InfoBrief, sponsored by Mitek
DECEMBER 2023

Biometrics Key to Customer Satisfaction and Combating AI-Generated Fraud

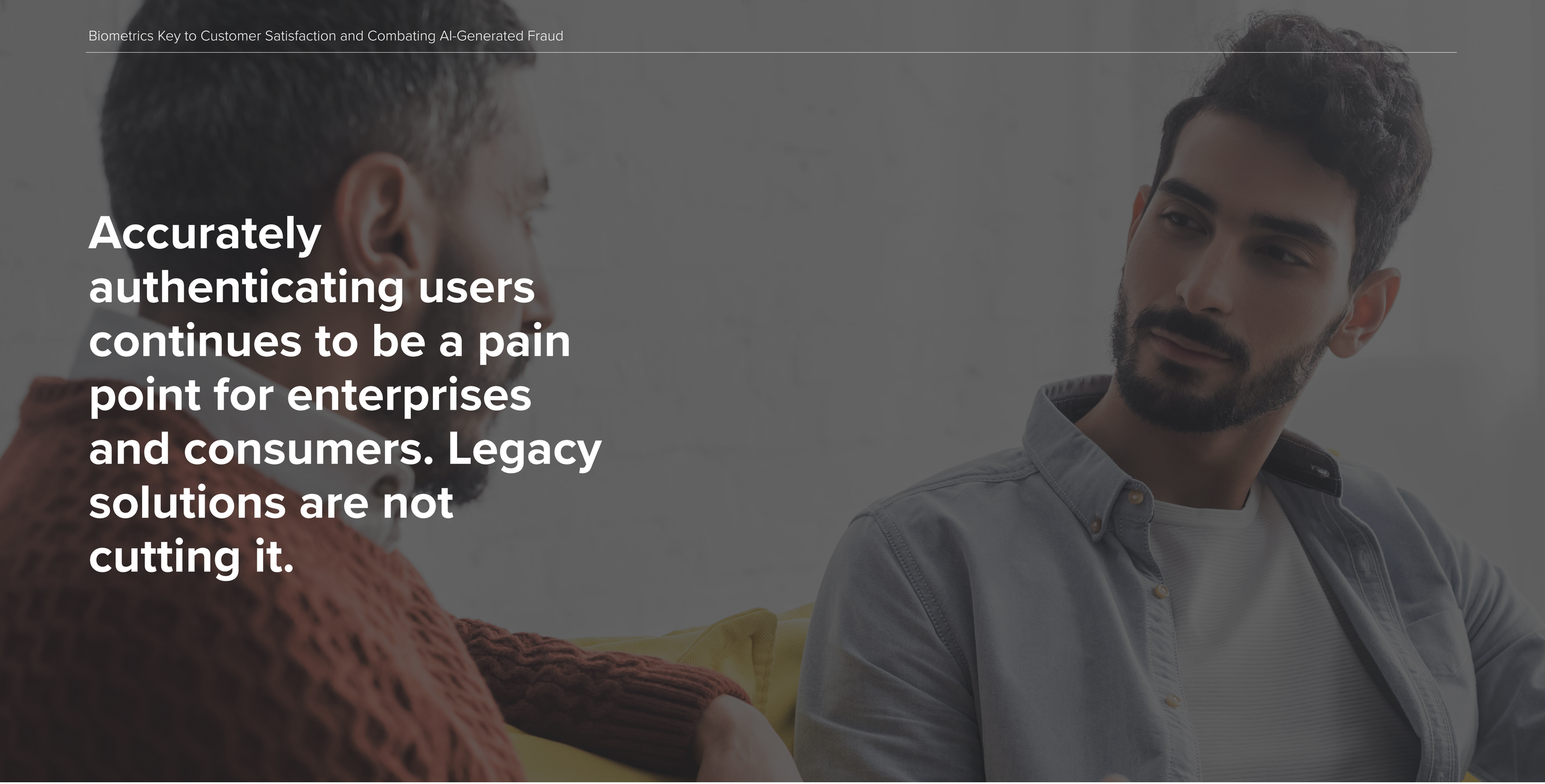
Mark Child
Associate Research Director,
European Security

George Briford
Research Director,
IDC Financial Insights

Synopsis

Account takeover and identity fraud can be concerns when using any online service, whether checking one's bank balance or booking a hotel. Biometric authentication methods (using factors such as fingerprints or face scans to log in to services) make authentication more secure and straightforward — without the need for complicated passwords that are often forgotten or can be targeted by criminals.

