

Overcoming identity and fraud challenges

Optimise technology and security to build trust and deliver winning online experiences



Experian's annual Identity and Fraud report has always focused on the need to protect customers online – while also improving the speed, quality, and convenience of their online experiences. This year, consumer expectations have increased to new highs, and secure, convenient experiences are now required as standard.

To deliver this, businesses are investing in a **diverse range of latest-generation security and identity technologies**. These include AI and process automation; security technologies such as physical and behavioural biometrics; and a range of other solutions that span ransomware protection, open banking, e-commerce, and authentication.

Despite organisations' investments, however, **fraud losses in the UK increased 22% in 2021, with 90% of those cases originating online¹**.

It's no surprise that **28% of UK consumers have become more concerned about the security of their online activities over the last 12 months**.

This report explores the **concerns, preferences and needs of today's digital consumers with regard to their online experiences**. We also look at the shifting responsibility for online security, with around three-quarters of consumers now expecting brands to protect them against fraud, and companies expecting consumers to also be more proactive in this regard.

There is evidence of a new digital contract, by which consumers are increasingly willing to share their personal data with brands in return for additional value. With security top of mind across all consumer demographics in the UK, we're also seeing that Identity and authentication technologies such as physical and behavioural biometrics engender high levels of trust in customers.

Finally, but equally importantly, the report shows that AI and Machine Learning are now key technologies for online customer identification, authentication, and fraud prevention.

For this reason, AI technology is now an investment priority for 100% of UK businesses.

Key topics for this year's report are:

- > Spotlight on today's digital consumers
- > Which security technologies do UK consumers trust the most?
- > The new digital contract
- > Fighting fraud with diverse security investments



About the Experian research

The 2022 Experian Identity and Fraud Report is based on two major global research surveys. The first asked more than 6,000 consumers across 20 countries – including over 600 respondents in the UK and Ireland – about their online interactions and their expectations with regards to customer experience and security. The second survey was completed by 1,900 organisations globally – including nearly 200 UK and Ireland businesses. Topics ranged from fraud management to identification and authentication of customers, to business strategy and investments in new security and technologies. Organisations surveyed include retail banks, fintech organisations, digital retailers, electronics providers, payment providers, and other verticals.



Introduction



Spotlight on today's digital consumers



Which security technologies do UK consumers trust



The new digital contract



Fighting fraud with diverse security investments



Balancing priorities to create an automated end-to-end identity



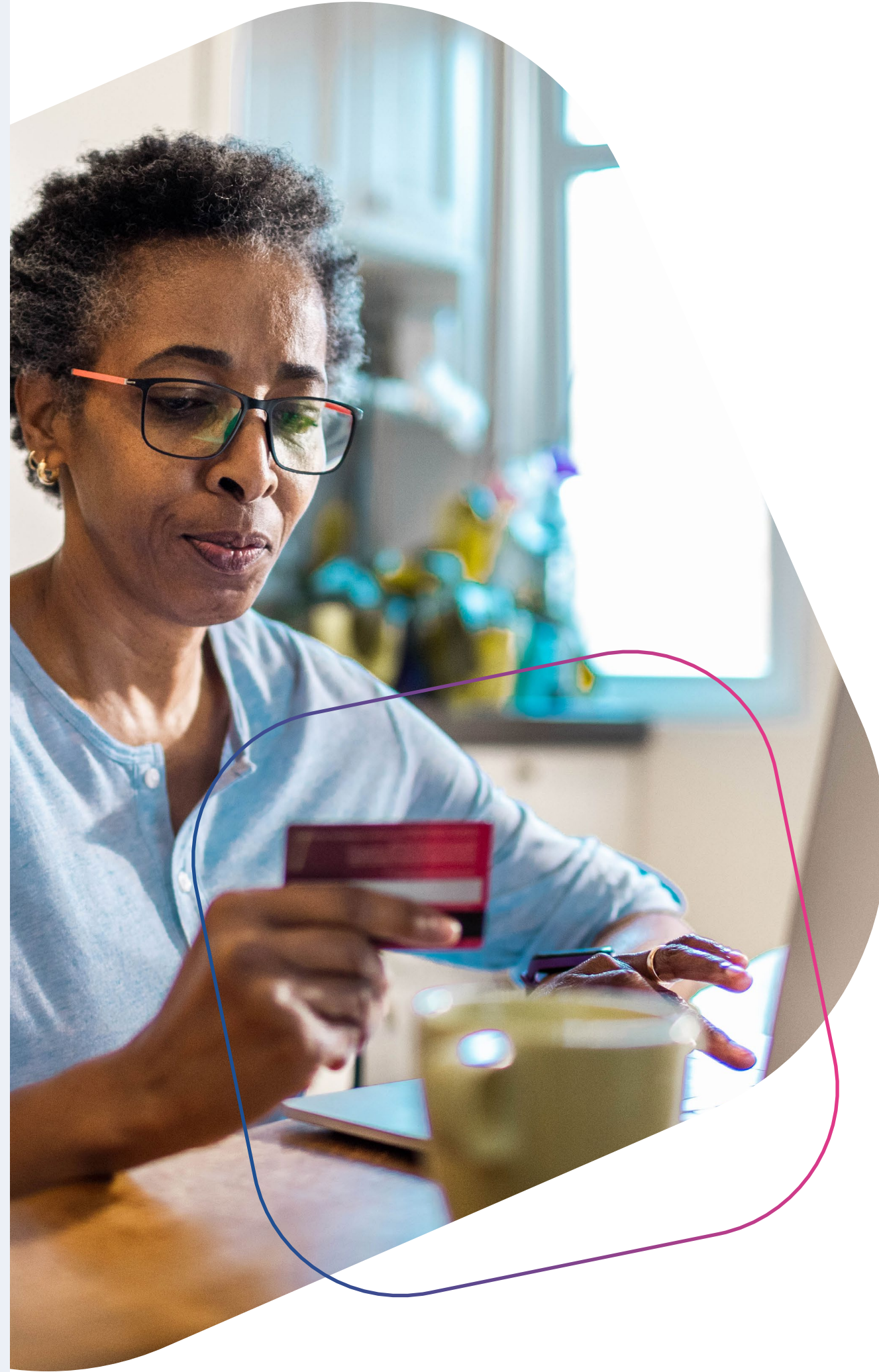
Increase your identity and fraud capabilities



