Fighting The Next Major Digital Threat: AI and Identity Fraud Protection Take Priority

PingIdentity®

Executive Summary

JAMIE SMITH
Decentralized Identity Expert
and founder of Customer Futures

It's a challenging moment for those working in digital identity and security. Over half of organizations say they are 'very concerned' about today's identity threats, and 48% say they are not effectively managing today's security and identity risks. When only 52% of respondents say they could spot a deepfake of their company's CEO, we need to start asking questions about our approach to digital identity — to protect both our customers and our businesses.

The timing matters. AI-powered cyber threats and identity attacks are about to explode, with over 40% of businesses saying they expect fraud to increase significantly next year. It's why two-thirds of enterprises say they will invest much more next year on advanced protections. And they're serious: on average they're spending over $30M this year alone on combatting new AI-enabled identity attacks.

When only around 4 in 10 businesses have adopted advanced identity protection technologies, there is more to do. But additional investment is not going to be enough. We need a new way to think about — and respond to — the challenges around security and identity fraud.

KEY GLOBAL TAKEAWAYS:

97% of organizations are experiencing challenges with identity verification.

54% are very concerned that AI technology will increase identity fraud.

52% are very concerned about credential compromise, followed by account takeover (50%).

52% Only 52% say they're fully confident they could detect a deepfake of their CEO.

48% are not very confident they have technology in place to defend against AI attacks.

45% Only 45% say their organization uses two-factor/multi-factor identification verification to protect against fraud.

41% expect cybercriminals' use of AI to significantly increase identity threats over the next year.

38% Only 38% have implemented a strategy to use DCI as a protection against fraud for both customers and employees.

There's good news: nearly 60% of businesses surveyed say that **Decentralized Identity** — the idea of giving a digital wallet to customers, so they can personally hold and selectively share their own personal data — will be 'highly valuable' to their organization. Why? Because first, it's a breakthrough approach to tackling digital ID threats and fraud. And second, executives believe this new technology can deliver opportunities *right across the organization*. From better customer experiences and reducing business overheads; to tackling fraud and responding to shifting data protection regulations.

And there's a twist: decentralized identity isn't just seen as a tactical upgrade to MFA and passwordless; it's more than a new cost-effective platform for digital ID. It's fast becoming positioned as a *strategic approach* to digital business transformation. Not only helping businesses *defend* against new identity threats, but becoming a **new driver for business growth**.

"Decentralized identity is now seen as the smart way to help businesses tackle today's identity threats, while also preparing for tomorrow's AI-enabled attacks. When can you implement a new digital approach that defends against identity threats, but also positions the business for growth? Well, it's a no-brainer. And 99% of businesses surveyed say they agree."

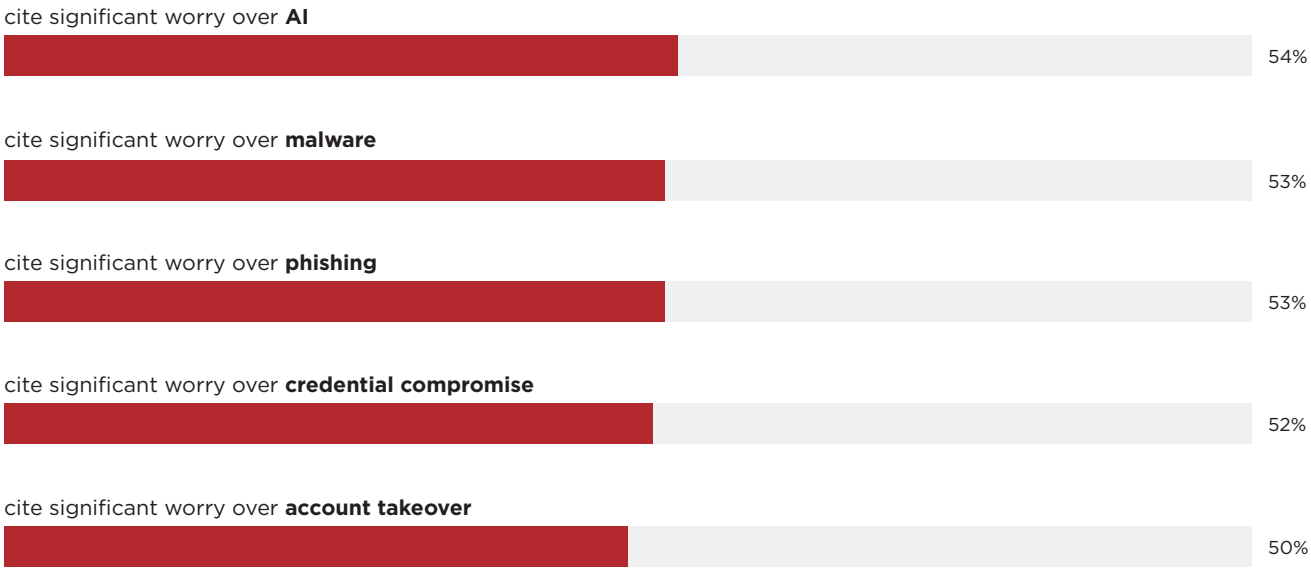
JAMIE SMITH
Decentralized Identity Expert
and founder of Customer Futures

