onfido
an Entrust Company

End-user expectations of digital identity

Onboarding dos and don’ts

Introduction

We've reached an age of digital cohesion. Today's end-users are digitally-minded with 81% online daily. And businesses are meeting them online. Businesses have broadly adopted digital processes that allow customers to access services online, whenever and wherever they need.

Digital identity verification has enabled widespread digital access to all kinds of services. The technology has come a long way in recent years. Today, users can open an account online via an app on their smartphone by proving their identity in seconds. All by taking a photo of their ID and snapping a selfie. This technology not only offers a fast, digital-first experience for users but also has built-in fraud detection. The result? Fraud prevention and compliance no longer have to compromise UX.

However, different countries have adopted digital identity verification processes at different paces. And local regulations reflect this — the exact requirements for different regions vary. While this is starting to change (especially in Europe with the introduction of eIDAS 2.0 and ETSI technical standards), in reality, we're still seeing some patchworked approaches to verification at onboarding.

This means end-user experiences can be wildly varied. What is normal for some, is not for others. While some onboarding processes set the gold standard, others fall behind, leaving users confused and frustrated. For businesses, they're fighting a battle on two fronts. User expectations define what you should and shouldn't do, while compliance defines what you can and can't do. But it's not all negative. Sometimes striking the balance between what you 'should do' and what you 'can do' might be easier than businesses think.

About this report

In this report, we'll dive into what businesses should and shouldn't do from a UX perspective, according to their end users. We asked 6,000 respondents* how they feel about onboarding and digital identity verification processes, to give businesses a better insight into their users' expectations. Spoiler: with the right approach, UX and compliance can work in harmony.

*1. 6,000 respondents based in US, Canada, UK, France, Italy and Spain. Respondents were equally weighted based on geo and age.

01 Digital access

How online are end-users?

From Boomers to Gen Z, 81% of end-users are online daily

We've reached a new era of digital transformation. With 81% of users accessing services online daily, businesses have broadly adopted digital solutions to meet end-user needs.

Why? For the first time in history, online services are now embraced across multiple industries, geographies, and most importantly, generations. 76% of those aged 55 and older are now online daily.

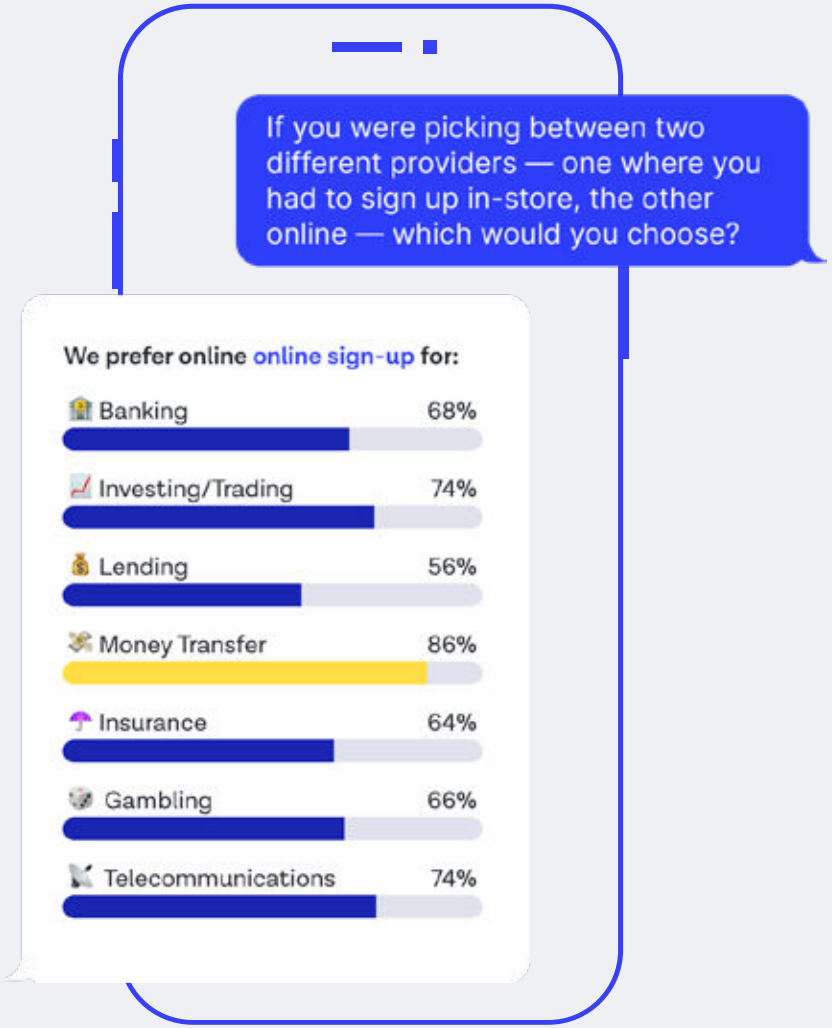
From Boomers to Generation Z, we're fast approaching digital saturation. This trend is only going to continue as tech-savvy and digital-first generations such as millennials begin to age.

	Total	UK	USA	France	Italy	Spain	Canada	18-24	25-34	35-44	45-44	55+
Daily	81%	85%	82%	72%	86%	81%	79%	78%	83%	85%	81%	76%
Weekly	15%	12%	13%	22%	11%	14%	16%	17%	13%	12%	15%	16%
Monthly	4%	3%	4%	5%	3%	4%	5%	4%	3%	3%	3%	6%
Yearly	1%	0%	1%	2%	1%	1%	1%	1%	1%	1%	0%	2%

In-store no more: 8 in 10 users satisfied with digital-first

Any business that hasn't done so already can confidently make the shift to digital, knowing that it meets their users' expectations. 8 in 10 users would be satisfied with fully digital services.

On the whole, users will choose digital-first over in-store services for all of the services shown on the right. The data suggests they are more likely to choose a digital-first option for things like opening a bank account, managing investments or making a money transfer, likely because convenience and speed are a priority. Whereas services that might involve more considered decisions or financial advice, such as lending and mortgages, users are more inclined to want an in-store element in addition to online services.



	UK	USA	France	Italy	Spain	Canada	18-24	25-34	35-44	45-44	55+
In-store	23%	33%	33%	32%	40%	28%	31%	30%	28%	30%	40%
Online	77%	67%	67%	67%	60%	72%	69%	70%	72%	70%	60%

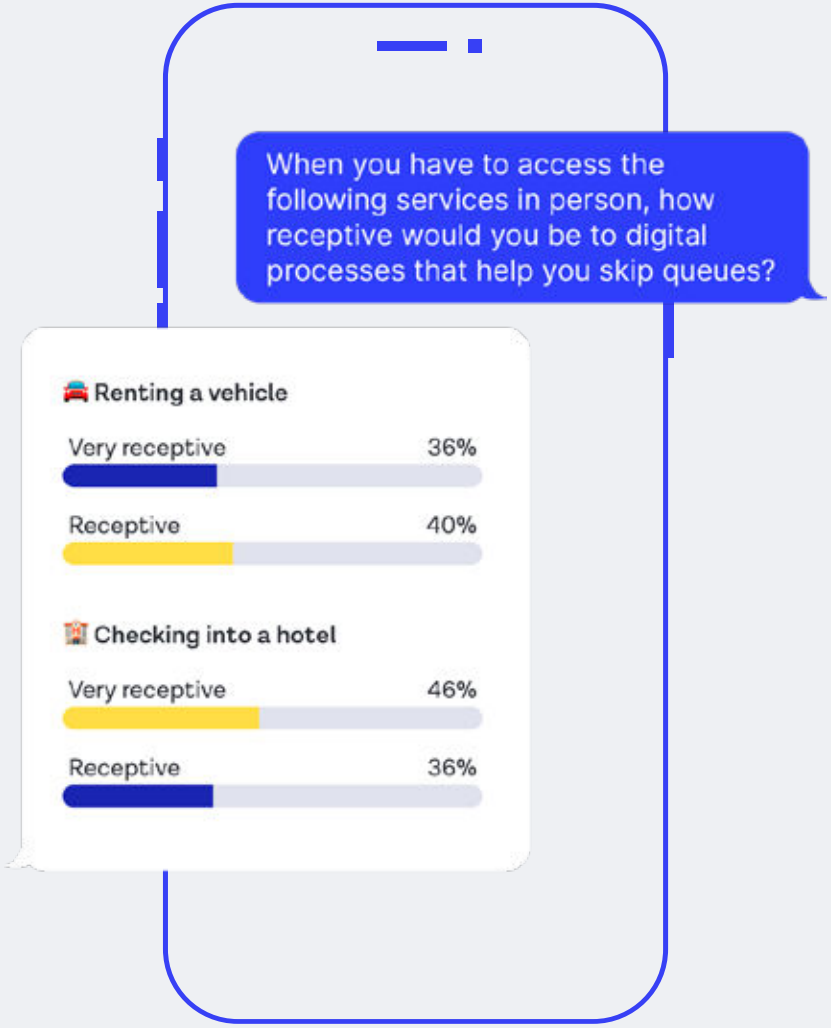
8 in 10 users embrace digital processes to speed up in-person services

On average, around 8 in 10 users would opt for digital processes that help speed up in-person services, such as renting a vehicle (76%) or checking into a hotel (82%).

End-users are notoriously friction averse. This applies not only to digital processes but also in person. For services that involve in-person experiences, nothing is more high friction than long, slow-moving queues.

In these scenarios, users are highly receptive to digital solutions that help them skip those queues. There are already many real-world examples of this. For example, validating identity documents online before picking up a vehicle rental, or checking into a hotel. Or using their biometrics to bypass long airport check-in lines.

For businesses that offer in-person services, introducing digital processes to help ease moments of friction will boost user satisfaction.

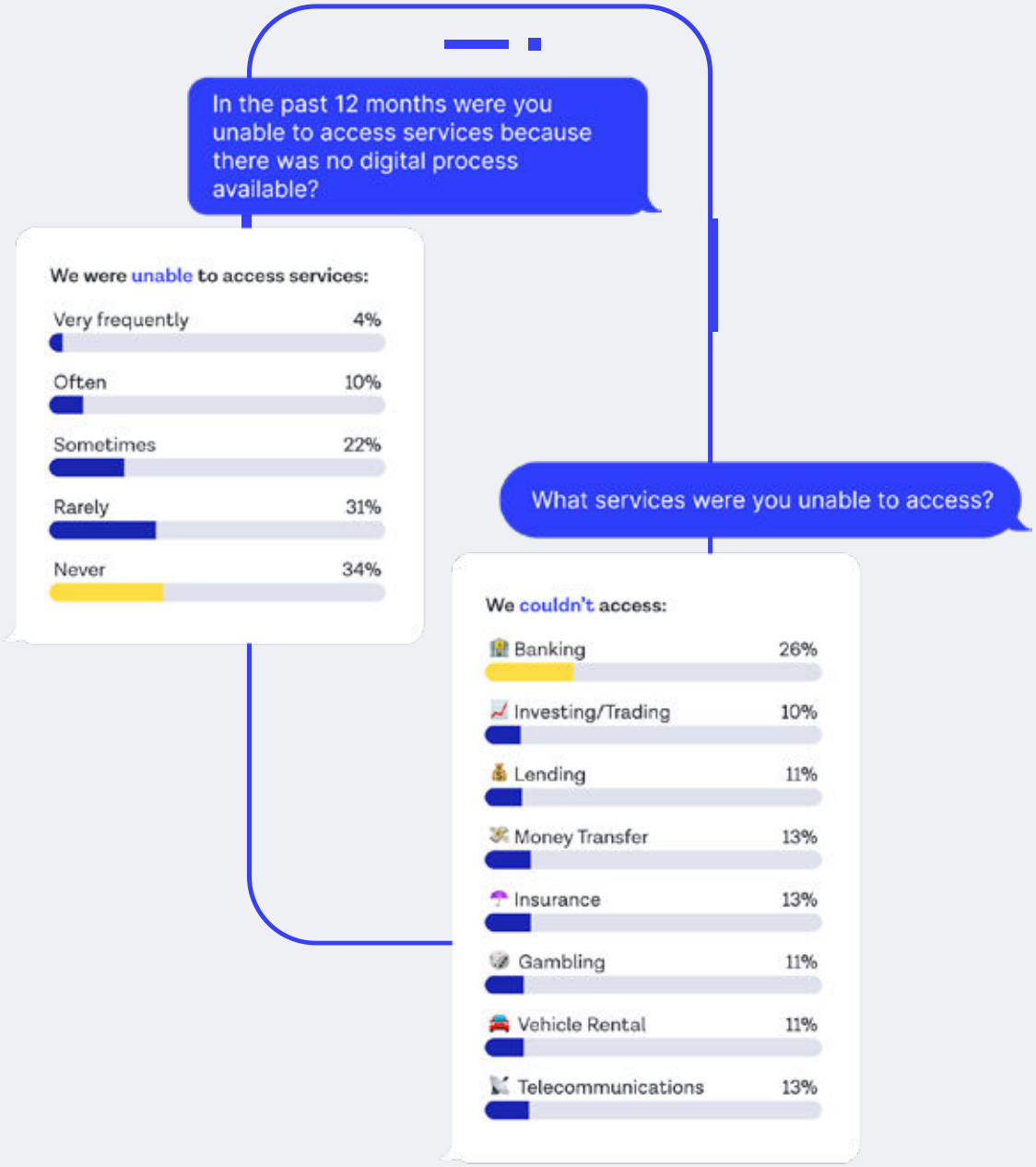


Post-pandemic progress: businesses halve digital access barriers since 2021

Businesses have significantly improved their digital infrastructure following the COVID-19 pandemic.

