Bridging the Trust Gap in the Age of AI

2025 CONSUMER SURVEY

Executive Summary

DARRYL JONES
Vice President of Consumer Segment Strategy, Ping Identity

As AI and the rise of agents continue to transform the world and permeate every aspect of our lives, consumers find themselves faced with not only new opportunities, but also new threats and problems. If concerns about security were high before, AI and agents have only expanded them. Consumers now question how — in an age of ever-advancing and sophisticated threats — they can trust brands to simultaneously keep up with technology advancements while protecting their data, and global brands must take notice or risk reputational and financial damage.

Ping Identity commissioned a global survey of 10,500 consumers to gain insight into consumers' behavior. Results showed how AI has further eroded an already rocky relationship with global brands, how AI has impacted their daily lives when it comes to privacy, security, and scams, and concerns over how continued evolution and legislation may shape AI.

We found an increasing sense of unease from consumers when it comes to global brands and their defenses against AI-powered threats, culminating in a crisis of confidence we call "the trust nothing era." Our survey reports that only 17% of consumers have full trust in the organizations tasked with managing their identity data. Global brands in particular took a hit in the survey, with 20% of respondents reporting they trust regional or local brands compared to only 14% who trust global enterprises.

AI isn't only translating into consumers' security concerns and global brand trust. Respondents say AI has infiltrated nearly every area of life, exacerbating their fears and heightening anxiety over what this technology can do. Expanded use means expanded understanding and worry: 75% reported greater concern over personal data, and only 32% reported not using AI in their own lives — down from the 54% reported in 2024, a 40% change year over year. It also leads to a myriad of evenly distributed concerns, from invasion of personal privacy by AI programs to AI-generated fishing, as consumers become more aware that these different threats exist.

Brands aren't alone when it comes to consumers' concerns about protecting their data. Less than a quarter (23%) of respondents felt very confident in their own scam-identifying abilities, while 73% said their fears drive their desire for better government regulations to protect against these advancing threats.

While these numbers sound bleak, organizations aren't completely at the mercy of AI and the adversaries who use it. In this report, we'll dive into consumers' fears and distrust when it comes to emerging technology, global consumer brands, and identity data. We'll provide insight into where and why concerns exist, and how organizations can take action to implement measures that create a safer, more secure, and more trustworthy digital experience.

KEY TAKEAWAYS:

17% of consumers have full trust in organizations that manage their identity

20% trust regional or local brands with their identity data, while only 14% trust global brands with their identity data

34% report biometric authentication as the top feature that would increase trust in online brands

23% feel very confident in their ability to identify scams

68% now use AI in their personal lives —an increase from 41% year over year

75% are more concerned about personal data security than they were five years ago

39% reported AI-driven phishing of highest concern when it comes to modern or future scams

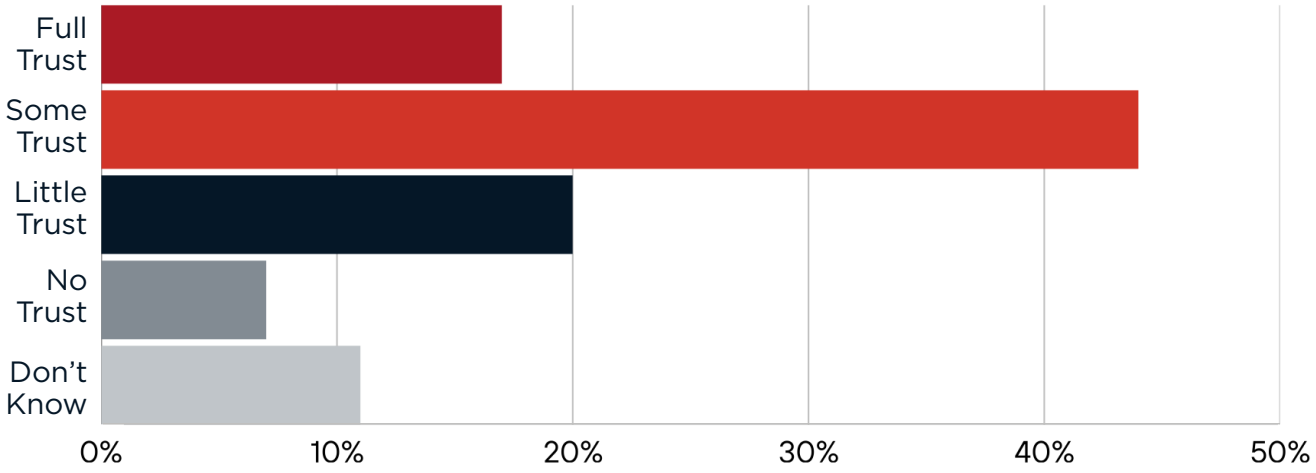
73% believe in the importance of government regulation of AI to protect their identity data online

52% do not feel sufficiently informed or protected from scams by guidance from safety organizations or government institutions

Consumer trust is on the decline as emerging technologies continue to expand the threat landscape.

