ENTRUST

ENTRUST CYBERSECURITY INSTITUTE PRESENTS

THE FUTURE OF IDENTITY REPORT

Executive summary

The days of using physical-only identity documents are numbered. Biometrics, blockchain, encryption, AI, and more are enabling digital and hybrid identity solutions — from biometric-enabled employee IDs to contactless ePassports and travel credentials.

This evolving identity space drives convenience and higher assurance for users, **but questions are arising for business and security leaders:** Is there a best way to validate identity? What's the public's appetite for digital identity? When IDs were only physical, individuals could simply show their identity document and then put it away — but as identity grows increasingly digital, how can individuals maintain control over their personal information?

To answer these questions and more, the Entrust Cybersecurity Institute surveyed 1,450 consumers from 12 countries. **Our report investigates three trending identity topics:**

01 Passwordless authentication

02 Hybrid identities

03 Ownership over personally identifiable information

In addition to the survey's findings, this report incorporates **analysis and recommendations** from Entrust industry experts to help your organization navigate the future of identity. Read on for a better understanding of three trends shaping the digital identity landscape.

Passwords are out, biometrics are in

Passwords have long been the primary way to access and protect digital goods and services. But every day the number and complexity of passwords grows more overwhelming.

This dynamic is changing. Passwordless authentication solutions — especially ones that employ user biometrics — are gaining traction, offering more convenient and secure experiences.

But do consumers feel the same way? We asked consumers to select the identity authentication methods they thought were more secure than a password. More than half of respondents believed biometric solutions are more secure, with 53% selecting fingerprint scans followed by facial recognition (47%). Only 6% of consumers said passwords are the most secure method.

Only 6% of consumers said passwords are the most secure method.

Authentication methods consumers believe are more secure than passwords

Fingerprint scan	**53%**
Facial recognition	**47%**
4- or 6-digit PIN codes	**41%**
SMS one-time passcode	**34%**
Device recognition	**17%**

In addition to security concerns, passwords have grown overly complicated. With more digital services available than ever, consumers struggle to recall an ever-growing inventory of login credentials. **Over half of respondents (51%) reset a password once a month or more frequently because they can't remember it.** Even more alarming, 15% of users do so at least once a week.

Entrust Insight

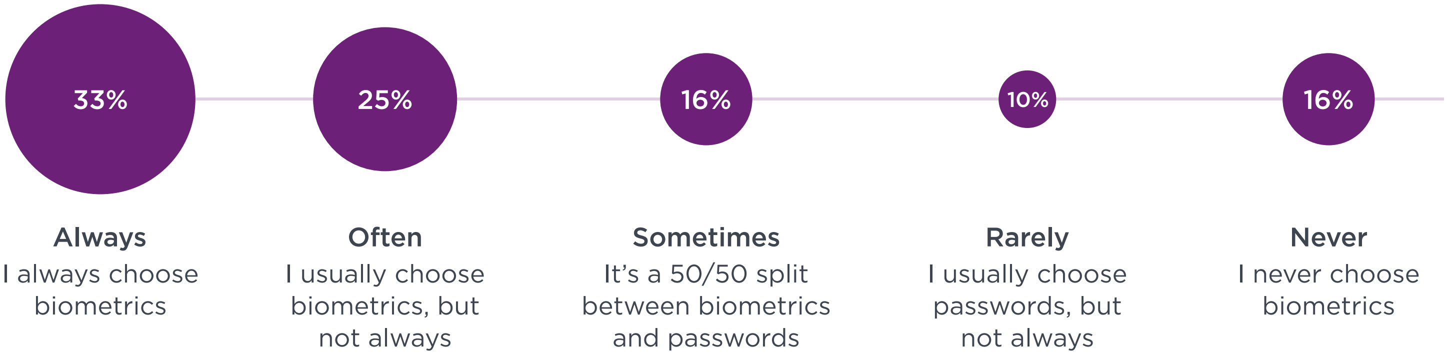
"Passwords are a necessary evil that is becoming less necessary by the day. Not only are passwords highly susceptible to compromise, but they're inconvenient to keep track of as we access an increasing number of applications and services through digital channels."