It's no surprise then that 38% of businesses say they already offer some version of decentralized identity. Issuing portable digital credentials directly to the individual so they can control the data they share. Of course, most organizations are cautious about adopting this new technology. Many are concerned about the risks of technical integration and accessibility. And over half want to make sure they avoid overburdening customers. But overall, businesses are optimistic about adoption. And they are putting in place plans to adopt decentralized identity technologies, both to protect customers and the business, but also to unlock new digital opportunities.

Businesses aren't using the most advanced technology available to prevent fraud.

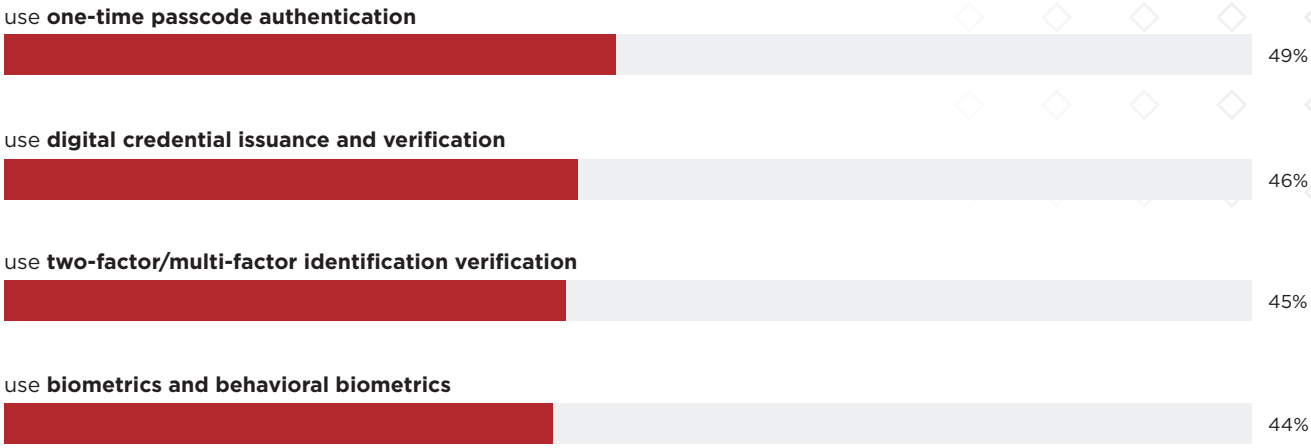
No question, organizations understand they're at risk. Every company and leader surveyed knows that processes must be put in place to guard against identity fraud; it's no longer optional. Nearly every organization surveyed reported that they have some solution in place to protect their workforce and customers against fraud. But where they fall short is in taking that protection to the next level. 94% of respondents have concerns over their organization's ability to protect against threats.

Organizations have multiple concerns when it comes to identity fraud:



Despite stronger protection solutions available, many organizations aren't taking full advantage. Just less than half of survey respondents reported using advanced protection technologies like multi-factor authentication (MFA) or biometrics— and that's a problem. What these companies do have in place right now spans a more rudimentary selection of security solutions, from the increasingly common passcode authentication to knowledge-based authentication and more.