AI hasn't just transformed our lives. It has disrupted relationships between consumers and brands as the former loses trust in the latter's ability to protect their identity data, especially when it comes to online transactions. Only 17% of respondents have full trust in the organizations that manage their data. While 44% have some trust in these organizations, another 27% have little to no trust in them at all.

When thinking about the brands you engage with online, how much trust, if any, do you have in the organization(s) that currently manage your identity data?



Global Snapshot

This is especially true of respondents in France where only 8% reported having full trust in these organizations, and 10% have none at all, while Australia wasn't far behind (11%). However, this level of mistrust isn't global. For example, almost two in five (37%) of respondents in the United Arab Emirates (UAE) have full trust in these organizations, more than any other country in our survey.

Trust in organizations varies widely

8%
of respondents in France have full trust.

11%
of respondents in Australia have full trust.

37%
in the UAE have full trust —the highest of any country surveyed.

When thinking about the brands you engage with online, how much trust, if any, do you have in the organization(s) that currently manage your identity data?

	Full Trust	Some Trust	Little Trust	No Trust	Don't Know
US	21%	41%	17%	8%	14%
UK	17%	41%	19%	8%	14.%
France	8%	40%	27%	10%	15%
Germany	12%	46%	22%	7%	13%
Australia	11%	50%	23%	8%	9%
Singapore	12%	56%	22%	6%	5%
India	35%	43%	15%	4%	3%
Indonesia	28%	35%	24%	7%	5%
Netherlands	11%	54%	16%	5%	13%
Sweden	16%	44%	22%	4%	14%
UAE	37%	44%	12%	3%	4%

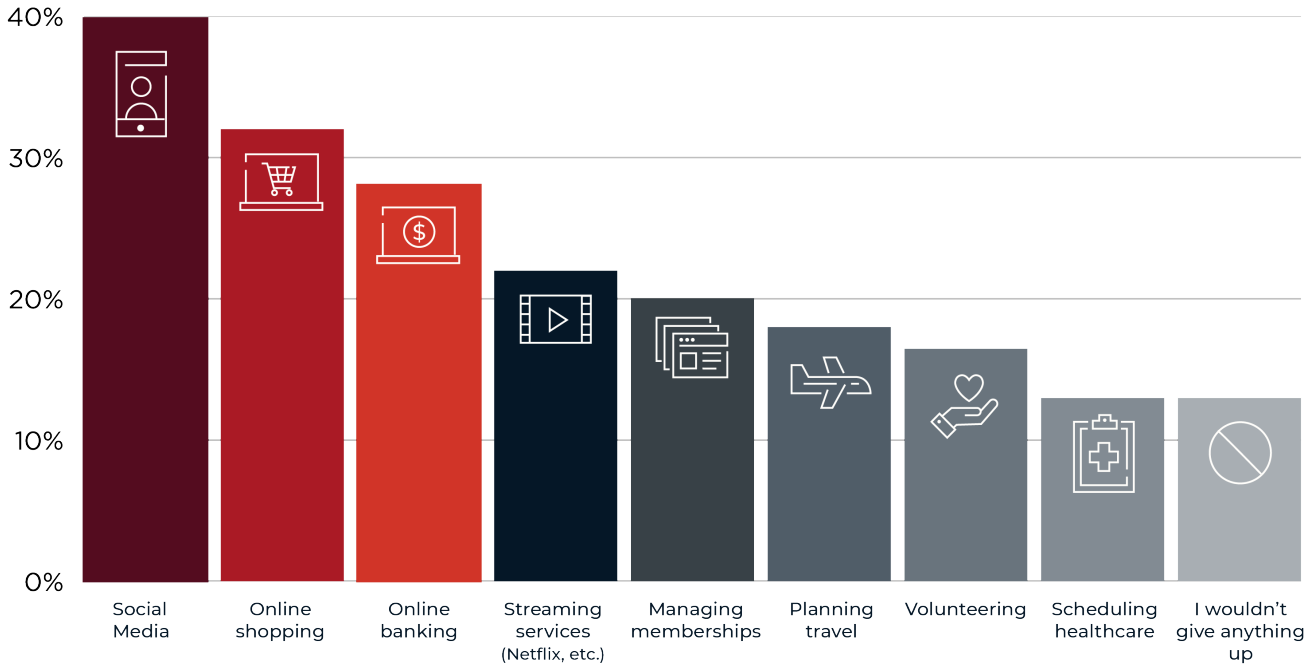
What's true across the world is that people are more likely to trust regional and local brands with their sensitive information, leading to implications for global brands. These organizations must strive to overcome the confidence crisis separating them from consumers.

While these numbers all revolve around online transactions and interactions, not every site or platform is created equal. Consumers expressed particular unease about identity data security when it comes to social media, with 39% ranking it as the service they trust least. Gambling/betting services and online retailers also rated highly as untrustworthy at 32% and 24%, respectively.

Only 14%

of consumers trust global brands, while **20%** trust local and regional brands.

Which types of online services do you trust least with your identity data?