Biometric authentication is already supported by most digital service providers and is now enabled on most devices, from smartphones and tablets to notebooks. IDC research found that consumers with high levels of biometrics exposure tend to be more satisfied with the authentication process. Nevertheless, while most consumers feel comfortable using biometrics for authentication, not all fully understand or accept this usage. Education initiatives focused on biometrics will be crucial as the market increasingly grapples with challenges such as AI-generated deepfakes.



Accurately authenticating users continues to be a pain point for enterprises and consumers. Legacy solutions are not cutting it.

Accurately authenticating users remains a pain point for both enterprises and consumers.

1 in 4

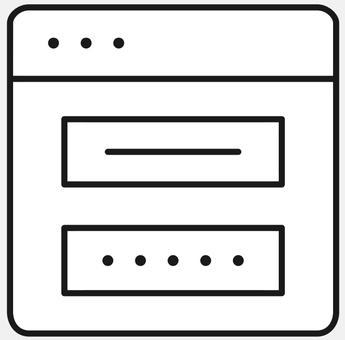
respondents to IDC's consumer survey said they had had one of their online accounts hacked and taken over: Criminals used stolen credentials to gain access to the account, locked the user out, and made unauthorized transactions.

Once that happens, resolution can be difficult and financial losses and other damage are possible.

More than one-third of respondents said that, due to unsatisfactory resolution, they switched to another service. So, would it not be better to avoid such an attack in the first place?

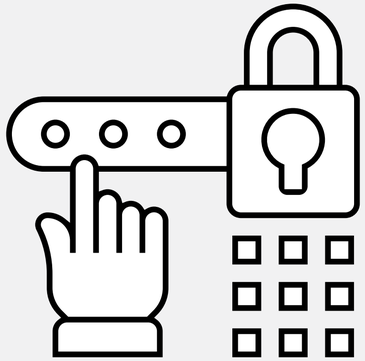
How would you want to authenticate?

Passwords are found to be less and less effective as a security measure, and consumer frustration with them is on the rise.



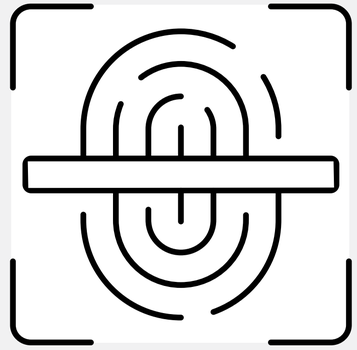
1 in 3

consumers said having to remember multiple usernames and passwords is their biggest authentication headache.



