMBs and Fortune 50 enterprises alike, we secure billions of authentications annually, enabling organizations to achieve modern, phishing-resistant security at scale.

Book a Demo

Visit us at: **https://doubleoctopus.com/**