Spotlight on today's digital consumers

Just a few short years ago, UK consumers interacting with businesses online tended to be from younger demographics. Now, accelerated by the pandemic, **people of all ages and all technical skill-levels, including non-digital natives, are accessing goods and services online.**

While increased access to customers via digital channels creates major opportunities for brands, the diversity of customers and their varying levels of comfort with technologies also creates new security challenges. This year's report shows that older demographics are most concerned about online security, while the same consumers may also be slower to accept advanced security technologies such as physical or behavioural biometrics, which are key technologies for improving online security.

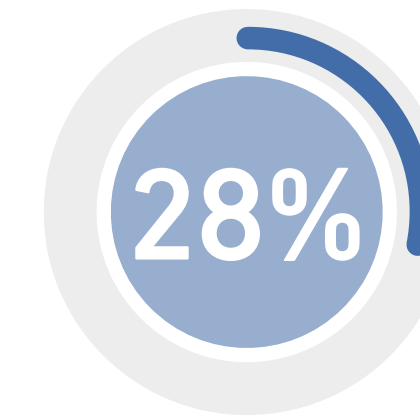


So what do we know about the evolution of digital customers in the UK in 2022?

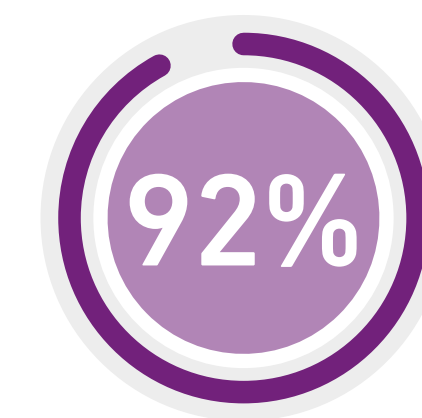


40% of UK consumers have increased their online spending in the last three months

Consumers are spending more across all demographics, with **61%** of high-income households and **63%** of younger consumers increasing their online spending the most.

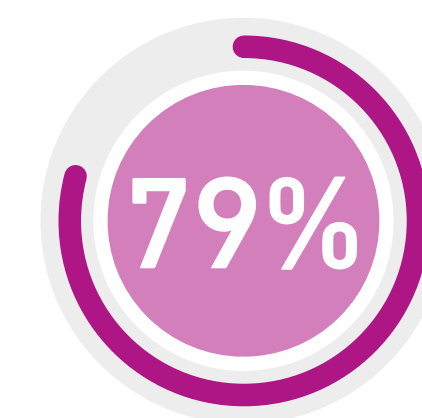


28% say their security concerns have increased in the last 12 months with **64%** citing identity theft as their biggest fear.



92% of UK customers say it is at least somewhat important that organisations they deal with regularly identify them online

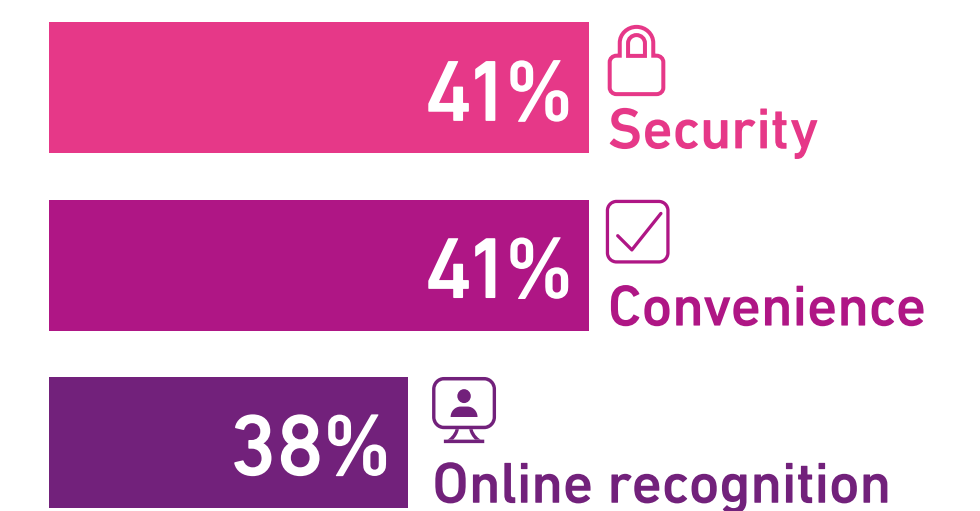
Consumers think organisations should be able to recognise them if they are existing or repeat customers, and authentication should be easier compared to first time interactions and onboarding. However, only a third of consumers are confident that organisations can identify them when they return to a site as a 'repeat' customer.



79% of UK consumers say businesses meet their expectations for digital experience

This is encouraging and shows that 'frictionless' online experiences are now expected and delivered by the majority of organisations.