The three most common protections organizations deploy against identity fraud are **one-time passcode authentication, digital credential issue issuance and verification, and two-factor/multi-factor identification verification.**



Despite not having the proper identity protections in place, the businesses surveyed do know something must be done. And there's a struggle to reconcile that knowledge with implementation that's putting these organizations and their customers at risk.

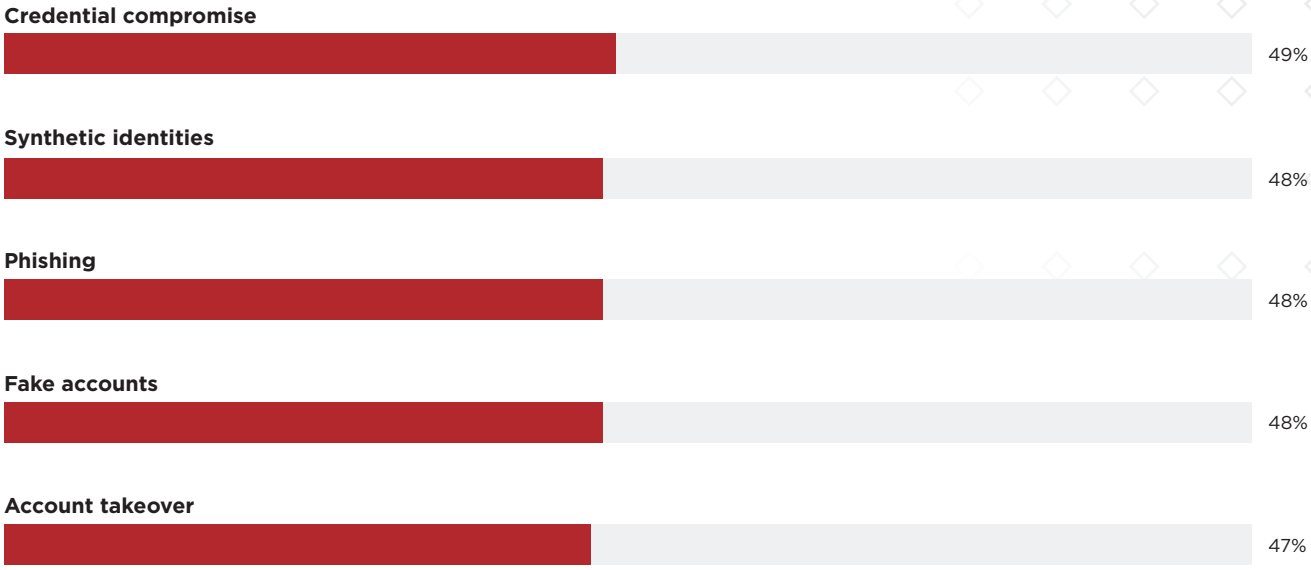
Identity fraud is acknowledged universally as a problem, yet often remains a vulnerability as leaders and companies struggle to implement the right methods and solutions to protect themselves. This will only get worse as AI continues to advance and evolve. While respondents noted malware and phishing as other top concerns, more than half (54%) reported newly emerging AI threats as a high source of anxiety.

These same companies know that the processes and solutions they have in place aren't cutting it. Their current protections, including recognizing and tackling identity fraud challenges simply aren't effective enough.

"Nobody will tell you that they don't worry about identity fraud in their organization. It's far too big a threat. To better protect against advancing fraud threats, companies need to incorporate more advanced technologies. Simpler, legacy solutions aren't enough to safeguard an organization from today's threats, particularly with AI."

PATRICK HARDING
Chief Architect, Ping Identity

Organizations aren't good at solving:



All of this points toward a significant problem: mitigation of identity fraud threats.

In addition to the common protections mentioned above (one-time passcode authentication, credential verification, 2FA & MFA, and biometrics), organizations are especially challenged with identity verification.

Challenges with identity verification troubles

97%

of respondents.

"Anyone today understands the pain points of being asked for multiple ways of proving they are who they say they are when they log into an account or a device. We all want our information to stay protected, but there's a line to walk between convenience and protection from risk. It's a tricky, yet necessary, balance to strike."