During the COVID-19 pandemic, physical restrictions forced many businesses to implement digital processes. This fast adoption left some kinks in the process. Today, most businesses appear to have ironed out these kinks, ensuring services are supported by robust digital processes.

Our 2021 research found that 70% of end-users were unable to access services because of a lack of digital processes either sometimes, often or frequently. In 2023, that number has halved. Only 36% of end-users reported being unable to access services because of a lack of digital processes sometimes, often or frequently. The remainder found that this happened rarely, with the majority (34%) finding that this never happens. For users who were unable to access services, they found it mostly applied to banking.



Uneven progress: some countries lag in improving digital access

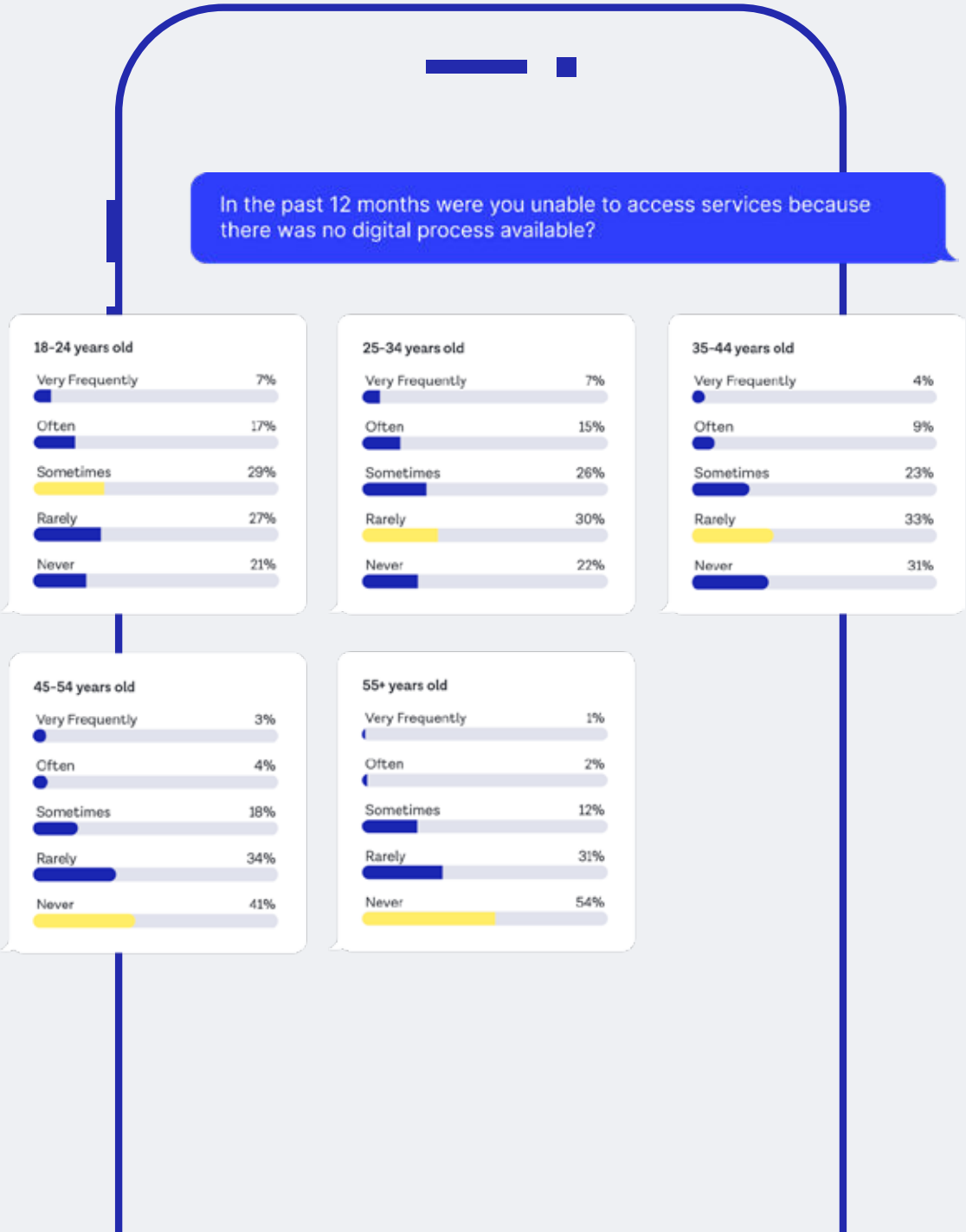
While businesses in general have come a long way in improving digital access, some countries have a higher proportion of people with difficulty accessing digital services.

49% of users in Italy reported being unable to access services because of a lack of digital processes.

Younger generations experience a lack of digital access more frequently

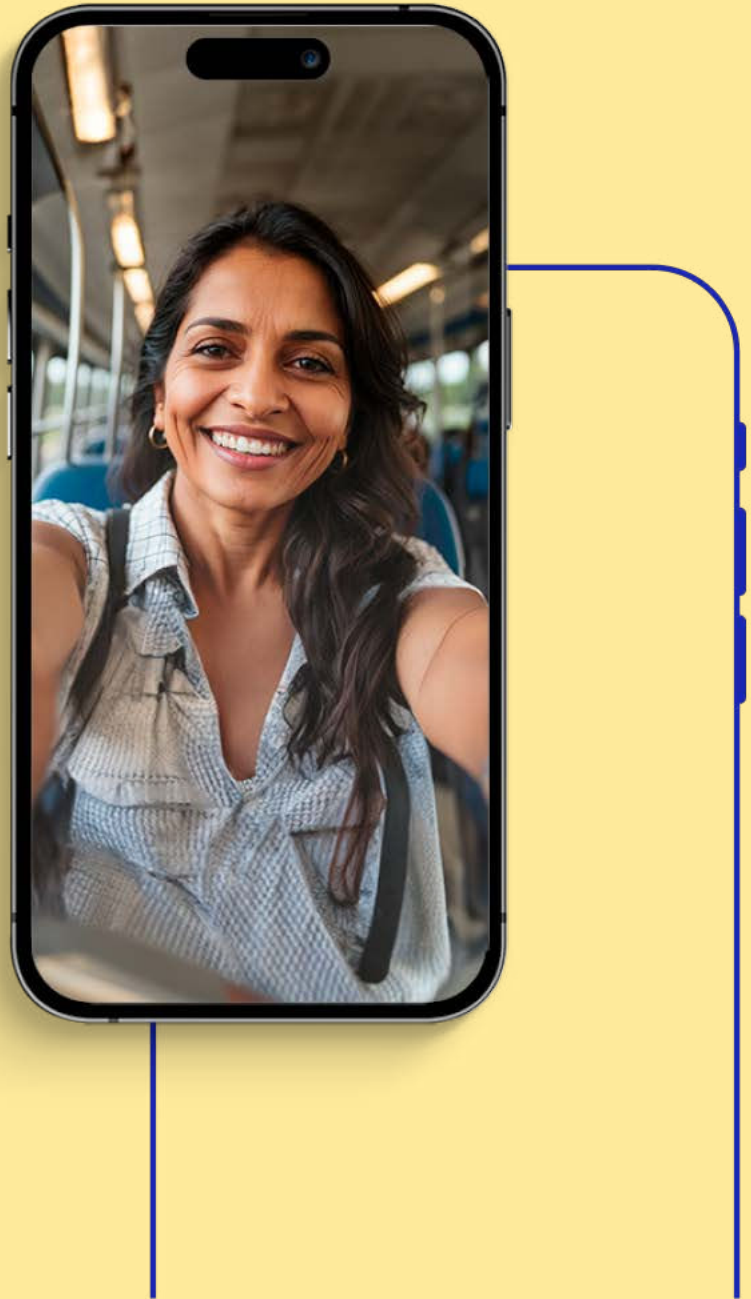
Interestingly younger generations are more likely to find they were unable to access services due to a lack of digital processes.

Whereas older generations more likely found they were never unable to access services. This could be because older generations are less reliant on digital processes than younger generations, or that younger generations are more demanding of digital processes with higher expectations, or a combination of both.



02 Account creation

What does user behavior reveal about onboarding experiences?



The app advantage: users embrace mobile apps for account creation

The new era of digital access is here, and it's no longer enough for businesses to simply have an online presence.

When we talk about being digital-first in today's environment, that means integrating digital processes into every customer channel, as well as finding new ways to reach those digital customers. At the same time, linking these digital channels to make customer journeys as seamless as possible.

This is true when it comes to setting up new accounts. Today's users are equally split between setting up new accounts via an app (40%) and setting up an account online (40%). Industries like banking, investment/trading, and gambling are leading the way when it comes to app usage. The seamless experiences customers now expect from banking apps, for example, is likely to have a knock-on effect across the rest of the financial services space and beyond. Users are going to want increasingly app-centric experiences from less digitally mature industries — such as lending and insurance — in the future.

	Banking	Investing	Lending	Money Transfer	Insurance	Gambling	Vehicle Rental	Telco
In-branch	21%	8%	18%	8%	22%	8%	13%	19%
I don't recall	2%	3%	5%	3%	5%	4%	7%	6%

1 in 2 users now experience digital identity verification

Ten years ago, digital identity verification methods such as document and biometric verification (using your phone or computer to send a photo of your ID and a selfie) were infrequent.

For the most part, they were adopted by digital-first innovators such as neo-banks or other fintechs. Today, document and biometric verification is the standard method when verifying identity for account creation. 1 in 2 end users experienced it in the last year, and it has overtaken credit checks to become the number one method for verifying identity.

However, despite the widespread adoption of document and biometric verification, many users are still experiencing outdated, high-frction, insecure methods of verification such as credit checks (48%) and in-person verifiation (37%). This is at odds with customers' expectations, given that 8 in 10 users would be satisfied with fully digital services (see page 5).

