

# Regula

## Identity Verification Investment: A Study on Its Business Impact

New research on how threats, solutions  
and businesses are evolving





# Contents

Key findings.....	4
The state of identity fraud in 2023.....	6
The evolving nature of identity fraud.....	8
The cost of identity fraud.....	10
How businesses are tackling fraud.....	11
Why businesses implement IDV solutions.....	13
Key considerations when choosing the right solution.....	14
Obstacles and concerns about IDV adoption.....	16
How do businesses measure success?.....	18
Conclusion. Identity verification takes center stage.....	19
Recommendations for businesses. Regula’s comprehensive solutions for streamlined identity verification.....	21
About this research.....	26
About Regula.....	27

# As fraud evolves, customer experience and peace of mind is a priority

Businesses today are facing an increasingly technologically sophisticated fraud landscape, while also trying to evolve their processes and customer experiences.

This report presents new research to help businesses tackle this issue by providing insight into both the nature of today's identity fraud landscape and the state of fraud prevention measures.

Around the world, identity fraud is a growing problem. In 2022, 26% of SMBs and 38% of enterprises experienced more than 50 identity fraud incidents. The cost is also significant, with 64% of all businesses reporting losses of at least \$120,000, and 37% of the world's largest businesses reporting losses of at least \$480,000. One of the biggest challenges for businesses as they grow is verifying identities. Finance and technology businesses are now dealing with more verification cases involving foreign documents, but many are still handling these cases manually, which is time-consuming.

Meanwhile, criminals are growing in sophistication too.

Many businesses report that they've dealt with synthetic identity fraud, and almost all leaders expect it to be a real threat in the future. Similarly, leaders believe deepfake video and voice fraud poses a threat to their businesses.

To tackle these challenges, businesses must evolve. Fortunately, many are rising to the challenge. For example, 93% of leaders already understand the importance of online identity verification in recognizing fraud, and as many as 65% of the businesses surveyed already use digital document verification. Additionally, 91% of businesses report that they plan to increase their spending on identity verification in the next three years.

In this report, we'll show you how organizations around the world are dealing with fraud, what's worked for them, and what you should consider when selecting a solution.

# Key findings

# 30+

identity fraud incidents were faced by enterprises on average during 2022.

# 91%

of businesses report that they're planning to increase how much they spend on identity verification in the next 3 years.

# 79%

of leaders believe deepfake video fraud poses a real threat to their businesses.

# 47%

Nearly half of all enterprises reported that the financial impact of identity fraud was greater than \$300,000, with the Banking sector found to be the most severely impacted.

# 80%

of finance and technology businesses are now dealing with more verification cases involving foreign documents, with 62% of them reporting that they're doing it manually.

# 56%

of enterprises consider both improved customer experience and reduced security risks as important success factors for IDV solution deployment.

# 11-20%

of businesses' annual IT budget is allocated for IDV solutions.



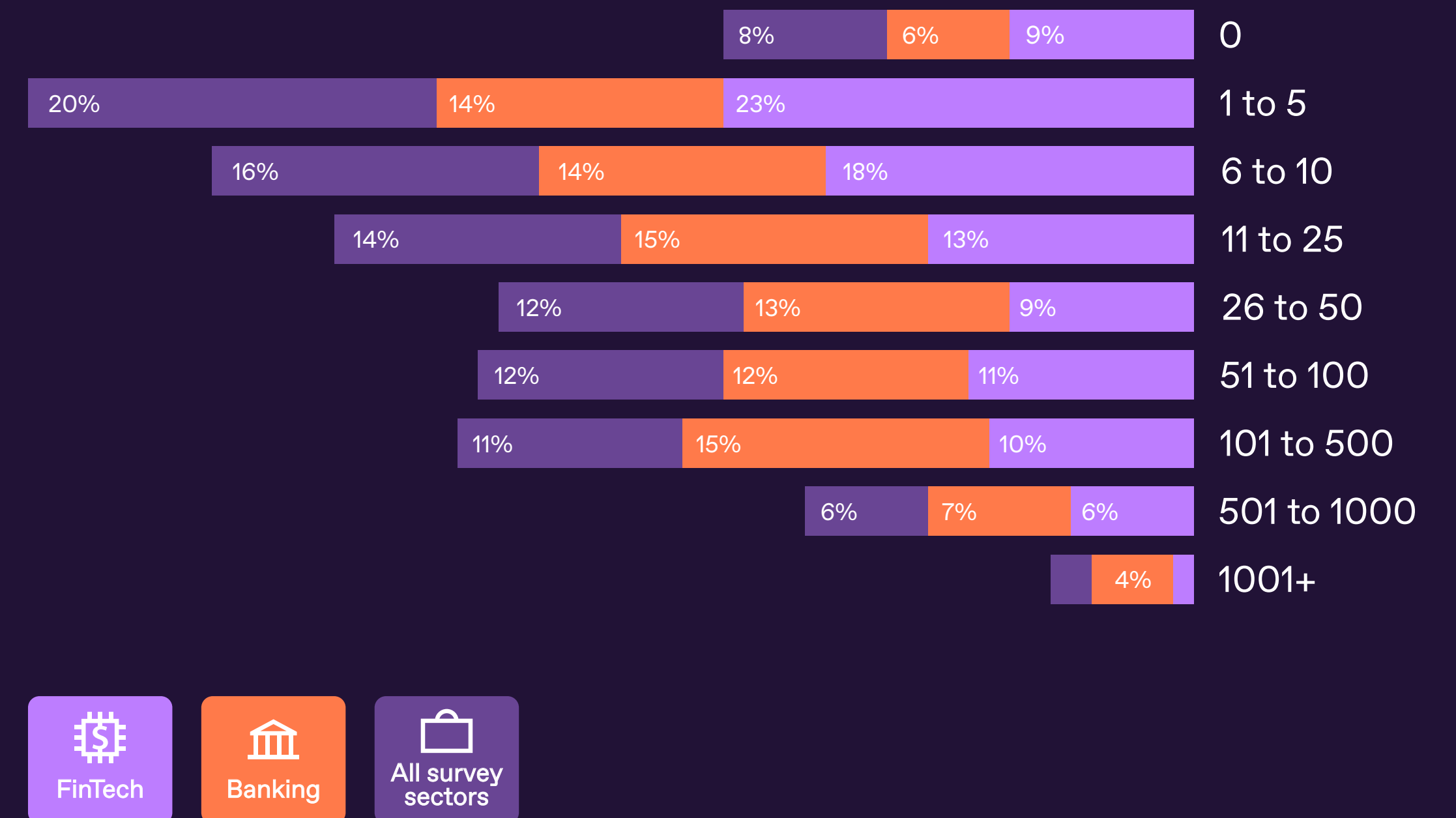
# The state of identity fraud in 2023

Over the past year, 95% of enterprises have reported experiencing identity fraud incidents within their organization. Specifically, the number of identity fraud incidents they dealt with exceeded an average of 30 per company in 2022.

Notably, this issue doesn't only affect the largest enterprises: small businesses reported experiencing a slightly lower average of 10 cases of identity fraud in 2022, yet still, 90% of these smaller organizations have been affected. Across sectors, the proportion of companies that have been affected by identity fraud remains high, with Banking most commonly being affected (94%).

Clearly, identity fraud affects every size of business in every sector. Last year, more than half of all enterprises (53%) reported dealing with fake or modified physical documents specifically, yet criminals are becoming increasingly creative in the way they approach identity fraud.

## Number of identity fraud incidents during 2022





# The evolving nature of identity fraud

Nearly half of all businesses (46%) around the world have had to deal with synthetic identity fraud. Synthetic identity fraud involves the creation of a new false identity using a mix of either real and false information, or a combination of real information from separate individuals. For example, a fraudster may use a fake Social Security number with real personal information (name, birthdate, address) to create a new identity, or they may use a real Social Security number from one individual and combine it with real personal information from another. Once the synthetic identity has been established, the fraudster can use it to apply for credit cards, loans, or other financial products, building up a credit history over time. The fraudster can then utilize the established credit to “bust out,” making large fraudulent purchases or taking out huge loans and then vanishing.