Global Snapshot

Again, this differs when broken out by country. In India, for example, greater than a third of respondents (35%) trust banks the least, more than any other country. In the UAE, this changes to government services, which they trust less than any other country surveyed at 30%.

Americans, meanwhile, may skew towards being more trusting than their counterparts across the world. About one in five (21%) didn't have any particular service to single out as trusting the least. Similarly, nearly two-thirds of Americans (62%) have at least some trust in organizations that manage their identities.

> "I will not consider online purchasing, using social media, or banking and insurance because [of] being hacked or defrauded."
>
> **SURVEY RESPONSE**

30%

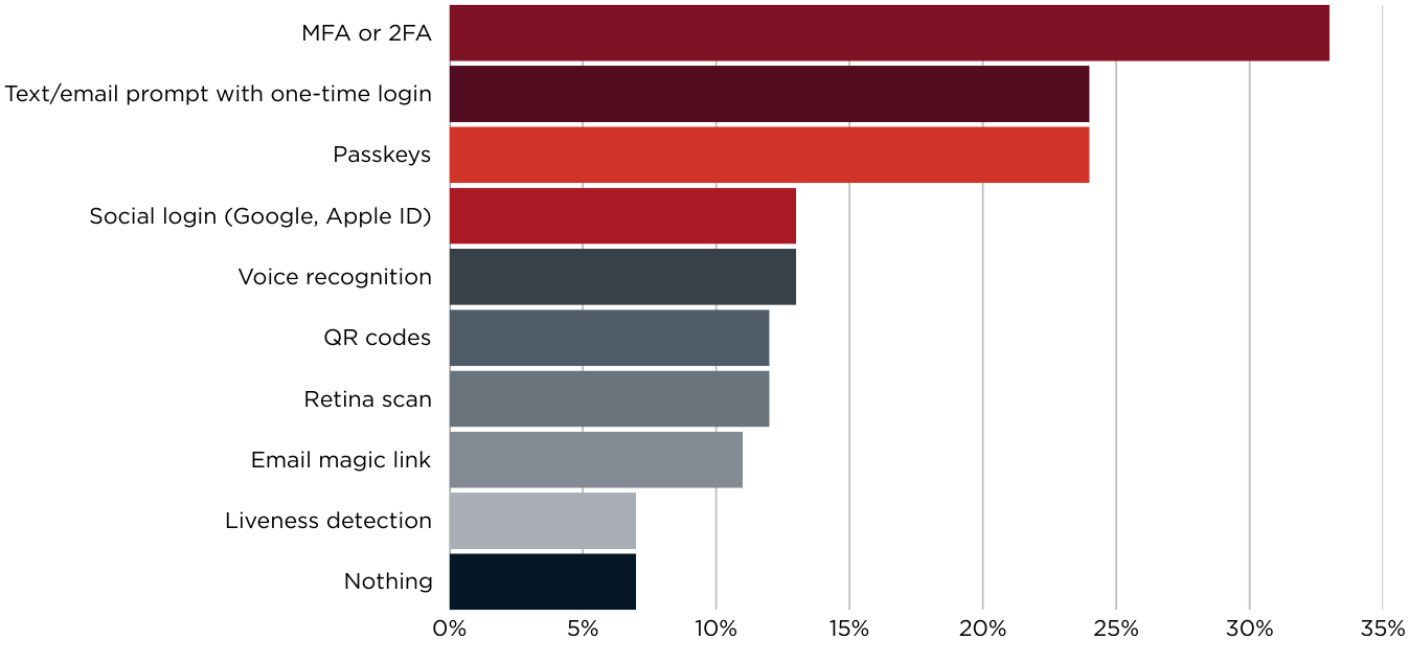
of respondents in the United Arab Emirates don't trust government services with their identity data.

> "In an age where everything is online, it's surprising to see how many consumers are willing to give up convenience to keep their data secure. We're reaching an impasse, and brands need to figure out how to fortify identity security with a strong user experience to maintain positive relationships with their customers."

CAYLA CURTIS
Director of Product Management, Ping Identity

However, consumers recognize that different means of security impact their comfort level with online services, offering a path forward for organizations looking to solidify consumer trust. Of the authentication methods suggested, biometric authentication and multi-factor authentication ranked highly and neck-and-neck at 34% and 33%, respectively, as the most likely to increase trust when engaging with brands online.

Which of the following authentication methods would most increase your trust when engaging with brands online?