1 in 5

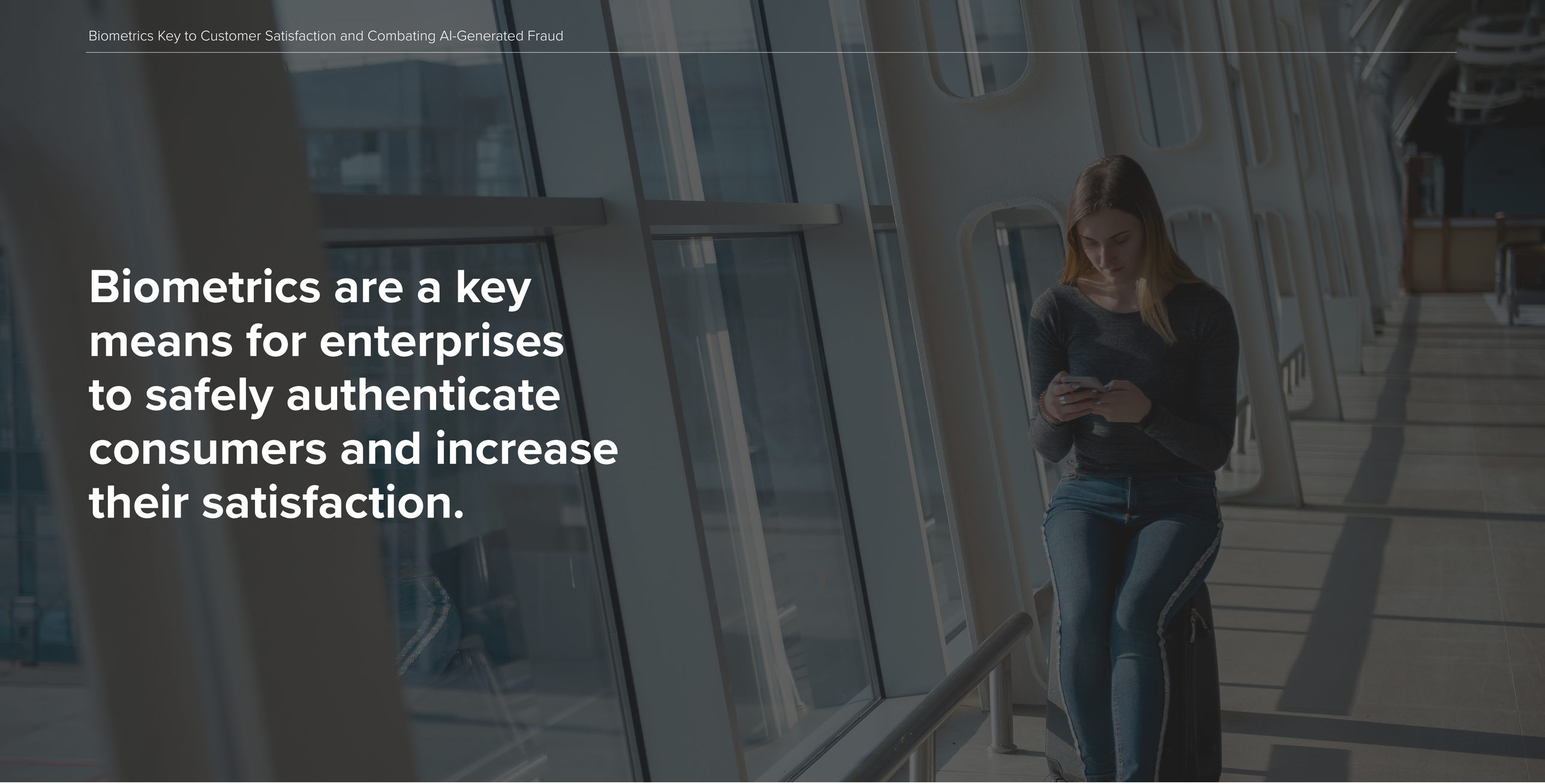
consumers dislike having to complete password reset processes if they forget a password.



In contrast, only

1 in 20

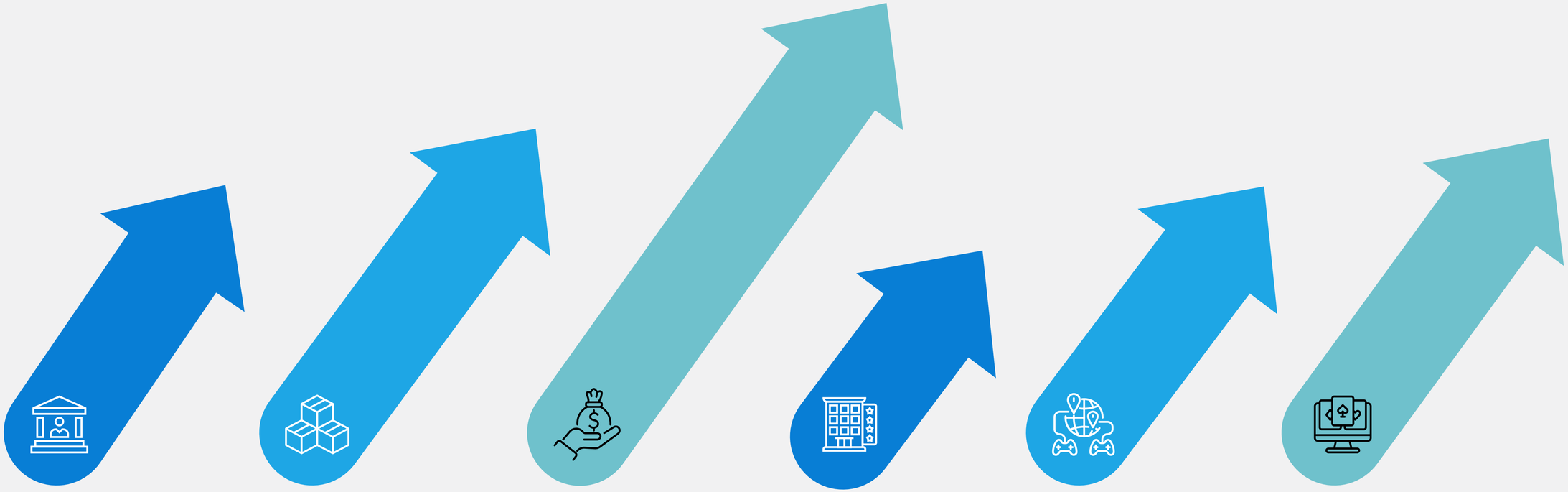
struggle with biometrics.