Mark Ruchie
Chief Information Security Officer, Entrust

Although consumers believe biometric-enabled identity authentication methods offer peak security, do they like using these options? It turns out that favorable perceptions do indeed match practical preferences. **When given the option between biometrics or a password, 58% of respondents choose to use biometrics over half the time.** A third will always choose biometrics when available.

Consumers who aren't on board with biometric login methods largely cite issues with practicality and availability. For those who don't always prefer biometrics, a third of those respondents say it's more troublesome than a password. Nearly a quarter (22%) say their device doesn't support that method of authentication, while fewer (17%) have security concerns.

Frequency of selecting biometric authentication over passwords



Entrust Insight

"There's no one right way for organizations to authenticate customer, employee, or citizen identity. It's always a trade-off between providing relatively frictionless access experiences and incorporating safeguards that confirm users are who they claim to be. **The authentication methods you employ can — and should — change depending on the circumstances**, like the sensitivity of data users are accessing, whether you're serving customers or employees, or if atypical login behaviors are exhibited."

Mark Ruchie
Chief Information Security Officer, Entrust

All aboard! The digital identity train is leaving the station

The electronic identity space is growing — fast. The global digital identity solutions market is **estimated to reach $70.7 billion by 2027**, compared to $27.9 billion in 2022.

But what exactly do consumers recognize as an electronic identity? Is it a physically issued driver's license hosted on a mobile wallet? A physical passport booklet containing a chip holding a digital copy of the data? Or something else entirely?

Consumers aren't entirely sure. When asked whether they had an electronic ID (eID)**, 43% of respondents said yes, 36% said no, and a fifth (21%) weren't sure.** For example, in the U.S. (where all passport holders have been **automatically issued ePassports since 2006**), only 27% of survey respondents agreed they have an eID. While these findings may include respondents who don't have passports, it's clear that a large percentage of Americans are unaware that their passports are a form of electronic ID.

But despite a general lack of awareness about eIDs, consumers are largely on board with the concept of electronic identities. **Seven out of 10 respondents** said they would likely use an electronic form of government-issued ID if one were available. The top perceived benefit of eIDs is improved convenience, cited by half of respondents who said they'd likely use them.

Even though consumers feel largely favorable toward eIDs, **they're divided on whether they are more or less secure than their traditional, physically issued counterparts.**

Proponents of the solution cited improved security (49%) as the second most important reason why they would use an eID. Conversely, consumers unlikely to use eIDs similarly named security concerns (45%), followed by worries about identity theft (36%), as their top two arguments against eIDs.

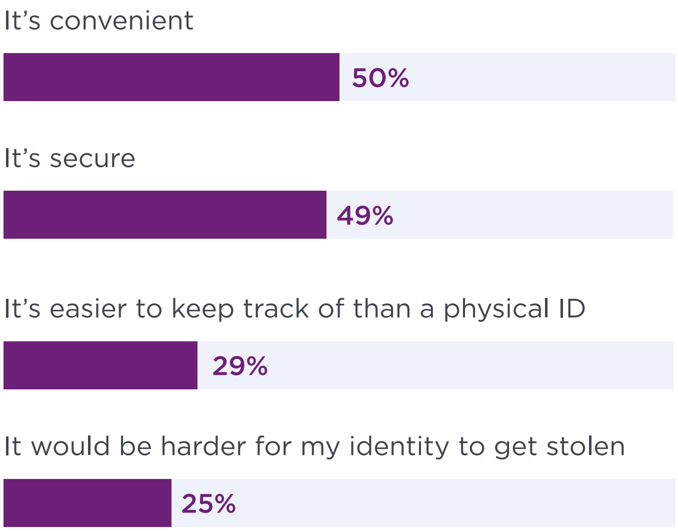
Entrust Insight

"Digital identities are a rapidly evolving space. **The line between physical and digital identities has blurred — it's all the same information used to access the same services**. As our digital and physical selves become one and the same, it's up to governments, security leaders, and technology creators to educate consumers and citizens about the trend.