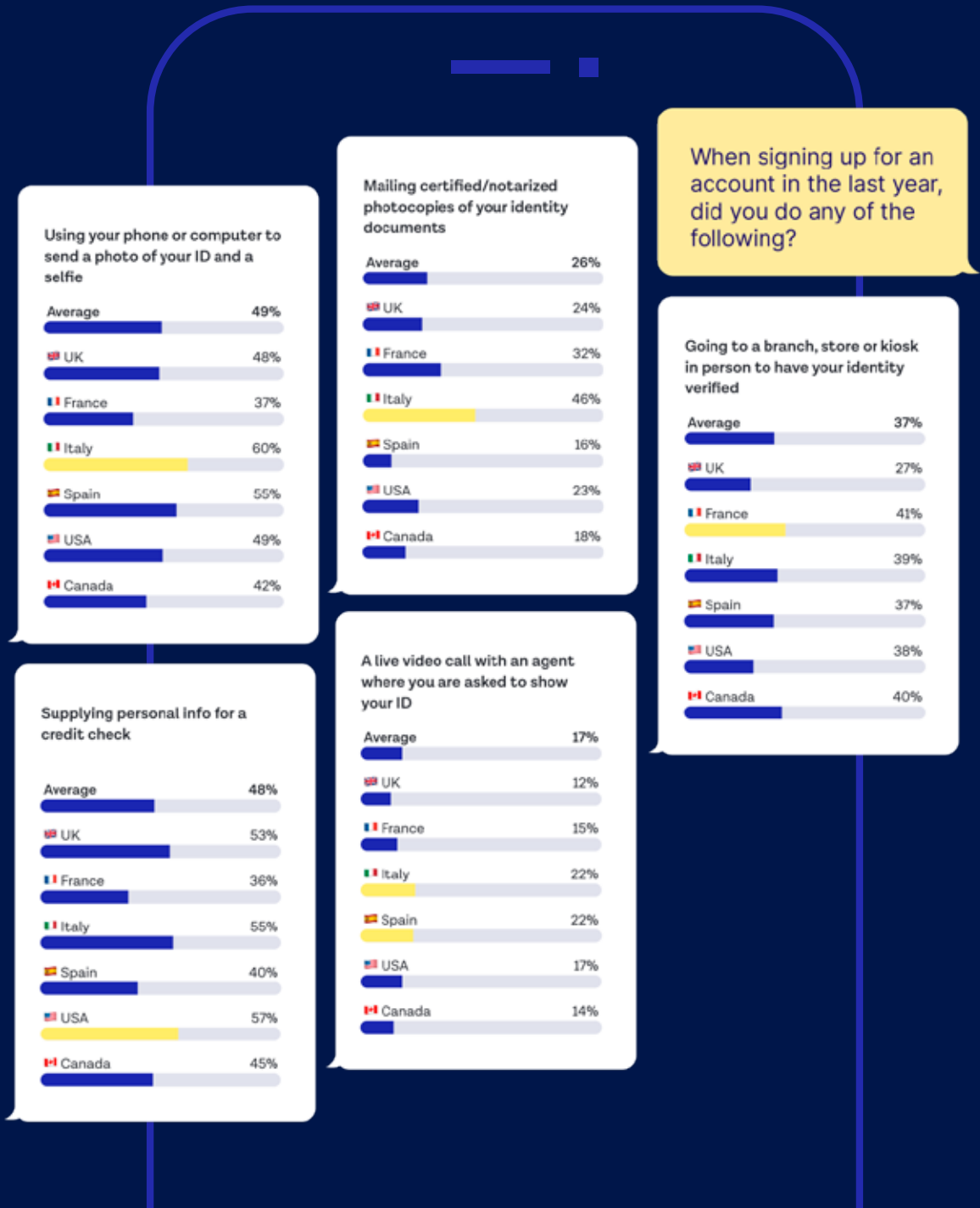
Lack of global standardization fuels patchworked IDV processes

But while document and biometric verification has broadly emerged as the predominant method of IDV, it's been adopted at different paces in different geographies.

Differing regulations and the lack of a globally acknowledged standard has resulted in a patchworked, fragmented approach to verifying customer identity. While steps are being made towards harmonization, right now, there isn't going to be a one-size-fits-all approach for every user.

This presents a challenge for business. Especially those with ambitious expansion plans. On the one hand, they could just rely on one onboarding experience and risk losing customers. Or, they could try and meet customers on their terms by using different onboarding approaches for different audiences.

Expansion-minded businesses may need to rely on multiple methods of identity verification for different customers in different geographies. Both from a regulatory standpoint and to meet user's expectations. This highlights the need for easily orchestrated, flexible customer journeys.



Onboarding realities by geo

US

57% of users in the US experienced a credit check when signing up for an account in the last year. US businesses rely on credit checks more than any other method to verify customer identities.

While credit checks are a necessary background check, and can bolster other forms of verification, relying on them alone leaves both users and businesses vulnerable, in the form of synthetic or SSN (Social Security number) fraud.

UK

Only 27% of users in the UK were asked to verify their identity in person in the last year. This is lower than any other country surveyed. The UK has been a big adopter of new identity verification technologies.

Users in this country are very used to using their phones to capture photos of their ID and their face as a form of verification. Businesses have adopted this (often combined with credit checks) as the predominant method of identity verification.

France

France has been slower to adopt identity verification technology compared to other countries.

Why? Historically, the compliance regulations in France have leaned towards in-person forms of verification (even if some portion of it is possible to do online). ‘Tabacs’ (local tobacconist shops) have been a long-standing part of identity verification processes in France, where users can have their identity verified in person. This is most likely why 41% of users in France experienced in-person identity verification in the last year. But this is changing, especially with the introduction of ANSSI.

Local regulations like ANSSI place more emphasis on video verification, in particular for users opening a bank account. While EU-focused regulations are placing more of an emphasis on document plus biometric verification combined with QES. Businesses should consider their priorities in terms of user experience when it comes to onboarding users in France.

Italy

In Italy, there is a high proportion of users who experience all methods of identity verification compared to other countries.

This is likely going to create a state of confusion for users. If different businesses are all adopting different types of identity verification, users are never going to know what to expect when they sign up for a new account. One business might ask users to capture photos of their ID and their face, another might use a credit check, another might ask for in-person verification, and another for photocopies of an identity document.

This will put strain on end-users who are never going to know what to expect and might have to jump through multiple hoops, just to sign up for an account.

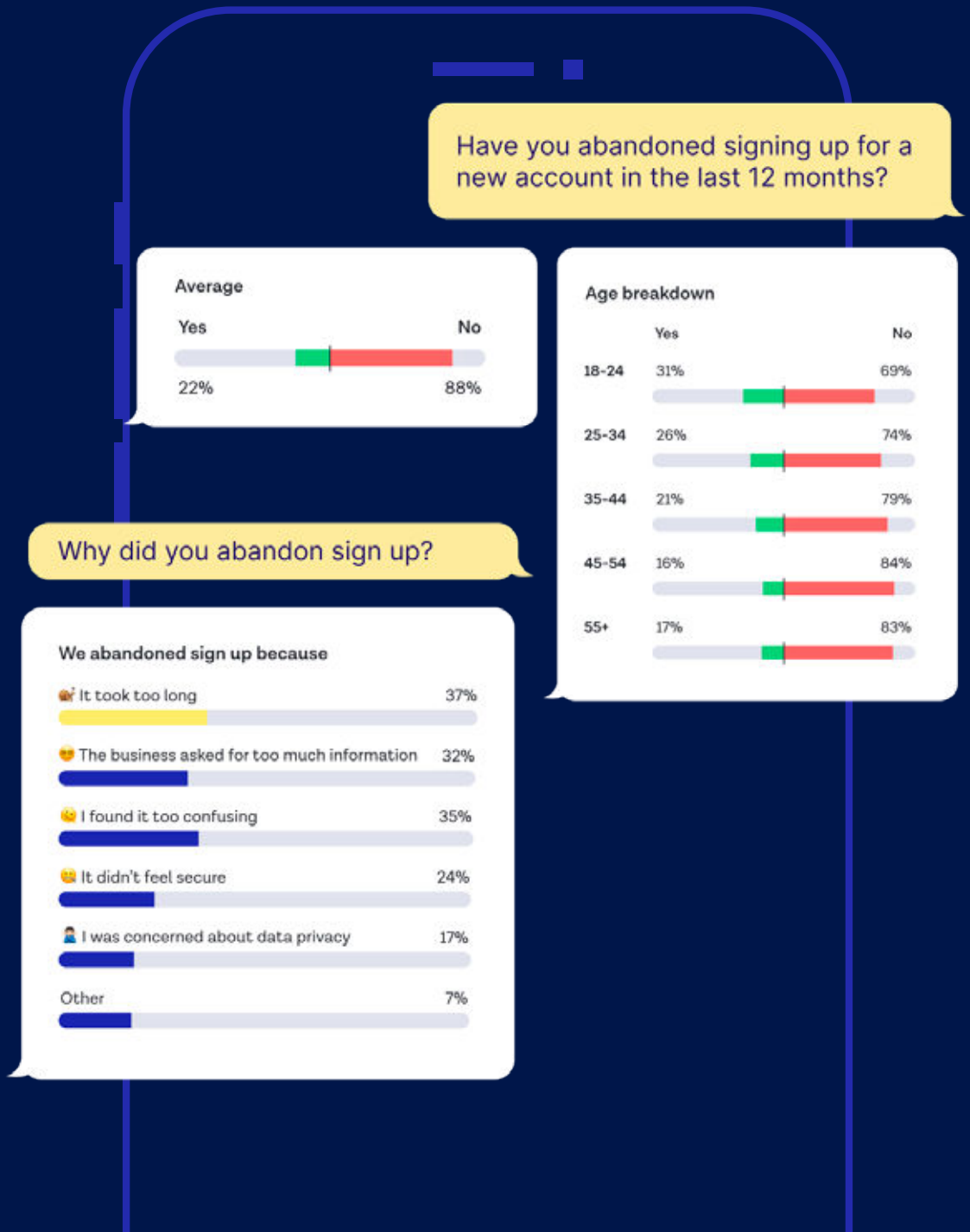
Sign-up struggles: 1 in 5 users abandon account creation

Roughly 1 in every 5 users abandoned signing up for a new account in the last year

In terms of potential business revenue, this amounts to a lot of missed opportunities. Despite high levels of adoption of digital processes, businesses still have room for improvement at onboarding to get more customers through the door.

Of users who abandoned, 37% did so because it took too long. 35% abandoned because it was too confusing.

Nowhere is this more true than for younger generations. The rate of abandonment rises to roughly 1 in 3 for younger generations. Gen Z and younger millennials are particularly sensitive to onboarding processes that take too long, or are too confusing.

