eBook

New Edition

Biometrics Business Guide 2024: Consumer Trust Report

AWARE

781.687.0300 | sales@aware.com | www.aware.com

Aware is a leading global provider of software products and solutions for biometric identification and authentication. They are used for variety of applications including financial services, enterprise security, border management, and law enforcement. Aware is a publicly held company (NASDAQ: AWRE) based in Burlington, Massachusetts.

Introduction: A note from Aware President and CEO, Ajay Amlani

After 9/11 I asked myself: 'What can I do for my country? What can I do to make sure that this doesn't happen again?' and that's where my journey in identity began.

Twenty years ago, I predicted that biometrics would emerge to help us own and protect what - in reality - makes us human: our identity. From my beginnings in the White House, to starting the Department of Homeland Security, to my role today as CEO of Aware, I've been a firm believer that strong identity programs are key to keeping us safe and protecting our most valuable assets.

At Aware, we understand that while biometrics offer unparalleled security and convenience, consumers still have valid concerns—particularly about data privacy and responsible stewardship. Our mission as a biometric authentication leader is not just to provide cutting-edge solutions, but to do so in a way that prioritizes transparency, security, and ease of use.

Our Consumer Trust Report provides a comprehensive look at how people use, perceive, and trust biometric authentication today. The findings are clear: while adoption is growing, trust in how organizations handle biometric data needs work. We created this report to highlight key insights for businesses looking to integrate biometrics successfully with a focus on addressing consumer hesitations.

Done right, biometrics will lead us to a safer, effortless society, and I'm excited to move us in the right direction with Aware. I invite you to explore this report and join the conversation on how we can shape a better future together.

Ajay Amlani
President and CEO
AWARE

> ***"Biometric authentication offers unique advantages over other credential-based methods, but concerns about novel attacks and privacy are barriers to adoption."***
>
> *- Gartner*

The State of Biometric Authentication & Consumer Trust

A decade ago, biometric authentication was often seen as something straight out of a sci-fi movie—intriguing but distant. Today, it's an integral part of daily life for millions.

Biometric authentication - encompassing voice, fingerprint, iris, or facial recognition - has become mainstream. Today, over 75% of American citizens[1] have used biometric technology in some form. In Western Europe, Asia, and North America, 80% of people have enabled biometrics on their phone[1].

This surge in usage isn't just about convenience. Organizations are increasingly recognizing that biometrics offer a powerful way to link data, devices, and users. The result: reducing risks, saving millions in fraud prevention, and delivering seamless user experiences.

However, this widespread adoption is also tempered by consumer concerns. As digital life and market saturation converge, companies are grappling with how to drive brand loyalty while navigating the complexities of privacy, safety, and public perception.That changes today. Our team at Aware conducted a wide-ranging survey of U.S. consumers with questions aimed at uncovering their perceptions, knowledge, usage and concerns of biometrics authentication. The results: an in-depth understanding of consumer sentiment and experiences surrounding biometric authentication usage.

In this ebook, you'll find everything you need to know about the state of biometric authentication & consumer trust.

3 Key Takeaways From Our Biometric Authentication Survey Results

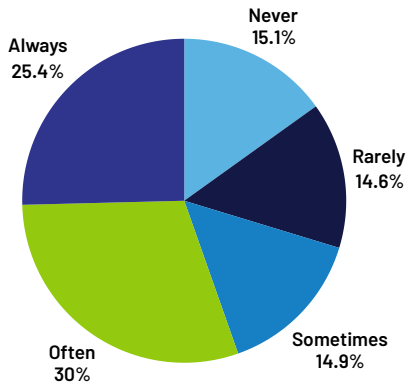
1. **How to overcome consumer concerns**
2. **What successful biometric authentication integration looks like**
3. **A preview at where the future of biometrics is headed**

Chapter 1: The State of Trust for Biometrics in 2024

Here are Aware, we're focused on creating best-in-class biometric solutions. In an effort to help you keep a pulse on industry trends, we surveyed 1,000 US consumers to better understand sentiments when to comes to using biometrics. Without further ado, here are the results:

QUESTION 1

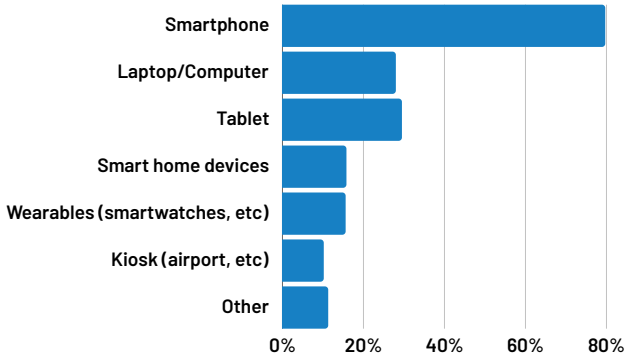
How often do you use biometric authentication in your daily life?