PATRICK HARDING
Chief Architect, Ping Identity

It's a two-part issue: the obvious need for security balanced against user experience. Companies who want to protect themselves must find a way to do that without impacting their employees' or customers' user experience.

Facing these challenges means changing an organization's mindset — and shifting priorities. Around ⅔ of organizations surveyed globally said they plan to increase their investment in fraud protection over the next year as a way to tackle these challenges — but it's not universal. Companies in the U.K. and Germany, for example, are less likely to prioritize budget increases in identity-based security over the next year outside of government organizations.

While organizations may differ in their plans to tackle this challenge, it's clear that they know there is a challenge. Risk is inevitable — so how can companies best defend themselves? Decentralized identity is emerging as a smart solution.

"Fraud is on the rise, and it's getting worse with AI. Leaders know that they need to level up, yet so many organizations don't have the right guardrails in place to mitigate or prevent these kinds of threats. The longer they go without, the more they put themselves in harm's way. Acting against tomorrow's attacks means removing vulnerabilities and limiting valuable data troves."

PATRICK HARDING
Chief Architect, Ping Identity

INDUSTRY SPOTLIGHT: RETAIL

Retailers are especially vulnerable to customer identity fraud, and they have a particular problem: synthetic identity fraud. Attackers Frankenstein different pieces of information from multiple people to create a new identity for someone who doesn't exist or they simply create an account with a real person's stolen information. Despite only 41% of retail respondents expressing significant concern, this emerging threat is at an all-time high, and is growing. These companies can't afford to refuse more advanced protection — which decentralized identity provides.

Not enough organizations are using decentralized identity to protect themselves against fraud.

Security teams face a major problem with identity theft, but there's a bigger problem. There's a disconnect between education and action that puts organizations in a difficult spot of not being able to guard against tomorrow's threats. Identity proofing paired with credential issuance and verification is a top solution, but not enough businesses are rising to the call to adapt and incorporate this technology into their security infrastructure for workforce or customer use cases.

"Everyone knows that identity management is a problem, and that it's getting harder to manage. Yet so many businesses are struggling. While most large organizations understand that decentralized identity presents a way out of the mess, only about half are putting things into practice. Concerns about integration and accessibility are preventing more widespread adoption, but the truth is that failing to adapt to this new approach to identity and security will only put organizations under more pressure - both financially and reputationally."

JAMIE SMITH
Decentralized Identity Expert
and founder of Customer Futures

Less than half of organizations (38%) surveyed have implemented a strategy to use decentralized identity as a protection against fraud.

But more are beginning to offer this solution, with our survey showing a 25% year-over-year increase over last year's adoption rates.

Decentralized technologies arm organizations against fraud by giving the user control over repeated, verifiable identity proofing and data sharing with either the verification source or any relying third party. Rather than collecting, storing, securing, and verifying data attributes, this approach combines verification, authentication, and authorization into one biometric scan on a mobile device, making mass attacks that much more difficult or even impossible. Organizations in the United States and Australia have most readily latched onto this solution, with respondents in those countries reporting the highest rates of adoption.

Despite nearly half (43%) not implementing this kind of technology for either their customers or employees, though, 99% of respondents agreed — there's value in decentralization. So what is stopping these organizations from integrating this kind of protection into their systems?

"The value of decentralized identity can't be stressed enough. Not only do you increase the difficulty of a large-scale attack, but you empower customers and employees by giving them full control over what they choose to share. It also enables seamless authentication and better verification."

PATRICK HARDING
Chief Architect, Ping Identity

97%

of respondents see challenges to implementation.

Organizations have a multitude of systems and processes within their existing infrastructure. It's not difficult to see why the majority (52%) of respondents would list integration as a major barrier to adoption. An additional 57% predicted technical problems, outages and system failures that could significantly impact an organization's operations.

These organizations also worry about shifting their existing infrastructure to better accommodate and prioritize decentralized identity as a means of risk mitigation. By necessity, adoption means shifting cybersecurity risk from the back end to the front end. Users have the power when it comes to this kind of protection, but it means they're also burdened with the risk. But that doesn't mean that integration is an impossible task. By planning and taking the time to examine existing systems, security teams can put themselves in a place to implement without incident.