Because the identity is fictitious and leaves no identifiable consumer victim, it can be difficult for lenders and credit bureaus to detect and prevent synthetic identity fraud. In the USA, as many as 55% of businesses report that this has happened to them.





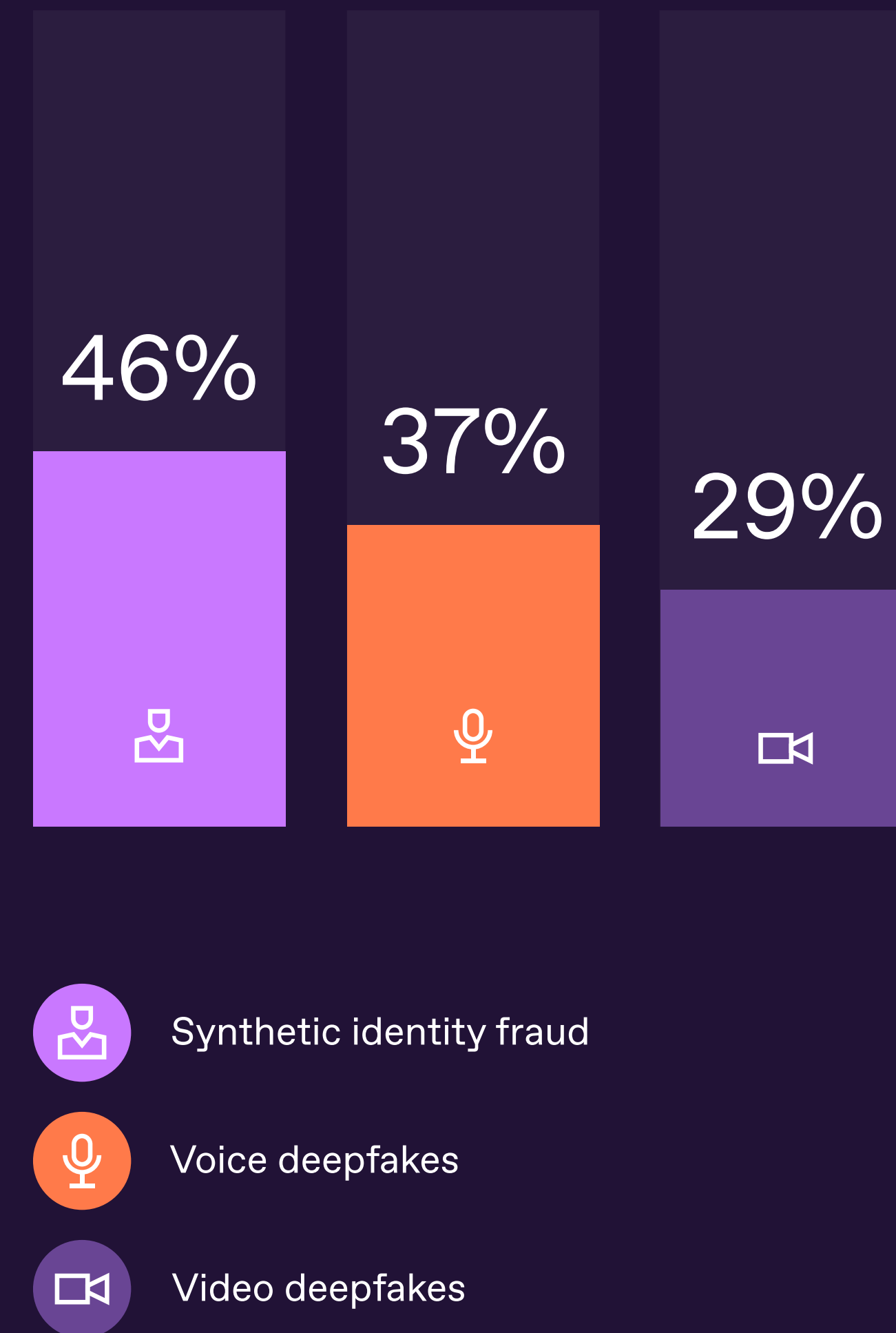
Meanwhile, even newer, more sophisticated approaches are gaining prominence. New technologies like generative artificial intelligence (AI) stand to empower criminals to attempt more kinds of identity fraud at a greater scale than was possible before. Generative AI includes algorithms (such as ChatGPT) that can be used to create new content, including audio, code, images, text, simulations, and video.

37% of all businesses have experienced deepfake voice fraud, a type of fraud that involves the use of AI to create convincing fake voice recordings of individuals for the purpose of committing fraud. Nearly half of all UAE (48%) and US (46%) businesses report experiencing this form of fraud. Even video deepfakes—manipulated videos that use AI to alter or replace the content of a video with fraudulent content—are presenting new problems, with 40% of US businesses reporting they’ve experienced these, far above the global average of 29%.

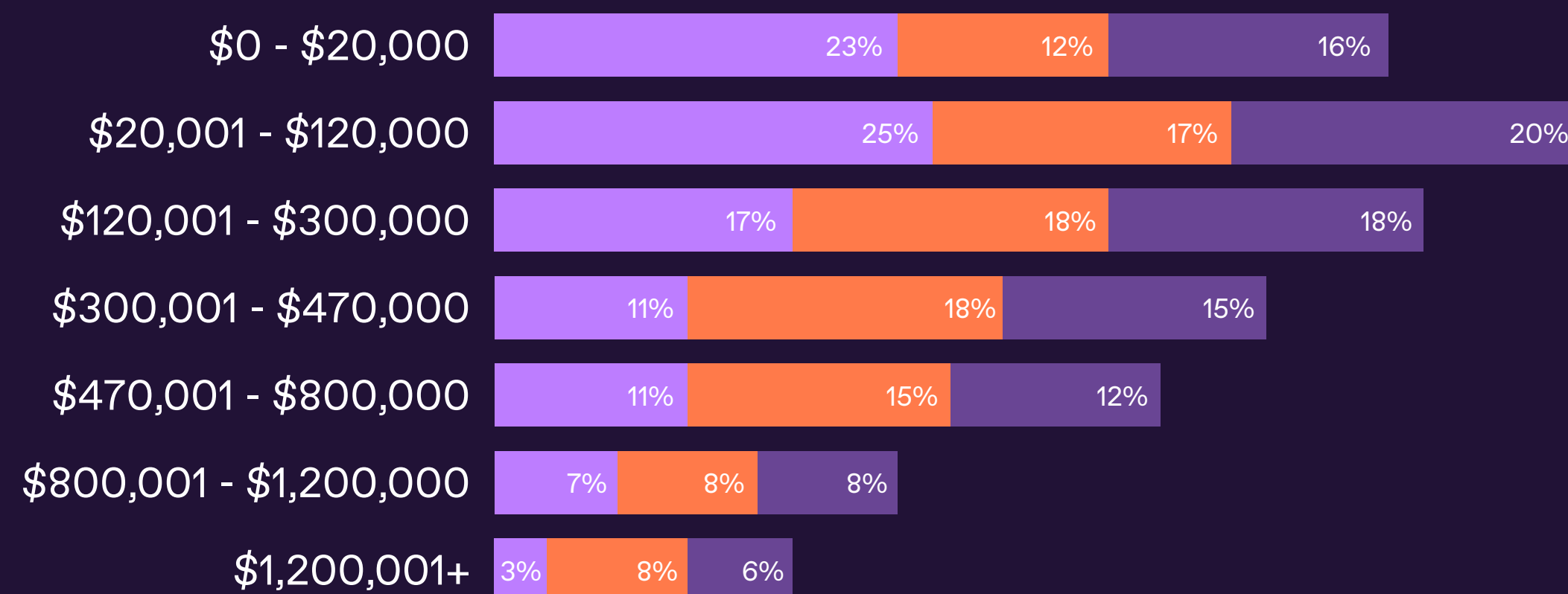
Again, these issues aren’t reserved for large enterprises. Almost half of all small and medium-sized businesses (46%) have already experienced synthetic identity fraud, and 28% have experienced deepfake video fraud.

As these technologies proliferate, the chances of any business—big or small—being affected by them only grows. Unfortunately, the costs to businesses’ time, money, and reputation are severe.