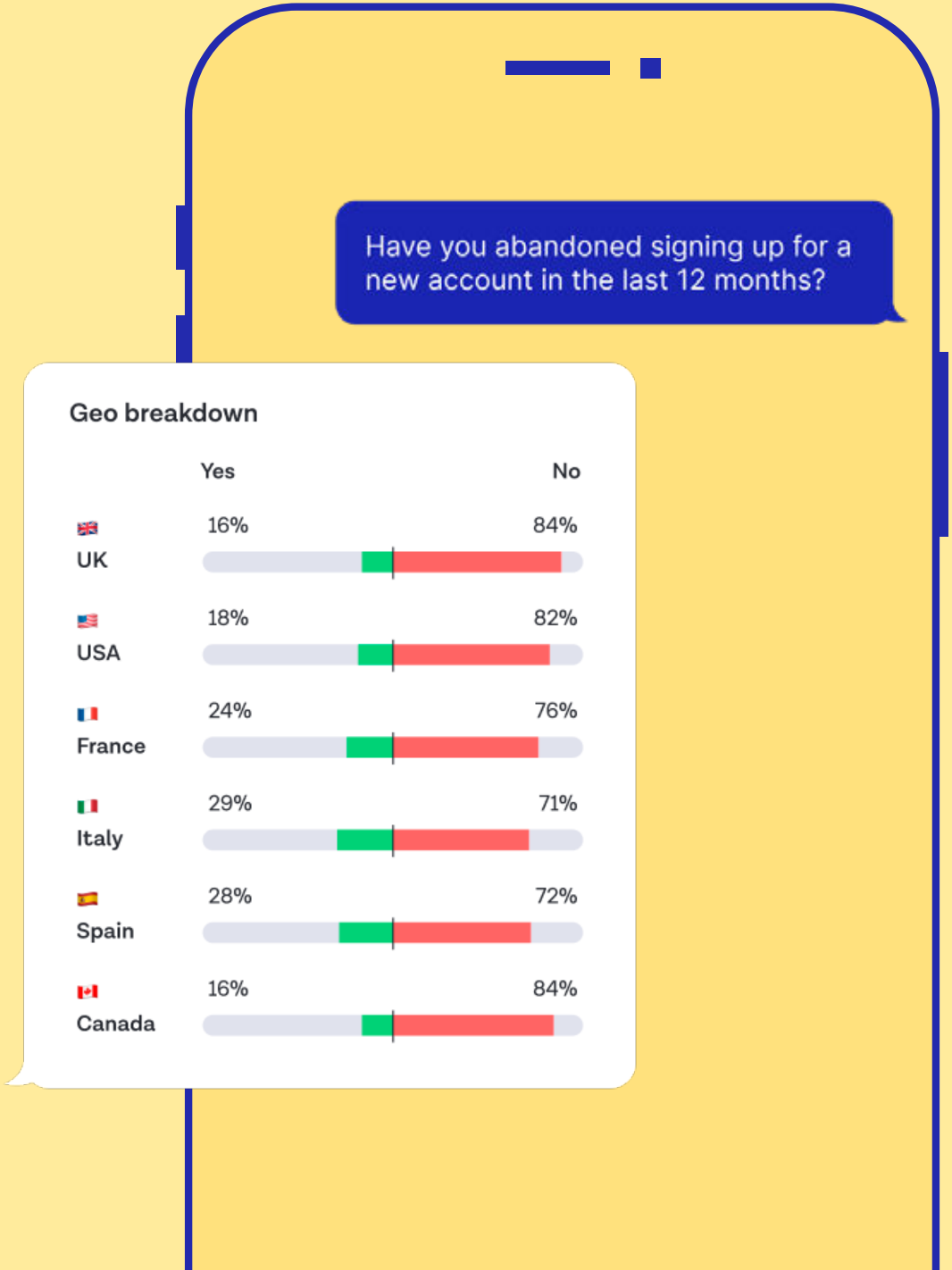


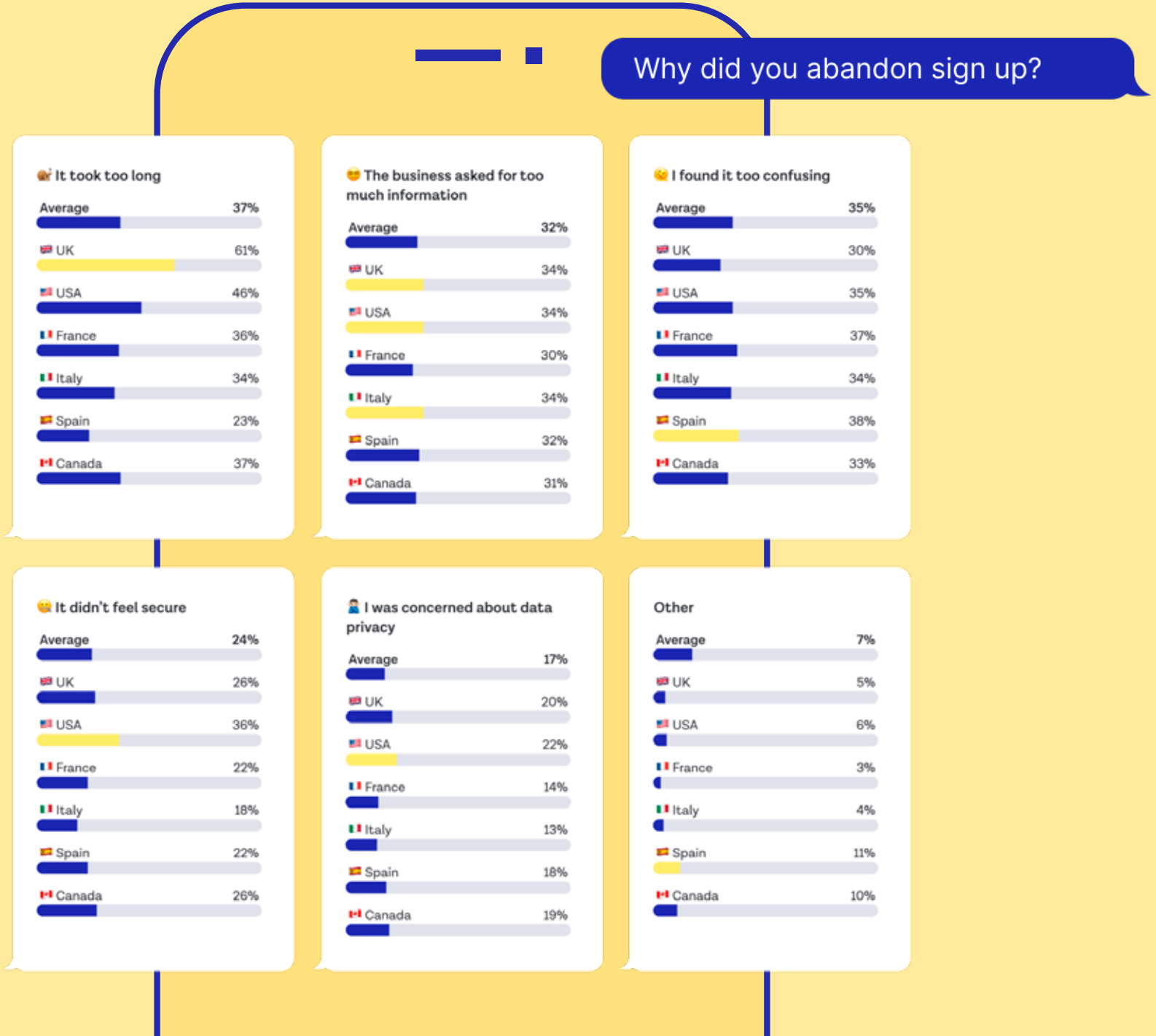
Fragmented IDV processes lead to higher abandonment rates

In countries where users experience many different types of verification at onboarding (see page 13), they are more likely to abandon when signing up for a new account.

This is true across France, Italy, and Spain, which saw higher-than-average rates of abandonment. Italy reported the highest rate of abandonment at 29% (~1 in every 3 customers).

Comparatively, in countries where there are more standardized forms of identity verification (such as in the UK where users predominantly experience document plus biometric checks, or credit checks), abandonment rates are lower.




Why did you abandon sign up?
It took too long
Average 37%
UK 61%
USA 46%
France 36%
Italy 34%
Spain 23%
Canada 37%
The business asked for too much information
Average 32%
UK 34%
USA 34%
France 30%
Italy 34%
Spain 32%
Canada 31%
I found it too confusing
Average 35%
UK 30%
USA 35%
France 37%
Italy 34%
Spain 38%
Canada 33%
It didn't feel secure
Average 24%
UK 26%
USA 36%
France 22%
Italy 18%
Spain 22%
Canada 26%
I was concerned about data privacy
Average 17%
UK 20%
USA 22%
France 14%
Italy 13%
Spain 18%
Canada 19%
Other
Average 7%
UK 5%
USA 6%
France 3%
Italy 4%
Spain 11%
Canada 10%

03 Fraud and security

What are users' key concerns during onboarding?

1 in 10 users was a victim of fraud in the last year

In the last year, 12% of users (roughly 1 in every 10) have fallen victim to fraud.

The US saw higher numbers of users that fell victim to fraud than any other country — 15% of US users were a victim of fraud in the last year. The US's overreliance on credit checks and personal information as a form of verification (57% of users experienced a credit check in the last year, page 13) means users are much more vulnerable to synthetic identity fraud.

At odds with traditional concepts of fraud, younger generations are nearly twice as likely to fall victim to fraud as those over the age of 55.

There could be a couple of reasons for this:

1. They are more comfortable online and openly share more personal information
2. They spend more time online and are more likely to encounter online scams
3. They are more invested in products like crypto, which are targets for fraudsters
4. They have less experience in recognizing the signs of fraud

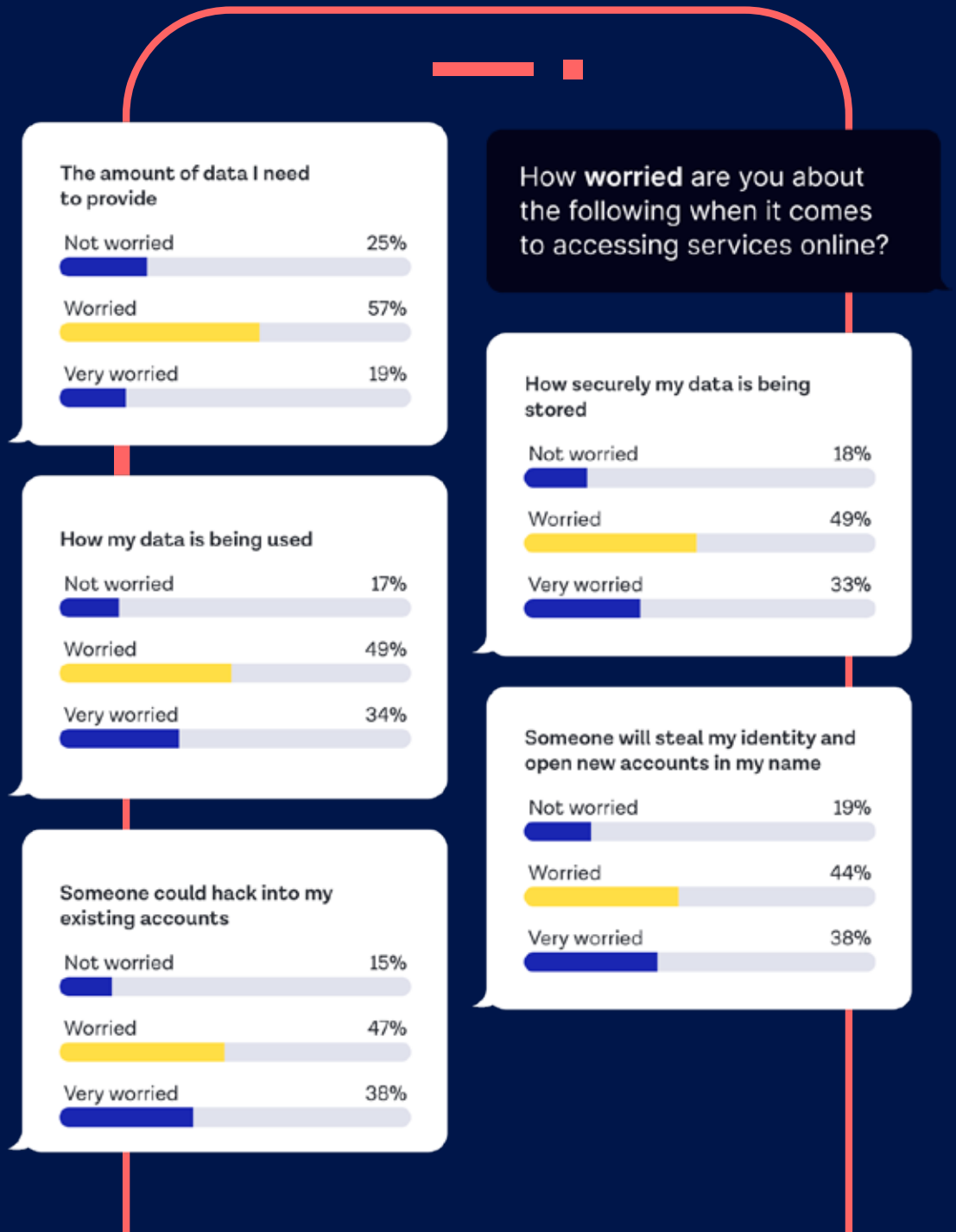
Digital insecurity: users concerned with data storage and hacking

Top user concerns include data storage and vulnerability to hacking.

85% worry that someone could hack into their accounts, 83% worry about how their data is used and 82% worry about how it's stored.

These concerns are intrinsically linked. If data isn't stored securely, it's easier for hackers to get hold of it. Plus, people hear about new cases of data breaches and hackings almost daily. There was a 20% increase in data breaches from 2022 to 2023.

Users appreciate transparency, so where possible, businesses should endeavor to communicate steps they are taking to make sure data is stored securely.



User's top concerns:

82%

of people worry about how their data is stored

85%

of people worry that someone could hack into their existing accounts

83%

of people worry about how their data is used

82%

of people worry that their identity will be stolen and used to open accounts in their name

76%

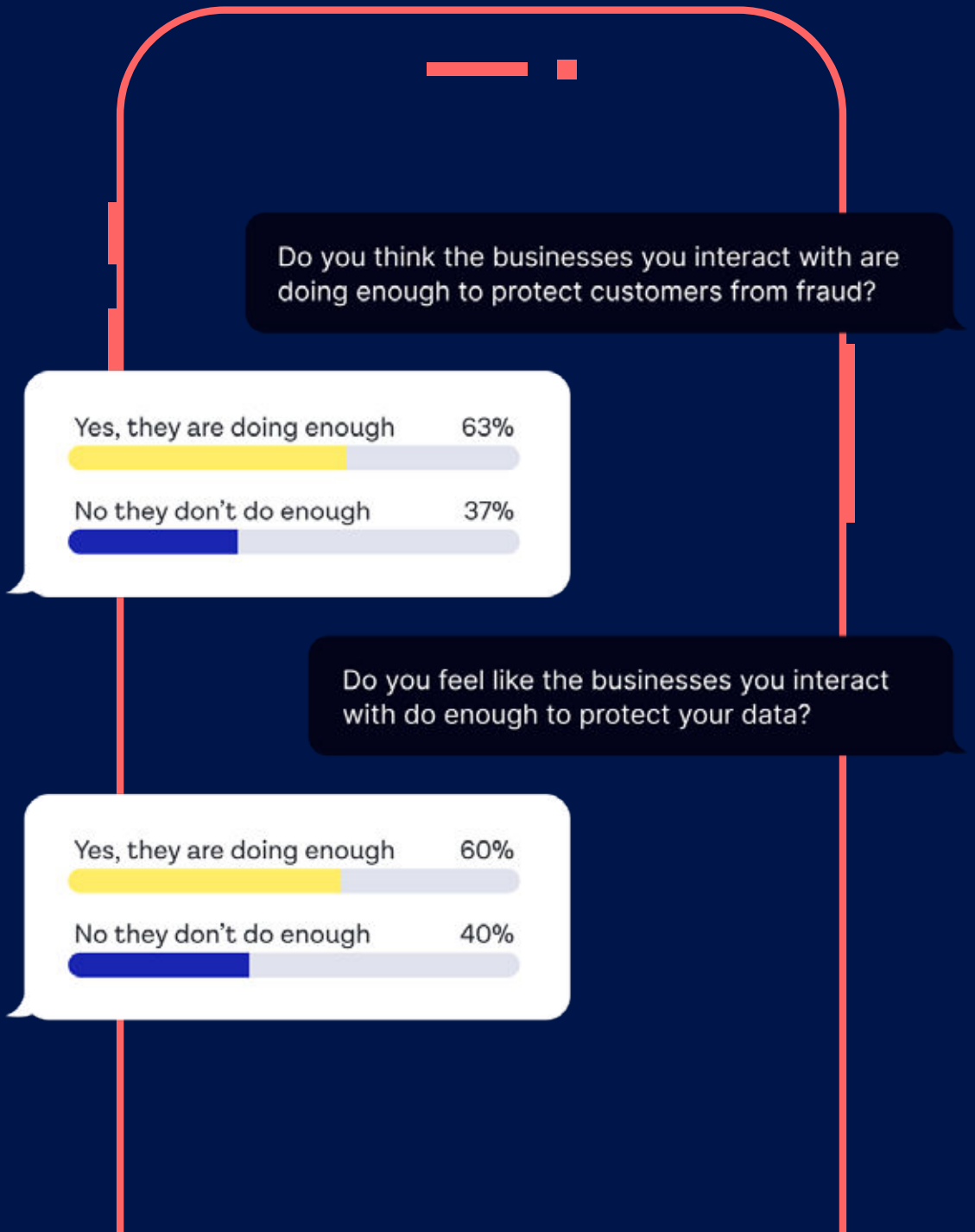
of people worry about the amount of data they need to provide

38% of users feel businesses could do more to protect them from fraud

Despite 63% of users feel businesses do enough to protect them from fraud, 37% still feel businesses could do more.

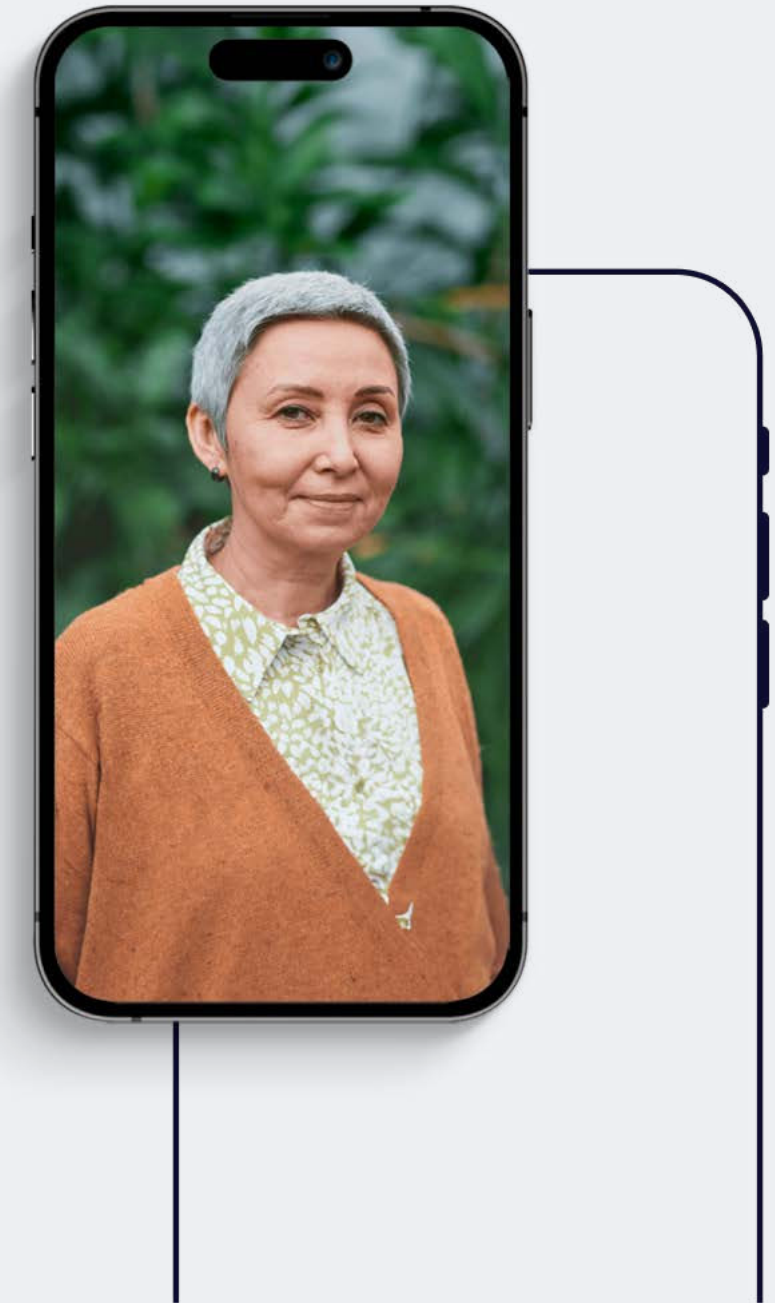
The same applies when it comes to data protection. 40% of users feel businesses could do more to protect their data.

One thing businesses could do to meet this expectation, is provide more guidance on what they currently do to protect their customers from fraud and to protect their data. A lot of fraud prevention happens in the background, which users might not even be aware of. Businesses should also take steps to deploy technologically advanced fraud prevention techniques, for example using AI to fight some of the most advanced fraud techniques, such as deepfakes.



04 Identity verification for better UX

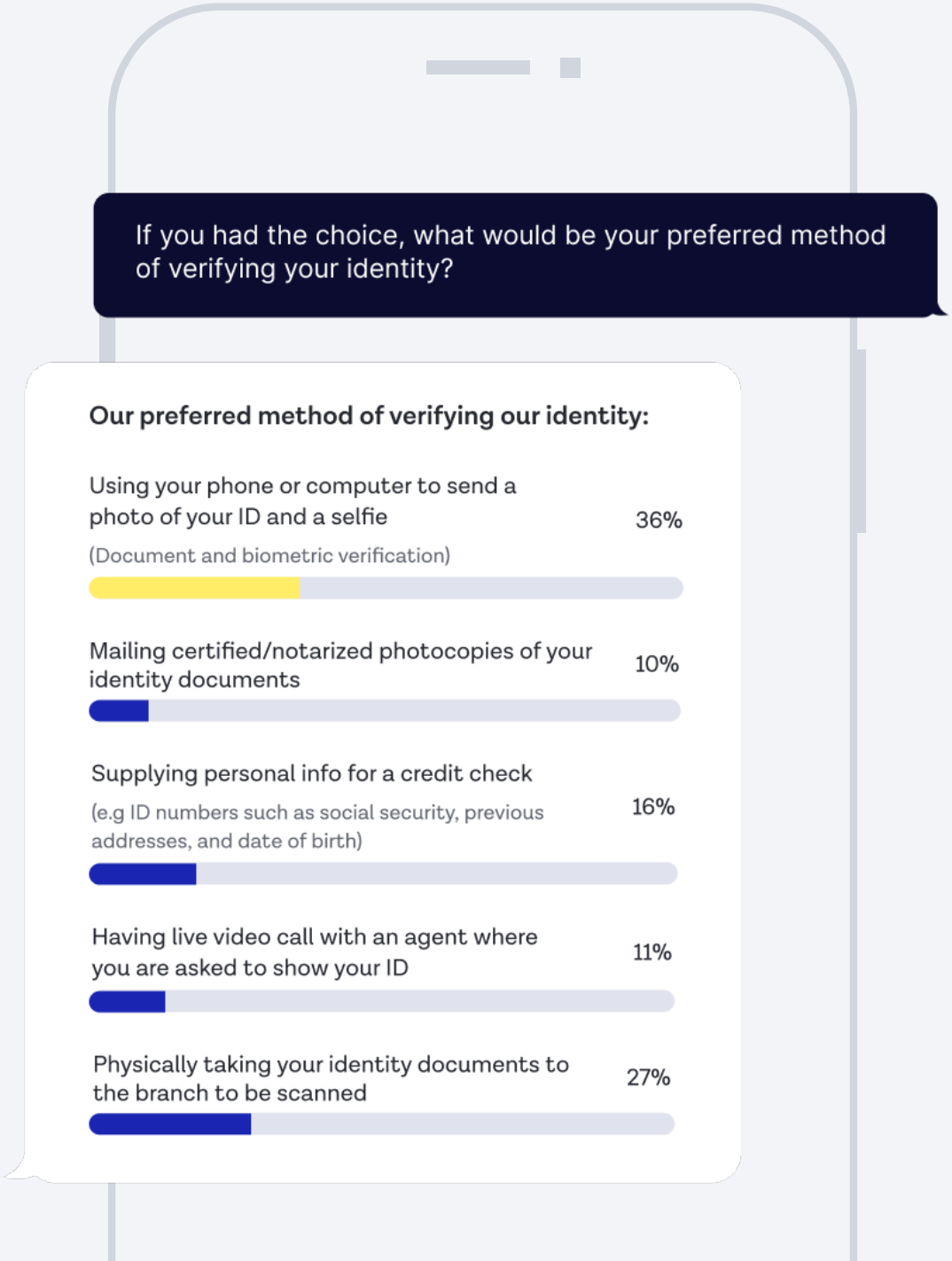
What do users want from identity verification processes?



User preferences: document and biometric verification is top choice

Remote identity verification has changed the face of onboarding.

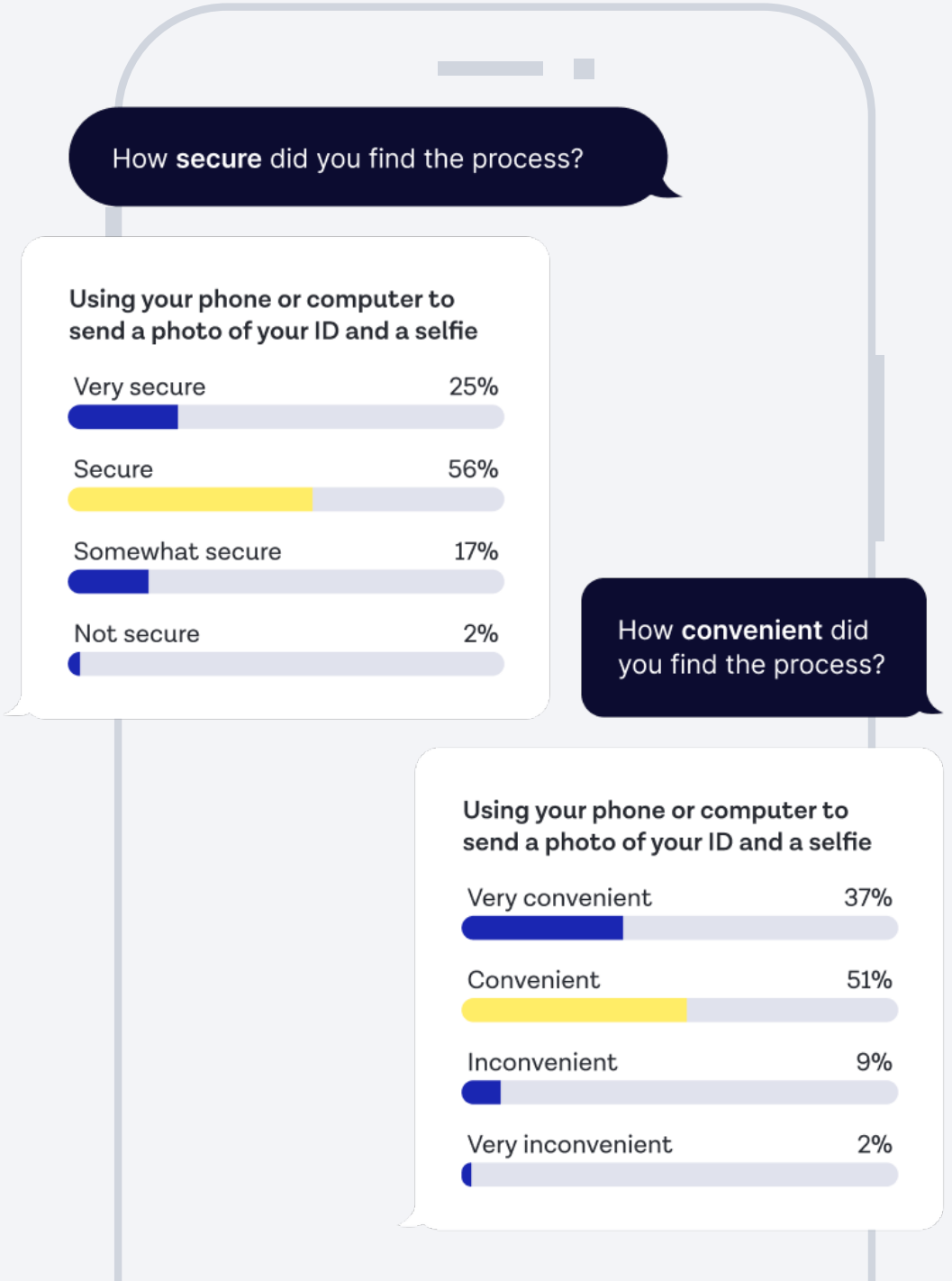
A decade ago, in-person verification was the accepted standard. Today, not only are the majority of people accessing online services daily, but digital identity verification is their preferred choice to prove their identity. 36% of end users would choose a document and biometric check over any other method of identity verification.



Why users opt for digital identity verification

Users find digital identity verification (doc and bio) both secure (81%) and convenient (88%). This highlights the advancement of identity verification services and how they've become streamlined enough that security and convenience can go hand in hand.

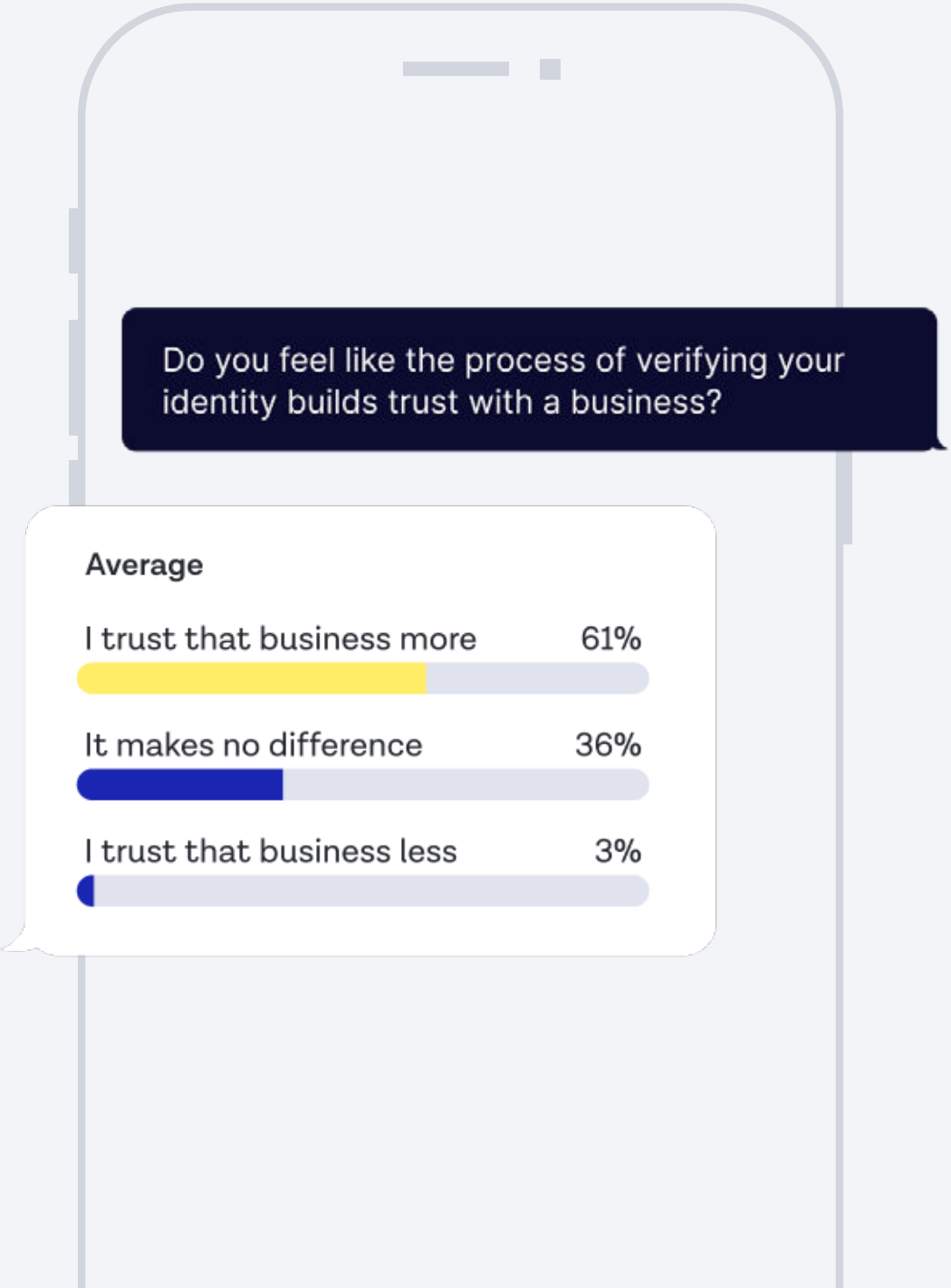
In other words, a highly secure verification process no longer needs to compromise UX or take hours (or days), and a streamlined experience with an excellent UI can also incorporate strong fraud detection and security measures. Users want both, and businesses should take this into account when implementing an identity verification solution.

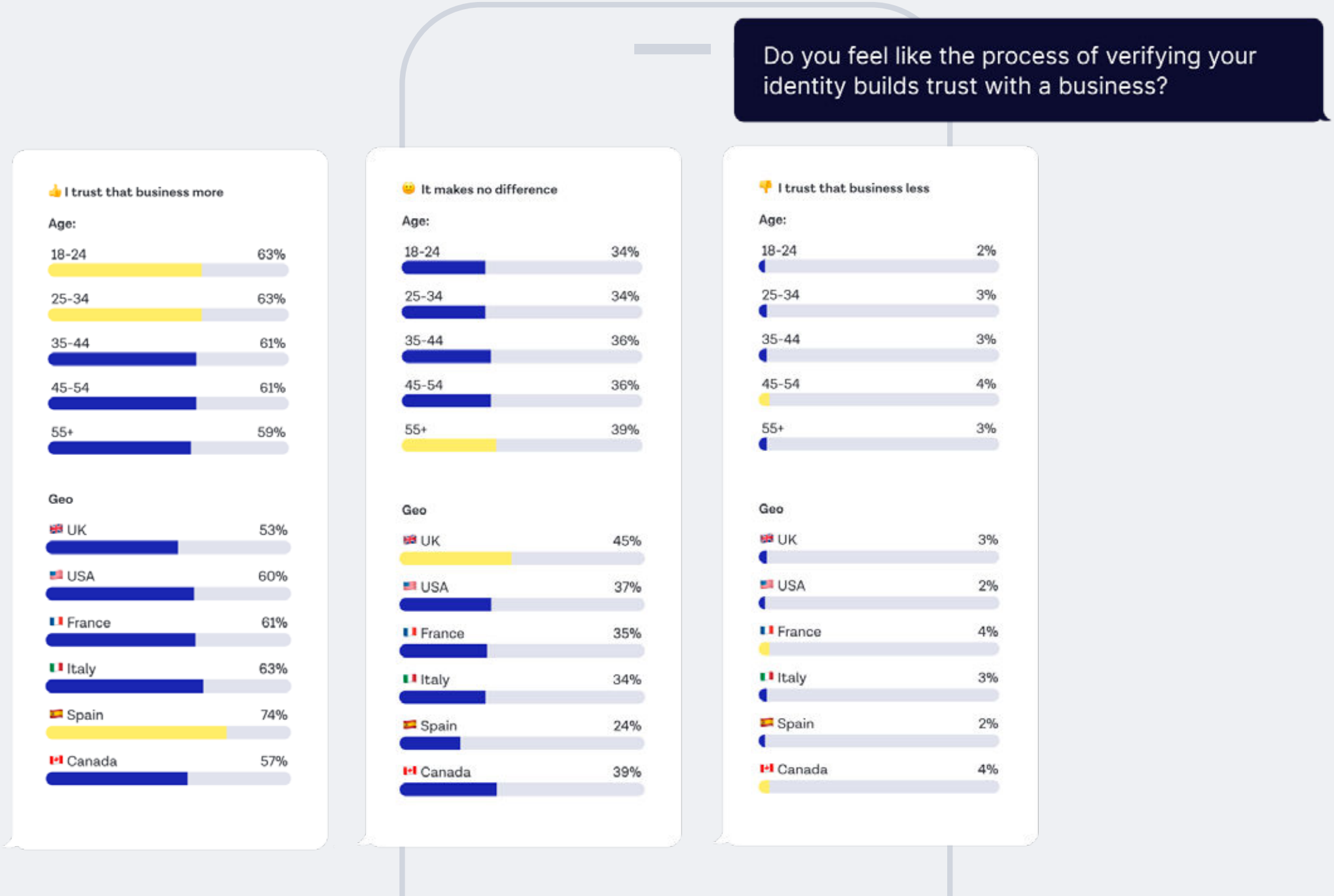


Building trust: identity verification goes beyond ticking regulatory boxes

Identity verification not only helps businesses build trust in their users' identities, but 2 in 3 users say they trust the business more as a result of identity verification.

While it's a non-negotiable for regulated businesses subject to KYC processes, it also presents a benefit to those who don't necessarily have to do it by law. For example, hotels, car rental agencies and other services can create a relationship of trust with users while also protecting their business against fraud.




Do you feel like the process of verifying your identity builds trust with a business?
👍 I trust that business more
Age:
18-24 63%
25-34 63%
35-44 61%
45-54 61%
55+ 59%
Geo
UK 53%
USA 60%
France 61%
Italy 63%
Spain 74%
Canada 57%
🙂 It makes no difference
Age:
18-24 34%
25-34 34%
35-44 36%
45-54 36%
55+ 39%
Geo
UK 45%
USA 37%
France 35%
Italy 34%
Spain 24%
Canada 39%
👎 I trust that business less
Age:
18-24 2%
25-34 3%
35-44 3%
45-54 4%
55+ 3%
Geo
UK 3%
USA 2%
France 4%
Italy 3%
Spain 2%
Canada 4%

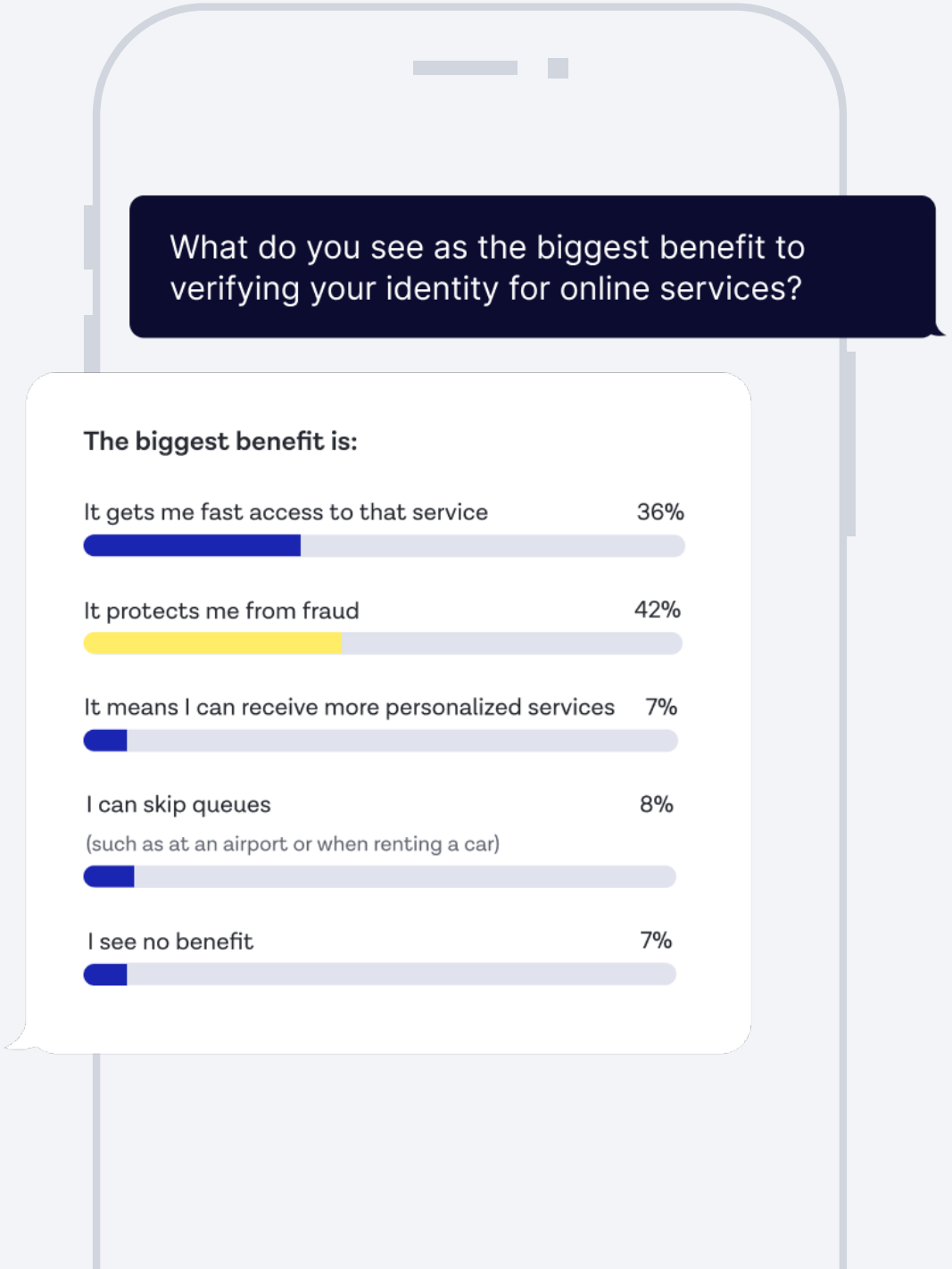
Striking the balance: users emphasize need for speed *and* security

End-users see fraud prevention (42%) as the biggest benefit to identity verification.

But they almost equally prioritize speed (36%). Getting the balance right between fraud prevention and fast, convenient access to services is therefore crucial for businesses.

From a business perspective, these priorities are often managed by different teams and can sometimes seem at odds with each other. Product and Growth teams are responsible for getting more users through the door and boosting conversion rates. Whereas Compliance & Risk teams are focused on implementing the necessary KYC checks, while Fraud teams need to keep fraudsters off the platform.

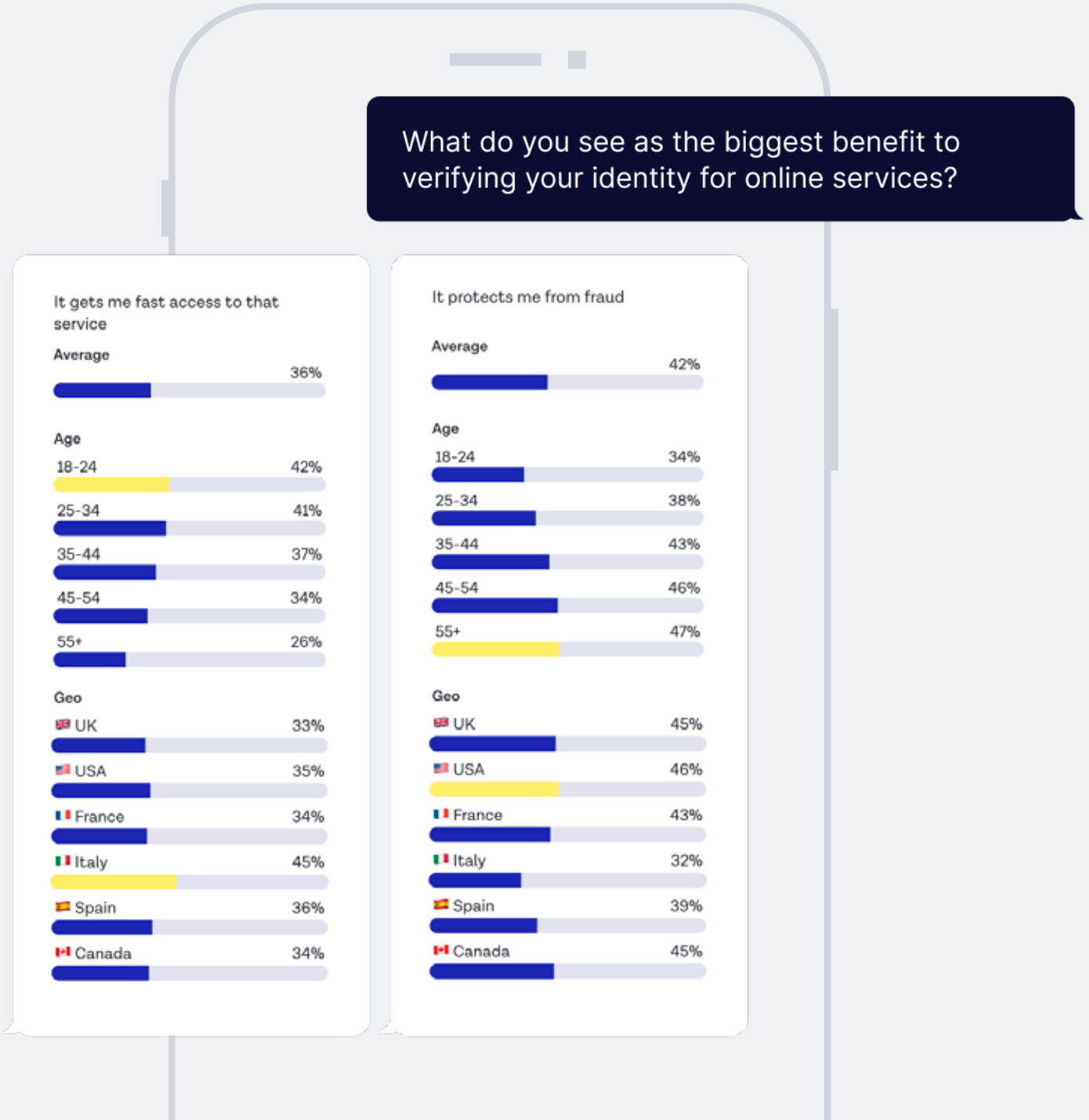
But the data highlights that users see the benefit of both — they want speed and security. Businesses should take this as a sign that balance is key. Onboarding is an opportunity to get different teams in the same room to find a solution that supports the different priorities.



While businesses should look to incorporate a balance of speed and security during onboarding experiences, it's important to bear in mind the expectations of different users. A lot of this will come down to what users are used to. For example, users who routinely experience fast, seamless onboarding experiences accept this as standard. Instead, they might want more assurance that they're protected from fraud.

This is arguably the case in the UK. In recent years, we have seen some over-correction when it comes to speed, where the technology is now so fast that users want some assurance that the necessary security checks have been completed — sometimes, a small amount of friction has its benefits.

On the flip side, users who still experience slow or confusing onboarding will want a fast onboarding experience above all else. As is the case in Italy.



05 The future of identity verification

Shaping tomorrow's security

Users' preferences point to reusability and privacy controls

What do end users want from the future of onboarding and identity verification processes?

User sentiment points to more flexibility, more control over who they share their data with, and how much data they share at any one time.

9 in 10 users

would be satisfied if they could control how much personal information they shared with individual businesses.

9 in 10 users

would be satisfied if they could revoke access to their personal information at any time via their phone.

7 in 10 users

would be satisfied if they only had to verify their identity once for multiple businesses.

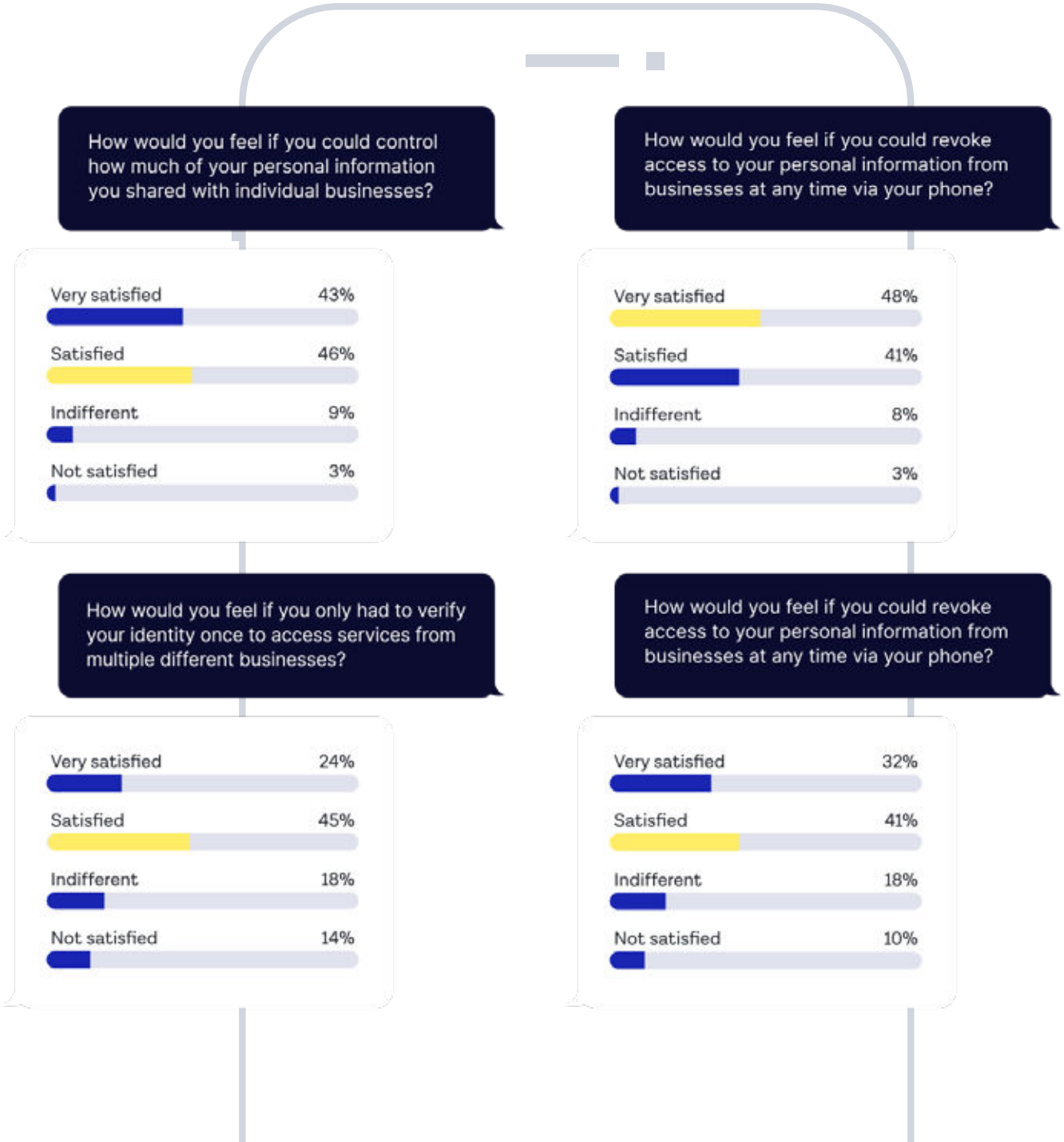
7 in 10 users

would be satisfied if they could store a digital version of their identity document on their phone.

Today, identity verification has digitized physical processes. While the technology that supports this process has developed — it's faster, more accurate, and better at detecting and preventing fraud — the actual process hasn't changed. Users are still required to hand their identity over to be checked every time they access a new service.

But the future could look very different. According to Gartner, "by 2026, 50% of smartphone users will frequently use one or more verifiable claims stored in their decentralized identity wallet." There is a market want and need for a process that gives users better control and organizations even greater confidence in who their customers are.

With a single user-controlled digital identity applied across multiple products and services, businesses eliminate the cost of maintaining and securing multiple identity profiles. They can also simplify compliance and regulatory requirements by minimizing storage and processing of extensive sensitive data.



Standardizing regulations to reduce fragmentation

While user-controlled identity could be the long-term solution, current regulatory changes are also impacting identity verification in the short term.

Identity verification has undergone a period of intense transformation. In ten short years, it has evolved from face-to-face verification in stores and branches to identity document and biometric verification that can be conducted remotely and processed automatically.

But as the data highlights (see page 13), different countries have adopted different technologies at different paces, meaning there is a mix of national eID schemes in place (and each using different methods to onboard users) alongside local and global identity verification providers. Just looking at Europe alone, these varied speeds of adoption, and mixes of national and global approaches have resulted in a notoriously complex and fragmented regulatory landscape.

But this is changing. The EU is undergoing a period of standardization. We're seeing this materialize in new AML laws, eIDAS 2.0, as well as ETSI guidelines. ETSI (European Telecommunications Standards Institute) sets technical standards for a wide range of ICT-related systems and services and is officially recognized by the EU.

Looking to the future, we expect these laws and standards to bring more harmonization and interoperability — which is good news for businesses — helping them reduce complexity as well as scale into new markets more easily. Plus, European standards might also form the basis for wider global standards. Businesses using KYC solutions will need to ensure that their solutions meet the rules and technical standards in the latest laws and regulations, which will apply EU-wide.

06 Onboarding dos and dont’s

How to improve verification experiences

How to improve verification experiences

01 Change the conversation around UX and compliance

Too often, UX, compliance, and fraud prevention are seen as competing business priorities. Nowhere does that competition come to a head more so than onboarding. It's easy to see why. 1 in 5 end users abandons the account sign-up, 1 in every 10 users falls victim to fraud, and regulatory hoops can seem endless. Product, Compliance & Risk, and Fraud teams, all have different metrics to monitor and different business priorities to meet.

But onboarding flows present an opportunity. Businesses should look to use onboarding as a way to open up and change the conversation. Instead of viewing UX, fraud, and compliance as competing priorities, instead, use it as an opportunity to define the business goals.

02 Tailor onboarding experiences for different users

In the past, businesses have adopted a one-size-fits-all approach to onboarding. Today, no two end-users are the same, so why should their experiences be identical? As the data shows, different ages and users based in different locations have different expectations regarding onboarding experiences. Plus, local regulations often dictate slightly different regulatory requirements.

Striking a balance between compliance and UX starts with understanding which end-users your business is comfortable funneling through low-friction 'happy paths', and which require additional assessment.

03 Leverage no-code orchestration tools

To tailor onboarding experiences for different users, businesses will need to manage multiple onboarding flows. Businesses should lean into orchestration platforms to prevent this from becoming a resource-intensive, operational nightmare for internal teams. No-code drag-and-drop workflow builders reduce the lift for onboarding teams when building out new workflows, or making changes to existing ones.

04 Optimize the UI of onboarding experiences

Most users are used to digital-first onboarding experiences. But without a well-thought-out UI, digital isn't necessarily better. Businesses and identity verification providers have a responsibility to create an experience that anybody can get through without difficulty. This benefits both the user, who'll have a great experience, and the business, who'll see less drop-off.

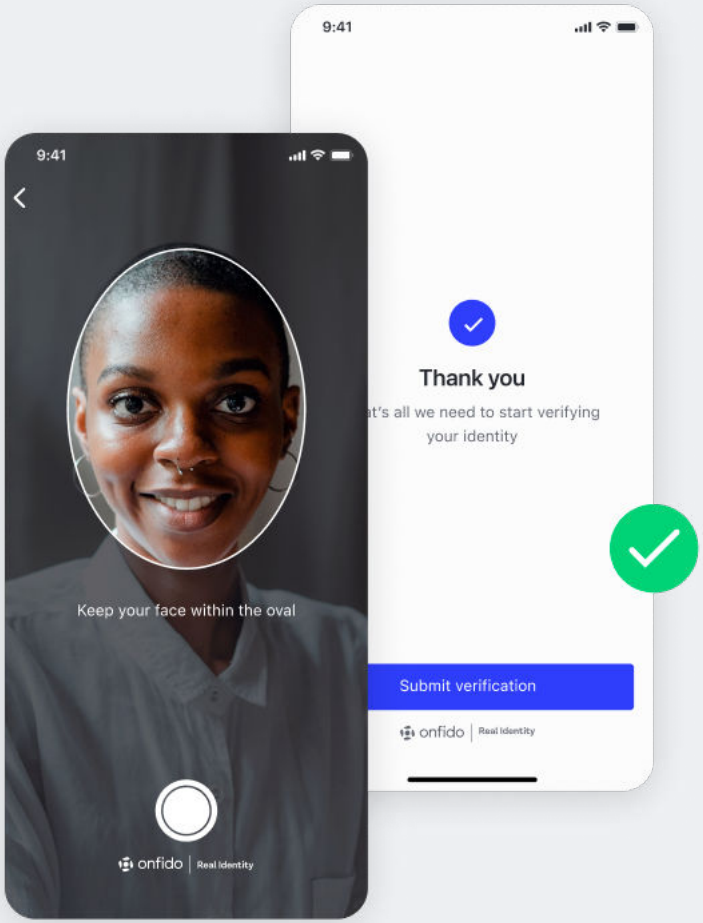
Users appreciate transparency, so businesses should take steps to explain the process during onboarding. Identity verification providers should design the digital process for the real world, for example, including real-time feedback and accessibility features.

07 Onfido's solution

How Onfido supports UX, fraud prevention, and compliance at onboarding

Smart Capture SDK

With today's users mostly setting up new accounts via an app (40%) or online (40%), it's essential to integrate identity verification into that digital onboarding flow.



Industry-leading UI

Onfido's SDKs provide real-time feedback, as well as blur and glare detection, as part of the document and selfie capture process. This ensures that image capture errors are eliminated instantly, resulting in faster turnaround times and improved conversion rates.

Easy to integrate

No need to rewrite lines of code to incorporate identity verification into an onboarding flow. Onfido's extensive documentation and quick-start guides make integration fast and simple, ensuring you can go live in days not months.

Cross-device capability

For users who prefer to start the onboarding process from a desktop or laptop (without a camera), they can easily move to a mobile device during the capture experience. No app installation is required; users simply scan a QR code. We guide them back to their web journey when capture is complete.

Fraud detection signals

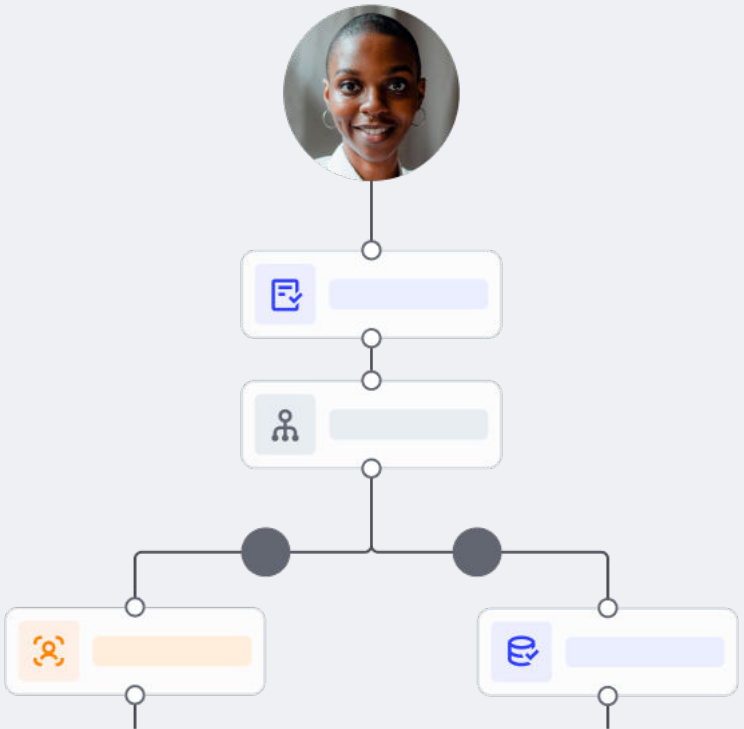
Device integrity, network intelligence, and geolocation signals detect and mitigate non-visual document and biometric fraud. NFC scanning provides an additional layer of protection when analyzing supported identity documents.

Onfido Studio

Every customer is different. A one-size-fits-all approach isn't going to work for every onboarding flow. This is where orchestration comes in.

Businesses need to be able to quickly and easily build new flows, or add requirements to existing ones, based on changing customer expectations and evolving (or geo-specific) regulations.

Onfido Studio allows businesses to respond to market and regulatory changes, faster, ultimately supporting that businesses' market expansion.



Build no-code workflows

Quickly build no-code workflows that move each user through the right verifications at the right time. Configure a flexible blend of UI components, verifications, and if-this-then-that conditions

Automate tailored experiences

Build and trigger the ideal experience for every customer, and automate internal processes, with workflows that respond to changing market conditions.

Navigate KYC and AML compliance

Adjust for risk tolerance and introduce new verification methods that address global and local compliance requirements as you expand into new geographies.

Motion: Biometric Verification

Today's customers are highly receptive to biometric solutions.

Motion is Onfido's next generation biometric product that helps businesses achieve that perfect balance between fraud prevention while offering market-leading UX.

Users simply take a video selfie and turn their head — the process takes seconds. Analysis is 100% automated with 95% of verifications returned in seconds. Motion is iBeta PAD Level 2 compliant and offers greater protection from sophisticated attack methods like injection attacks, display attacks, and 2D/3D masks.