Biometrics are a key means for enterprises to safely authenticate consumers and increase their satisfaction.

Biometrics can bring a significant boost to customer satisfaction.

In many of the surveyed sectors, enabling biometric authentication brought significant increases in customer satisfaction:



+8%
Bank account with a challenger bank

+9%
Insurance products

+22%
Loan with a traditional bank

+5%
Accommodation and hotel booking

+8%
Online gaming

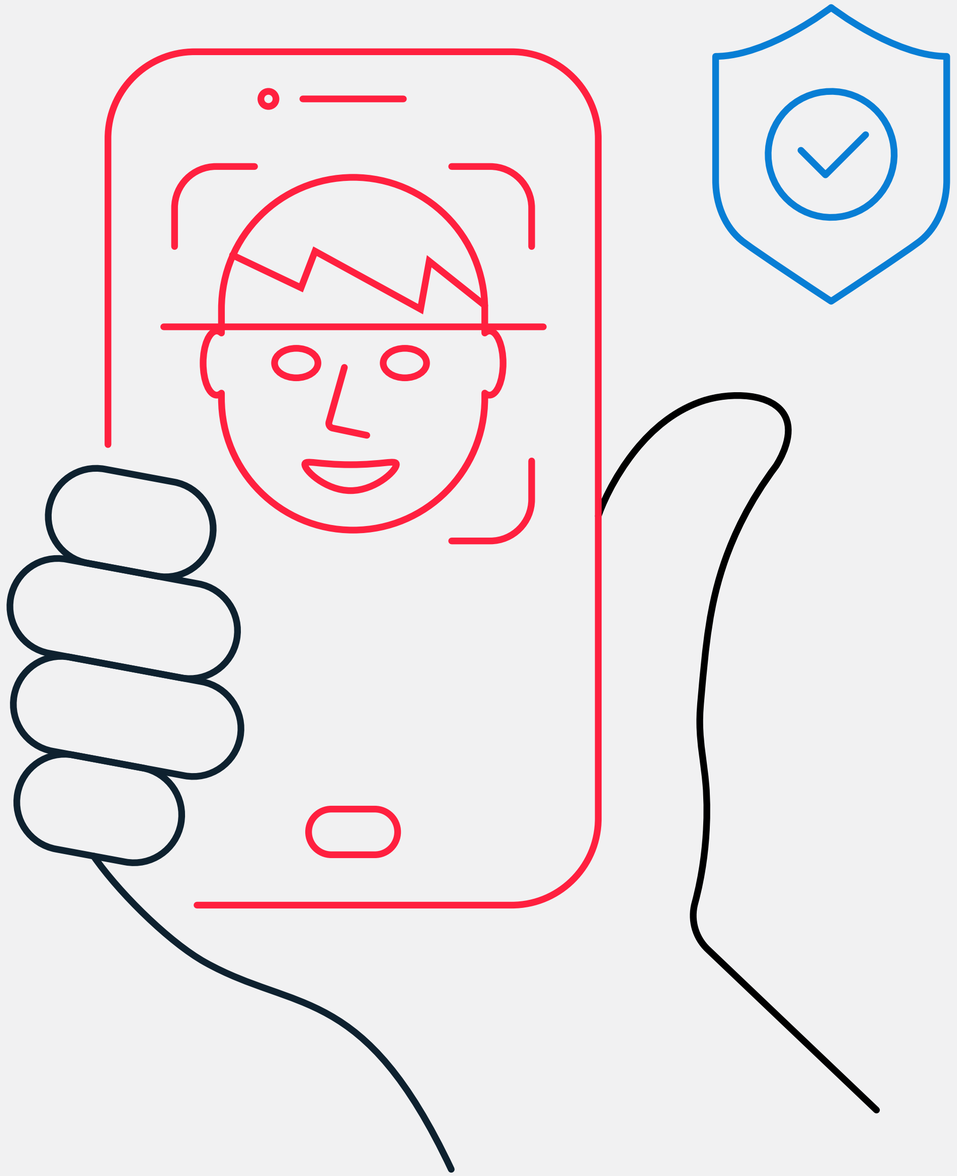
+14%
Online gambling, betting, and lottery