## Organizations targeted by the new and sophisticated methods of identity fraud



## Economic impact of identity fraud incidents



# The cost of identity fraud

Nearly half of all enterprises (47%) reported the financial impact of identity fraud was greater than \$300,000. In fact, nearly a quarter of enterprises (24%) with more than 10,000 employees reported that identity fraud cost them more than \$1 million in 2022. The Banking sector was the most severely impacted, losing an average of over \$310,000. In fact, for 31% of banking organizations, the cost of such incidents was nearly half a million dollars (\$479,000 or more). On average, FinTech businesses had to pay less than this, but at an average cost of over \$120,000, the impact of identity fraud is hard to ignore.

The important thing to note about these costs isn't just the dollar amounts, though they are sizable. The fact of the matter is that identity fraud costs businesses in a number of ways. When asked about the biggest costs of identity fraud, most (44%) respondents cited "business disruption" as the key issue. At the same time, more than a third of respondents cited legal expenses (36%) and the loss of current and potential clients (34%).

That last issue is particularly severe in certain areas. 66% of Mexican businesses and 47% of UAE businesses highlight this reputational damage as the biggest cost, as do 40% of FinTech businesses.



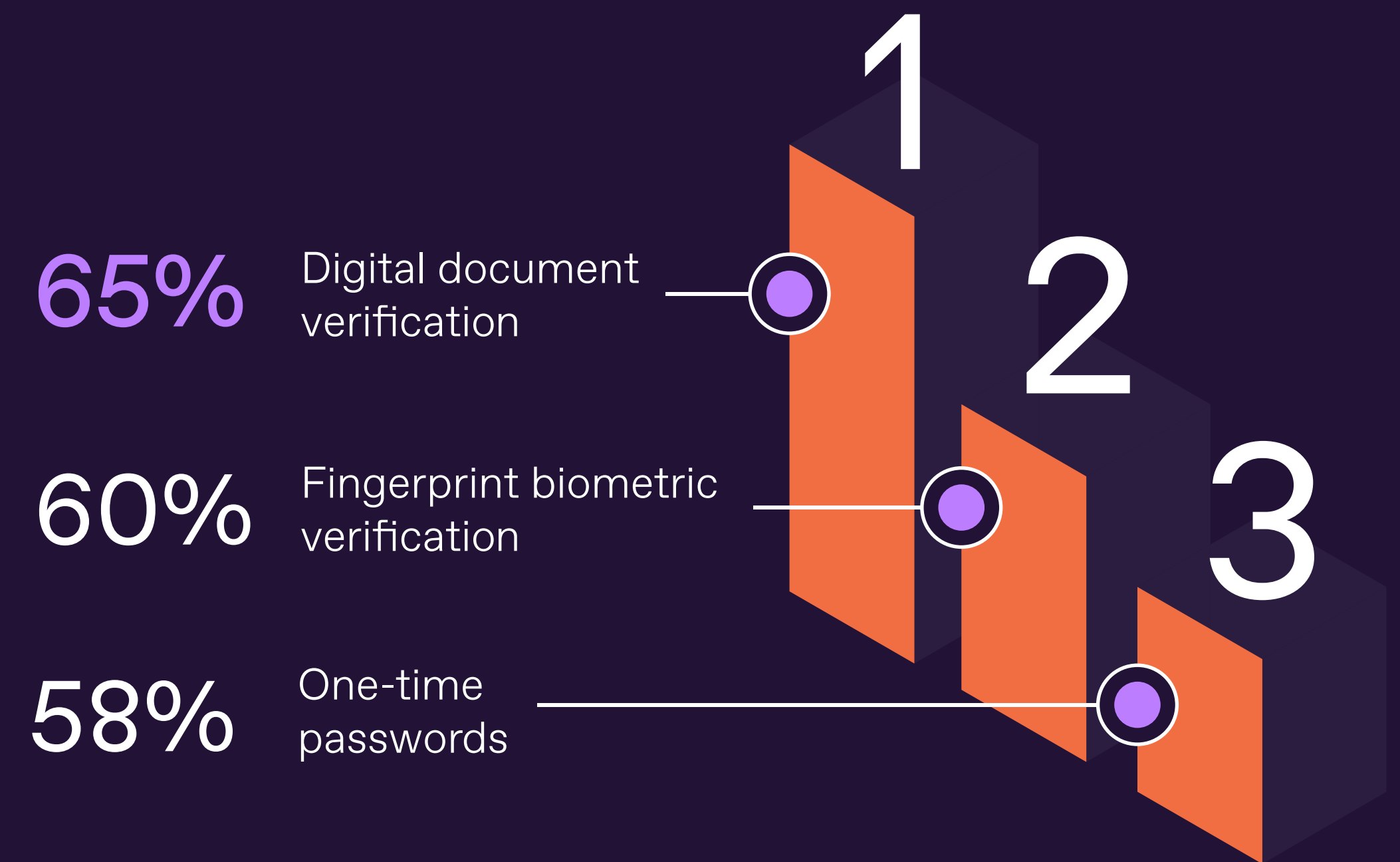
# How businesses are tackling fraud

In the past, when the vast majority of customer transactions took place in person, it made sense for businesses to rely on largely manual processes to verify their customers' identities. Today, consumer expectations have changed. More often than not, customers prefer transacting online and making it fast. And businesses can't afford to scale their manual processes to keep up. This is especially important in industries where speed is of the essence, such as e-commerce, financial services, and telecommunications.

This is why 93% of businesses believe online identity verification is so important to their business, and why 94% of businesses have been using an online identity verification tool for more than two years. Globally, 65% of businesses are already doing digital document verification, with 56% also offering biometric verification through facial recognition. Indeed, in the US, 71% of businesses now rely on digital document verification—and 94% of businesses that aren't currently using digital document verification will be enrolling in a document-centric identity proofing method within the next year.

## Top 3 methods of identity verification

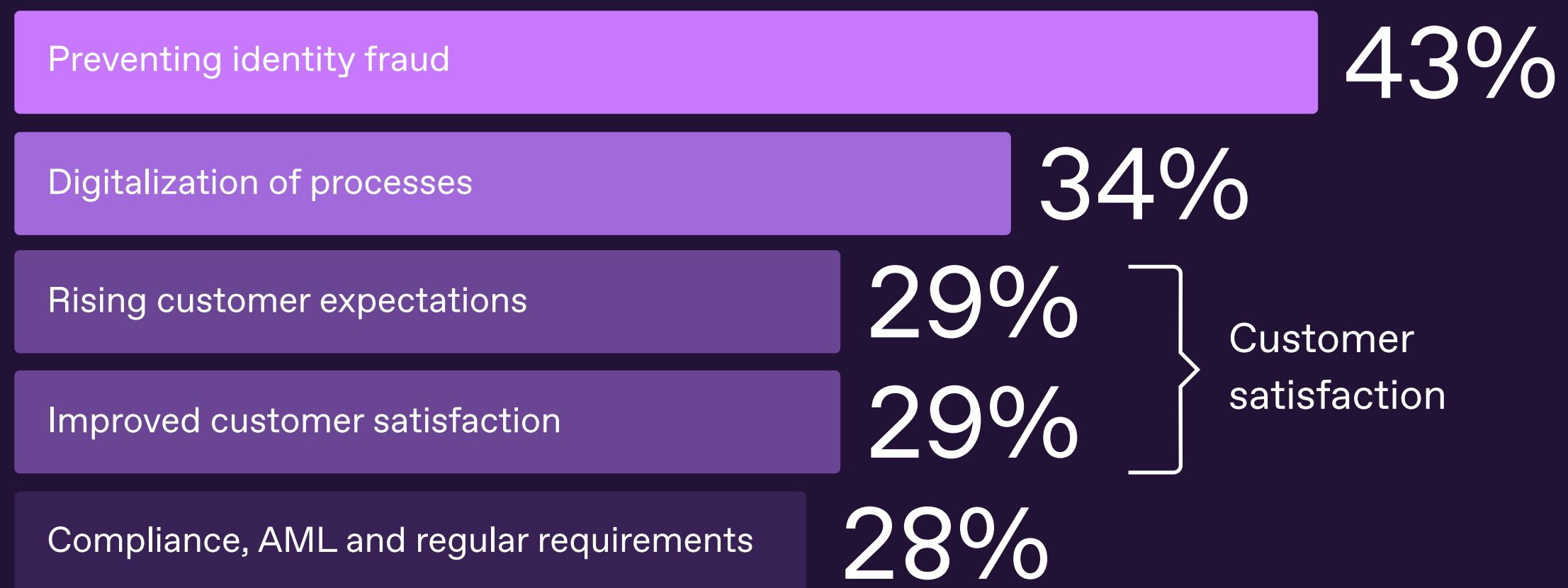
Which of the following online IDV methods do surveyed organizations use?