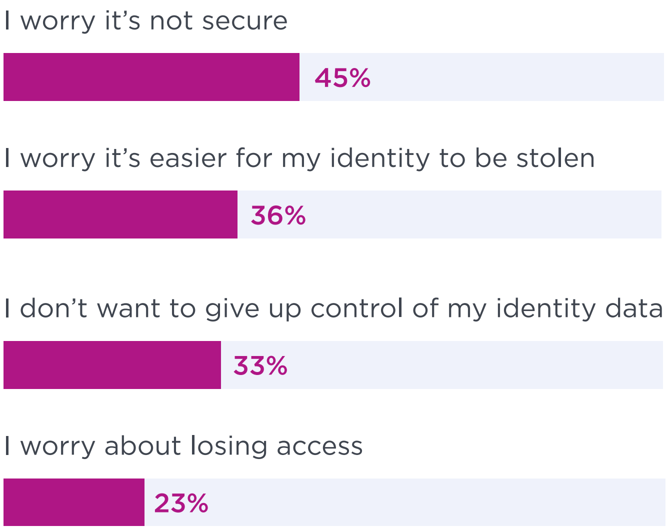
Let's unpack ePassports, for example. An ePassport is simply a passport book with a machine-readable ereader chip in it. It's not a totally digital credential. However, it still is an eID. It's a digital assertion of one's identity, wrapped inside a physical document."

Anudeep Parhar
Chief Operating Officer, Entrust

Top 4 reasons respondents would use an eID

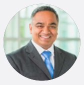


Top 4 reasons respondents would not use an eID



Entrust Insight

"Identity is highly personal, so I'm not surprised to see concerns about different forms of ID in our report's findings. The truth is that there is no zero-sum game here. The identity pie is getting bigger as identity types and their use cases grow. **The global trend is toward credentials that work seamlessly in-person and online, in ways that respect both the need for the security, and the privacy rights of the individual.**"



Anudeep Parhar
Chief Operating Officer, Entrust

Consumers view data control as diminishing — and many are okay with it

Data privacy has been top-of-mind for virtually all business and security leaders for decades. Data breaches have broken many corporate reputations, yet it sometimes seems like the loss of control over personal data is the price one pays to participate in modern life.

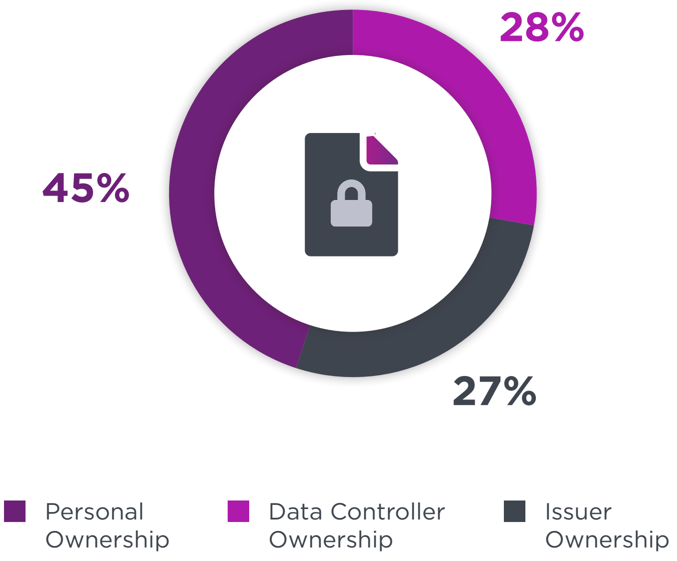
Our findings reveal consumers largely understand that their control over personal information is diminishing — **but they're divided on how they feel about it**. For example, the results were surprising when respondents were asked who should have the right to maintain ownership over identity credentials and personal data. See the chart below to find out.

Perhaps many consumers don't believe they own their own information because data sharing has become so ubiquitous. **Nearly three-quarters of respondents (74%)** agree sharing personal information in exchange for access to goods, services, and applications is unavoidable and **they have no choice but to allow access.**

Consumers are evenly divided as to whether this diminishing control is a worthwhile price to pay for convenience and personalization or a trend to be wary of. We asked consumers if they would be comfortable with an organization they trust owning and storing an online digital identity for them if it improved the user experience. The results were split: 54% said yes, they would be comfortable, but 46% of consumers said no, they should be the only one who owns their online digital identity.

Consumers' uncertainty about whether they're comfortable allowing their digital identity to be stored by institutions is likely tied to the **degree of trust they have in an organization's ability to keep their data safe.** With some organizations, like employers and financial institutions, respondents express a high degree of trust. But for others, like advertisers/marketers and retailers, respondents are far more skeptical — which makes sense considering the **many high-profile data breaches** that have occurred in these types of organizations.