IDC's Authentication Survey, 2023, B2C, n = 1,045

Get some biometric satisfaction!

77% of the respondents who use biometrics on their smartphones and tablets say they are satisfied (top two boxes on a 5-point scale: very satisfied + somewhat satisfied) with biometric authentication.

67% of the respondents who use biometrics on their computers say they are satisfied (top two boxes on a 5-point scale: very satisfied + somewhat satisfied) with biometric authentication.



IDC's Authentication Survey, 2023, B2C, n = 1,045

How and why are companies and consumers using biometrics today? What needs to be done to expand biometric adoption to combat AI-generated fraud?

Providers of online products and services are looking out for their customers.

- According to our B2B survey, the top priority of online service providers is the provision of user-friendly authentication and convenient user experience **(48%)**.
- The security of authentication processes **(39%)** and the provision of immediate customer support in the case of difficulties **(37%)** round out the top 3 priorities.
- In short, online service providers are doing everything in their capability to help their customers.

- Some **63%** of organizations use biometric identification capabilities to enable their customers to access services — most commonly, fingerprints and face scans.
- In some market segments, the rate is even higher:
  - In the U.K. and Ireland, **71%** of online service providers have enabled biometric authentication for their customers.
  - In the finance sector, **97%** allow biometric authentication.
  - The majority of the largest service providers (with 1,000 or more employees) use biometrics — **77%** of such organizations.

- Providers cite multiple reasons for enabling biometric authentication:
  - Improved compliance: It protects customer data and ensures compliance **(60%)**.
  - Improved security: It improves security, as it is more secure than other authentication methods **(54%)**.
  - User convenience: It is easier to use than other authentication methods **(48%)**.

IDC's Authentication Survey, 2023, B2B, n = 300

Consumers biometrics usage varies by industry.

- Some **46%** of consumers use biometric authentication to log in to their regular traditional bank accounts online. Only **22%** use it to check their credit card accounts and **20%** to check their savings and deposit accounts.

- The lowest penetration of biometrics is seen in the peer-to-peer lending sector (**2%**). This sector also has the highest dissatisfaction (**25%**) with current authentication processes.

- In the non-finance services market, the highest penetration of biometric authentication is in online marketplaces such as Amazon and eBay (**18%** of consumers). This sector also has the highest satisfaction with current authentication methods (**83%**).

- Some **11%** use biometrics to log in to accommodation booking platforms such as Booking.com and Airbnb, and only **9%** use biometrics for online gambling and betting.

- Two-thirds of users said they do not use biometrics for any non-finance services.

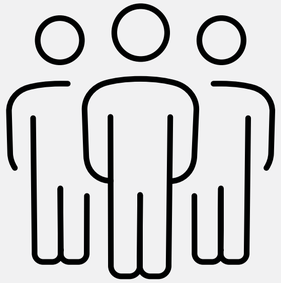
As of November 2023, Amazon has enabled the use of passkeys on browsers and mobile shopping apps, making biometric authentication an even more prolific way to achieve security and user convenience.

Fingerprints and face scans are the most common biometrics across all devices, with slightly higher usage on smartphones and tablets than on PCs and notebooks.