## Main business drivers for IDV implementation

Customer-centricity is becoming critical for businesses



# Why businesses implement IDV solutions

Most businesses implement identity verification solutions, naturally, to prevent incidents that involve identity fraud. But notably, 34% of businesses worldwide also do so because they're digitizing all their processes. This is especially true for large enterprises with more than 10,000 employees (41%) and Mexican organizations (44%).

Moreover, 80% of financial services and technology businesses report that they're now dealing with more verification cases involving foreign documents—especially in countries like France (86%), Turkey (85%), and the USA (85%). Almost half of organizations (44%) face as high as a 25-percent increase in the volume of foreign document verification cases. 62% of these businesses report having to handle such cases in manual ways that take a lot of time. In situations like these, the right identity verification solution can have a big impact on productivity, speed, and, when implemented well, even employee morale.

It's also important to note that, globally, 29% of all businesses implement identity verification solutions because they represent customer requirements and will improve customer satisfaction levels. Indeed, 41% of US businesses that have implemented identity verification technology say they've done so for this very reason.

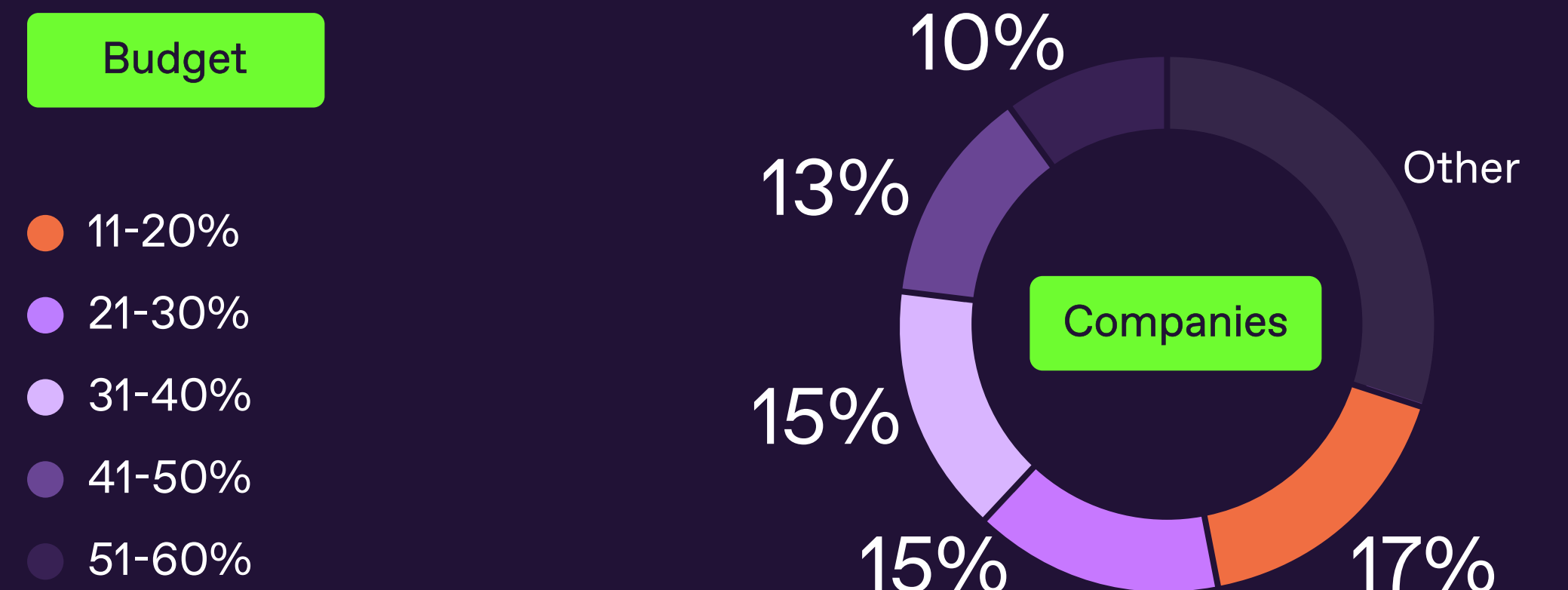
Today, the way businesses verify customer identities represents more than a mere process. It reflects how easy the business is to work with (initial as well as on-going engagement, e.g., onboarding, high-value transactions, and support). Lack of these capabilities puts organizations at a competitive disadvantage in the eyes of customers.

Key considerations when  
choosing the right solution

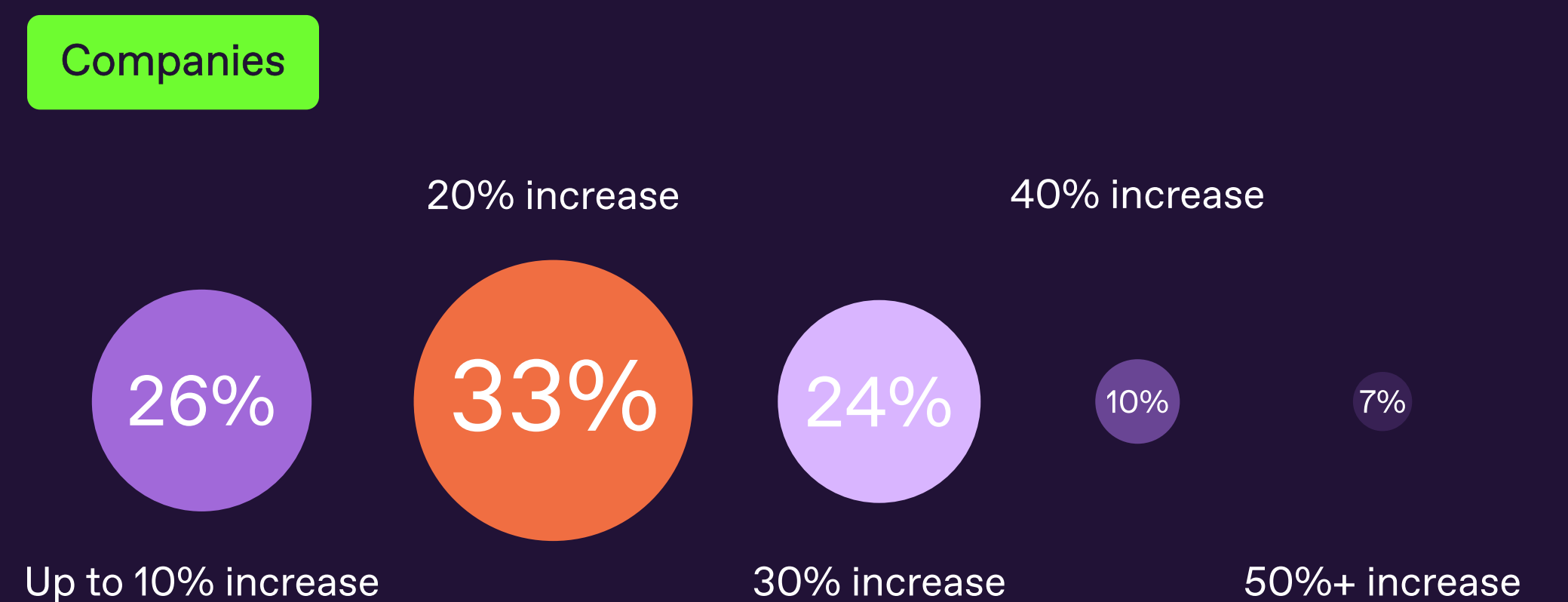


In terms of how much money is set aside for IDV solutions by enterprises, the most popular choice (18% of businesses) is to dedicate 11-20% of their IT budget annually, with 13% opting for 21-30%. This is similar for SMBs, as 17% also dedicate 11-20% of their annual IT budget to IDV solutions, and 16% dedicate 21-30%. Looking forward, 91% of all businesses plan to increase their investment in identity verification solutions. As seen in this report, there is a variety of compelling internal and external reasons for them to do so. Yet there are several important factors to consider before implementing them.