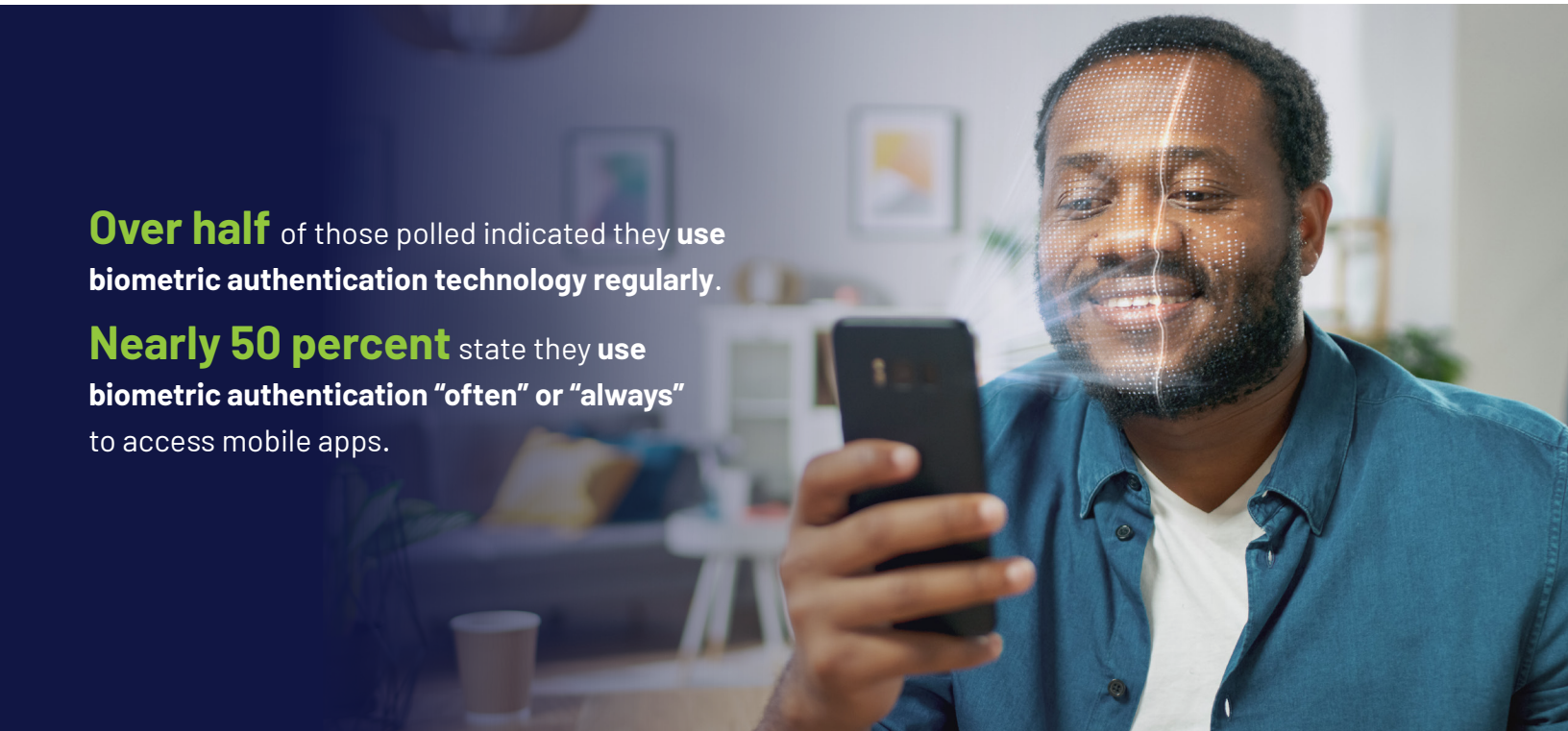
Over 50% of surveyants polled are already using biometric authentication daily. This is a positive indication that the technology is headed for mass adoption.

QUESTION 2

In which of the following devices do you use biometric features?



An overwhelming majority of respondents use biometric features on smartphones, followed next by laptops and tablets.

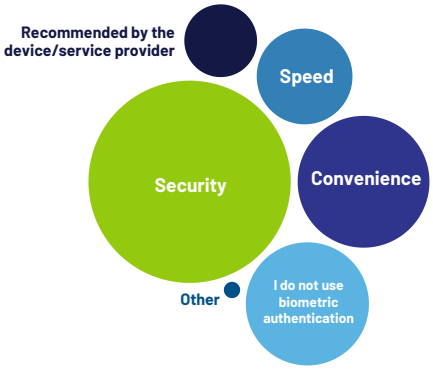


Over half of those polled indicated they **use biometric authentication technology regularly**.

Nearly 50 percent state they **use biometric authentication "often" or "always"** to access mobile apps.

QUESTION 3

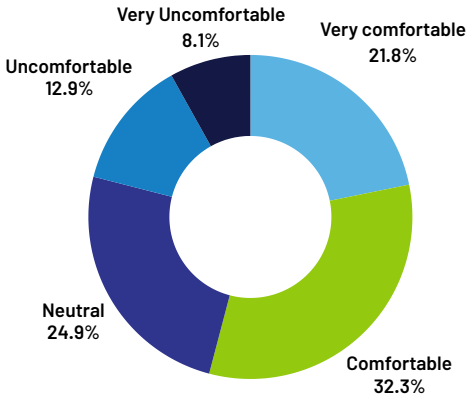
What is your primary reason for using biometric authentication?



Nearly half of all respondents primarily use biometric authentication for security, followed by convenience and speed of use for access.

QUESTION 4

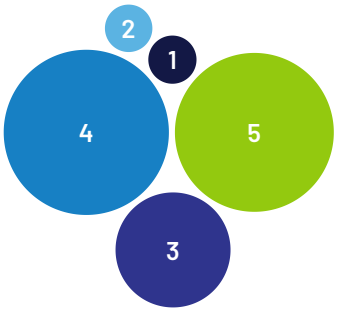
What is your level of comfort with biometric technology in public spaces, such as airports or stadiums?