IDC's Authentication Survey, 2023, B2C, n = 1,045

While customer adoption and satisfaction are high, there still remains a small subset of customers who have concerns around biometrics. Two key reasons for this were identified.

Challenges to Trust: Spoofing



26%

of respondents do not believe biometrics are safe or cannot be spoofed.

In the past, hackers might have tried to spoof scanners with things like photos, videos, or masks for face scans. However, modern biometrics scanners have much higher technical capabilities.

Biometrics hardware and software components are increasingly advanced, providing high image quality and meeting international standards. Together with improved matching algorithms, this makes it much harder to spoof biometrics scans.

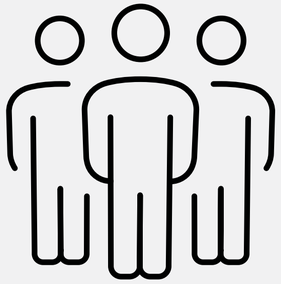
Biometric authentication capabilities include checks for additional factors such as subject "liveness" to ensure they are authenticating the correct and actual user.

Advanced security measures such as action-based factors are augmenting biometric authentication to protect against deepfakes. Providers also increasingly build deepfake detection into the backend. Voice scans and fingerprints are particularly hard for deepfakes to mimic.

The reality is that modern biometric authentication solutions are powerful tools for tackling fraud.

IDC's Authentication Survey, 2023, B2C, n = 1,045

Challenges to Trust: The Safety of Biometric Data



22%

of respondents are worried about their biometric data being stolen

A frequent misconception relates to around personally identifiable information (PII). Some consumers fear that companies will store their picture, fingerprint, or voice recording where hackers could potentially steal it.

The reality is that biometric data is not stored as images or audio files, but rather as unique numerical templates. Biometric records are converted into distinct templates of ones and zeros that cannot be decrypted by any third parties.

Modern biometric authentication solutions do not store any biometric records that could be stolen and used by fraudsters.

IDC's Authentication Survey, 2023, B2C, n = 1,045

Reasons for Driving Biometrics Adoption

83% of the organizations surveyed for this study have made investments into improving customer authentication/login technology and processes.

60% of organizations have enabled, or are in the process of enabling, multimodal authentication for their customers. A further **1 in 3** service providers is planning to enable multimodal authentication in the next year or two.

Malicious use of generative AI may present a challenge for authentication in the future, which is why **more than one-quarter** of service providers are already actively working to counter the threat and **37%** are looking at how GenAI tools can help their security teams.

Multimodal authentication seamlessly adds a second authentication factor (e.g., fingerprint + voice scan) to biometric authentication to make it even more secure.

IDC's Authentication Survey, 2023, B2B, n = 300

As we build our defenses for the new world of fraud, enterprise adoption and consumer education will be of paramount importance.

Supply-side investment in biometric authentication has brought enormous advances to help counter fraud. However, **consumer awareness of these improvements remains low**, and media reports of breaches and fraud cases are sowing fear.

A **robust education and awareness effort is required** by service providers to help increase consumer adoption of biometric authentication. This will bring benefits to both service providers and customers — reduced fraud, losses, frustration, and customer churn.

Improved user experience of biometric authentication will also drive greater traction in the market, creating a virtuous cycle.

Reusable Identity Everywhere

In the future, governments or certified providers may offer a single reusable digital identity that consumers can authenticate once for access to all their online products and services. This will deliver enormous benefits in user convenience.

Strong biometric authentication built into such a service will also deliver robust security throughout all digital activity.

Message from the Sponsor

Mitek (NASDAQ: MITK) is a global leader in digital access, founded to bridge the physical and digital worlds. Mitek's advanced identity verification technologies and global platform make digital access faster and more secure than ever, providing companies new levels of control, deployment ease, and operation, while protecting the entire customer journey.

Trusted by 99% of U.S. banks for mobile check deposits and 7,900 of the world's largest organizations, Mitek helps companies reduce risk and meet regulatory requirements.

Learn more about biometric authentication

Mitek

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data, and marketing services company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC UK
5th Floor, Ealing Cross, 85 Uxbridge Road, London, W5 5TH, United Kingdom
T 44.208.987.7100

@idc | @idc | idc.com

© 2023 IDC Research, Inc. IDC materials are licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.