## Share of annual IT budgets allocated towards IDV solutions



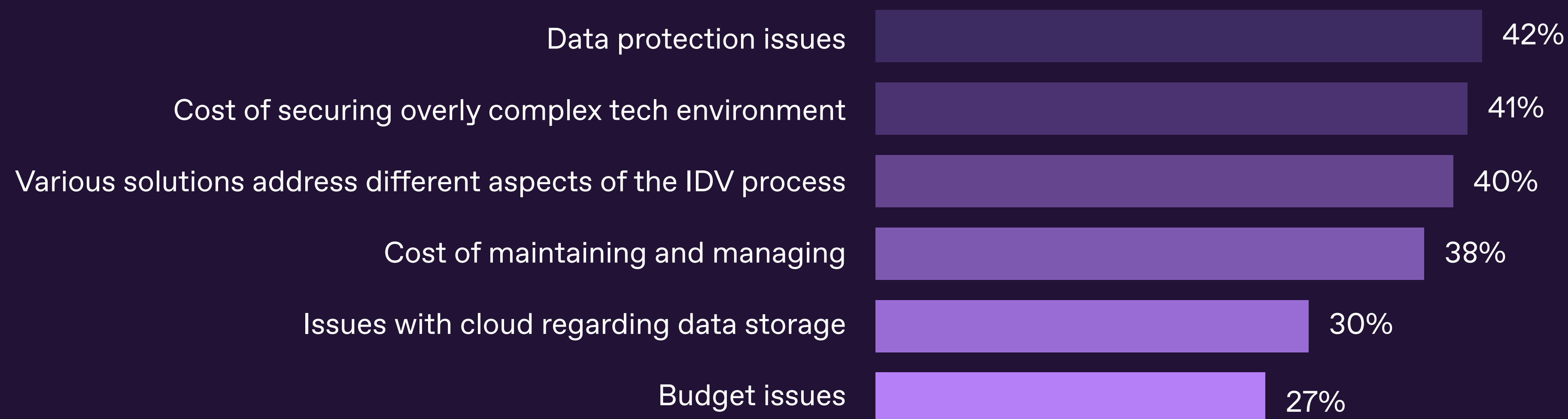
## Planned increase in IDV spending for organizations over the next 1-3 years







## The main constraints organizations encounter when deploying IDV



Despite the prevalence of cloud-based operations in today's business landscape, many businesses still find on-premise solutions—self-hosted along with private cloud options—to be highly attractive for IDV. Globally, there's an even split between businesses that have a preference for on-premise deployments of identity verification solutions (47%), and those that prefer SaaS, cloud-based solutions (47%). It is, however, important to note that this does vary between regions. For instance, in Germany, only 34% of businesses have a preference for on-premise deployments. Meanwhile in Turkey, 63% of businesses prefer this model.

Businesses primarily see security risks associated with cloud-based identity verification, but are also concerned about network outages and the security of personal data. Of course, these concerns also vary by industry. For instance, FinTech businesses see privacy and personal data protections as the primary risks associated with cloud-based identity verification.

# How do businesses measure success?

When assessing any kind of solution, decision-makers need to consider what success would look like from a business value perspective.

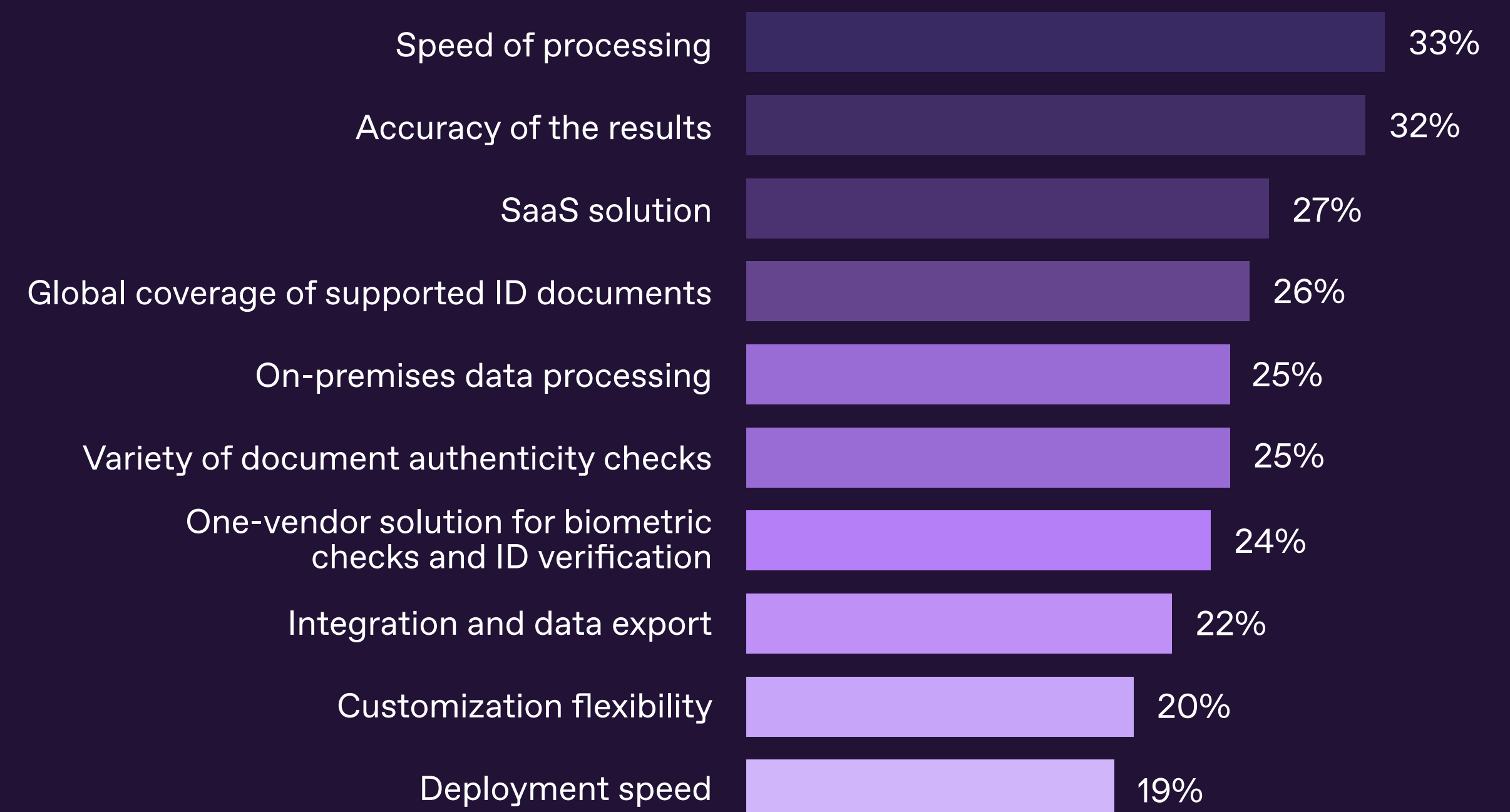
Globally, 50% of leaders believe the key metric for success would be the number of fraud attempts successfully prevented. And for good reason—at the very least, an identity verification solution should be making the business more efficient in its approach to tackling fraud. And yet, according to this research, most businesses actually prioritize the customer experience when it comes to assessing these kinds of solutions.

More than half of leaders (55%) around the world believe an improved customer experience—through faster and simpler on-boarding and registration processes—is the key determinant of success for identity verification solutions. In the US, as many as 64% of leaders prioritize improving the customer experience. Similarly, most leaders in FinTech (57%) and Banking (61%) are focused on using these solutions to improve the quality of their customer experience.

Indeed, even when it comes to choosing more specific solutions such as document verification, “speed of processing” was voted the most important factor, followed by “accuracy of results.” In the US, the most important consideration for document verification solutions is the variety of authenticity checks they offer. Meanwhile, in global hubs like the UAE, the most important consideration is the global coverage of supported ID documents.

In all these cases, what’s clear is that the priority for businesses is to improve customer experiences. And fast, simple identity verification solutions that can efficiently and successfully safeguard against fraud are critical to achieving that goal.

## Top 10 criteria when choosing a document verification solution





Conclusion

Identity verification takes  
center stage

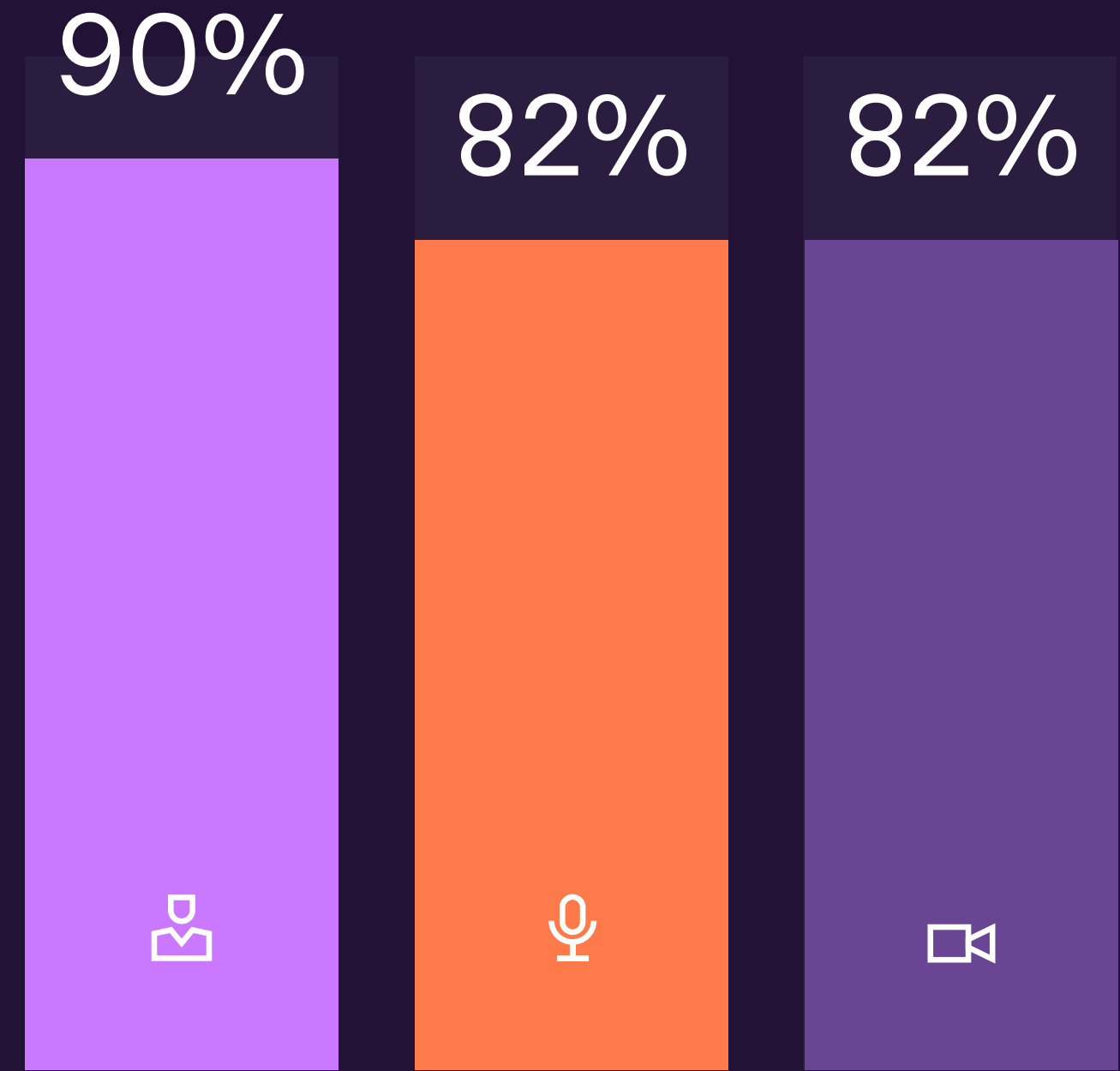
# Types of advanced identity fraud that are seen as a growing threat in the next couple of years




Businesses around the world are realizing they need to change the way they tackle fraud.

For some, the pressure is coming from the market: customers who simply won't tolerate older, more manual verification processes, and competitors who are moving quicker to deliver experiences that match modern customer expectations. For others, the pressure is coming from within the business itself. Under pressure to grow, businesses scale the volume of their customer base without first simplifying their verification processes. The result is a tangled web of complex manual processes.

In either case, leaders around the world are acutely aware of the many pressures they face to modernize. But just as technology holds so much promise for businesses that are trying to protect themselves and their customers, it's vital to remember that it also holds a lot of promise for cybercriminals. This is why it's imperative that businesses evolve their approach to identity verification, for the sake of their market, their efficiency, and their security.

We hope the data and context provided in this research report help you determine the appropriate solution for your business.



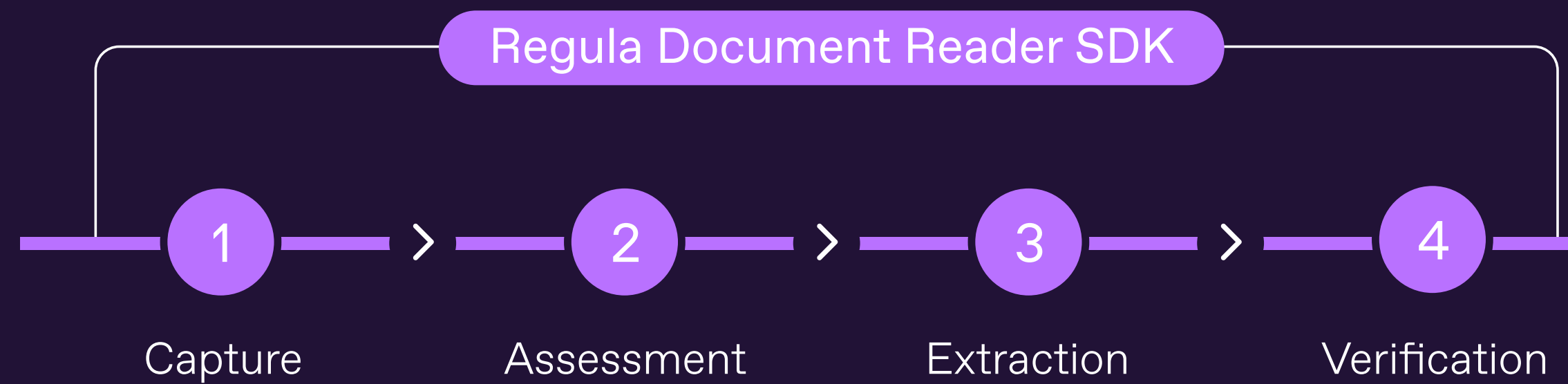
-  Synthetic identity fraud
-  Voice deepfakes
-  Video deepfakes



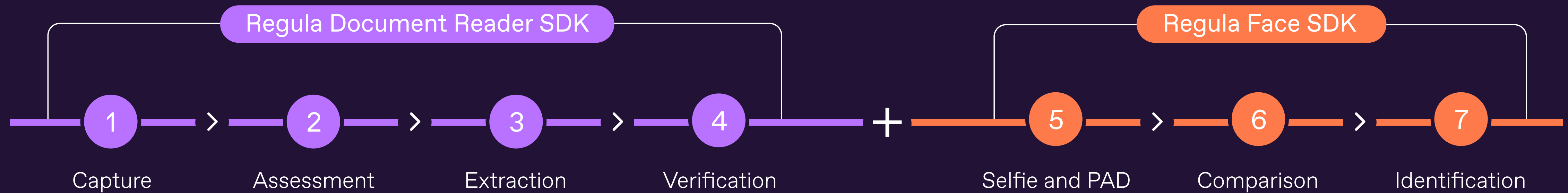
Recommendations for businesses

Regula's comprehensive  
solutions for streamlined  
identity verification

## Identity Document Verification



## Biometric Verification



Regula's solutions cover the entire identity proofing flow, including document and biometric verification. This allows for a seamless, single-vendor identity verification process that can be completed in just a few seconds.

By streamlining the whole procedure, Regula's solutions make verifying individuals' identities easier and more efficient, while improving the overall customer experience and ensuring security and compliance.





# Regula Document Reader SDK

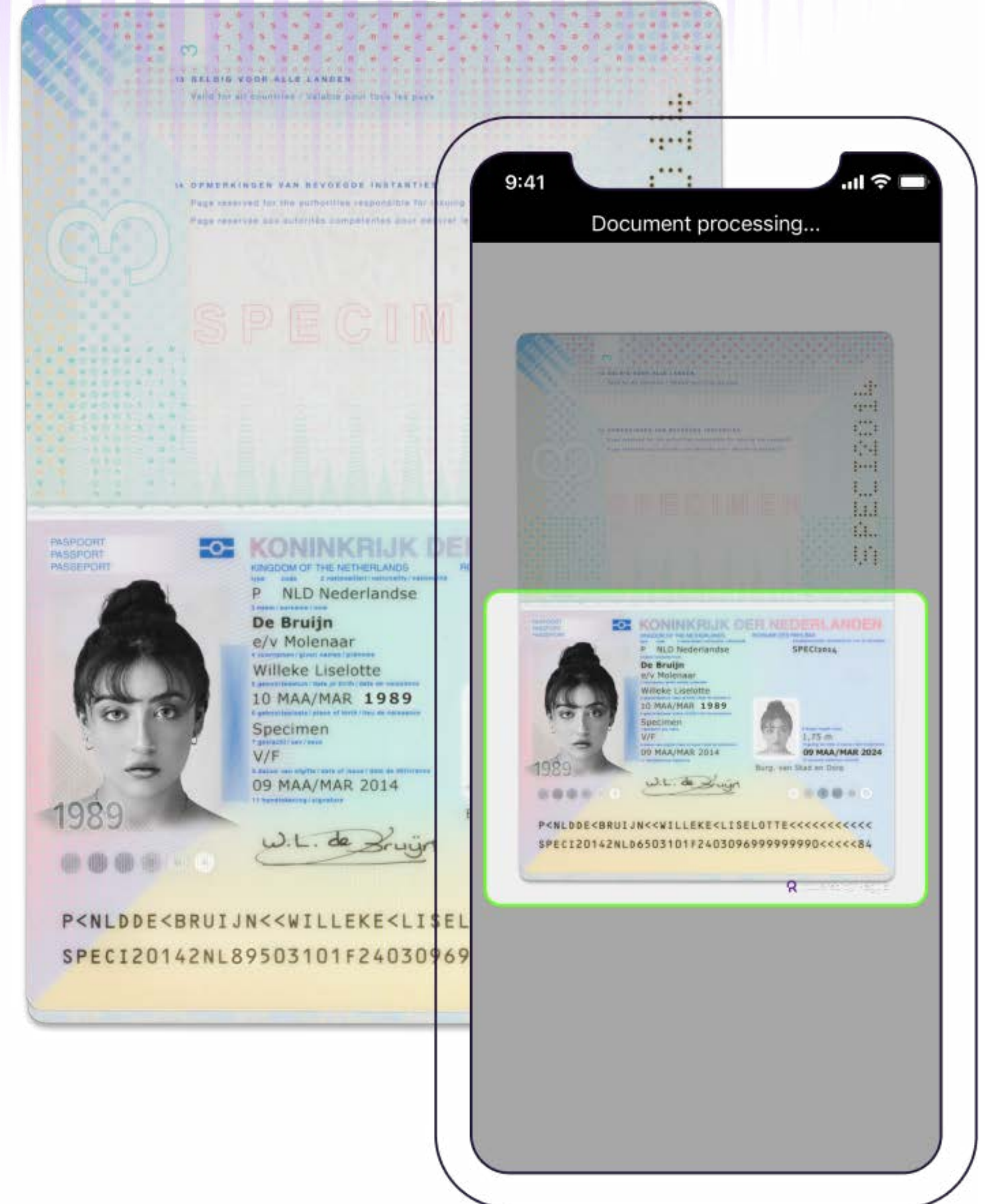
Regula Document Reader SDK completely covers the identity document verification process and effectively prevents fraud. It accelerates customer onboarding via seamless and secure identity verification that relies on more than 12,000 identity document templates from 247 countries and territories.

Regula's solution fully automates reading and verification of personal data in passports, ID cards, driver's licenses, visas, and other identity documents.

The solution instantly performs a large variety of cross-checks to prove the document is authentic. It cross-validates and verifies data from:

- the visual zone;
- the MRZ (incl. size and format);
- the barcode (incl. size and format);
- the RFID chip.

It also checks whether a photo has been changed or replaced. And much more.







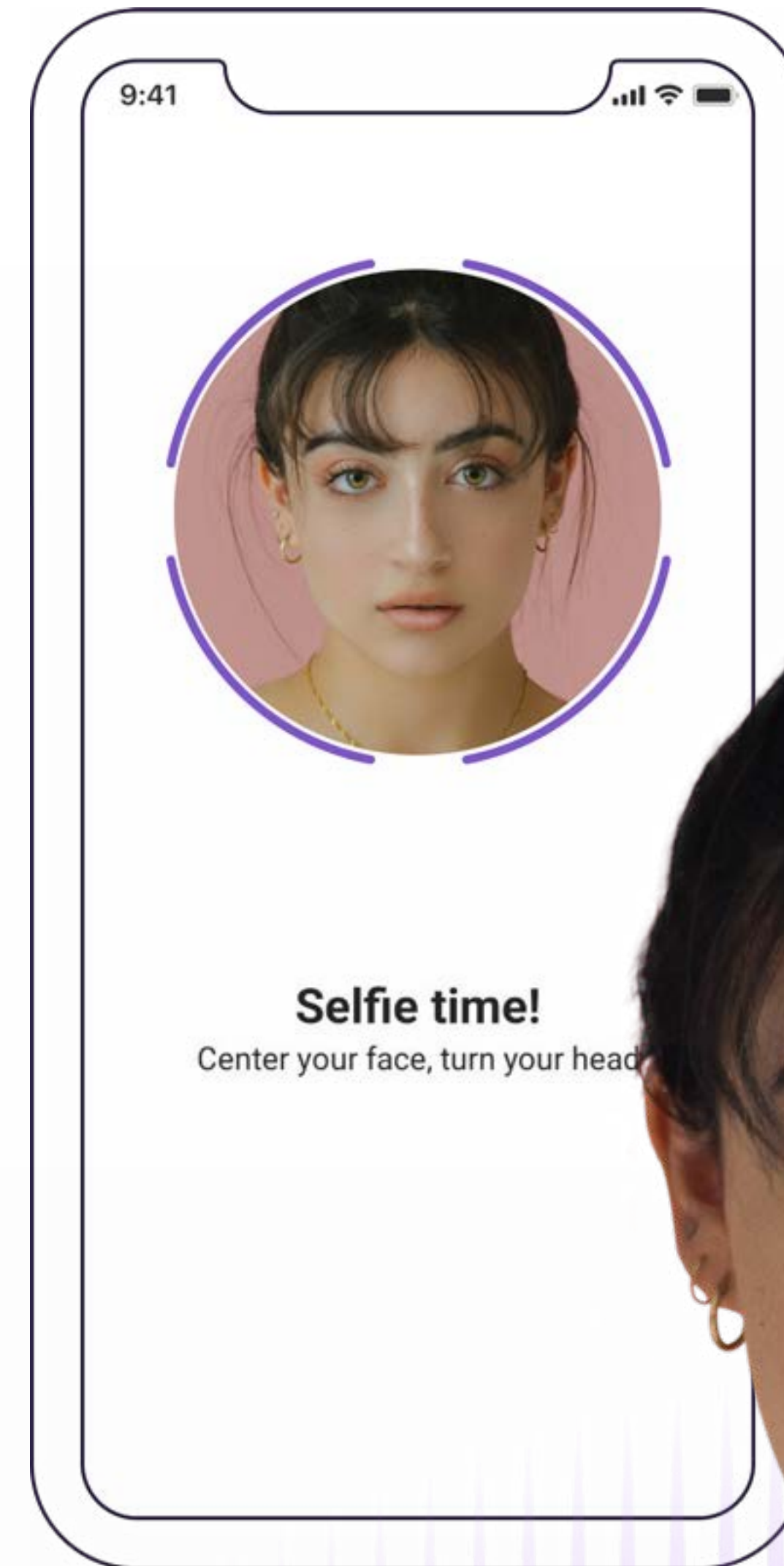
# Regula Face SDK

Regula Face SDK enables convenient and reliable biometric checks. It delivers an additional layer of security for the identity verification process, thanks to fast and accurate technologies such as:

- Face detection
- Liveness detection
- Face matching
- Face identification
- Face attribute evaluation
- Face image quality assessment

Paired with Regula Document Reader SDK, Regula Face SDK verifies a selfie against a photo from an ID matching the printed portrait, the RFID chip photo, a selfie uploaded via web or mobile device, and a portrait from an external database to ensure the person is the same in all the different photos.

Regardless of the device, it effectively verifies identity and detects fraudsters.



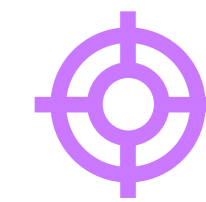


Stay one step ahead of fraudsters who use fake identities to pretend to be legitimate customers. Regula detects fraud before it happens, whatever industry you operate in: Banking, FinTech, Travel, Aviation, Telecom, Education, and others.



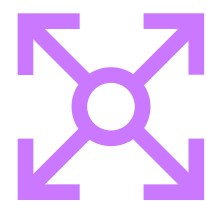
### Stop fraud from the get-go

With Regula, you can be sure you acquire real customers and block fraudsters before they manage to access your service. A combination of advanced document verification and biometric data checks effectively safeguards your business, profit, and reputation.



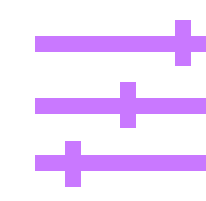
### Detect even sophisticated fakes

Regula leverages AI algorithms to analyze the whole page of a document and detect any mismatches in data from the visual zone, MRZ, RFID chips, barcodes, and holograms. Thanks to these cross-checks, you get the most effective identity verification tool available for businesses.



### Enlarge your coverage

Accept customers from anywhere in the world with the help of the world's largest document template database. Grow your revenue and business with market-proven identity verification solutions, no matter the volume or origin of the identity documents.



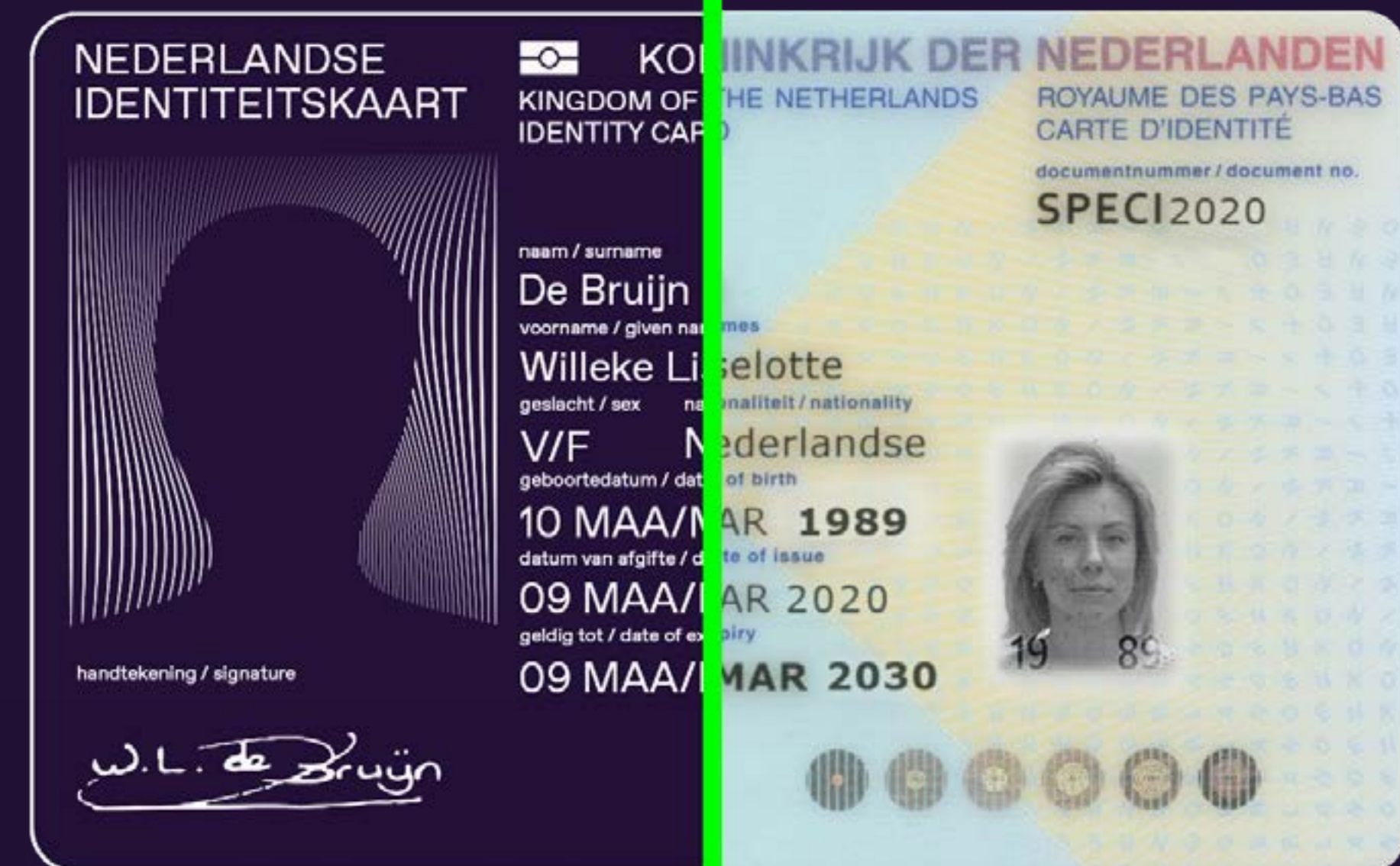
### Ensure seamless UX and instant verification

Make document verification simple, fast and secure, streamlining user authentication for both users and businesses. Personalize and customize the customer journey by organizing an ID verification process on any platform: mobile, web, or passport readers.

# About this research

This report is based on primary research conducted to help decision-makers understand how businesses around the world are working with identity verification. The research was conducted by Sapio Research and surveyed 1,069 decision-makers in the Banking, FinTech, Technology, Telecoms, and Aviation sectors.

The respondents to this survey represent businesses in the UK, the US, Germany, Australia, Mexico, Turkey, the UAE, and France. By analyzing the latest trends and practices in the identity verification landscape, this report aims to provide decision-makers with a clear understanding of the best practices and tools to implement robust identity verification measures. The goal is to enable decision-makers to allocate their resources effectively and efficiently based on sound data and evidence, and ultimately make better-informed decisions to protect their businesses and customers from identity fraud.





# About Regula

With our 30+ years of experience in forensic research and the largest library of document templates in the world, we create breakthrough technologies in document and biometric verification. Our hardware and software solutions allow over 1,000 organizations and 80 border control authorities globally to provide top-notch client service without compromising safety, security or speed.

Regula was named a Representative Vendor in the Gartner® Market Guide for Identity Proofing and Affirmation in 2022.

➤ Contact us: [pr@regulaforensics.com](mailto:pr@regulaforensics.com)  
Learn more at [regulaforensics.com](https://regulaforensics.com)