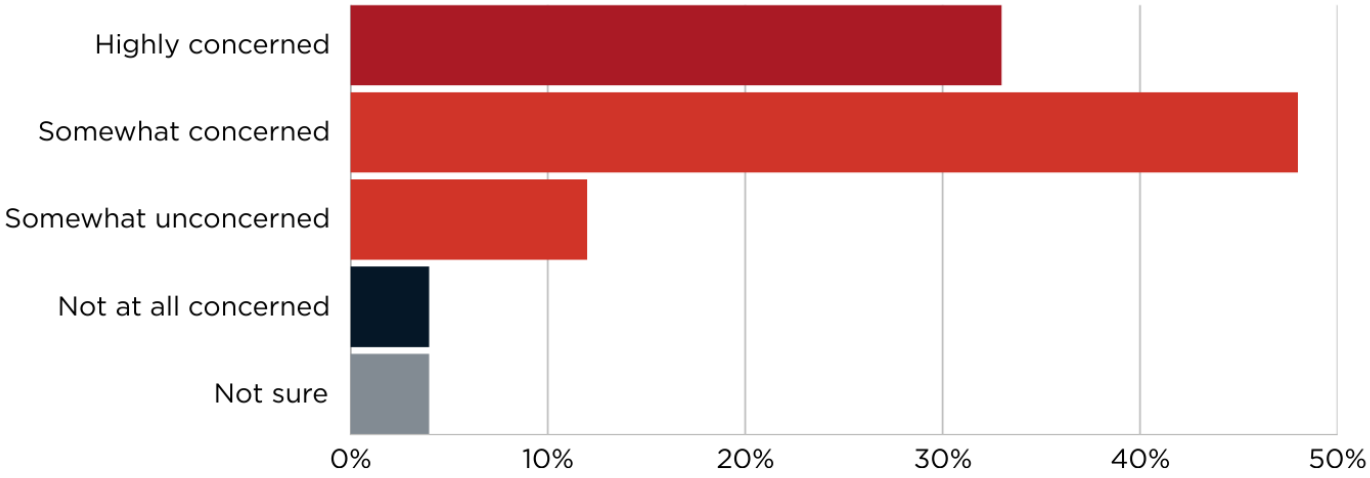


Global Snapshot

Broken down by country, these numbers and preferences change. For example, text and email prompt log-ins are popular in Australia (34%) and the UAE (32%) compared to the rest of the world. Indonesians prefer passkeys (44%), second only to biometric authentication (60%). Greater than a quarter of Indians (28%), meanwhile, say QR codes would increase their trust more than any other method, more than any other country surveyed. This points toward a trend of new login methods helping to increase trust with consumers, which is a strong choice for brands looking to solidify their relationships with their customers.

Overall, survey results displayed a clear concern for identity theft or fraud following interactions with online services, with 81% reporting at least some concern. The number of those highly concerned remains consistent with last year's data at 33%.

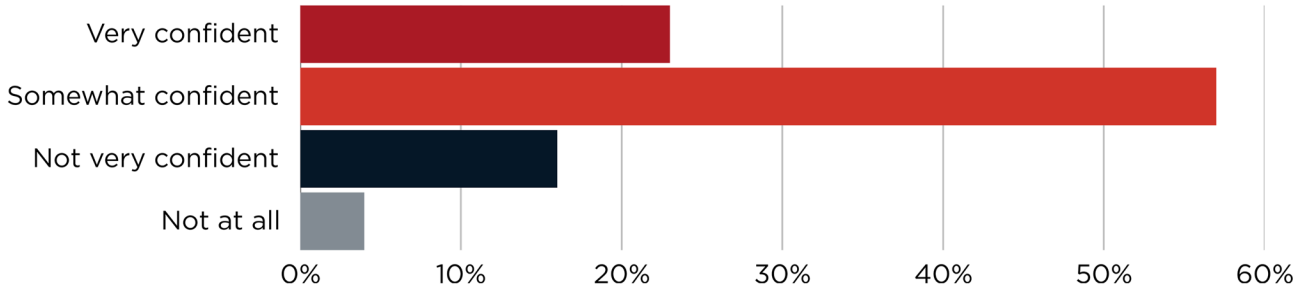
To what extent, if at all, are you concerned about identity theft or fraud?



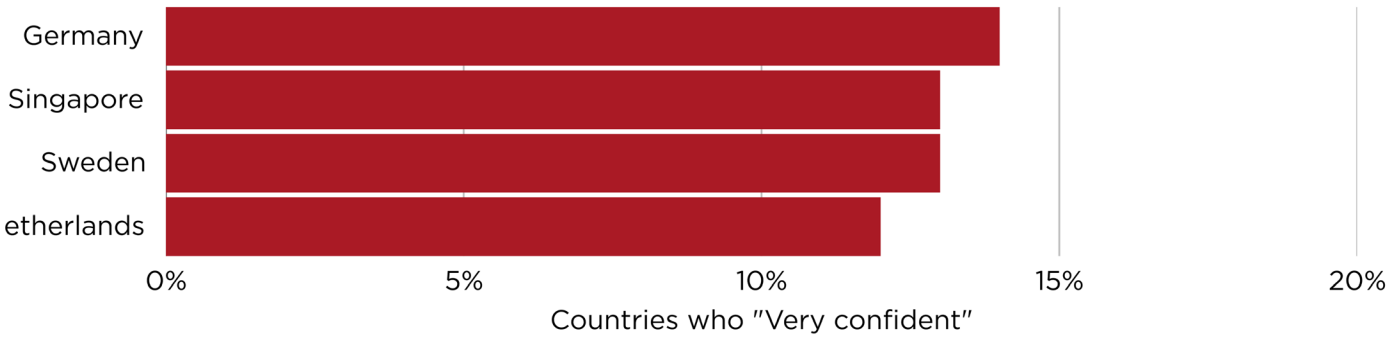
52% of those in India and 50% of those in Indonesia reported high levels of concern about identity theft or fraud, more than any other country. In Europe, however, 28% of respondents from the Netherlands and 26% from Sweden aren't concerned about these scams at all.