Accessibility, app explosion and exclusion respondents also listed among concerns, but none of these are unsolvable.

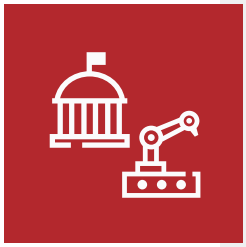
The more security teams can educate their colleagues about the benefits of decentralized identity and, most importantly, proper use, the more they can solve those issues before they become real problems. Respondents understood that, too. Additionally, 61% reported believing that decentralized identity could increase new account fraud and account takeover.

These concerns aren't without merit, but they aren't without solutions, either. With the right planning and education, organizations can position themselves for a solid, streamlined implementation of the kind of technology that only saves them from costly attacks down the line.

Organizations are beginning to understand that this technology can't be ignored when it comes to fraud prevention. Stakeholder buy-in, too, makes a strong case for adoption, with 54% stating they'd be more likely to seek these solutions based on higher demand from leadership, partners and customers.

"What businesses have to understand is that decentralized identity is an inevitable part of the future. The smarter AI becomes, the more it becomes a significant threat to every organization in every industry. Planning now and educating key executives is the only way for leaders to protect themselves against rising threats."

JAMIE SMITH
Decentralized Identity Expert
and founder of Customer Futures



INDUSTRY SPOTLIGHT: MANUFACTURING, GOVERNMENT & FINANCE

Manufacturing and government organizations are well on their way to wider strategy adoption, with both sectors hovering at around 50%. On the flip side, finance reports the lowest strategy adoption rates of decentralized identity at only 26% — despite cyber attacks often targeting financial institutions.

Organizations aren't confident in their ability to defend against AI-based threats.

"AI is and will continue to redefine life as we know it. It's a double-edged sword in the truest sense. We can use it to make the day-to-day easier both in professional and personal terms, but we also have to look at the way it widens the risk landscape. From an identity standpoint, AI compromises trust. It gives attackers greater ability to execute, and it can't be ignored."

PATRICK HARDING
Chief Architect, Ping Identity

AI has become an undeniable and powerful part of the digital landscape, for better or for worse. This powerful technology makes systems stronger and more automated — but it also presents a hindrance to security efforts that, left unchecked, puts companies at major risk of threats.

AI brings another complication to identity protection. Respondents agreed: worry over this new and growing threat ranked highly as 54% of organizations expressed extreme concern that this technology will increase identity fraud and attackers' ability to cause real harm and damage. Only 52% expressed high confidence in their ability to detect a deepfake of their CEO.

The problem is that with this technology continually advancing, many organizations don't yet have the proper protection in place to guard against AI-based threats. 48% of survey respondents lacked confidence in their existing infrastructure's ability to fight these kinds of attacks. The manufacturing industry and respondents in France particularly expressed the greatest concern, but it's a universal and pressing fear: 41% of respondents globally expected cybercriminals to significantly increase their use of AI over the next year.

These organizations are working on a solution: investing in systems ready to defend against AI. Even those with a strategy in place are already planning to invest an average of U.S. $35 million in AI protection, with a hybrid approach between in-house and vendors ranking most popular at 56%.

95%

of organizations surveyed are expanding budgets to fight AI-based threats.

AI also presents a major opportunity when it comes to risk protection and management. In Germany, especially, those surveyed see the potential for better security with the incorporation of AI. With this tech, security teams will see the ability to dynamically change user authentication, increased automation and better training for fraud detection. And those are only a few of the benefits.

"Organizations across the board have to arm themselves with AI even as they look to fight against it. Security teams have an opportunity to harness this powerful, continually evolving technology as the threat landscape spreads and becomes capable of greater harm."