UK consumers care most about



Introduction



Spotlight on today's digital consumers



Which security technologies do UK consumers trust



The new digital contract



Fighting fraud with diverse security investments



Balancing priorities to create an automated end-to-end identity



Increase your identity and fraud capabilities

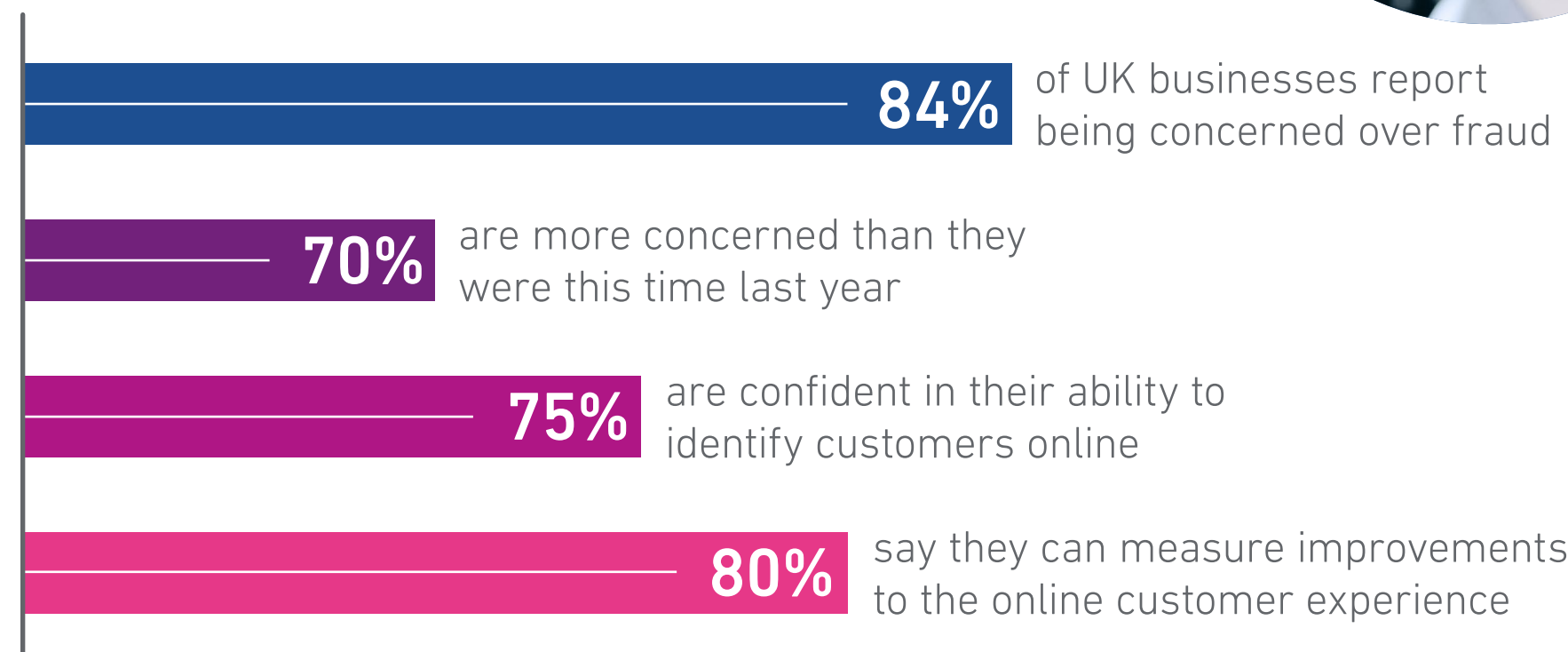


Spotlight on today's digital consumers

Consumer viewpoint

Today's digital customers value security above all else, but also expect to be recognised online for easy access to goods and services. This requires organisations to embed security into the online journey with minimal impact, while also reassuring consumers that they are being adequately protected against identity fraud and other risks that are 'top of mind' for them.

Business viewpoint



This firm foundation for fraud prevention can only be strengthened through closer collaboration with consumers – including data sharing – for increased security and better online experiences.



Experian viewpoint

To maximise security and improve customer experiences simultaneously, organisations and consumers need to work together. This requires providing relevant data at initial onboarding, with the ability to recognise customers on all subsequent visits. As a key part of this process, organisations need to explain, clearly and concisely, why a customer's data is being collected and how it will be used. By collecting only the data needed for online identification and authentication – and taking the measures needed to protect it from end to end – organisations can reduce their exposure to fraud risks, while also streamlining their regulatory compliance.

Who's responsible for online security: businesses or consumers?

Fraud prevention has always been a joint responsibility of businesses and consumers. However, this year's report shows that consumers think businesses should be taking all the necessary measures to protect them online. At the same time, businesses expect consumers to do their bit in terms of safeguarding their data and accessing sites and services securely.

- **64%** of consumers expect businesses to take the necessary security steps to protect them online
- **69%** of businesses say customers should be doing more to protect themselves online
- **37%** of consumers are concerned about the safety of conducting activities online



Which security technologies do UK consumers trust the most?