Despite (or maybe because of) widespread concern about identity theft, respondents did largely have some confidence in their ability to spot a scam. Only 20% of respondents reported being not very confident or not confident at all in their abilities.

How confident are you in your ability to determine whether something is legitimate or a scam?



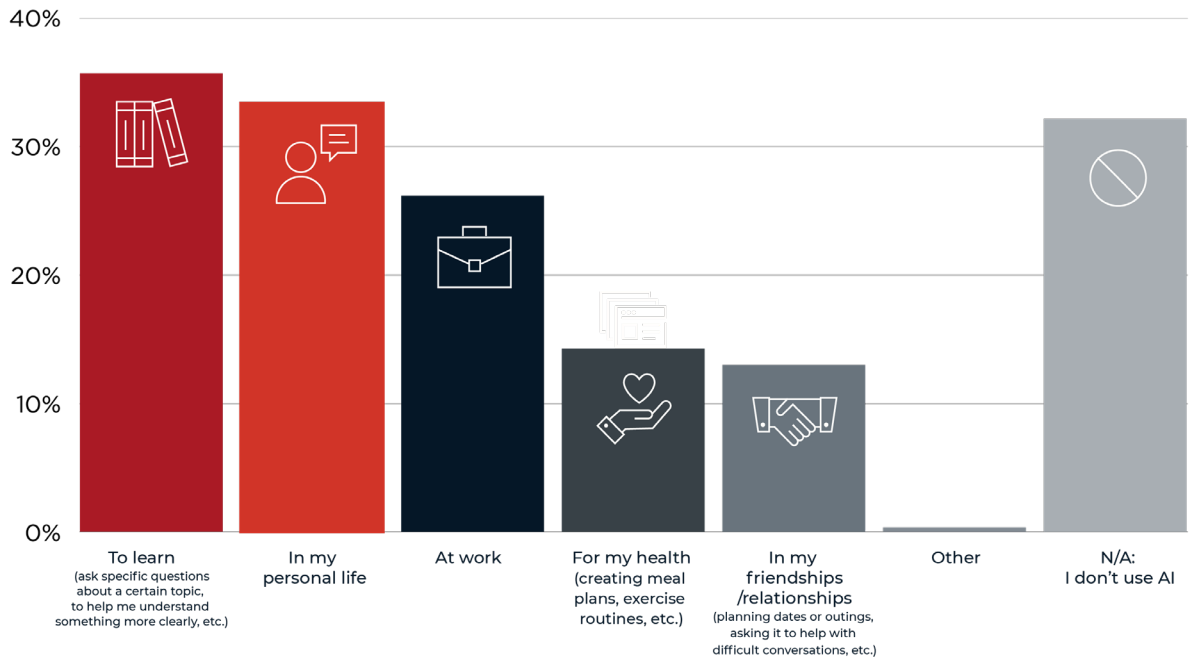
In some countries, confidence is even lower



AI has changed specific consumer concerns and habits when it comes to identity data security.

While consumers remain concerned about AI when it comes to their identity data, this ubiquitous tech is impossible to avoid in other aspects of life, too. It's no surprise that 68% report using AI in their daily personal or professional lives, a strong increase from last year's 41%. AI has officially hit the mainstream, shifting from early adopters to widespread use. Our survey reports learning and knowledge as respondents' top use case at 36%. AI can be a threat, yes, but it's clear consumers also see it as a tool for education, development, and skills enhancement.

How are you currently using artificial intelligence (AI)?



"While knowledge is power, the increased use of AI in our everyday lives has only informed many consumers of its capabilities. They see firsthand how powerful this technology can be when applied to their own use cases. They're also seeing more news stories and data points about increases in security threats and cyberattacks. Combined, it's understandable that this contributes to a crisis of confidence in brands' abilities to keep consumers' identity data secure."

DARRYL JONES
Vice President of Consumer Segment Strategy, Ping Identity

Several survey respondents pointed out that AI is often integrated into websites or platforms they'd be using otherwise, making it nearly impossible to stay separate from this technology. As the pressure builds for web services to seamlessly integrate AI into everyday use, people may be using it whether they want to or not.

> I know it's there, but I don't know [if] I am using it.
>
> **SURVEY RESPONSE**

This escalation and normalization of AI understandably translates to a data security landscape. Our survey found that consumers are more specifically concerned about invasion of personal privacy by AI programs (27%) and AI-generated phishing (27%), with AI impersonation of themselves or a person/brand they're engaging with following closely behind (26%). Newer, more sophisticated threats are also beginning to gain ground: for example, 24% of consumers reported concern about AI-generated voice cloning, while 22% reported concerns about targeted deepfakes.