Slightly over half of respondents said they don't believe they own their information and that it should belong to the data controller or the issuer.



Level of trust in institutions to keep personal data safe

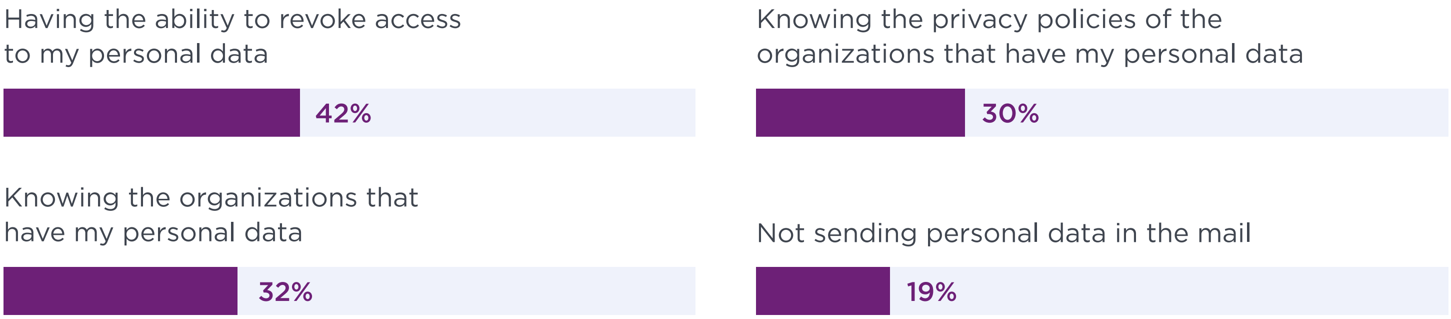
No. 1	Friends/family	82%
No. 2	**TIE:** Most recent employer	77%
No. 2	**TIE:** Financial institutions	77%
No. 4	Governmental entities	70%
No. 5	Retailers/service providers	61%
No. 6	Advertisers/marketers	51%

At this crossroad of opinions, decentralized identities are poised to offer a solution to growing concerns over data ownership and control, while still enabling convenient user experiences. While decentralized identity solutions are yet to be fully realized, they would allow individuals to store and manage access to their identities via an app or digital wallet.

Those experimenting with decentralized identity solutions are turning to encryption and digital keys as ways to protect user information and confirm an individual's identity without exposing critical elements of that identity to the receiver. Looking ahead, the **World Wide Web Consortium (W3C) Verifiable Credentials Data Model** offers great promise in accelerating digital identity trust and interoperability.

In addition to obscuring personal information at the source, decentralized identity solutions could allow consumers to see who has their personal information and revoke access if desired — the two highest actions respondents shared would help them **feel more in control of their personal data.**

Top 4 actions that help consumers feel in control of personal data



Entrust Insight

"While decentralized identity solutions are still some time away from full delivery and established interoperability standards are a work in progress, **they could ultimately help businesses regain consumer trust.** The solution offers a highly secure way for consumers to share personal data and identity information without giving away sensitive information — helping users feel more confident and in control, while also giving businesses and organizations the information they need to provide personalized services."

Greg Wetmore
Vice President Software Development, Entrust

The future of identity is hybrid

Hybrid identities offer the best of both worlds. To ensure both security and convenience — the two aspects that consumers care about most — enterprises and governments need to rethink how they issue, authenticate, verify, hold, and share identity credentials. Until the universality and interoperability of identity solutions improves, both digital and physical credentials are necessary to navigate an ever-changing world.