PATRICK HARDING
Chief Architect, Ping Identity

"We can't predict where AI will be next year, let alone in five or 10 years. What we can do is understand that the use of AI will only continue to grow, presenting ever more opportunities and challenges. If organizations haven't already incorporated AI into their security and identity management systems, they're going to pay the price. Especially when this becomes a competitive threat: customers will quickly migrate to those companies and brands that can protect them and their data. And that's going to take cutting-edge technologies and approaches to identity management"

JAMIE SMITH
Decentralized Identity Expert
and founder of Customer Futures

For better or for worse, AI is the present and the future. While we can't predict its trajectory, organizations can understand what the current environment looks like. Sophisticated email phishing and deepfakes are only two examples of how attackers can use it. Companies can't afford to step onto the battlefield without defenses just as advanced as their opponents' weapons. Already, they're taking steps toward arming themselves for a fight, with 60% improving or adapting their monitoring tools to increase detection capabilities.

INDUSTRY SPOTLIGHT: HEALTHCARE

Despite being in possession of incredibly personal information, only 27% of healthcare organizations surveyed have implemented a strategy to protect against AI-based identity threats. Without the proper safeguards and forward-thinking, these organizations are leaving their patients especially susceptible to fraud.

Conclusion

As technology evolves, so does the threat landscape for identity management. Identity fraud is a widespread issue across every sector and geography, plaguing businesses and consumers alike. With the expansion and evolution of AI-based threats, we can only expect this to become more of a business-critical problem. Yet while all businesses have some levels of defense, the truth is that for many, those protections aren't enough.

These companies must take proper precautions for the sake of their reputations, bottom lines and their users. Despite common concerns around integration and accessibility, robust mitigation that leverages threat detection, common protections, and identity verification, in conjunction with a decentralized approach, is the best solution to defend against increasing AI-enabled digital threats.

With the right education, planning and partnerships organizations can put themselves in a strong position to fight increasingly sophisticated identity and fraud attacks. This is a necessity, not a choice, as attackers seize the power of AI for their bad intentions. The more an organization can do to prepare today, the better equipped it will be to defend tomorrow.

WE RECOMMEND THREE ACTIONS FOR BUSINESS EXECUTIVES:

1. Consider how decentralized identity can form part of your wider AI response, and part of the business case for digital growth and building competitive advantage.

2. Engage and educate your leadership teams right across the organization around decentralized identity, making the case for a digital identity strategy that includes both 'defense' (dealing with AI-enabled security threats) as well as 'offense' (delivering digital growth).

3. Get started now — it will take time to develop the right strategy, engage the right teams and partners, and implement solutions. With AI-enabled identity threats only increasing, you don't have time to waste.

"Implicit trust is something businesses can no longer afford, and leaders know that. Risk is only going to grow alongside technology. Respondents understand they need better capabilities to fight against identity fraud. Until these businesses plan and educate to drive better adoption of decentralized identity, they remain vulnerable. Those working on a strategy to implement, on the other hand, will see the rewards as they mitigate and manage fraud through trusted solutions."

PATRICK HARDING
Chief Architect, Ping Identity

"Most businesses have some kind of identity management and protection strategies in place. But in most cases, it's just not advanced enough to provide real protection. Organizations are aware of the major risks of fraud. However, they're also aware that decentralized identity has major value in preventing it. We're beginning to see strategy implementation, but for companies to fight tomorrow's AI-based identity threats, businesses need to act faster, towards integrating new decentralized identity management tools and infrastructure. The hidden opportunity is that this approach won't just help protect your customers and business. It can unlock new digital growth too."

JAMIE SMITH
Decentralized Identity Expert
and founder of Customer Futures

Methodology

Ping Identity and Vanson Bourne surveyed 700 IT decision-makers between February and March 2024 from the U.S., U.K., France, Germany, Australia and Singapore. These respondents came from organizations with at least 500 employees and U.S. $100 million in global revenue, and represented a range of sectors.

ABOUT PING IDENTITY:

Ping delivers unforgettable user experiences and uncompromising security. We make crafting digital experiences simple for any type of user—partners, customers, employees, and beyond. We are anti-lock-in. That means integration with existing ecosystems, clouds, and on-prem technologies is simple. Out-of-the-box templates let businesses leverage our identity expertise to give their users frictionless experiences. Whether they're building a foundation of modern digital identity, or out-innovating their competitors with cutting-edge services like digital credentials, AI-driven fraud prevention and governance, Ping is the one-stop shop for game-changing digital identity.

ABOUT VANSON BOURNE:

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.