What are your concerns about AI with regard to identity security, if any?

Invasion of my personal privacy by AI programs	27%
AI-generated phishing	27%
AI being used to falsely impersonate me or a brand/person that I am engaging with	26%
Lack of transparency in how AI systems are using and storing my personal information	25%
Increased cybersecurity risks – threatening the safety of my personal data	25%
AI-generated voice cloning	24%
Deepfake impersonations of people I know and trust	22%
AI impersonation via chatbots	20%
Lack of accuracy/bias in AI systems	18%
I don't understand what my legal protections are for how AI uses my information	18%
Authorizing AI to work on my behalf	17%
I don't have any concerns related to AI and identity security	9%
Don't know	13%
Other	1%

Global Snapshot

These concerns vary by country. Australians in particular worry about a lack of transparency in the use and storage of personal information when it comes to AI systems at 34%, more than any other country. In Singapore, respondents reported high concerns of deepfake impersonations (39%) and AI-generated voice cloning (33%), more than any other country. Swedes—many of whom, as stated earlier, aren't as worried about scams—are less concerned about AI impersonation via chatbots at 14%, the lowest rate in the survey.

In a similar question, 39% of respondents reported AI-driven phishing to be their chief concern when it comes to modern and future fraud and scams in general, proving that phishing remains top of mind as threats continue to change and evolve. While in Singapore, deepfake attacks are of highest concern (49%).

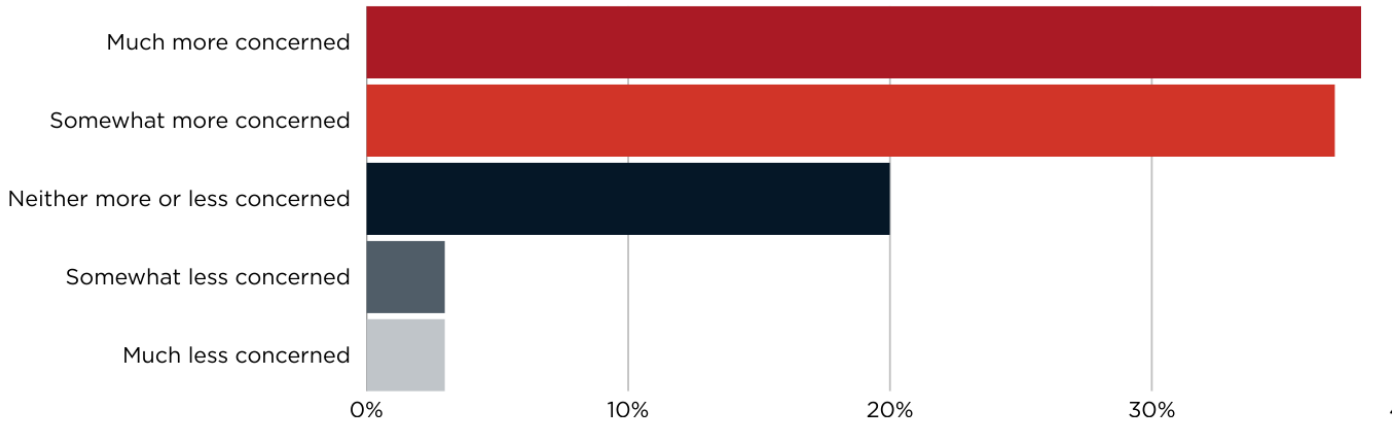
39%

of consumers are most worried about AI-driven phishing when it comes to modern or future fraud and scams.

What's undeniable across the board is that security concerns surrounding personal and private information are on the rise and have multiplied over the past several years. The AI revolution has only compounded these fears as threats become more advanced, sophisticated, and prevalent. As a result, a whopping 75% of consumers reported that they're at least somewhat more concerned about the security of their personal and private information than they were only five years ago.

