fido ALLIANCE | simpler stronger authentication

Remote ID Verification: Bringing Confidence to Biometric Systems

Consumer Insights 2024

www.fidoalliance.org

Executive Summary

How can we verify users are genuine in an online world?

As services continue to invest in digital transformation and e-identity schemes across the globe, governments and organizations alike remain stuck on this critical question.

Biometric face verification is a robust, established solution for “selfie matching” users remotely with their trusted identity documents, such as passports and driver’s licenses. However, not all face verification solutions are created equally. As the adoption of identity verification technology rises, two critical concerns and challenges need to be addressed: bias and new security threats.

Online identity theft has steadily risen in recent years, while the generative AI boom has driven a new wave of deepfake-powered attacks that threaten remote enrollment and identity security. Meanwhile, bias in biometric systems has been monitored for some time, varying significantly across solutions and impacting consumer trust and perception of the technology.

This eBook reveals the trends discovered by an independent study of 2,000 respondents across the U.S. and the U.K. to understand consumer perception towards remote identity verification, online security, and biometrics.

Key findings

- Consumers want to use biometrics to verify themselves online more, especially in sensitive use cases like financial services - where one out of two people said they would use biometric technology **(48%)**.
- One in four feel they experience regular discrimination when using automated facial biometric systems **(25%)**.
- Equity in biometric systems is vital to trust – with half saying they would lose trust in a brand or institution **(50%)**, with one out of five saying they’d stop using a service entirely if found to have a biased biometric system **(22%)**.
- Over half of respondents are concerned about deepfakes when verifying identities online **(52%)**.

As services become more digital, security and speed are most important to consumers.

When enrolling to a new service of verifying online, which is most important to you?

	Combined	UK	US
Trusted security method	84%	81%	86%
Speed of process	75%	75%	74%
Intuitive user experience	58%	59%	57%
Nothing to remember	47%	46%	47%
MFA used	37%	39%	36%

Consumers want to use biometrics more to verify themselves online.

Which of the following online services would you most like the option of using biometrics to enroll? Select all that apply.

	Combined	UK	US
Financial services	48%	47%	49%
Digital identity	44%	41%	47%
Government services	37%	40%	40%
Healthcare	37%	35%	35%
Utilities	24%	24%	23%
Retail	21%	21%	21%
Gaming	17%	20%	15%
Other	6%	7%	5%

In separate research from The FIDO Alliance's Annual Online Authentication Barometer Report, **biometrics has ranked the top authentication method** among global consumers for the past two years (2022 and 2023).

When given the option to use biometrics, people prefer this authentication method for more convenience and security.

In this survey, consumers demonstrated strong appetite to use biometrics to enroll and verify themselves among key online use cases, especially financial services, government services and digital identity.

Source: Annual Online Authentication Barometer. 2023. FIDO Alliance report. https://fidoalliance.org/barometer-2023

Bias in biometric facial verification systems remains a worry.

To what extent do you agree current facial verification technologies can accurately identify individuals across different races, genders, and ages?

	Combined	UK	US
Strongly agree	22%	26%	19%
Somewhat agree	34%	31%	37%
Neutral	25%	26%	24%
Somewhat disagree	6%	6%	7%
Strongly disagree	3%	4%	2%
Not sure	10%	8%	11%
% Agree (Total)	56%	57%	56%

Organisations like NIST have been monitoring the disparities in performance of some low-performing solutions across different demographics.

Consumers largely agree biometric face verification systems can be accurate, but there are clear disparities in the accessibility, usability, and equity in system performance.

Source: Face Recognition Technology Evaluation: Demographic Effects in Face Recognition. 2024. NIST report. https://pages.nist.gov/frvt/html/frvt_demographics.html

Some have felt discriminated against by biometric face verification systems.

How often have you felt discriminated against by automated facial biometric systems?

	Combined	UK	US
Frequently (nearly every time I have used these systems)	11%	15%	7%
Somewhat regularly (this has happened more than once using these system)	14%	13%	15%
Rarely – this has happened once	13%	13%	12%
Never	53%	47%	58%
Not sure	10%	12%	8%
% Frequently / Somewhat regularly (Total)	25%	28%	21%

Not everyone agrees on the accuracy of these systems; one in four say they feel they have been discriminated against by automated face verification systems.

Source: Annual Online Authentication Barometer. 2023. FIDO Alliance report. https://fidoalliance.org/barometer-2023

Equity across biometric identity verification systems is vital to trust and reputation.

How would your trust in a brand or institution change if its biometric system was proven to be biased against certain groups?

	Combined	UK	US
Significantly decrease - I would stop using their services/products entirely	22%	25%	20%
Somewhat decrease - I would be cautious about using their services/products	28%	26%	29%
It would not change my trust level in the brand or institution	21%	19%	23%
I am not concerned about the bias in biometric system	9%	9%	9%
I am not sure / No opinion	20%	21%	20%
% Decrease (Total)	50%	51%	48%

Equitable and inclusive biometric systems are vital to ensure all users can use and benefit from new biometric programs - but opinions are also tightly linked to an organization's brand reputation and trust.

Deepfakes and the changing threat landscape are raising consumer concerns and demands for increased security.

Generative AI has made creating deepfake imagery and video easier than ever. How does this impact how you view the use of biometrics to secure and verify yourself online?

	Combined	UK	US
Increased concern: It makes me more concerned about the reliability and security of systems	34%	37%	31%
Need for enhanced security: It emphasizes the need for stronger, more sophisticated biometric systems	18%	14%	21%
No change in perception: It doesn't change my view; I still see biometrics as reliable	19%	18%	19%
Preference for traditional methods: It makes me want to use more traditional security methods, like passwords, over biometrics	8%	7%	9%
Seek more information: It makes me want to learn more about how biometric systems can combat these challenges	6%	7%	6%
Not sure: I am unsure about the impact or need more information to decide	16%	17%	15%

Online identity theft has risen while the generative AI boom has brought threats like deepfakes into the public perception and is making them more concerned about using biometrics to secure and verify themselves online.

In ENISA's latest remote ID report, researchers observed that while deepfake injection attacks are increasing and more sophisticated, deepfake presentation and injection attacks remain the top two biometric attack types most difficult to mitigate.

Source: Remote ID Proofing - Good practices. 2024. ENISA report. https://www.enisa.europa.eu/publications/remote-id-proofing-good-practices

Addressing bias and deepfake threats with independent global validation

For any organization looking to implement face verification for its identity verification procedures or to include it in related regulations, testing levels vary and are often completed on a case-by-case basis, per organization. This means it's expensive, time consuming, and widely variable, which makes it difficult to establish what 'good' performance should be.

Find out more about how FIDO Alliance is helping to fast-track and secure the rollout of remote identity verification at https://fidoalliance.org/certifications/identity-verification

fido ALLIANCE | simpler stronger authentication

Research Methodology

The survey was conducted among 2,000 consumers across the UK and US - with 1,000 in each country.

The interviews were conducted online by Sapio Research in April 2024 using an email invitation and an online survey.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. In this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 2.2 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.