There is no one size fits all approach when it comes to secure online technologies. Preferences tend to depend on age and demographics, but also on consumers' digital skills and comfort level with different security, authentication and payment technologies. However, many technologies used to protect consumers online are reaching new levels of maturity and are also achieving new levels of acceptance among end users. In fact, **companies that use advanced security technologies are trusted more by consumers.**



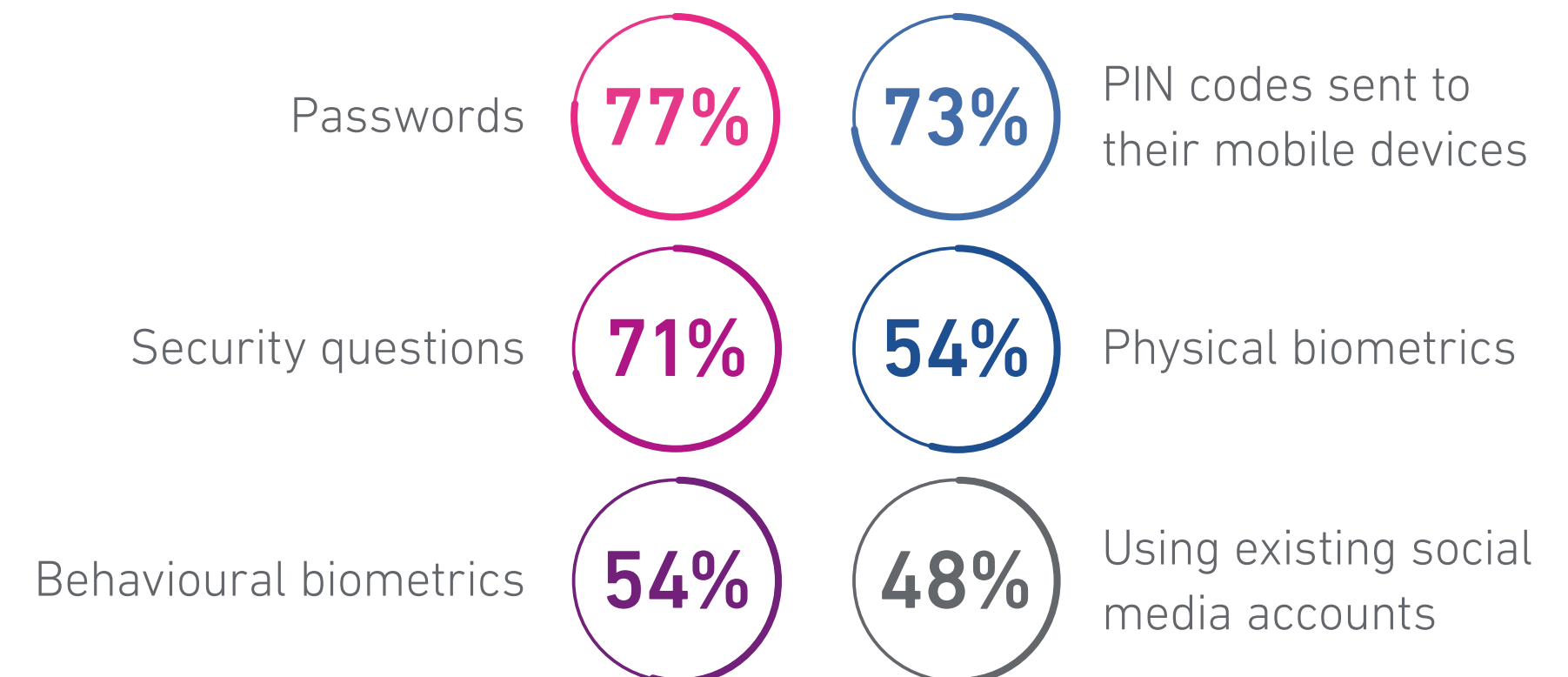
In terms of preferences among different consumer demographics, **higher-income consumers** tend to trust security questions to a greater extent than consumers with lower incomes. Higher-income groups also think more highly of businesses that use **multiple authentication methods.**

Regarding generational differences, Baby Boomers tend to feel more secure with physical and behavioural biometrics than their younger counterparts.

Consumer viewpoint

When it comes to delivering a secure online experience, consumers have most confidence in PIN codes and physical and behavioural biometrics. Physical biometrics is the authentication method that most strongly enhances the view of consumers' opinion of a business, with PIN codes and behavioural biometrics following closely behind.

Consumers think that the authentication methods that deliver the 'best customer experience' are



83% of UK businesses agree that improvements in identifying consumers online will help mitigate the impact of fraud on the business

☞☞ This shows that trust in advanced authentication technologies is growing among consumers from all demographics. With no clear preference among consumers for a single authentication technology, organisations are investing in multiple tools. However, all solutions in the authentication strategy must be seamlessly integrated and orchestrated across processes and channels to avoid silos and security loopholes that could be exploited by fraudsters.

Traci Krepper, Head of Product and Portfolio Marketing, Experian UK&I



Introduction



Spotlight on today's digital consumers



Which security technologies do UK consumers trust



The new digital contract



Fighting fraud with diverse security investments



Balancing priorities to create an automated end-to-end identity



Increase your identity and fraud capabilities

Which security technologies do UK consumers trust the most?

Business viewpoint

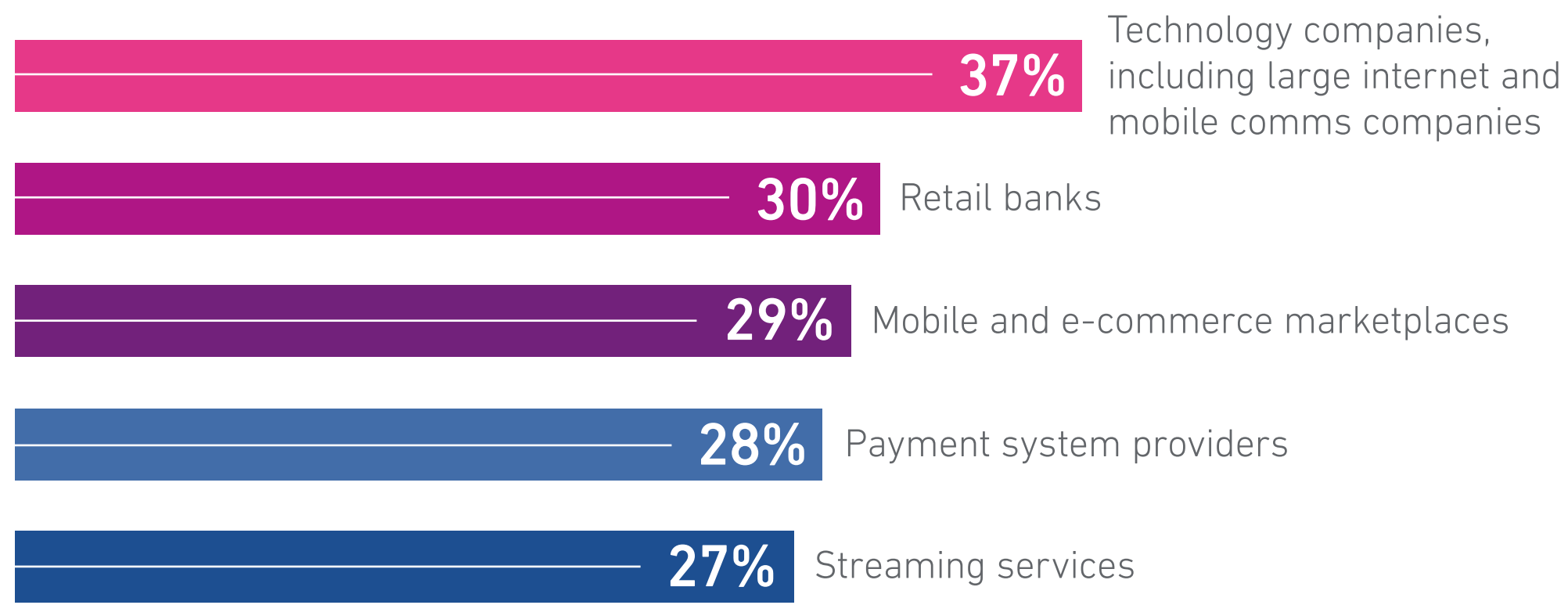


of UK businesses are confident in two-factor (or multi-factor) authentication for securely identifying customers online.

This is closely followed by know your customer (KYC) measures, PIN codes, and the use of security questions and passwords. Consumer confidence in physical biometrics and other advanced security and identity solutions is growing rapidly and have become a priority investment area for businesses.




Top 5 most trusted organisations for protecting consumers online are





Experian viewpoint

Trust in advanced authentication technologies is growing among consumers from all demographics. With no clear preference among consumers for a single authentication technology, organisations are investing in multiple tools. However, all solutions in the authentication strategy must be seamlessly integrated and orchestrated across processes and channels to avoid silos and security loopholes that could be exploited by fraudsters.

To meet consumers' demands for safe, convenient online experiences, UK businesses are investing in technologies such as:

 Device-in-hand solutions that use one-time passcodes or push notifications
20%

 Physical biometrics, including fingerprint, facial or voice recognition or retina scanning
13%

 Two-factor or multi-factor authentication
9%



Introduction



Spotlight on today's digital consumers



Which security technologies do UK consumers trust



The new digital contract



Fighting fraud with diverse security investments



Balancing priorities to create an automated end-to-end identity



Increase your identity and fraud capabilities



The new digital contract: consumers are willing to exchange their data for more value

Not long ago, few consumers were aware of how their data was captured and used by organisations – and even fewer understood the value of data for improving security and customer experiences.

Today, that's changing slowly..



68%

of consumers now understand that sharing their data can increase security



67%

understand the value in terms of accessing more convenient online experiences

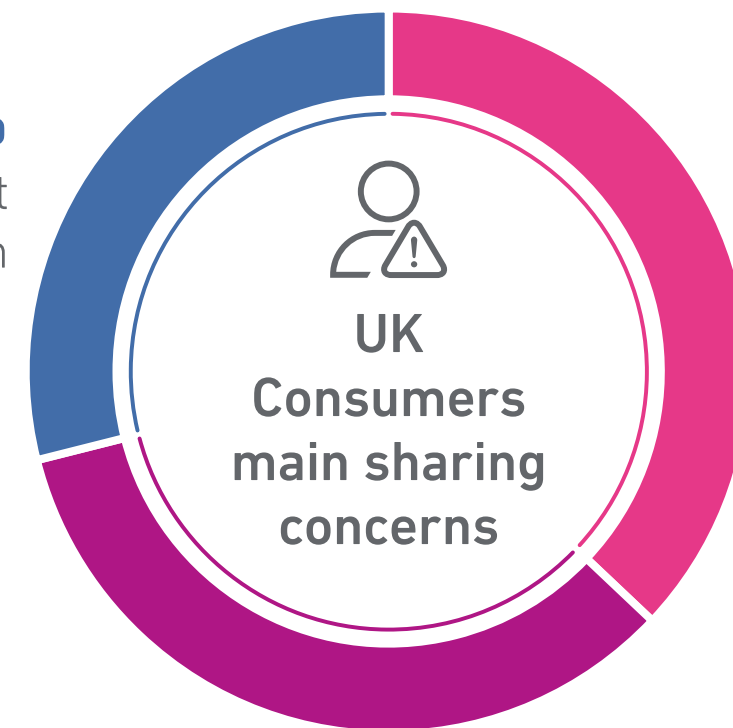
But despite increasing awareness around the value of data sharing, most consumers are still concerned about sharing their personal data with organisations.

In general, customer segments most concerned about sharing their data are higher-income consumers, and the over 40s, who are often the same customers.



of UK consumers are **willing** to share their personal data with organisations in return for the right benefits and value.

57%
Contact information



73%
Financial data

67%
Name and date of birth

Consumer viewpoint

Interestingly, consumers are **no more willing** to share data with organisations they deal with regularly. Instead, customers are **most willing** to share their data if the 'value exchange' is clear and compelling enough – irrespective of whether they are a regular customer or not.

Business viewpoint

The fact that over **60%** of consumers in the UK are willing to share their personal data with organisations shows the enormous opportunity to learn more about customers and to create personalised offers and services that **improve commercial outcomes**. This can be achieved with **clear, concise communication** on how customers' data is being collected, used and protected, and – critically – **how customers can benefit**.



Introduction



Spotlight on today's digital consumers



Which security technologies do UK consumers trust



The new digital contract



Fighting fraud with diverse security investments



Balancing priorities to create an automated end-to-end identity



Increase your identity and fraud capabilities



The new digital contract: consumers are willing to exchange their data for more value

Experian viewpoint

By asking for appropriate data for the interaction at hand, rather than engaging in excessive and non-relevant data capture, organisations can form **closer, more value-based relationships** with customers. Companies can also access **new, data-driven insights** that improve a wide range of processes and outcomes, from new product development to more effective, personalised marketing. The key to achieving this is to work with partners who can **convert customer data into actionable insights**, and combine it with external data sources for even more context and business value.



The most trusted organisations for protecting and securing personal data

The research shows that the top five most trusted organisations in the UK for **securing and protecting customers' personal data** are:



Introduction



Spotlight on today's
digital consumers



Which security
technologies do UK
consumers trust



The new
digital contract



Fighting fraud with
diverse security
investments



Balancing priorities to
create an automated
end-to-end identity



Increase your
identity and fraud
capabilities

Fighting fraud with diverse security investments



Consumers now expect **faster, better, more secure experiences** across a wide range of interactions and transactions. Additionally, they are more comfortable than ever when it comes to using a wide range of **advanced security and authentication technologies**.

In view of these trends, organisations have recognised that no single technology is able to cover all the bases in terms of improving security and customer experience. For this reason, we are seeing multi-lateral investments in a **wide range of solutions** as the fraud landscape becomes increasingly complex and challenging.

Projected investments are increasingly focused on **transformative technologies**, such as AI and automated decisioning processes, which stand to automate and optimise security and fraud-prevention activities. This focus on automation is especially relevant in terms of **faster, more effective decisioning**.

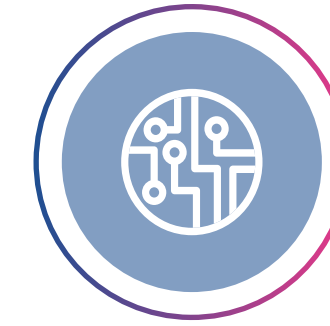


The challenge of fraud detection is that **more than 99%** of applications and attempts to access sites and services are genuine. This inevitably leads to unnecessary investigation of genuine applicants – which increases admin costs and disrupts the customer experience. The great strength of AI is the ability to automate identity management and authentication to a much greater degree, keeping applications out of manual review queues to reduce operating costs, and ensuring that all genuine customers get faster, better, more secure service.

Eduardo Castro, Managing Director, Experian Identity and Fraud, UK&I.

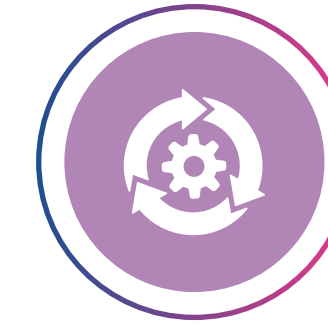


The four top investment priorities for UK&I businesses in the fields of security, fraud prevention, authentication/identity management and online customer experience are:



Building new AI models to improve customer decisions

UK	Ireland
14%	4%



Automation of business processes (including fraud decisions)

UK	Ireland
13%	9%



Strengthening the security of mobile channels

UK	Ireland
13%	9%



Improving fraud detection/prevention

UK	Ireland
10%	7%



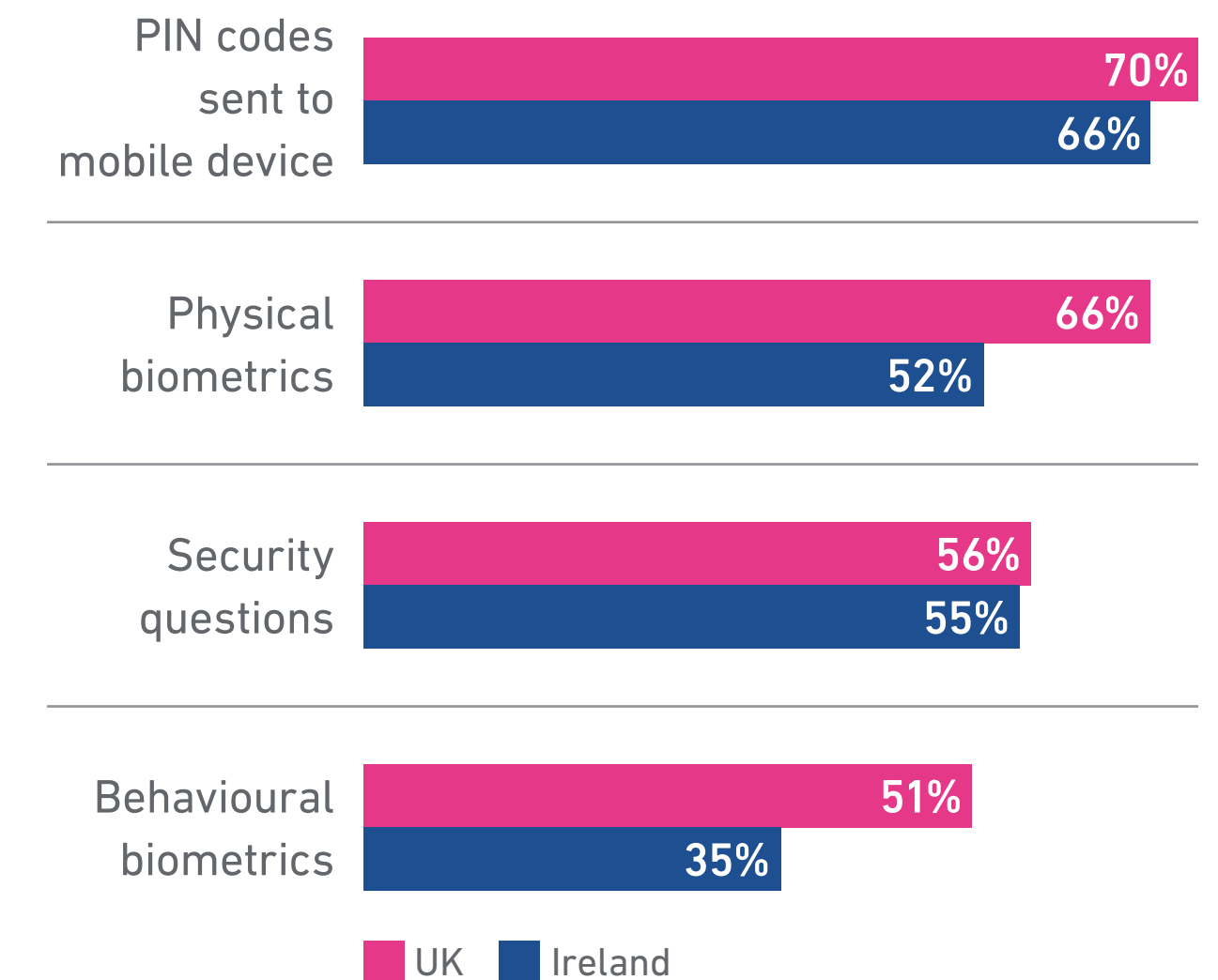
Consumer viewpoint

Consumers now use and trust a wide range of security and authentication methods, with only small variations in the experience they report. For example, many favour **PIN codes** sent to their mobile devices for security, but physical biometrics, behavioural biometrics and security questions are also highly rated.

This increasing acceptance of a wide variety of authentication and security solutions is a **key driver for organisations' multi-lateral investment strategies**.



UK&I most used and trusted security and authentication methods



Introduction



Spotlight on today's digital consumers



Which security technologies do UK consumers trust



The new digital contract



Fighting fraud with diverse security investments



Balancing priorities to create an automated end-to-end identity



Increase your identity and fraud capabilities

Fighting fraud with diverse security investments

Business viewpoint

The sophistication of the fraud landscape, demands for frictionless online experiences, and organisations' varying risk appetites mean that there is no single, silver-bullet solution for security and fraud prevention. However, organisations are making very **significant investments** in areas that are **vital for security**.

Experian viewpoint

While investments in a wide variety of identity and fraud-prevention solutions is healthy and appropriate, there has to be a way to bring security solutions together to minimise the risk of loopholes and to ensure that an **organisation's 'attack surface' is as small as possible**. This requires orchestration that integrates **multiple security measures** and provides **integrity and efficiency** from end-to-end.



AI is coming of age in the fight against fraud



of UK businesses identified AI as a key target for investment

This is not surprising considering that the technology offers major opportunities to improve security based on **faster, more accurate customer identification and authentication**. AI is also almost universally seen as **important for improving customers' online experiences** by companies in the UK and Ireland.

Consumers are also becoming far **more aware of the use of AI**, and a majority of consumers trust organisations who use AI to **reduce fraud and improve their experiences online**.



60% of consumers trust organisations who use AI

However, there are also limiting factors to the implementation/adoption of AI, as many organisations (even large retail banks and other large organisations) **lack the skills and experience** needed to develop and deploy AI models that help to improve their ability to identify and protect customers online. This, in part, explains the **significant growth in outsourcing to drive transformation projects** – and particularly AI projects – outlined in the following section.



Introduction



Spotlight on today's digital consumers



Which security technologies do UK consumers trust



The new digital contract



Fighting fraud with diverse security investments



Balancing priorities to create an automated end-to-end identity



Increase your identity and fraud capabilities

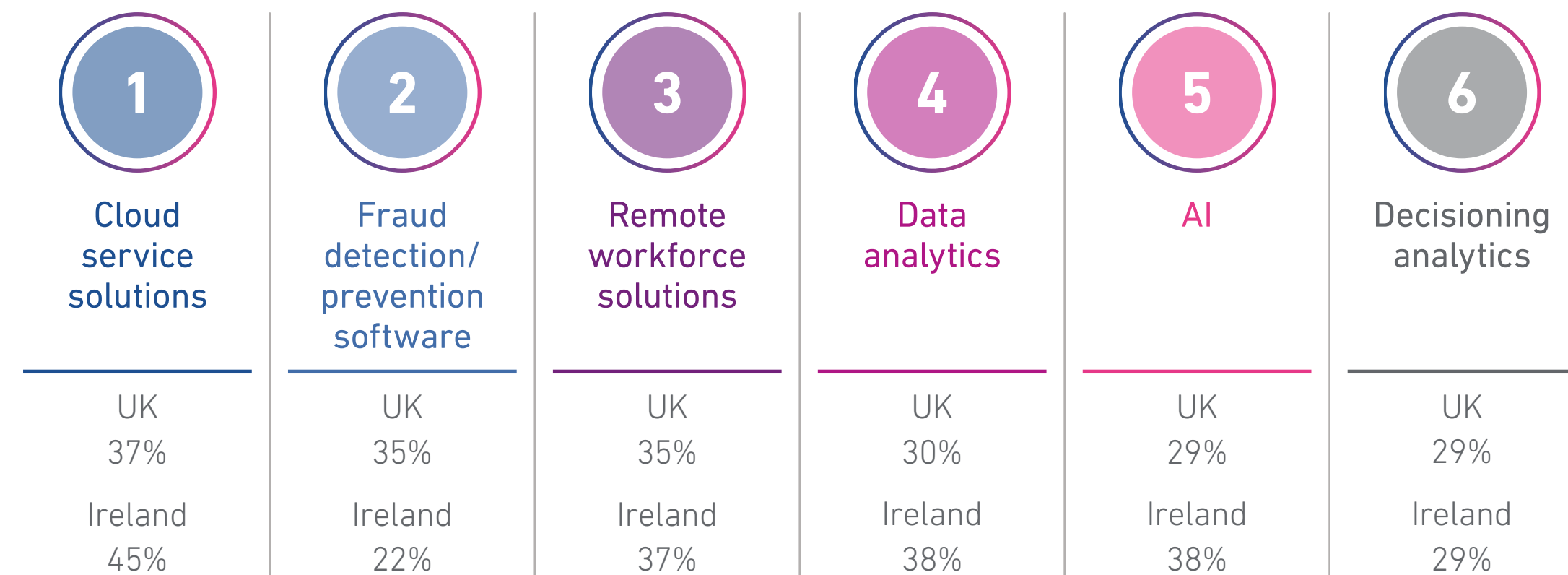


Fighting fraud with diverse security investments

Filling the innovation skills gap: outsourcing on the rise

Adapting to the fast-evolving fraud landscape requires **rapid technology innovation** and **sustained investment**. To keep pace with the demand for new solutions, **70%** of companies in the UK and Ireland are either currently outsourcing specialised areas of their business or have the intention to do so. Areas being outsourced include a range of digital innovation and transformation projects, including AI and machine learning model development.

The areas most likely to be outsourced by UK and Ireland businesses are:



While outsourcing is helping organisations bridge the skills gap for digital projects, there is a risk that siloed development could result in **security loopholes** and **increased fraud risks**.

To mitigate the potential risks of outsourcing critical security functions and development work, proper oversight and governance is needed across the full range of outsourced activities.



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

Here are five tips from Experian's identity and fraud prevention experts for strengthening your digital capabilities for detecting and preventing fraud, and for delivering even better customer experiences.



1 Revisit the end goal for your 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 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 your online customers

Online is the new normal, and people of all ages, incomes, and regions are transacting digitally. However, no two digital customers are the same. Dive into the demographics of your customer base to understand their expectations and comfort levels 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 creates the potential for a poor customer experience, while also increasing the risk of fraud attacks. Take advantage of a single platform that can bring all your tools and data sources together, allowing you to mitigate fraud 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 increases the depth of the relationship; and the core of that relationship is trust. Elevating your authentication and security efforts in light of the continued onslaught demonstrates that your business also values the relationship – and can help preserve it for years to come.



Increase your identity and fraud capabilities with Experian

Organisations of all sizes, spanning multiple industries, work with Experian to **maximise their fraud prevention capabilities** and to **create more frictionless customer experiences**. In particular, our [CrossCore platform](#) can help you bring together a range of fraud, Identity and authentication solutions to drive security and customer experience KPIs.

How Experian can help

Real-time analytics and fraud detection

When it comes to making fast, accurate decisions on credit risk, fraud and identity management, technology and analytics play a central role. Combating fraud relies on incorporating continuous authentication and advanced recognition into your decision-making strategy.

Experian has a proven track record in delivering solutions to protect businesses and their customers. We can help you build trusted relationships with legitimate customers at every touchpoint, with solutions that address risk and provide safeguards at every stage of the customer journey across industries. Whether you're looking for fraud prevention, age verification, online identity checks or a host of other solutions to keep fraudsters at bay, we have the complete future-proof solution.

- > We can help you detect, and prevent fraud across products, devices and channels.
- > Our analytical, data-ready tools can provide actionable insight that can be seamlessly connected into existing processes.
- > Our continuous investment in innovation and partnerships, means we can provide fast access to the latest tools and techniques.

CrossCore™:

Your complete fraud and identity management platform

Using a flexible and scalable API with powerful workflow and decisioning functions, CrossCore™ allows you to connect, access and orchestrate decisions across multiple systems. Machine learning techniques create decision-making models and monitor performance for continuous improvement – providing a frictionless, secure customer experience while reducing time and costs.

The CrossCore™ platform makes it fast and easy for businesses to access fraud and identity services. Enabled by the cloud, firms can benefit from easy integration of multiple use cases relating to fraud and identity tasks.

Including:



Account takeover

Complete defence package, enabling you to continuously monitor customer accounts across all interactions.



Age verification

Unique capability allowing businesses selling age restricted goods or age-threshold services to authenticate customer age.



Digital onboarding

Accurate and automated identity checks, reducing manual processes and streamlining the customer journey.



Device intelligence

Create trusted profiles that recognise customers' devices and associated attributes to identify suspicious device activity.



Account opening

Increase fraud detection rates whilst generating less referrals, enabling you to onboard good customers and keep fraudsters out.

To find out more about our capabilities in this area, please contact us:

T: 0844 481 9920

E: businessuk@experian.com

W: www.experian.co.uk/business/regulation-and-fraud