While over 50% of respondents are either very comfortable or comfortable with using biometric technology in public places, over 40% are still either neutral, uncomfortable, or very uncomfortable with this idea.

QUESTION 5

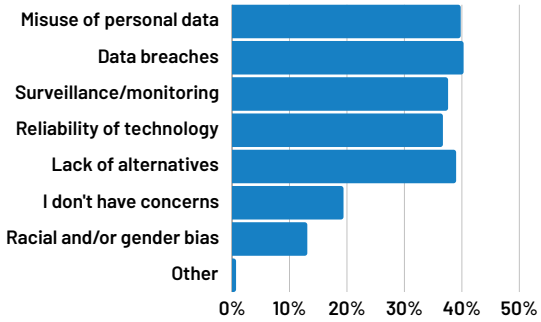
On a scale of 1-5 (5 being most secure), how secure do you believe biometric data is compared to traditional passwords?



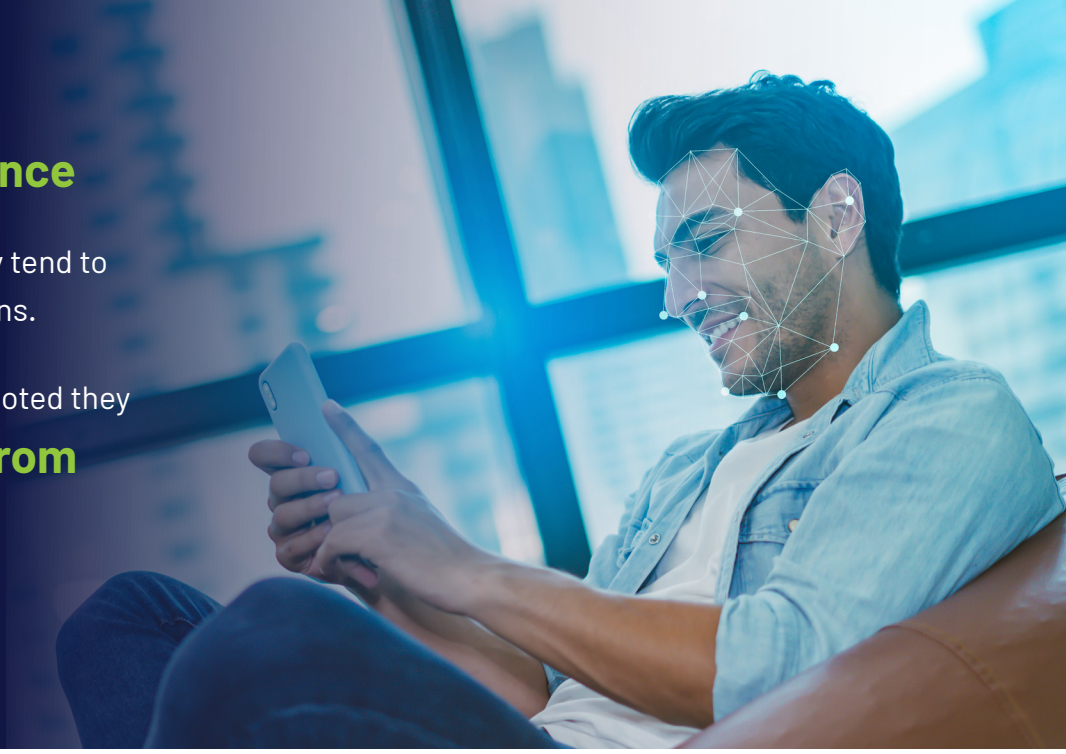
An overwhelming majority (75%) believe that biometric data is secure or very secure compared to traditional passwords.

QUESTION 6

What concerns, if any, do you have about using biometric authentication?



The concerns about biometric authentication were fairly split, but center around data privacy concerns and confidence in the technology.



Security and convenience

are the two main reasons for using biometric authentication, and they tend to hold more clout than trust concerns.

62 percent of respondents noted they **have never refrained from using the technology** as a result of trust issues.

QUESTION 7

What would make you more likely to adopt biometric authentication methods?

Respondents would be more likely to adopt biometric authentication methods if the following four concerns were addressed:

- **Improved security**
- **Guarantees about data privacy**
- **More control over data**
- **Better reliability**

QUESTION 8

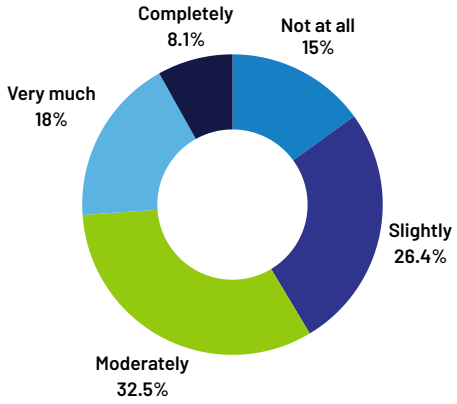
Have you ever refrained from using a biometric option due to privacy concerns?

Yes	22.9%
No	62.2%
Not sure	14.9%

While respondents expressed previous concerns when it comes to privacy and biometric authentication, 62% of them have never refrained from using the technology as a result.

QUESTION 9

Do you trust companies to responsibly handle your biometric data?



41% of respondents either don't trust companies at all or only slightly trust companies to responsibly manage their biometric data.

QUESTION 10

How would you rate your trust in the following types of organizations to responsibly handle your biometric data?

Levels of trust varied by industry—with respondents polled having the least amount of trust in online gaming/gambling sites and the most amount of trust in banks.

QUESTION 11

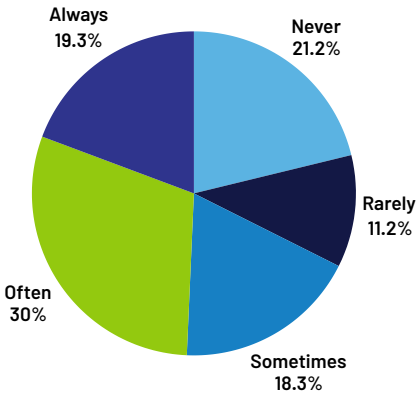
For which of the following purposes would you be most comfortable providing biometric data:

- To your employer for workplace security and/or access control
- To retail companies for access to your account
- To banks for account security
- To online gambling companies for identity verification
- To law enforcement agencies for forensic investigation, crime prevention and public safety
- To travel-related government agencies for faster security screenings at borders and airports
- To other government agencies for identification and/or access control purposes

Comfort level varied by purpose and had a mean across all options of ~4, which means comfort levels are fairly neutral using our scale of one being the most comfortable to seven being the least comfortable.

QUESTION 12

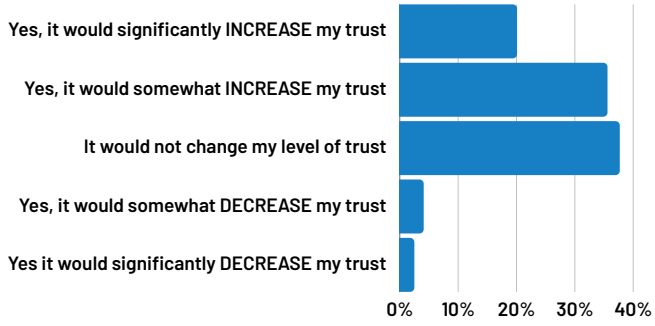
How often do you use biometrics to gain access to an account via a mobile application?



Nearly 50% of all participants regularly use biometric authentication to access their mobile applications.

QUESTION 13

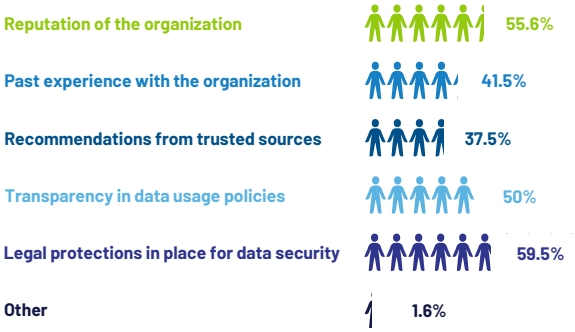
Would transparent communication from companies about biometric data use change your trust in biometrics?



Over half of all respondents said that more transparent communication would either somewhat or significantly increase their trust in biometrics.

QUESTION 14

What factors influence your trust in different types of organizations with your biometric data?

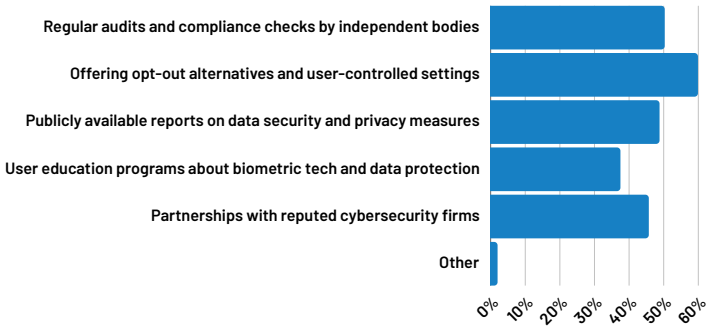


Responses were fairly split in regards to which factors influence trust most.

Still, significant concerns linger, especially when it comes to data breaches and trust in supporting technologies. An **overwhelming majority of respondents** felt **neutral** or **uninformed** about how their biometric data is used and stored by companies.

QUESTION 15

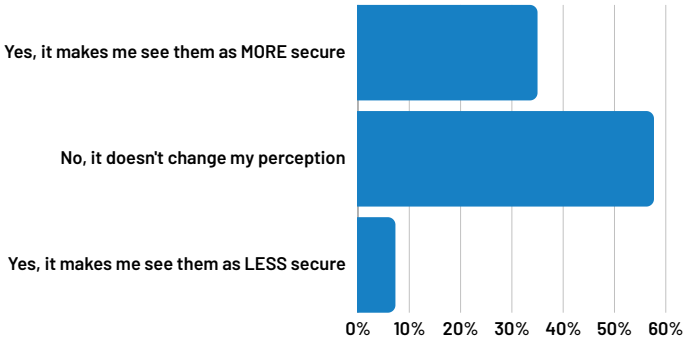
What actions could organizations take to increase your trust in their use of biometric technologies?



60% of all respondents cited that offering opt-out alternatives and user-controlled privacy settings would increase their trust in biometric technologies.

QUESTION 16

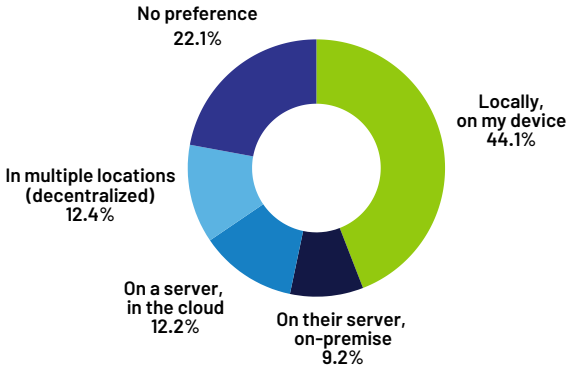
If a company uses biometrics, does it affect your perception of their commitment to security?



60% of all respondents currently don't feel that a company who uses biometrics is more committed to security than one that doesn't.

QUESTION 17

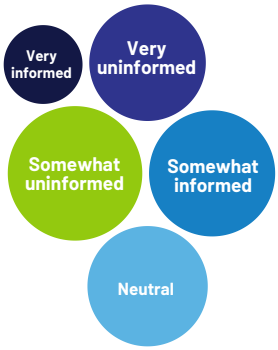
Where would you prefer that a biometric system stores your data?



Close to half of respondents polled would prefer that a biometric system stores data on their device.

QUESTION 18

How informed do you feel about how your biometric data is used and stored by companies?



An overwhelming majority of respondents felt either neutral or uninformed when it comes to how data is used and stored by companies.

QUESTION 19

If a data breach occurred, which type of organization would you trust most to adequately resolve the issue and protect your interests?

While the responses were fairly split across four organization types, respondents would most trust their employer followed by law enforcement to resolve a data breach.

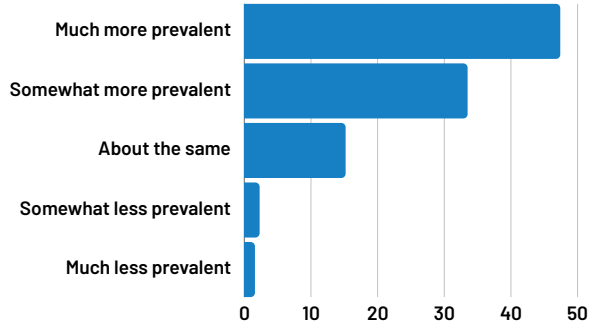
QUESTION 20

How likely would you be to stop using a service provided by these organizations if you found their handling of biometric data to be inadequate?

More than half of respondents would stop using biometric data with online gaming/gambling or retail sites for mishandling their biometric data.

QUESTION 21

Do you believe that biometric technology will become more or less prevalent in the next five years?



An overwhelming majority of respondents agree that biometric technology will become more prevalent over the next 5 years.

"I am hoping that as it advances we can trust it even more." -Survey response

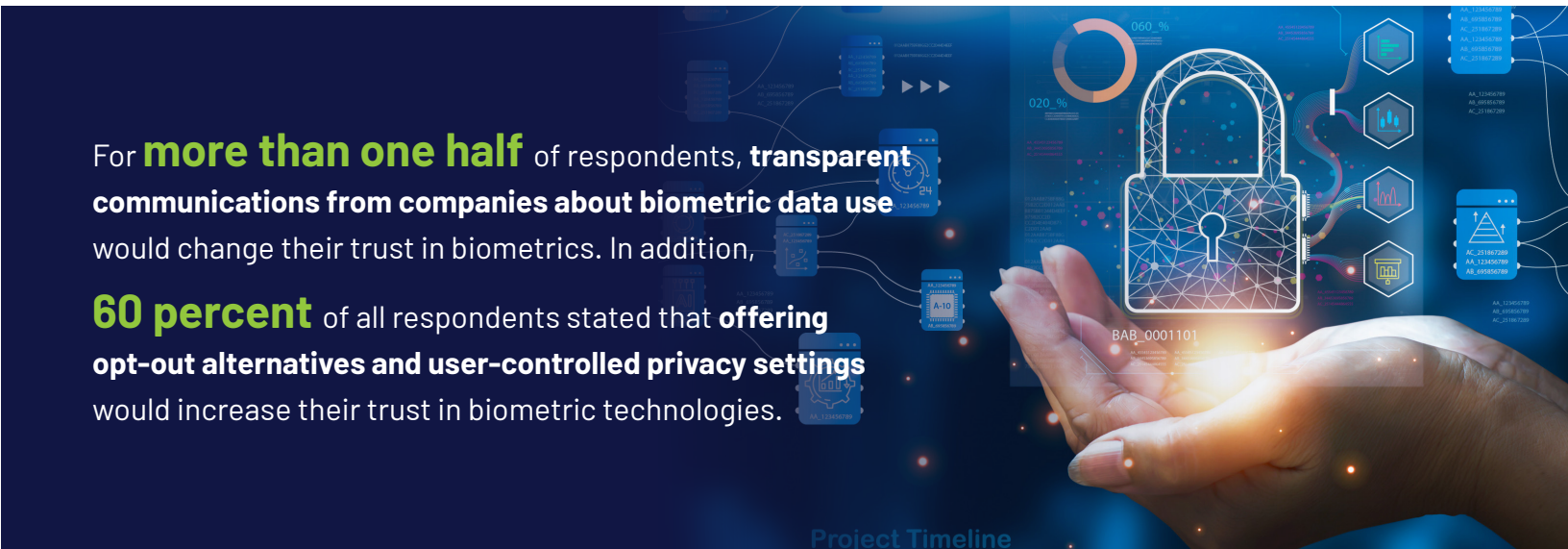
QUESTION 22

What are your thoughts on the future role of biometric technology in everyday life?

Open-ended responses from those polled.

For **more than one half** of respondents, **transparent communications from companies about biometric data use** would change their trust in biometrics. In addition,

60 percent of all respondents stated that **offering opt-out alternatives and user-controlled privacy settings** would increase their trust in biometric technologies.



Chapter 2: Key Takeaways For Organizations

TAKEAWAY #1:

Consumers are more comfortable with biometrics than you think.

Over half of the consumers we polled were accustomed to using biometric authentication technology on the regular.

The majority of consumers surveyed use the technology on their smartphones (think: Face ID, fingerprint sensors, etc.), with nearly 50% of consumers polled stating they use biometric authentication "often" or "always" to access mobile apps.

The two main reasons for using biometric authentication according to the consumers we polled? Security and convenience.

Not only did those polled use biometric authentication regularly, but they also feel largely comfortable with the technology—both for personal use and in public settings. Over half of all respondents cited that they felt "comfortable" or "very comfortable" using it in public spaces like airports and stadiums.

> ***"I think it is convenient and makes my life easier overall."*** *-Survey response*

This is great news—considering airports across the globe are rapidly expanding their use of the technology. Last year, Miami International Airport approved a contract to rollout biometric boarding[2] at all of their 130+ gates. After a test program found that the technology significantly improved boarding times, they became the largest implementation of the technology at any U.S. airport.

The expanded use of biometric authentication doesn't end at airport security. It's also playing a major role in other industries. Below are just a few examples:

1) Credit Card Account Authentication

To combat the fact that 80% of data breaches are the result of weak or stolen passwords, Mastercard announced it was rolling out Mastercard Biometric Authentication Service[3] in 2024. This effort will 'resolve the friction and vulnerability that endless passwords and multi-factor authentication prompts can create'.

2) Mobile Payments

According to TechCrunch[4], biometrics are the future of mobile payments—combining both security and convenience to efficiently process payments from your smartphone. But that's just the beginning, as the use cases for biometric authentication spans far beyond mobile.

3) Fast Identity Online Alliance (FIDO)

FIDO[5] is an alliance launched by the tech industry in an effort to thwart the uptick of hacking-related breaches for both consumers and the workforce. FIDO uses a passkey that is stored on a person's phone that only their biometrics can unlock and can be used across all your devices. It's not only groundbreaking, but far more seamless and secure than traditional passwords.

What This Means For Businesses Using Biometrics

The rise in use cases for biometric authentication is only expanding as consumers grow more accustomed to the technology. This is a positive indication that more wide-spread adoption of the technology for both government and commercial use will be tolerated and even welcomed.

Image source: International Airport Review

Now is the time for businesses to follow Mastercard's lead and start highlighting the benefits of biometrics to their customers to promote more widespread adoption.

The most important benefits according to our survey were **security** and **convenience**. To aid with adoption, companies should emphasize these benefits and focus on expressing how biometric authentication is far more seamless and secure for customers/users than traditional access methods and will:

- Eliminate the need for users to remember their passwords
- Allow near instant access to accounts with simple face scans
- Give users a more personalized experience

TAKEAWAY #2:

Companies need to do more to instill trust surrounding customers' biometric data.

While consumers have fairly strong trust in biometric technology, they're weary when it comes to how well their data is protected. Over 40% of the consumers we polled said they either don't trust companies at all or only slightly trust companies to handle their biometric data responsibly.

When we look at the growing number of consumer data breaches[6] at the hands of businesses, we can't really blame them.

"Scary Stuff" *-Survey response*

A recent survey from GetApp[7] showed that trust in biometric data has declined from 28% in 2022 to 5% in 2024. When we analyzed our survey data, we may have found the source of the mistrust. Our survey revealed consumers' hesitance with biometric authentication focused on three underlying reasons:

- **Data breaches, privacy violations, and information misuse**
- **Reluctance to use biometric authentication has nothing to do with the technology itself**
- **Everything to do with a lack of trust in companies**

> ***"I think if it works right and no data is being breached or anything then it's fine. but it still seems sketchy."*** *-Survey response*

What This Means For Businesses Using Biometrics

There's a long way to go when it comes to repairing consumer trust in data protection by companies. If positioned correctly however, biometric technology can be the answer.

Businesses need a world-class biometrics software partner to help alleviate growing concerns surrounding data breaches, facial recognition misidentification, and identity theft. They also need to be transparent about their practices to help rebuild consumer confidence.

Here are two steps businesses can take to increase transparency:

- **Vigilant security measures:** Businesses need to not only practice vigilant security measures, but highlight the safeguards they have in place to protect their customer's data.
- **Choose a leading biometrics partner:** Not all biometric solutions are created equal. It's important to choose a partner that uses the latest advancements and has a proven track record of success.

TAKEAWAY #3:

Biometrics acceptance varies by age group

Our survey found that younger age groups are more likely to adopt biometric technology. Younger generations (specifically those aged 12- 27) grew up accustomed to using technology and tend to be early adopters.

According to Biometric Update[8], Gen Z consumers are 25 percent more likely than other generations to provide personal information to gain a more predictive, personalized digital experience.

Older generations like Millennials, Gen X, and Baby Boomers (age 28-77) will need a bit more convincing. Our survey revealed that nearly 70% of those who responded that they've refrained from using a biometric option in the past due to privacy concerns, were over the age of 35.

What This Means For Businesses Using Biometrics

Older generations need more educational resources and support when it comes to biometric authentication in order to become fully comfortable with it.

In the same token, expect biometric authentication to play an even bigger role as Gen Z comes into economic power. Business should still focus on establishing a foundation of trust with older generations who may be more hesitant to adopt the technology.

Tips for increasing adoption rates in older generations:

- **Education:** Much of the hesitation surrounding biometric authentication adoption is simply lack of education. Users may not know that biometric authentication is actually more secure than traditional login metrics. Educating all users from Gen Z to Baby Boomers about the security benefits of biometrics is key to boosting adoption rates.
- **Experience:** When done well, biometric authentication offers an incredibly seamless experience. Invest in the right biometric solution that is both reliable and consistent. Once your customers experience the benefits of biometrics first-hand, adoption rates tend to pick up.

Chapter 3: How To Successfully Integrate Biometrics

Our survey revealed that many customers are already comfortable with using biometric authentication software, which is a great sign for businesses looking to provide the most secure user experience possible.

Here are three tips to continue to drive customer adoption for biometric authentication.

Tip #1: Highlight The Convenience and Security

As TechCrunch[4] puts it, many people choose convenience over security. But with biometrics, you can accomplish both.

Entering passwords or showing physical IDs are slow, outdated ways to authenticate your identity. Plus, if you forget your password or accidentally leave your ID at home, it quickly becomes problematic.

With an accuracy of over 99.5%[9], biometrics authentication is both seamless and secure. Just ask the 131 million+[10] Americans who use the technology daily.

> ***"I think biometrics will make authentication easier and more convenient provided your data is handled properly."*** *-Survey response*

Tip #2: Earn Their Trust

According to our poll, one of the biggest biometrics barriers to entry is trust. Consumers are weary of how their biometric information will be protected by companies and even the government after experiencing a data breach in the past or hearing about them on the news.

Businesses need to earn consumer trust by protecting customer data with more vigilance. Choose best-in-class data security partners, be transparent about your practices and make clear the steps you take to mitigate security breaches.

Look for the following when choosing a biometric authentication partner:

- **Use of in-house experts**
- **Advanced certifications (NIST levels, SOC2, iBeta, etc.)**
- **Advanced compliance with regulations**

Tip #3: Address Key Concerns

While the benefits of biometrics are clear, organizations must also be prepared to address potential concerns to ensure successful implementation.

Privacy: Customers may have concerns about how their biometric data is collected, stored, and used. Organizations must be transparent about their data policies and comply with relevant regulations to build trust and keep data secure. When partnering with a biometrics provider, it's essential to carefully evaluate the privacy policies and data protection measures of that vendor to ensure compliance.

Bias in Biometric Algorithms: Not all biometric solutions are created equal, and some biometric systems exhibit biases based on race, gender, or age. Those considering using biometrics should choose vendors and solutions that prioritize and can demonstrate equity, inclusivity, and accessibility, ensuring the technology won't come to any false conclusions. By conducting thorough due diligence, promoting ethical use, and implementing complementary security measures, buyers can help maximize the benefits of biometric authentication while addressing potential concerns like these.

Chapter 4: The Future Of Biometrics & Business

In today's rapidly evolving business landscape, biometric technology offers powerful solutions to both current and future challenges. Whether it's defending against emerging threats like deepfakes, enhancing accessibility, ensuring compliance with stringent, changing regulations, or preventing fraud, biometrics provide a secure, efficient, and user-friendly approach. As businesses adapt to new demands and risks, the role of biometrics in addressing these critical issues will only grow in importance.

Deepfake Defense

Deepfake technology, which uses artificial intelligence to create realistic but fake audio, video, and images, poses a significant threat to businesses. These fabricated media can be used to manipulate public perception, impersonate individuals, or even commit fraud. Biometric technology, such as facial recognition and voice authentication, can help detect and defend against deepfakes[11] by analyzing unique biological traits that are difficult to replicate. A critical component of this defense is liveness detection, which distinguishes between a real, live person and a static image or pre-recorded video. Liveness detection[12] works by assessing subtle cues, such as blinking, breathing, or natural variations in speech, which are nearly impossible to replicate convincingly in deepfakes. By integrating biometric verification with advanced liveness detection, businesses can ensure the authenticity of communications and transactions, providing a robust safeguard against the growing threat of deepfake technology and protecting their reputation and assets.

Accessibility

Biometric technology can play a crucial role in enhancing accessibility[13] for individuals with disabilities. Traditional security measures, like passwords and PINs, can be challenging for people with cognitive impairments, physical disabilities, or vision issues. Biometric systems, which rely on unique physical characteristics such as fingerprints, facial features, or voice patterns, provide a more intuitive and accessible way to interact with

technology. For instance, facial or voice recognition can allow users a touchless way to unlock devices or access services without needing to enter complex credentials. By adopting biometric solutions, businesses can create more inclusive environments that cater to the diverse needs of their customers and employees.

Compliance

As data privacy regulations become more stringent worldwide, businesses face increasing pressure to ensure that their security measures comply with these laws. Biometric technology offers a solution by providing a secure and efficient means of verifying identities, thereby reducing the risk of unauthorized access to sensitive information. This is particularly relevant in industries where Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations are crucial. Biometric authentication helps businesses meet KYC and AML requirements by accurately verifying the identities of customers, ensuring that they are who they claim to be, and reducing the likelihood of fraudulent activities.