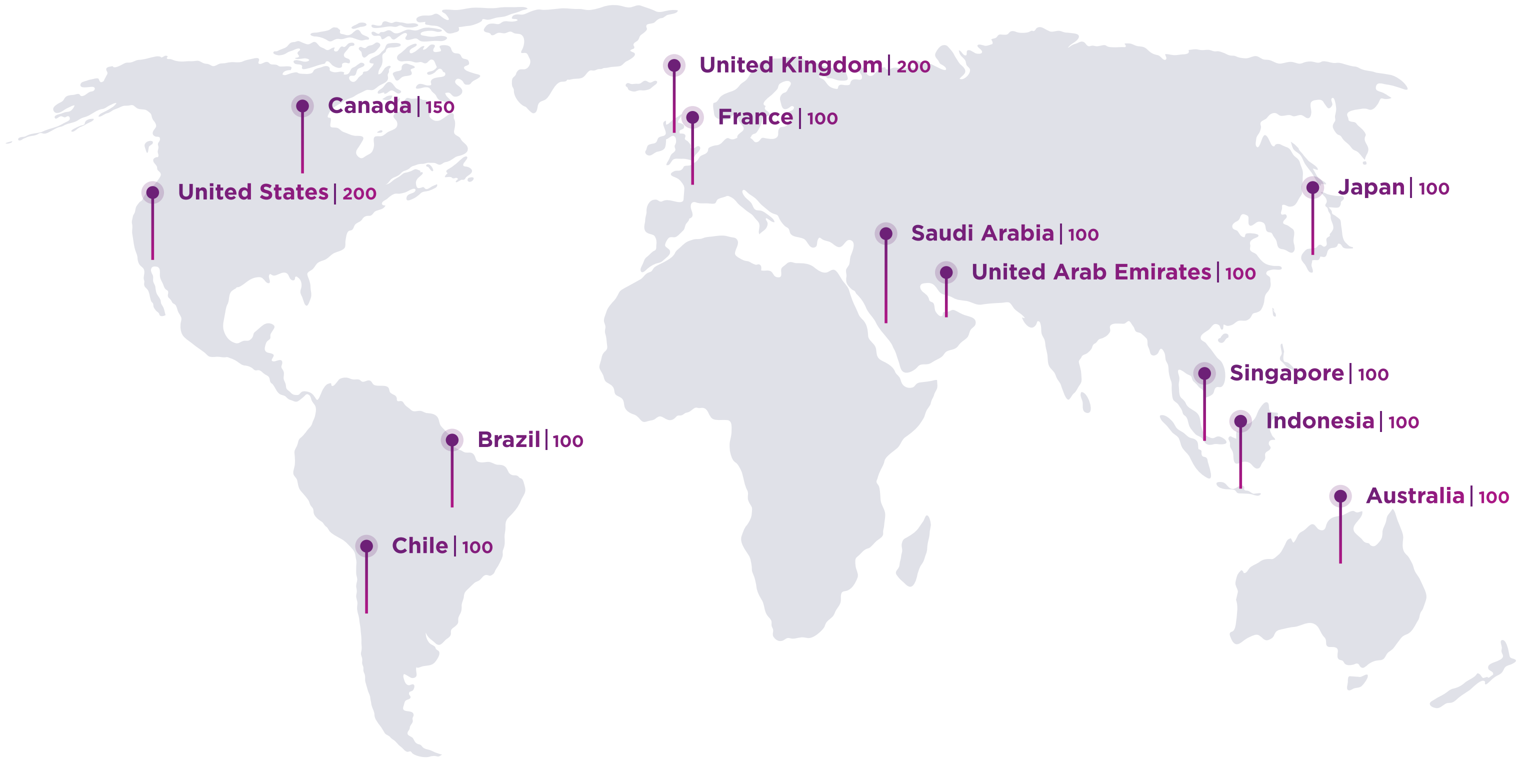
About the Entrust Cybersecurity Institute

The Entrust Cybersecurity Institute shares news, analysis, insights, and commentary for IT and business leaders charged with protecting and enhancing IT infrastructure. The Cybersecurity Institute leverages insights from Entrust, a global leader in protecting identities, payments, data, and infrastructure. Learn more at: www.entrust.com/cybersecurity-institute

Methodology

The Entrust Cybersecurity Institute surveyed 1,450 global consumers over the age of 18 about their use of and attitudes toward trending identity solutions. The survey was conducted via an online survey platform between December 8 and December 16, 2022.

Respondents were located in the following regions:



Number of global consumers	
Global Consumers	1,450

Age of global consumers	
Over 18	100%

About Entrust Corporation

Entrust keeps the world moving safely by enabling trusted experiences for identities, payments, and digital infrastructure. We offer an unmatched breadth of solutions that are critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption, and more. With more than 2,800 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us. For more information, visit **entrust.com.**

Legal Disclosure

Entrust, nShield, and the Hexagon Logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners.