

2022 Global Identity and Fraud Report

Building digital consumer trust amidst rising fraud activity and concerns



Executive summary

In past years, this report has called on businesses to meet consumer expectations for online recognition and security while also improving their digital customer experience. Our latest research reveals that companies have received the message and are investing in multiple digital initiatives. But the fraud risk persists. In fact, 70% of businesses say that their concern about fraud has increased since last year.

The worry is understandable, given that identity fraud in the UK alone increased by 22% in 2021 compared to the prior year, with 90% of those cases originating online.¹ While in the US, the Federal Trade Commission reported that consumer losses related to fraud increased by 70% in 2021 to more than \$5.8 billion.² What's more, a report from Europol (the law enforcement agency of the European Union) suggests that cybercriminals will continue to innovate and capitalise on new opportunities.³ For this 2022 Global Identity and Fraud Report, we dive into the growing expectation that businesses recognise and protect consumers online, and the challenges businesses must overcome to meet them.

The survey underpinning these insights encompasses 1,849 business respondents and 6,062 consumers from 20 countries, including Australia, Brazil, China, Chile, Colombia, Denmark, Germany, India, Indonesia, Ireland, Italy, Malaysia, The Netherlands, Norway, Peru, Singapore, South Africa, Spain, UK, and US. We've also included interviews with consumers from Brazil, Germany, the UK, and US.

The responses showcase an evolving digital consumer who is regularly conducting financial transactions online, prioritises security, and trusts businesses that provide it. Meanwhile, businesses worldwide are working to safeguard consumer identity, prevent fraud and improve the online customer experience, yet with decidedly mixed results.

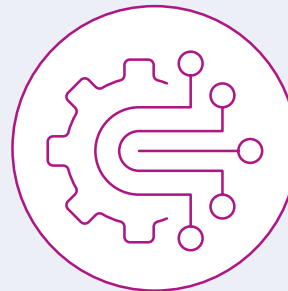
1. <https://www.fraudscape.co.uk/>
2. <https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0>
3. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

So what leads to success? Our research shows that companies earning consumer trust leverage automated solutions to identify and protect customers across their online journey and complement these efforts with robust staffing of digital support programmes.

Read on to discover:



How online security yields engagement and trust with today's digital consumers



The current opportunity for businesses to implement multiple identity and fraud solutions



The role of businesses in protecting online consumers and the benefits of doing so



The role that orchestration and outsourcing play in helping companies prevent fraud



Executive summary



Fraud concern and activity continue to increase



Consumer keep security top-of-mind



Consumer expectations



Businesses need orchestration solutions



Outsourcing and security knowledge



5 Key Actions



Regardless of business investment, fraud concern and activity continue to increase

This year, nearly half of all business respondents reported that fraud was a high concern and 90% reported fraud as a mid-to-high concern. Moreover, 70% of businesses say that their worries about fraud have increased over the past 12 months. This increase in concern tracks with the uptick in fraud activity in every corner of the world. From benefits and unemployment fraud to phishing and more advanced scams such as synthetic identity fraud and deepfake fraud, cybercrime has been on the rise—and businesses and consumers have noticed.

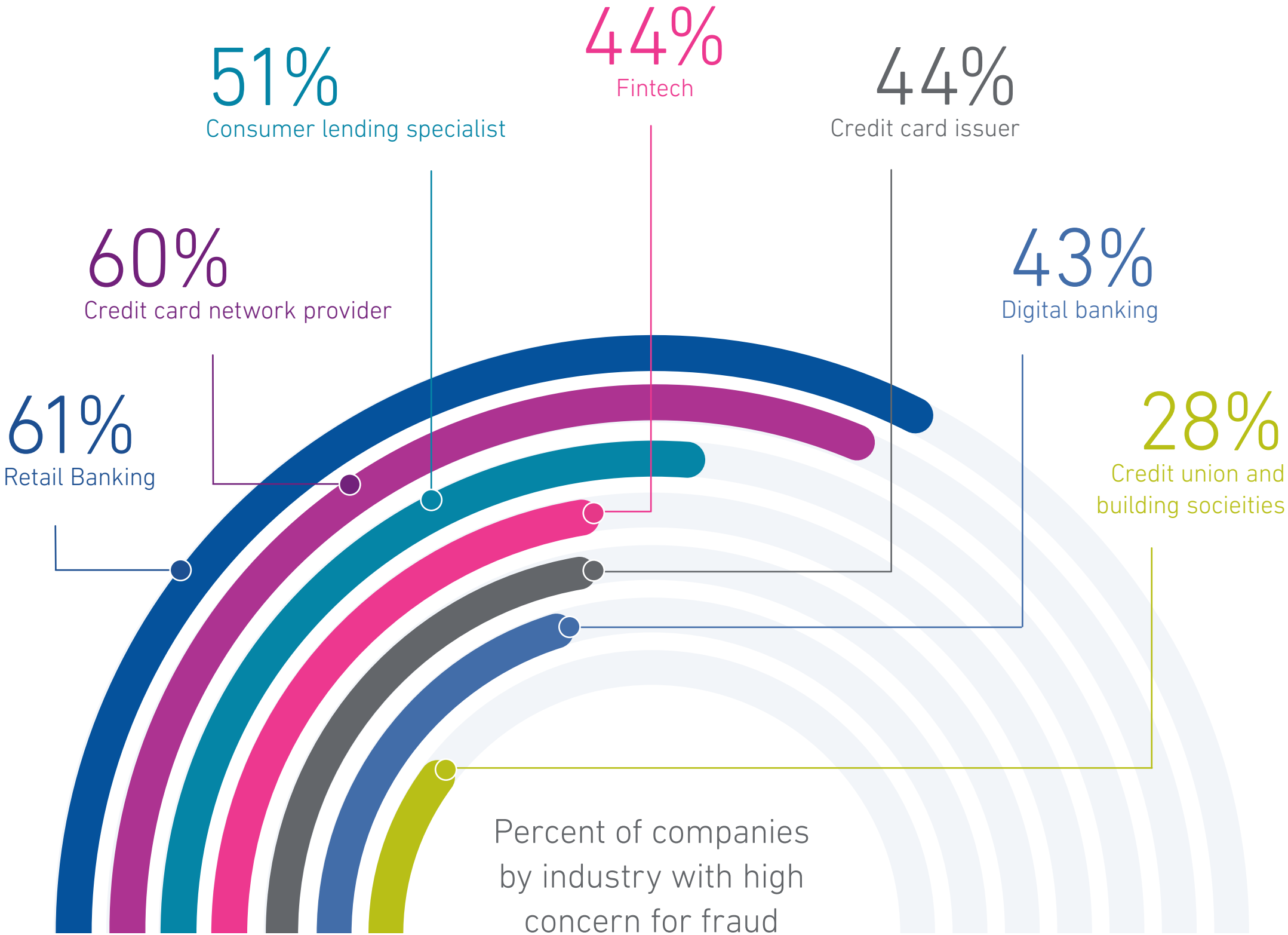
The concern varies by industry. More than half of the respondents from retail banking, credit card networks and consumer lending specialists (home loans, car loans, personal loans) categorise their fraud concerns as high. However, less than half of fintech and digital banking organisations reported the same. Credit unions and building societies remain the least worried, with less than one-third of respondents saying they have high concern about fraud.

There are multiple reasons for the varied level of concern across verticals. In some cases, the industries most worried are those that have been hit the hardest by fraudulent activity such as retail banking. In other cases, it may reflect different experiences and points-of-view about fraud. For instance, many traditional banks and longstanding ecommerce companies have been battling fraud for decades and experienced the consequences of poorly designed solutions. Newer fintech companies, on the other hand, may not have suffered significant attacks.

Regardless, fraud concern informs conversation and action. For example, 80% of businesses—representing all industries—say that fraud is often or always discussed within the organisation. And companies surveyed reported the automation of fraud risk decisions, investment in ransomware prevention, and strengthening the security of mobile channels among their top strategic investments.

The reverberating impacts of fraud

Traditional financial service companies are most concerned



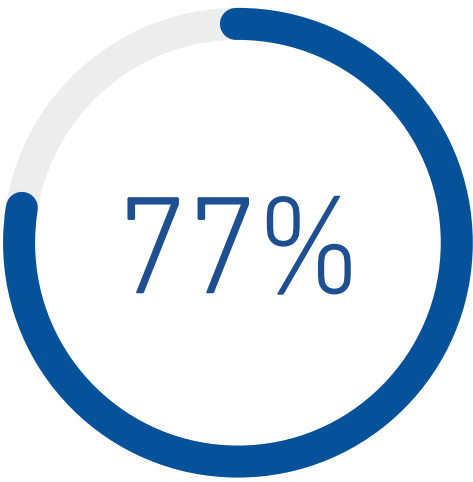
Fraud concern and activity continue to increase

The increase in fraud risk hasn't escaped consumers. More than half report that they're concerned about online transactions, and 40% say that concern has increased over the past year. In addition, 58% of consumers have been a victim of online fraud, know someone who has been a victim, or both. While these first-hand encounters with cybercrime understandably increase consumers' concern, they don't prevent them from transacting online; instead, consumers select transactions and businesses they perceive as safe.

On the crime front, fraud activity is still rising despite the time and resources companies are investing to stop it. In the US, the Federal Trade Commission reported that consumer losses related to fraud increased by 70% in 2021 to more than \$5.8 billion.⁴ The tactics employed by fraudsters continue to evolve. For example, the Europol report highlighted the rise of mobile malware, which enables criminals to circumvent security measures such as two-factor authentication.⁵

Ongoing data breaches and cyberattacks cause financial problems for consumers and businesses alike. But equally as important, they also erode trust. In an era in which security is an ever-growing priority, consumer trust, retention, and business growth go hand-in-hand. And these digitally savvy consumers know exactly what they want in order to stay safe.

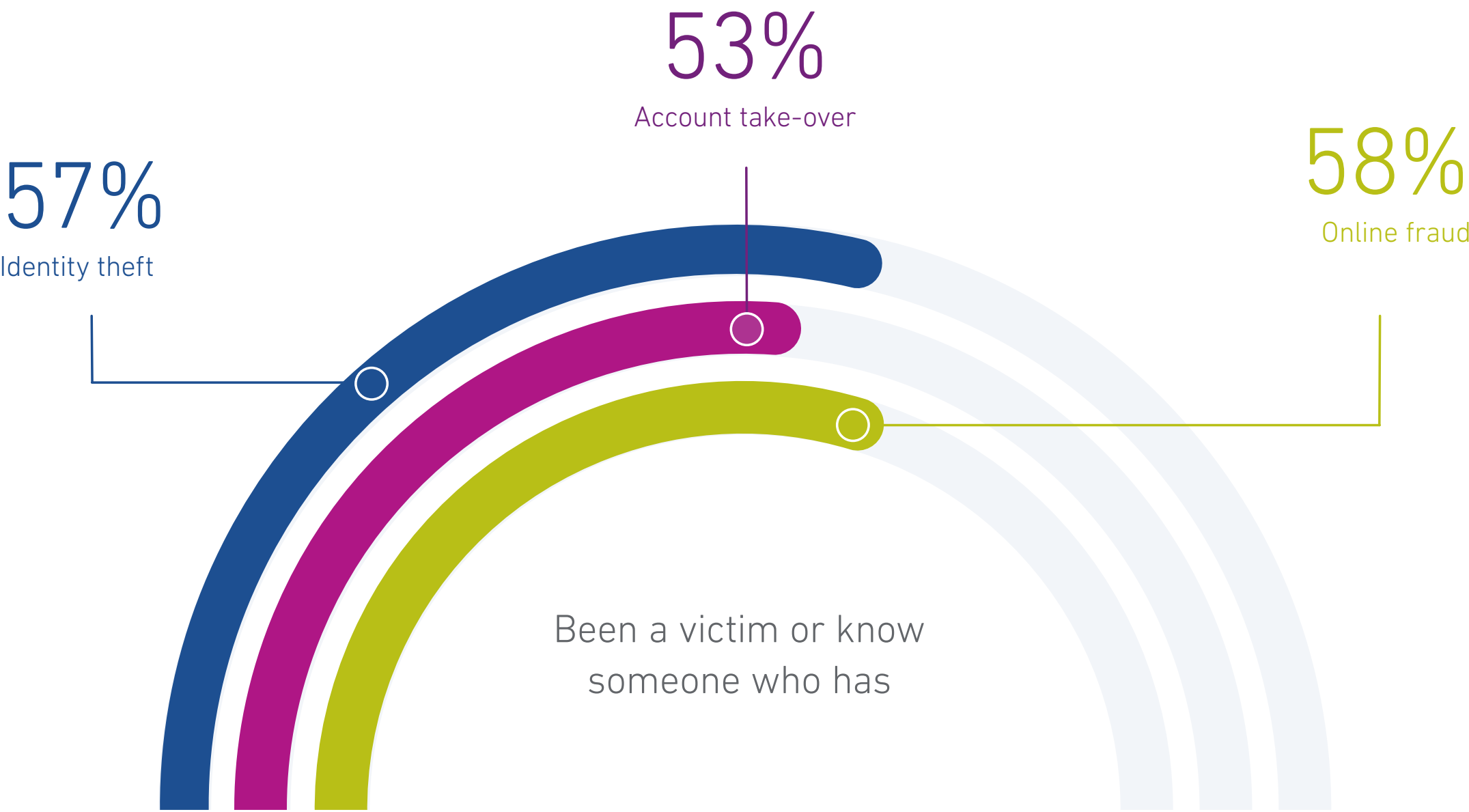
Encountering fraud increases concern for consumers



of consumers say their concern increased after experiencing an online fraud incident

Concern was highest in Colombia, Peru and Brazil

Many consumers have experienced fraud



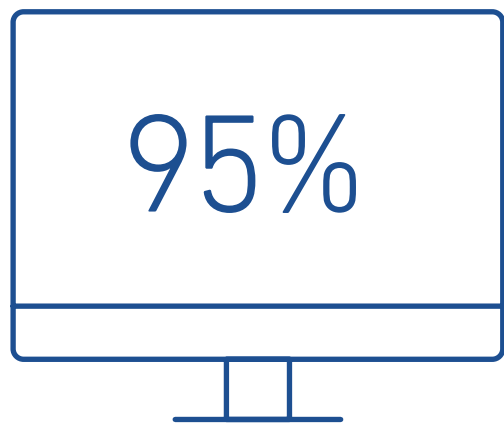
4. <https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0>
5. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

Consumers keep security top-of-mind, even as they increase their online activity

Digital financial transactions have become as regular a part of everyday life as sending and receiving emails. In fact, this type of online interaction is now commonplace across age groups, income levels, and regions of the world.

Our latest research shows a global digital cohort of consumers that's highly active and only getting more so. More than half of consumers say that their online spending has increased over the past three months. While higher-income groups and hyper-engaged younger spenders drive the activity, it's still broad-based. Consider that 48% of consumers ages 40 to 54 and 32% of consumers ages 55 to 64 have ramped up their online activity. And it's not stopping anytime soon. Half of the global respondents say they plan to increase their online spending over the next three months.

These new digital consumers are savvy about their online transactions, and they're aware of the fraud risks and the role that recognition and security tools play in protecting them. For example, when evaluating online experiences, consumers rank security and privacy as their top priority—more important than convenience and personalisation. This trend gets stronger as consumers age. Security and privacy have taken the top spot every year, ahead of personalisation.



of Baby Boomers cite security as the most important aspect of their online experience

10 percentage points more than their Generation Z counterparts

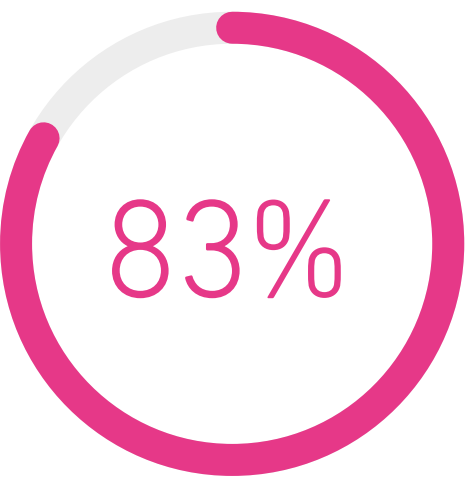
So how do consumers balance their need for security with the convenience of online transactions?

For many, it's about which businesses they trust. Our in-depth consumer interviews revealed that people often prefer bigger, well-known brands with financial resources to reduce their online fraud risk. They perceive the security of these brands to be better (though they don't actually know this to be true). For example, many consumers are more likely to transact with an unknown brand if that brand uses a well-known payment system provider because of the additional payment protection that it provides and the trust they have in the company.

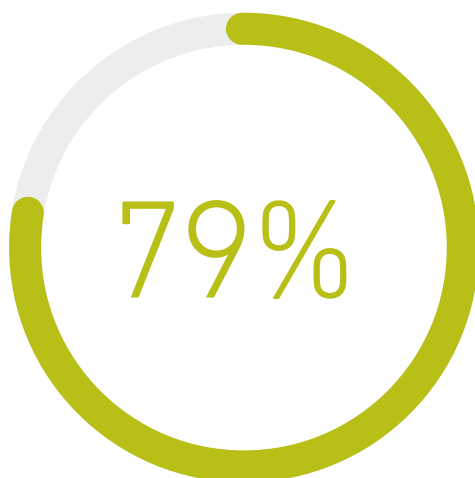
Consumers also noted that they're less likely to trust businesses headquartered in other countries due to previous fraud, poor user experiences, and the tendency toward digital-only service with no in-person recourse when there are problems. That said, a track record of good business interactions trumps everything. Consumers say that regardless of company size if a brand consistently provides positive experiences, they will trust that the company is protecting their data.

Online security is a global consumer preference

Global consumers value security above all

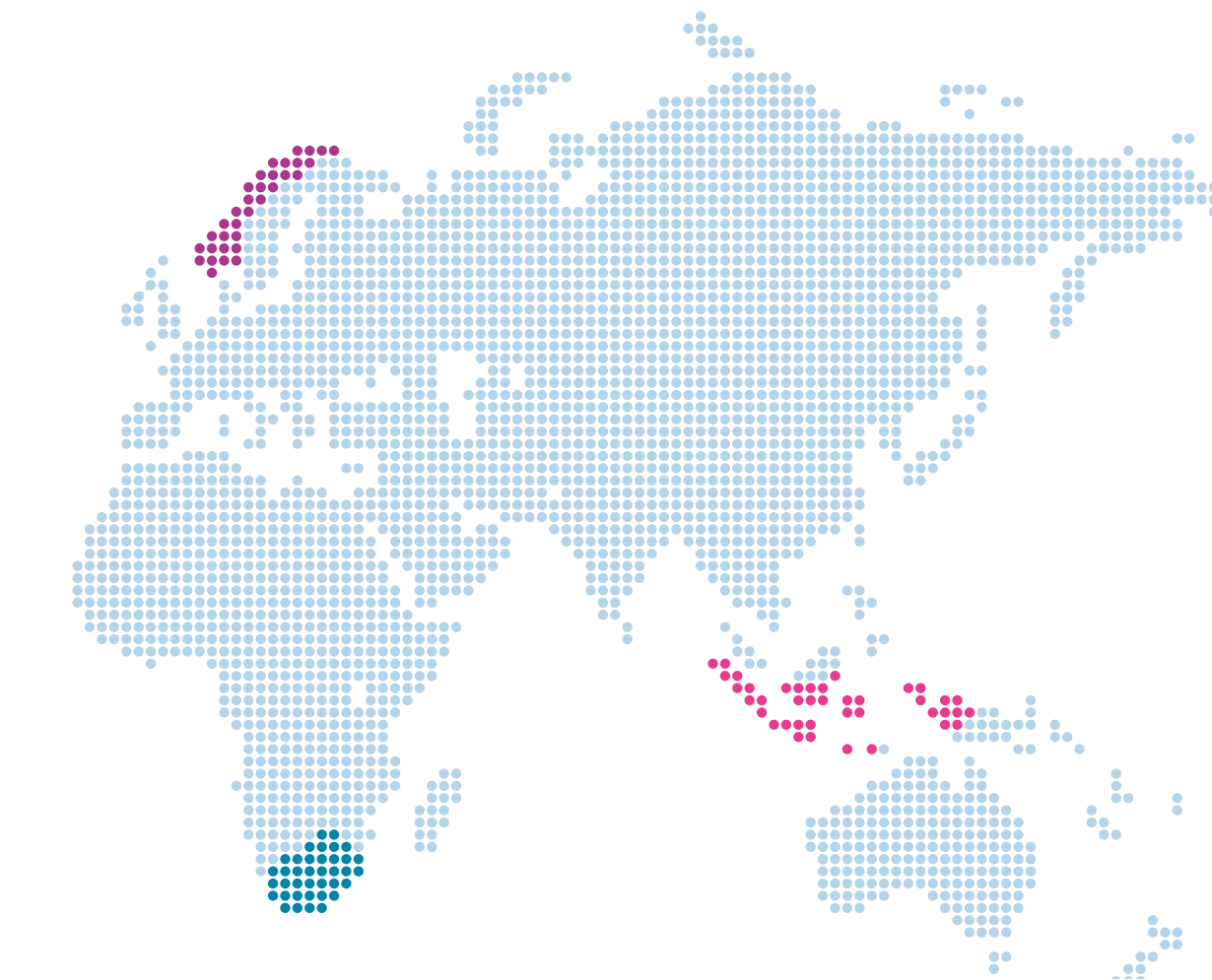
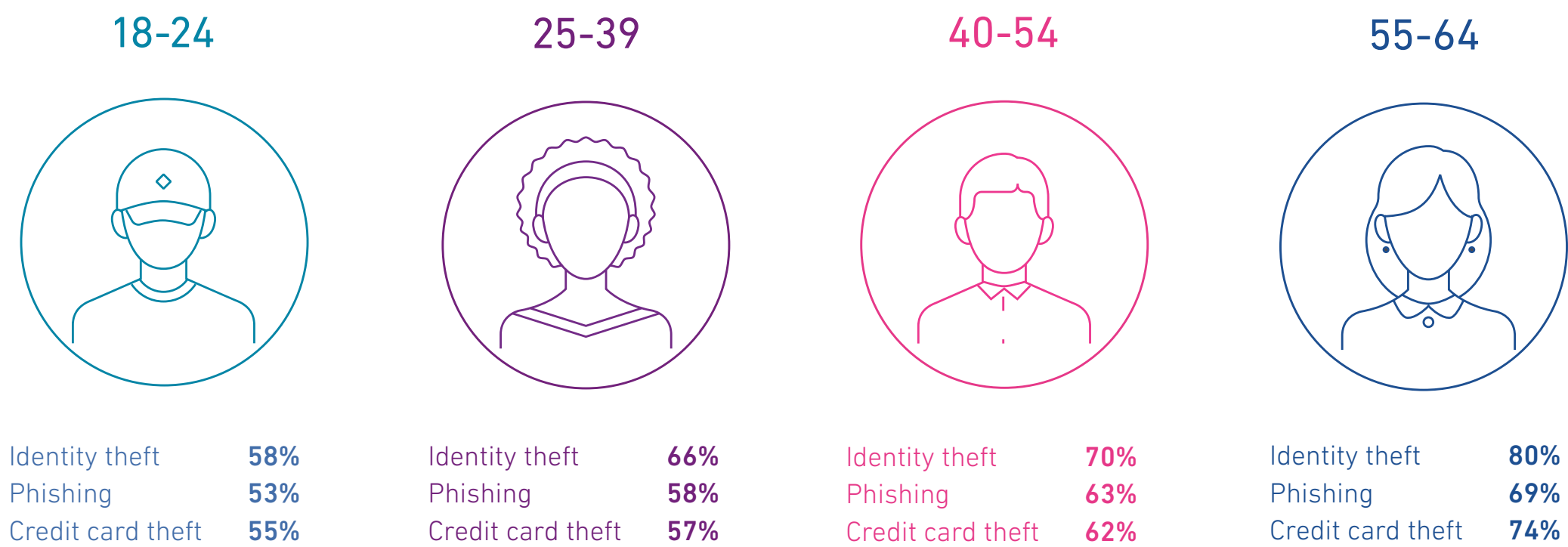


say security is most important factor of online experience. That figure is highest—89%—in Colombia, Chile, Ireland and South Africa



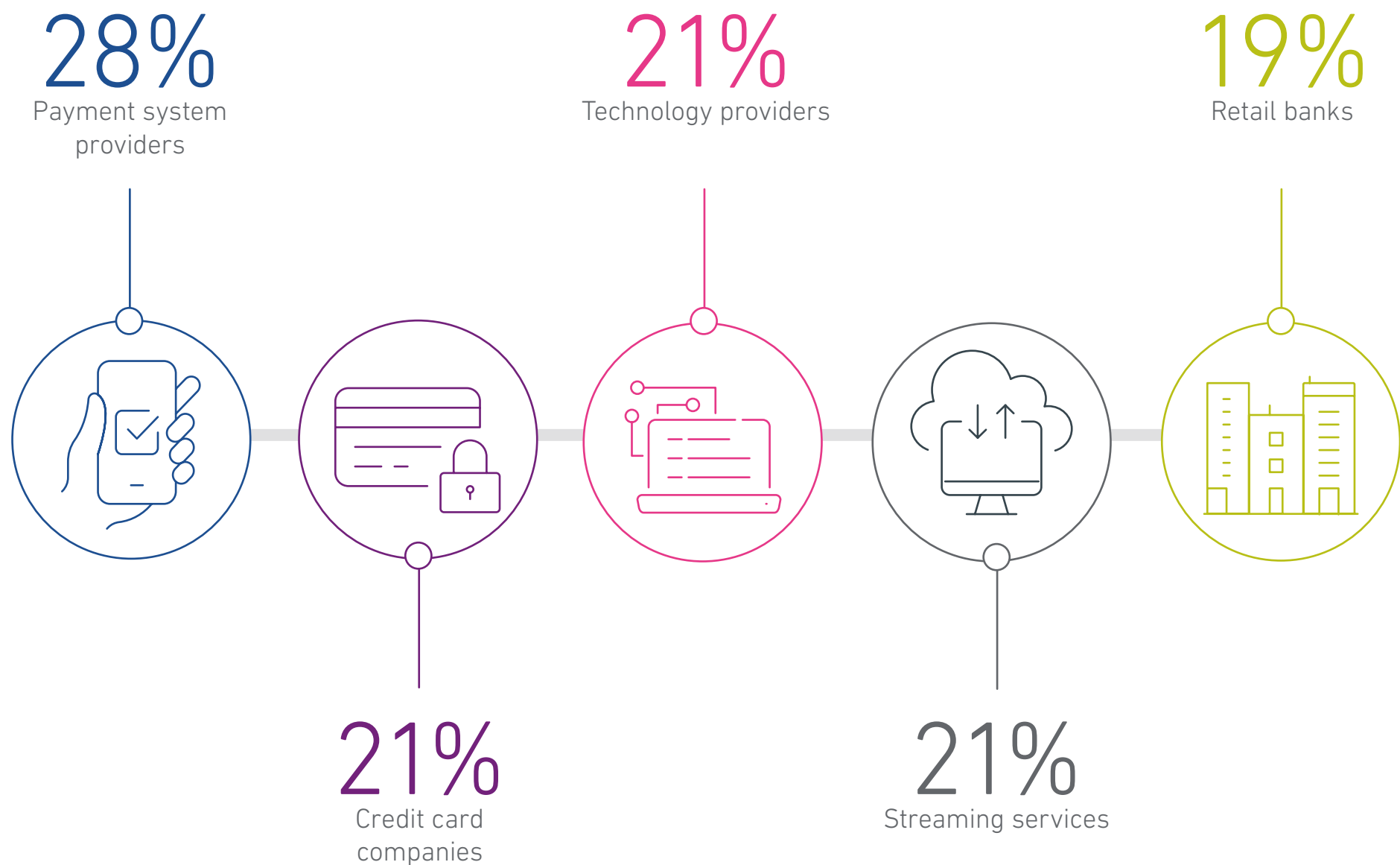
say privacy is the most important factor

Identity theft has bested credit card theft as consumers' biggest security worry—and the concern increases with age



8 in 10 consumers in Indonesia, Norway and South Africa are concerned about identity theft

Industries that consumers trust the most



But businesses overall still have a lot of work to do to garner trust in the digital age

“It’s the same with meeting a stranger. You want to meet them with someone else. PayPal is like that friend who is there to support me. They sort of hold your hand and reassure [you] that things will be OK.”
— UK survey respondent

Consumer expectations place the obligation for online protection on businesses

Nearly three-quarters of consumers expect businesses to take the necessary security steps to protect them online. And seven out of 10 say it's important that companies they frequently deal with online are able to identify them across visits. This isn't a surprise to businesses, a majority of which expect consumers to cite security as a top priority.

Brewing regulations may force businesses to take on even more security liability, in line with consumer expectations. For example, U.K. regulators have made banks liable for fraud, even when the customers were victims of authorised push payment scams, in which consumers are deceived into approving a payment to a criminal.⁶ While this isn't the case across the rest of Europe or the U.S., it's a prescient look at how regulations may evolve.

However, consumers are beginning to better understand the role that sharing personal data can play in improving online security. In our interviews, they noted that if businesses want to collect their data, then companies should also protect them from online threats that are too complex for consumers to handle. For example, 57% of consumers report that they are willing to share data if it ensures greater security or prevents fraud. And 63% of consumers say that sharing data is beneficial, increasing from 51% in 2021.

This new era reflects a digital contract of sorts, with consumers expecting protection from companies in return for their business and data. But are businesses upholding their end of this bargain? In our consumer survey, only 23% of respondents were very confident that companies were taking steps to secure them online.

6. <https://www.gov.uk/government/publications/government-approach-to-authorised-push-payment-scam-reimbursement/government-approach-to-authorised-push-payment-scam-reimbursement>

Additionally, only one-third of consumers are confident that businesses will recognise them repeatedly online, despite the fact that 84% of businesses say recognising customers is very or extremely important. **The research indicates that there is still a significant gap between consumer sentiment and businesses intentions related to recognition.**

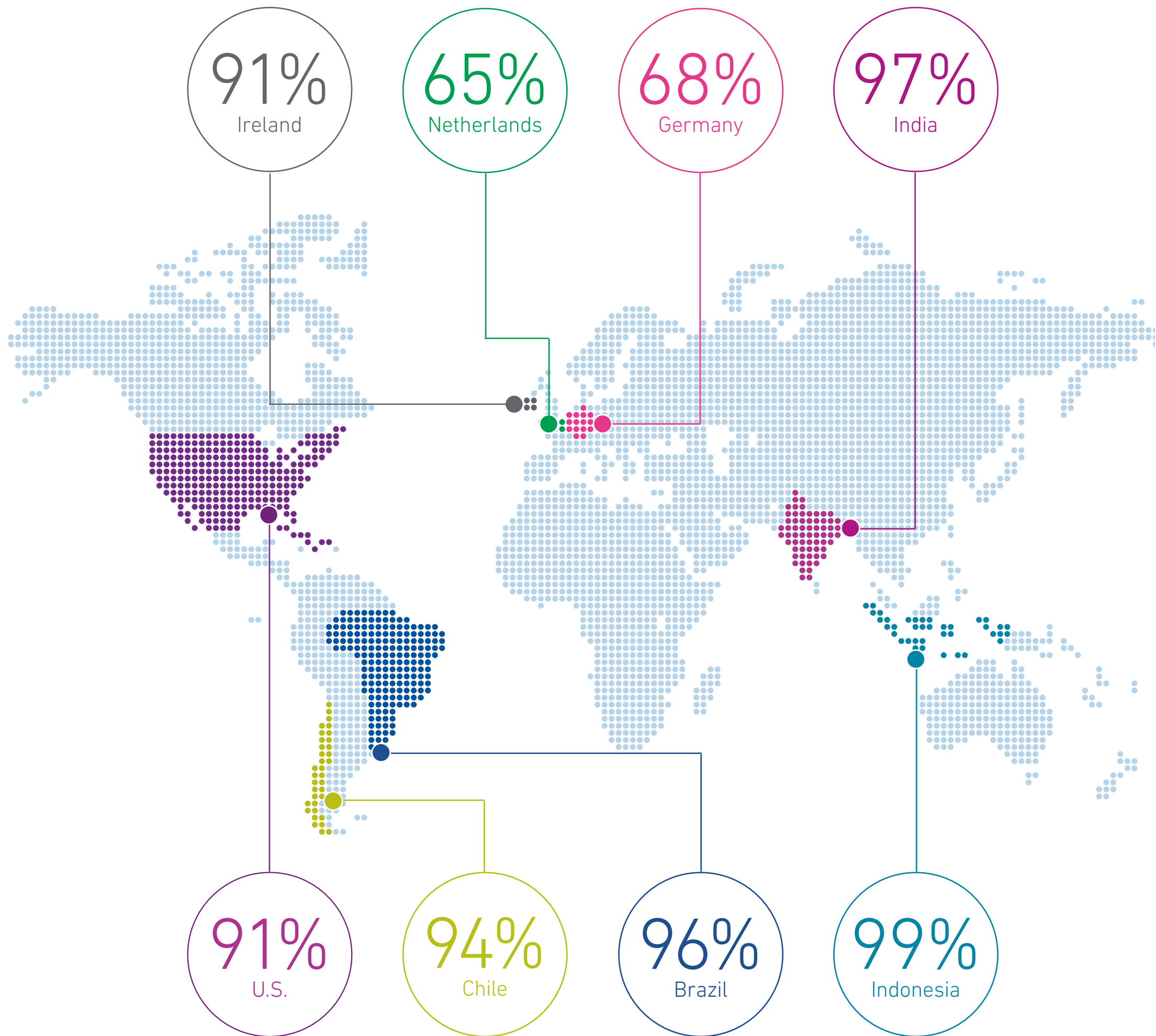
This may be because businesses are still struggling to prioritise advanced recognition tools that enhance consumer engagement over more blunt methods that err on the side of suspicion. These gaps also erode trust between consumers and businesses and negatively impact the customer experience. That's because recognition and security are integral components of the customer journey, something that nearly all companies say they want to improve. Fortunately, emerging technology offers solutions that decrease fraud and reduce the work required of the consumer.

For instance, only 1 in 5 customers report that they were offered a pre-fill form option as part of their account opening experience. However, new tools, such as phone-centric identity verification solutions and online identity document verification solutions, provide pre-fill capabilities as part of their offerings. In doing so, they automate and improve recognition and create a friction-free onboarding process.

While technology can help improve online security, our customer interviews highlighted the importance of maintaining some human-centred customer service for more complex problems. Interviewees said that even when they had no intention of contacting a customer service rep, they appreciated businesses that communicated the option as available. Indeed, balancing a human touch with the ease of automation remains an essential component of gaining consumer trust. For their part, 33% of businesses noted in 2021 that they planned to increase staff and support for their digital operations this year. And 27% planned to increase call centre staff.



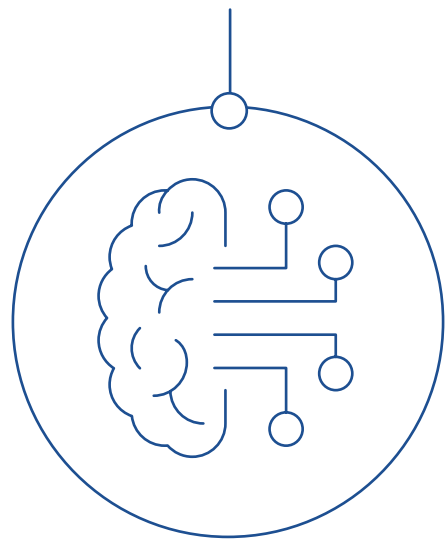
Businesses say improving the customer journey is also paramount



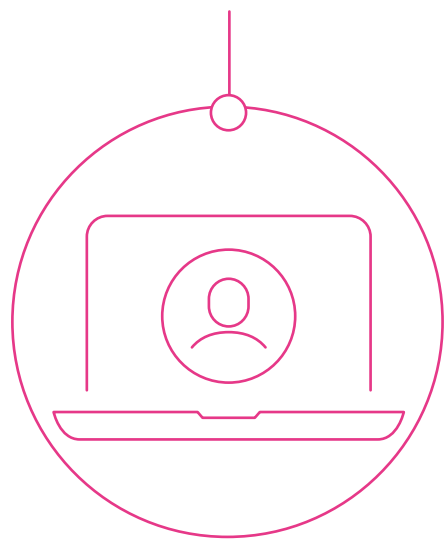
Technology connects the dots

How businesses are improving the digital customer journey

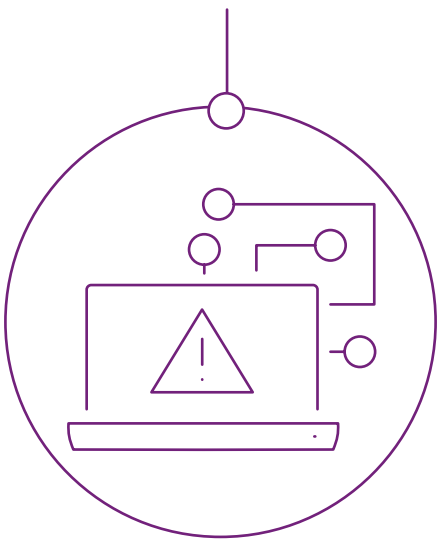
Improving customer decisioning with AI



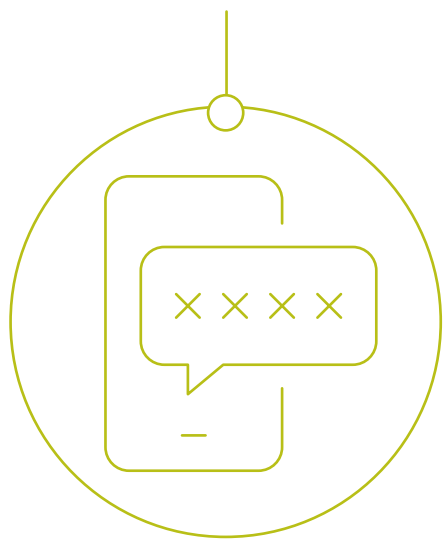
New AI models to improve decisioning



Investing more in digital operations and automation

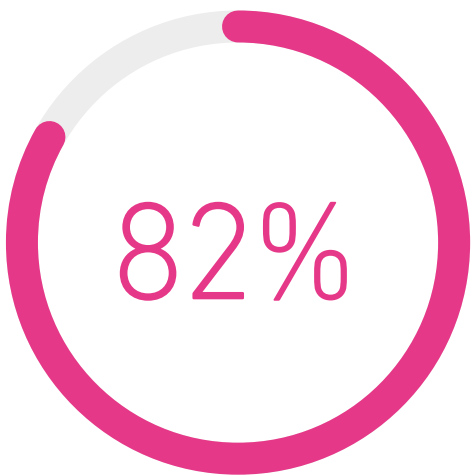


Strengthening security of mobile/digital channels



Businesses know that security is a consumer preference

Security is the most important dimension across almost every country



82% of businesses expect customers to place more importance on security

Businesses need orchestration solutions to effectively manage their growing suite of tools

This evolving fraud and risk landscape requires that companies utilise multiple types of recognition and security solutions. However, while nearly 7 out of 10 consumers say it's important that businesses identify them online across multiple visits, there's no runaway leader in terms of which methods they prefer. For example, consumers rate physical biometrics and pin codes nearly equally in terms of what they prefer to use. But those also are the top two methods that consumers perceive as most secure. Notably, passwords have fallen out of the top three for a second year in a row when it comes to perceived security (behavioural biometrics takes the third spot).

In interviews, the responses vary by what consumers value in their online experiences. For instance, those that prioritise security over convenience like the additional reassurance that two-factor authentication provides. Those that value convenience the most say that physical biometrics are easier to use. And though consumers still utilise passwords frequently, those interviewed noted that as complex passwords become the norm, the security method becomes more of a hassle.

The lack of a clear preference opens the door for companies to introduce new tools and educate consumers about their benefits. For example, consumers report that they feel increasingly secure with newer recognition tools. In fact, more than 80% of consumers ranked physical biometrics as the safest when they encountered the technology, an increase from 74% last year. Consumer interest in behavioural biometrics continues to rise as well, with 76% considering the technology as safest this year, compared to 66% last year.

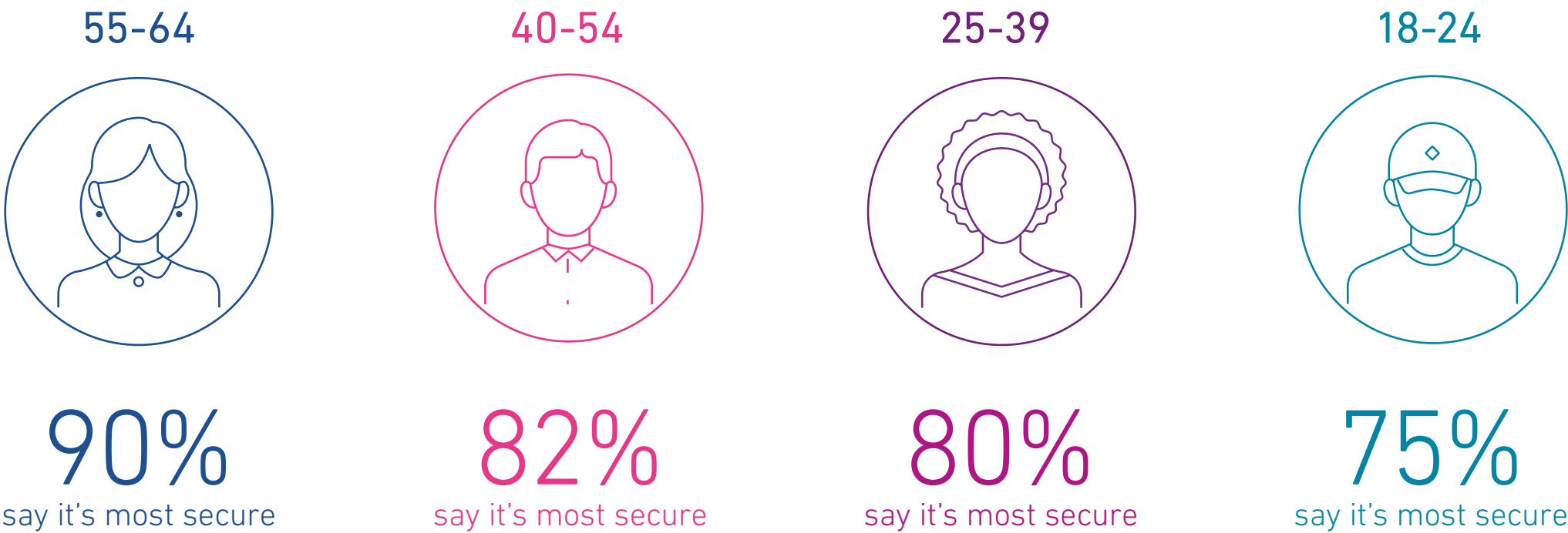
Businesses also have an opportunity to implement methods that speak to various demographics. Higher-income consumers have more confidence in security questions than consumers with lower incomes. They also think more highly of businesses that use multiple authentication methods. Regarding generational differences, Baby Boomers feel most secure with physical biometrics, more so than their younger counterparts (18-25 year-olds). They're also significantly more confident in behavioural biometrics.

However, companies shouldn't implement these tools independently of each other. Doing so creates silos and gaps between channels ripe for fraud attacks. A siloed approach also doesn't provide the level of nuance required to create a more elegant consumer experience and better fraud detection. This is where orchestration solutions make all the difference. Orchestration platforms enable companies to manage risk across the customer journey, coordinating security and recognition strategies to reduce the user burden and decrease fraud risk. Companies can also use the richness of the total output in a unified manner, allowing them to improve on all the key metrics for digital success, from fraud prevention to customer experience to recognition and more.

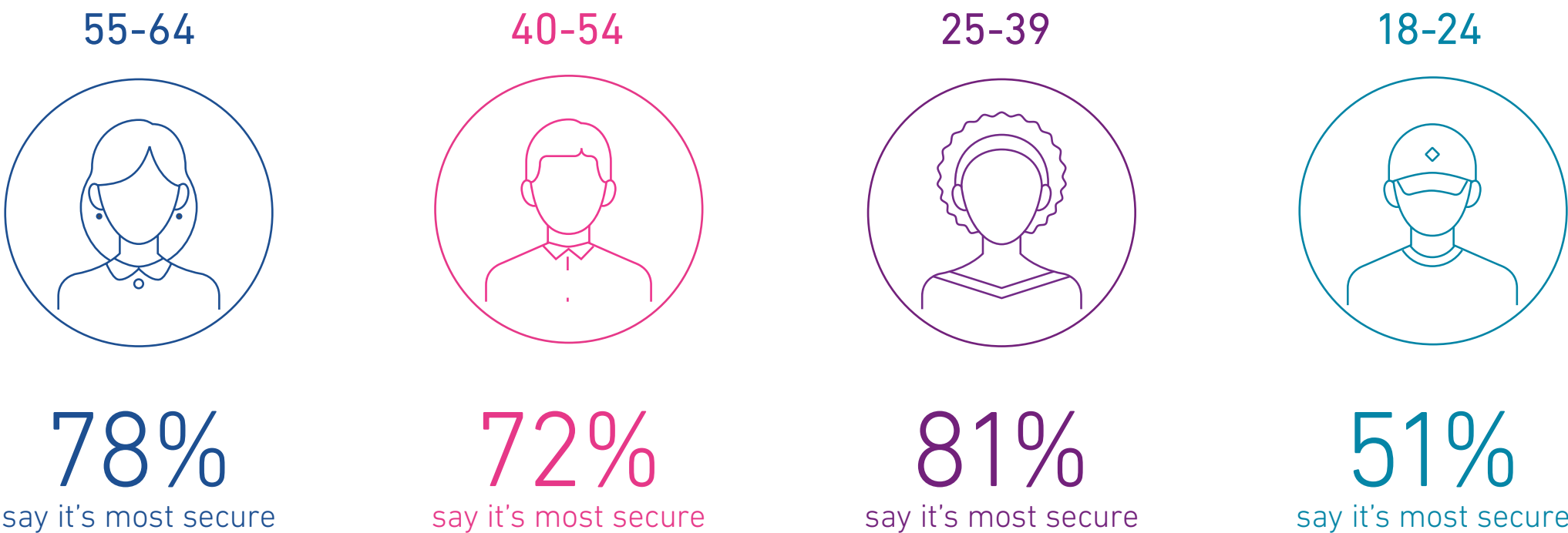


Baby Boomer and Gen X consumers like physical biometrics, while Millennials lean toward behavioural

Physical biometrics

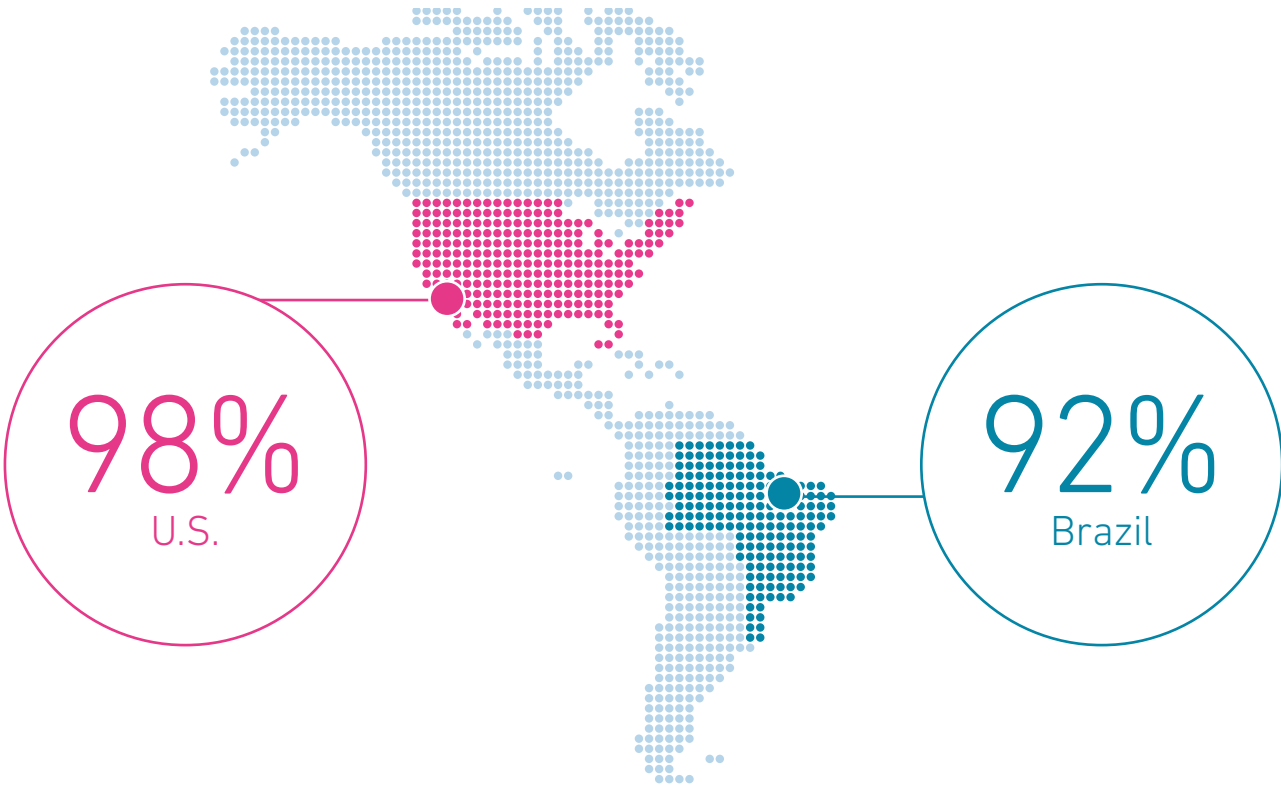


Behavioural biometrics



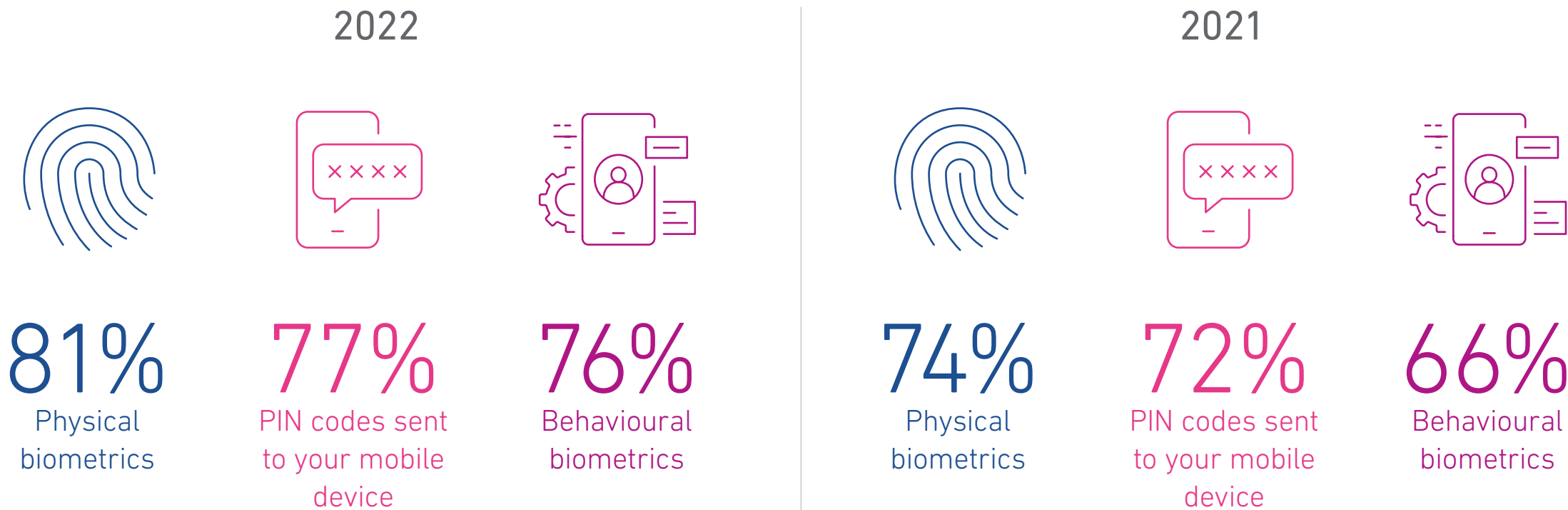
One Time Passwords (OTP) are perceived as convenient by consumers who have used them

96%
of consumers opening
a new account say OTP
is convenient



What do consumers say are the safest recognition methods?

Confidence in biometrics is growing, and passwords have notably fallen out of the top 3 for the second year in a row



Outsourcing enables businesses to do significantly more, but security knowledge must transfer too

Businesses aren't pursuing a single strategy for improving or securing their online customer experience. Instead, most are trying to tackle multiple initiatives at once. Companies surveyed gave nearly equal weight to 20 strategic priorities that touched on automation, ransomware protection, open banking, e-commerce, AI, security, fraud prevention, authentication, and more.

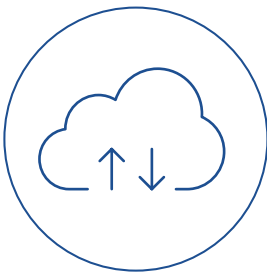
Companies are struggling to prioritise their digital efforts—all of them seem important—and it's creating organisational challenges. Preventing new types of fraud attacks, assessing customer affordability, and reducing the cost of analytic models represent the top issues that keep financial service and fintech leaders up at night.

It's no wonder many are turning to outsourcing to bolster their digital capabilities, such as cloud services, AI, fraud detection, mobile channel security and more. An increasing number of organisations lack the depth of technical resources to shoulder the increasing IT demands, not to mention develop solutions that keep them ahead of fraudsters or deploying advanced technology such as machine learning. That's why seven out of 10 businesses rely on outsourcing to help them pursue multiple digital initiatives.

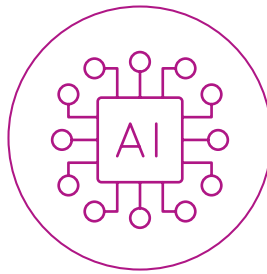
But the industry's previous foray into technology outsourcing provides a cautionary tale that companies should keep in mind today. As financial service companies moved into smartphone apps over the last decade, many outsourced the development work to reduce the development time, and to accelerate their time-to-market. Still, they often failed to include the robust fraud and risk management they'd garnered from their internet channels. The oversight led to increased fraud activity via mobile apps, with the losses often negating any potential new revenue bump.

The Top 5 outsourced digital capabilities


- 1




Cloud service solutions
- 2




Artificial intelligence
- 3



Fraud detection and prevention
- 4

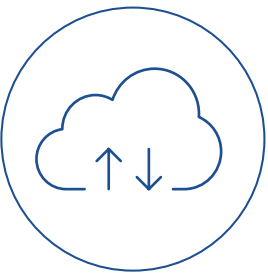


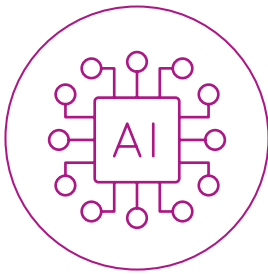
Mobile channel security
- 5





Remote workforce technology


Vertical most likely to outsource

- 

Credit unions:
Cloud service solutions
- 

Retail banking:
Artificial intelligence
- 

Credit card networks:
Fraud detection and prevention
- 

Consumer lending specialists (home loans, car loans, personal loans):
Mobile channel security
- 

Credit card networks:
Remote workforce technology



Balancing priorities to create an automated, end-to-end identity and fraud reduction programme

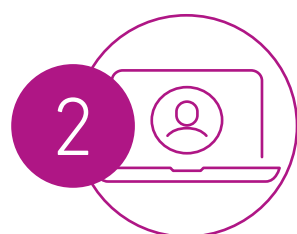
When everything is important, there's always the risk that something won't get the attention it deserves. Given the demands, financial service organisations must find ways to create more online security while improving the experience across the customer journey.

Here are 5 tips from Experian identity and fraud prevention experts for strengthening digital capabilities to benefit your customers' experience and reduce fraud risk.



1 Revisit the end goal for consumer recognition and security programmes

The reality is that most people are legitimate consumers trying to complete an activity online. The mission should be to leverage identity solutions that allow the vast majority of users to conduct their digital business seamlessly while identifying a relatively small number of fraudsters. This requires rethinking identity and fraud solutions to create a more integrated approach that encompasses both.



2 Understand the expectations and capabilities of online customers

Online is the new normal, and people of all ages, incomes, and regions are transacting digitally. But they're not all the same. Dive into the demographics of your customer base to understand what their expectations and comfort levels are with recognition and fraud prevention tools. Then take the opportunity to educate segments that could benefit from more information.



3 Leverage orchestration solutions to connect recognition, fraud prevention and customer experience

Siloed approaches to any one of these digital areas create the potential for misfires with consumers and vectors for potential fraud attacks. Focus on applying the right solution to match the use case. Take advantage of a single platform that can bring all your tools and data sources together, allowing you to adapt to changing risks and improve the customer journey.



4 Outsource to increase capabilities but keep fraud prevention in the picture

Outsourcing allows you to scale your digital capabilities across multiple areas, from security to remote worker engagement. However, you need to find a way to transfer not just your needs to your outsourced partner but also the invaluable security learnings you've gleaned from years of online transactions.



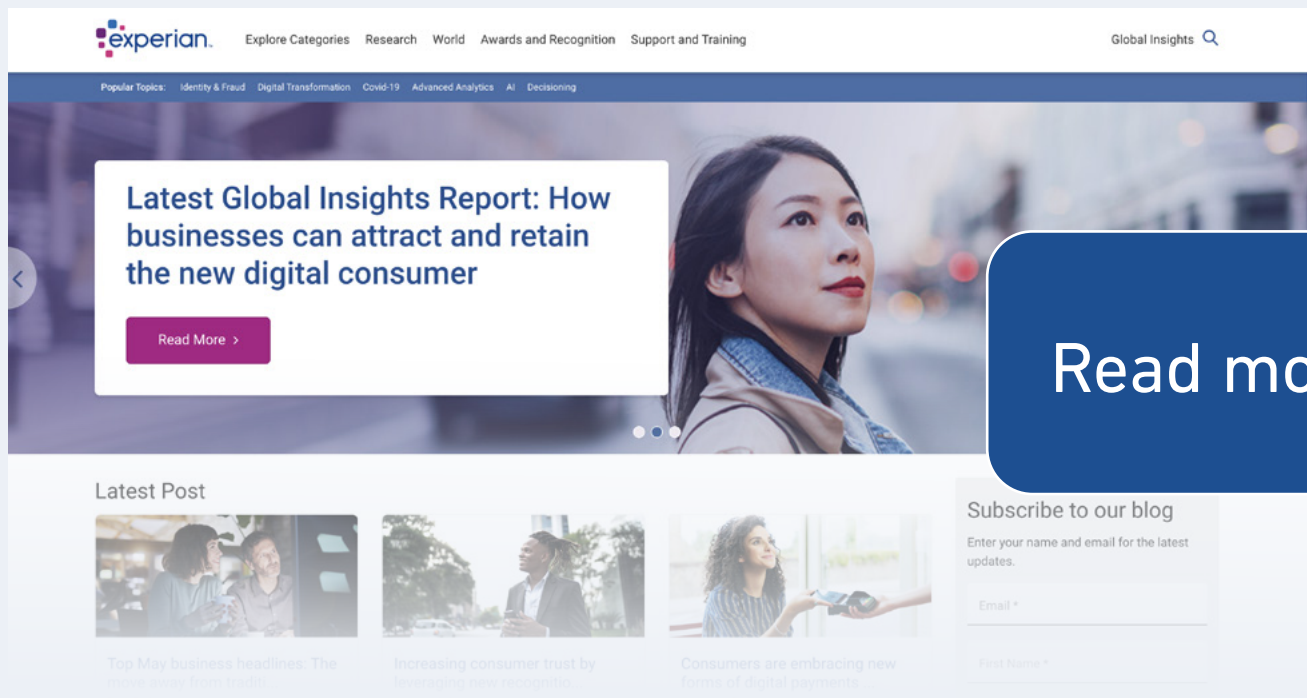
5 Double down on initiatives that build consumer trust

Establishing a track record of accurate recognition and secure online transactions with consumers only increases the depth of the relationship. And the core of the relationship is trust. Elevating your authentication and security efforts demonstrates that your business also values the relationship—and can help preserve it for years to come.



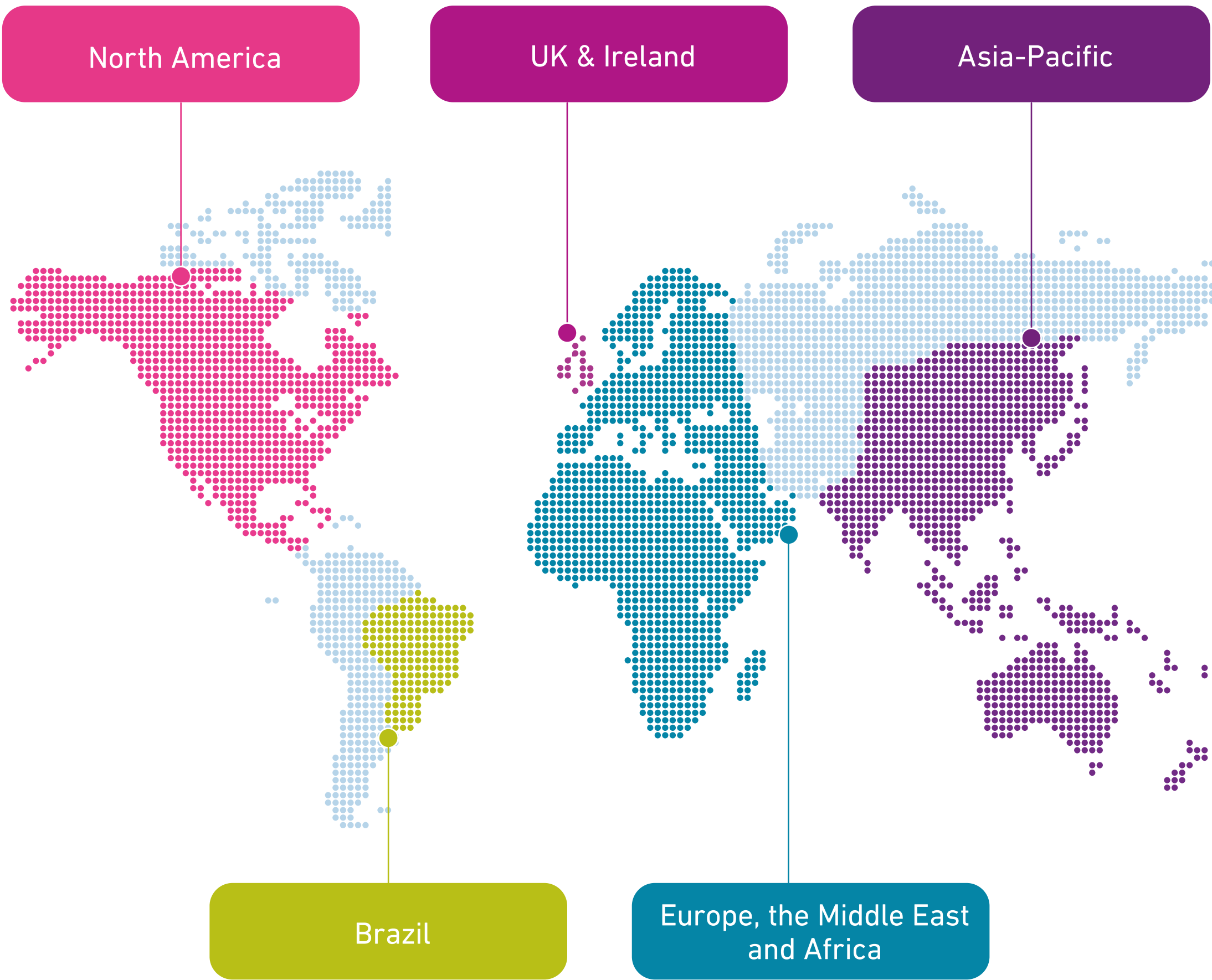
Methodology

From January to March 2022, Experian conducted research among 6,062 consumers ages 18-69 and 1,849 business respondents across the financial services sector, including retail banks, FinTech, credit card network provider, digital banking, to non-financial services businesses in consumer technology, electronics providers, and online and mobile retailers in 20 countries including Australia, Brazil, China, Chile, Colombia, Denmark, Germany, India, Indonesia, Ireland, Italy, Malaysia, The Netherlands, Norway, Peru, Singapore, South Africa, Spain, UK, and US. Findings were further validated through qualitative interviews with consumers from Brazil, Germany, UK, and US. This is the seventh year of the study.



Read more of our global research

Contact us



Executive summary



Fraud concern and activity continue to increase



Consumers keep security top-of-mind



Consumer expectations



Businesses need orchestration solutions



Outsourcing and security knowledge



5 Key Actions