Plus, compliance with the General Data Protection Regulation (GDPR) is essential for businesses operating in or dealing with customers in the European Union. GDPR emphasizes the protection of personal data, and biometric data is considered highly sensitive under these regulations. By implementing biometric systems that are secure and privacy-focused, businesses can demonstrate their commitment to data protection and regulatory compliance. Additionally, biometric systems often include audit trails and detailed logs, which can be invaluable during compliance audits, helping businesses to avoid costly fines and legal repercussions.

Fraud Prevention

With the rise of cybercrime, fraud prevention has become a top priority for businesses across all industries. Traditional security measures, such as passwords and security questions, are increasingly vulnerable to hacking and phishing attacks. Biometric technology offers a more secure alternative, as biometric traits like fingerprints, facial recognition, and iris scans are unique to each individual and difficult to replicate.

For example, in Brazil, the banking sector has seen a significant rise in fraud rates, particularly with the increase in digital banking and online transactions. Cybercriminals have become more sophisticated, exploiting weaknesses in traditional security methods to commit identity theft, unauthorized transactions, and other forms of financial fraud. To combat this growing threat, Brazilian banks have increasingly turned to biometric authentication[14] solutions. By implementing systems that require biometric verification, such as facial recognition for mobile banking apps or fingerprint authentication at ATMs, banks in Brazil have been able to significantly reduce the incidence of fraud.

7 out of 10

Brazilian banks use biometrics

This approach not only protects the financial institutions but also builds trust with customers, who are more likely to feel secure when their personal information and financial assets are safeguarded by advanced biometric technologies. As fraud rates continue to rise globally, the adoption of biometric solutions in high-risk sectors like banking will be crucial in maintaining security and customer confidence.

Across industries,
trust is lowest in the online gambling sector and highest in banking;

also trust in biometrics is
higher among Gen Z and lower across older generations
including Millennials,
Gen X and Baby Boomers.

Epilogue: Looking Towards the Future of Biometric Authentication

As biometric authentication continues to evolve, one thing is clear: trust, usability, and inclusivity will define its future. While this technology has already become an essential part of how we verify identity, organizations need to go beyond simply offering biometric solutions—they must earn and sustain consumer confidence.

In the coming years, we expect to see **trust will take center stage** in biometric adoption. With data privacy regulations tightening and consumers becoming more aware of how their personal data is handled, companies will need to prioritize transparency and security. Organizations that clearly communicate their data policies, implement privacy-first practices, and offer user control over biometric information will emerge as industry leaders.

At the same time, **reducing friction and improving user experience** will be critical. Consumers expect fast, seamless login and access, whether they're unlocking their devices, making payments, or entering secure spaces. Biometric authentication is poised to replace cumbersome passwords and PINs, delivering a seamless and secure experience. Innovations in multimodal biometrics—combining facial, fingerprint, and behavioral authentication—will enhance both security and convenience, ensuring authentication is nearly invisible to the user.

Inclusivity will play a key role in shaping the next generation of biometric technology. **Historically, bias in** any machine learning or AI-based system has been a concern, but forward-thinking organizations are investing in **more diverse datasets for training, continuous model improvements, and fairness-driven algorithms** to ensure biometric authentication is accessible and accurate for everyone, regardless of age, gender, or ethnicity.

Finally, **biometric authentication will expand into new avenues**, revolutionizing industries beyond finance, healthcare, and border security. Expect **biometric-powered smart cities, identity verification for metaverse applications, and biometrics as a key enabler for decentralized digital identity**. As we see deepfake threats rise, biometric authentication combined with liveness detection will also become a frontline defense against identity fraud and AI-driven impersonation.

The path forward is clear: biometrics will be an indispensable part of the digital world, but its success hinges on **prioritizing trust, reducing friction, ensuring inclusivity, and responsibly expanding its use**. At Aware, we are committed to leading this charge—building a future where security and user confidence go hand in hand.

Thank you for joining us on this journey.

Interested in learning more? Visit www.aware.com/contact/

Sources:

1. https://www.coolest-gadgets.com/biometrics-statistics/
2. https://www.internationalairportreview.com/news/176877/miami-international-airport-launches-biometrics/
3. https://www.internationalairportreview.com/news/176877/miami-international-airport-launches-biometrics/
3. https://www.mastercard.com/news/perspectives/2024/biometrics-will-soon-replace-passwords-once-and-for-all/
4. https://techcrunch.com/sponsor/no-sponsor/forget-passwords-how-biometrics-are-transforming-the-security-of-mobile-payments/
5. https://fidoalliance.org/
6. https://www.upguard.com/blog/biggest-data-breaches-us
7. https://www.securitymagazine.com/articles/100424-trust-in-biometric-data-is-declining-among-consumers
8. https://www.biometricupdate.com/202312/how-the-next-generation-is-changing-the-future-of-payments
9. https://www.nist.gov/news-events/news/2021/07/nist-evaluates-face-recognition-softwares-accuracy-flight-boarding
10. https://photoaid.com/blog/facial-recognition-statistics/
11. https://www.aware.com/powerful-defense-against-deepfakes-with-biometrics-blog/
12. https://www.aware.com/blog-what-is-liveness-detection/
13. https://www.forbes.com/sites/stevenaquino/2023/08/25/aware-cto-dr-mohamed-lazzouni-talks-the-digitalization-of-identification-voice-tech-more-in-interview/
14. https://www.aware.com/blog-bank-reduced-credit-application-fraud-with-biometrics/
15. https://www.aware.com/blog/
16. https://www.aware.com/blog-industries-being-transformed-by-biometric-technology/