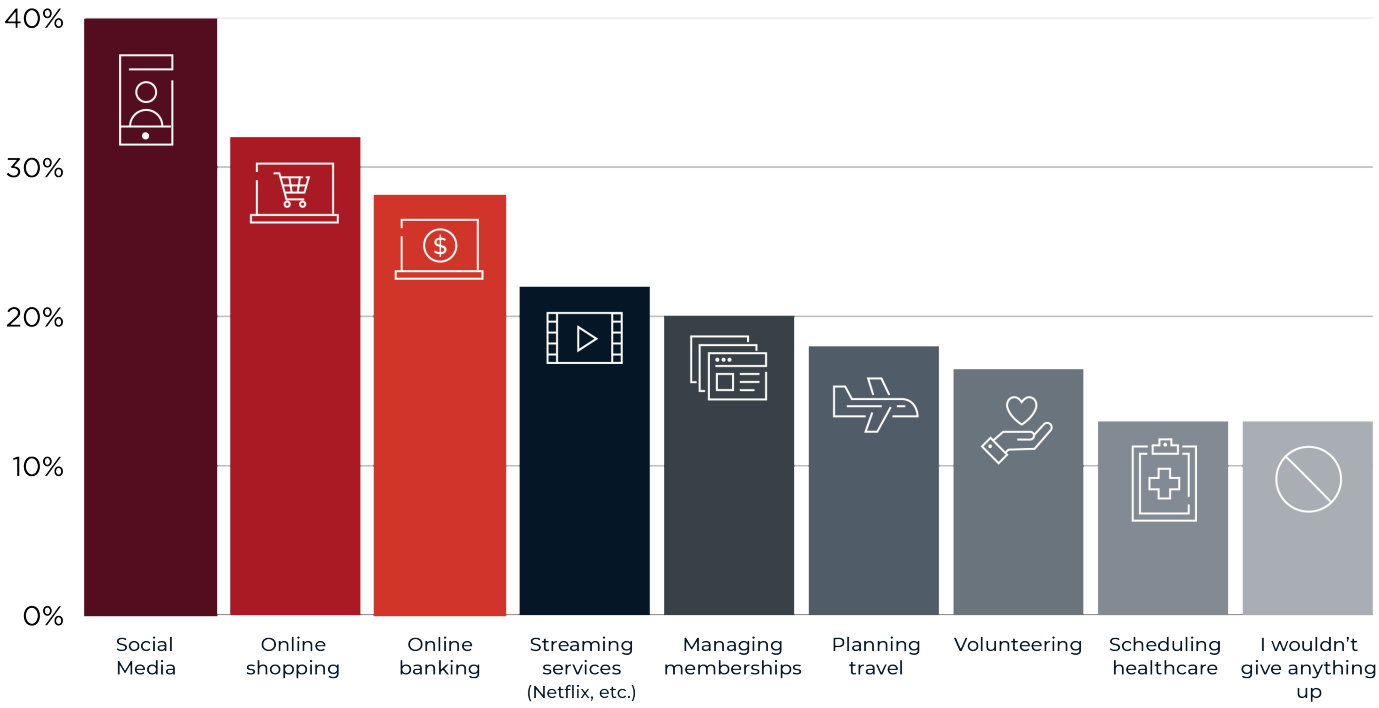
75% of consumers reported that they're at least somewhat more concerned about the security of their personal and private information than they were only five years ago.

Compared to 5 years ago, how much more or less are you concerned about the security of your personal and private information?



As this technology continues to evolve alongside consumers' concerns, though, so has their willingness to make a change to protect themselves. When asked what they'd do to avoid the risk of identity theft, many consumers reported they'd be willing to give up three major habits: social media (40%), online shopping (33%), and even online banking (28%). This shows a retreat in the trend of a digital-first lifestyle pervading modern culture.

Which of the following would you give up before risking your identity being stolen?



> "We think of social media as a part of everyday life for many. But it's clear from these numbers that growing concerns about identity data security are pervading the convenience and connection of these platforms. Social media services that can't find a way to guarantee security as a part of their user experience will see the effects, particularly as AI continues to expand the threat landscape

CAYLA CURTIS
Director of Product Management, Ping Identity

Global Snapshot

A quarter of Australians (26%) were willing to give up streaming services, more than any other country, while more than one in five Germans (22%) would rather give up planning travel than risk identity theft, another high among country surveys. In the Netherlands, more than a third of respondents (36%) wouldn't give anything up. This tracks with the earlier figure that 28% of the Dutch aren't worried about identity theft or fraud at all.

As technology continues to advance and grow, consumer fears and behaviors are bound to change. Global brands will simply have to keep a finger on the pulse to understand what they can do to help alleviate these fears and keep their customers across the world feeling safe and secure about their data.

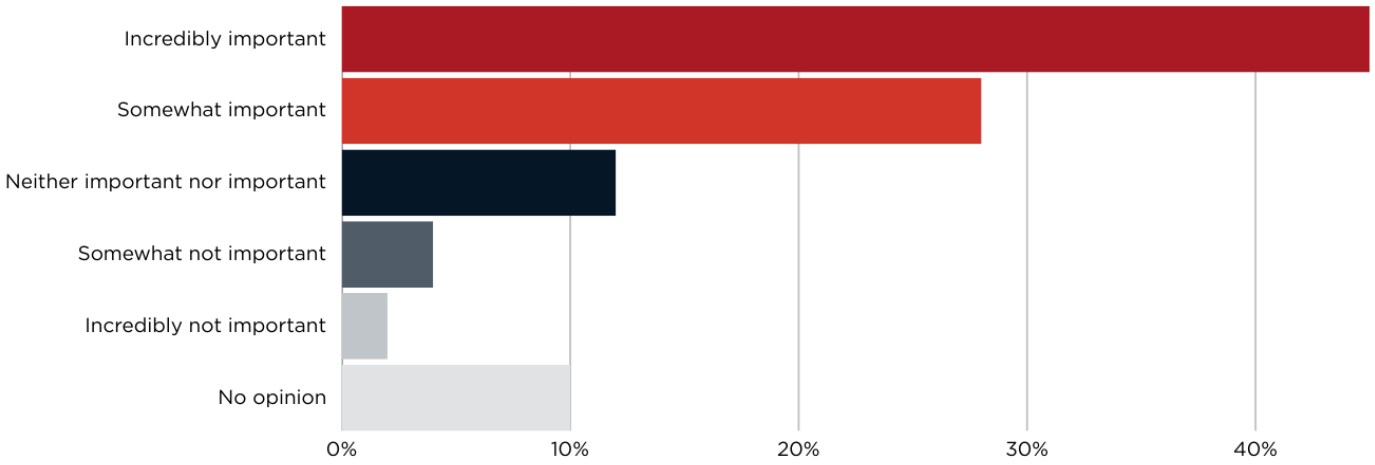
Consumers expect government regulation to protect them from the impact of rising, AI-powered security threats.

In the security space, government regulation of AI is another area of consumer interest and even concern. This is no surprise; as technology evolves, so does the law, and respondents see this fact as imperative to protecting their private data during online interactions. Nearly three-quarters (73%) of respondents globally reported feeling that government regulation of AI to protect their identity data online is important.

73%

of respondents reported feeling that government regulation of AI to protect their identity data is important.

How important is government regulation of AI to protect your personal identity data online?



"The pressure is building for governments to implement regulations as a way to safeguard consumers. We're still in an era where AI is fairly nascent, meaning we'll experience a great amount of change as leaders grapple with the question of how to harness AI while ensuring they protect their constituents. Consumers are demanding greater transparency and holding businesses accountable, and that will have to extend to government leaders as well."

DARRYL JONES
Vice President of Consumer Segment Strategy, Ping Identity

Global Snapshot

This rang especially true in Indonesia, where 74% of respondents said government regulation of AI is incredibly important. That's more than double the amount who said the same in the Netherlands (35%), where AI and identity data privacy seem to be largely deprioritized. The same can be said about respondents in Sweden, only 31% of whom said government regulation is incredibly important, fewer than any other country.

When it comes to government information, education, and protection related to security risks, however, respondents were split.

Do you feel sufficiently informed and protected about current scams by the information you receive from official online safety organizations/governmental institutions?

As AI and related threats continue to advance and increase worldwide, consumers largely expect their governments to take control and protect their identity data. But with respondents unsure whether they're currently doing so, only time will tell if regulatory bodies take control and make an impact.

Conclusion

As consumers grapple with the permeation of AI and its impact on personal data security, global brands have a lot to contend with. Increased anxiety, decreased comfort with online engagements, and a desire for government regulations for protection are only a few key considerations as brands prepare for an advanced technological future.

But there's hope yet: while 17% seems like a disheartening number for those with complete trust in global brands' ability to protect their data, the 61% who reported at least some trust indicate the potential for a path forward. Better education about threats and the leverage of security methods like AI optimization and biometric authentication may help strengthen that trust. The number of consumers who use AI in a learning capacity proves that people want to learn, and it's up to organizations to provide them with the opportunity.

Organizations wanting to maintain strong relationships with consumers and alleviate their concerns about identity data security must find ways to improve security and increase trust with consumers. Those who don't will find many willing to leave their digital interactions behind — but those who do will reap the rewards.

The Path to Rebuilding Trust

As organizations look to mitigate consumer concern, anxiety, and mistrust surrounding online interactions, there are actions they can take to preserve identity data security:

1. Add stronger (and more seamless) authentication methods like biometrics, multi-factor authentication, text/email prompts with one-time log-ins, passkeys and more to instill a higher sense of security while preserving a seamless customer experience.

2. Quickly capture new customers' trust and build returning customer loyalty with frictionless and secure authentication methods during login.

3. Share how your organization uses and secures consumers' data to alleviate fears of identity theft or fraud, and provide opportunities for consent and for self-service consent management.

4. Mitigate third-party risk and build resilience in your supply chain by monitoring vendors to ensure protection from all angles and establish comprehensive consumer confidence.

5. Continuously monitor, assess, and mitigate threats in real-time to protect against emerging risks, and govern AI agents with the same rigor as humans.

> "Consumer confidence in global brands is eroding fast. We've entered a 'trust nothing' era, where people are questioning every call, message, and even the companies they once relied on. The challenge now is for organizations to prove they deserve that trust, and that starts with stronger, smarter identity protection."

DARRYL JONES
Vice President of Consumer Segment Strategy
Ping Identity

About the Study

Methodology

This random double-opt-in survey, commissioned by Ping Identity, was conducted by market research company Talker Research, whose team members are members of the Market Research Society (MRS) and the European Society for Opinion and Marketing Research (ESOMAR). Talker Research interviewed 10,500 consumers across the US (2,000), UK (2,000), France (1,000), Germany (1,000), Australia (1,000), Singapore (1,000), India (500), Indonesia (500), Netherlands (500), Sweden (500) and the UAE (500). Year over year comparisons based on Ping Identity's 2024 Consumer Survey.