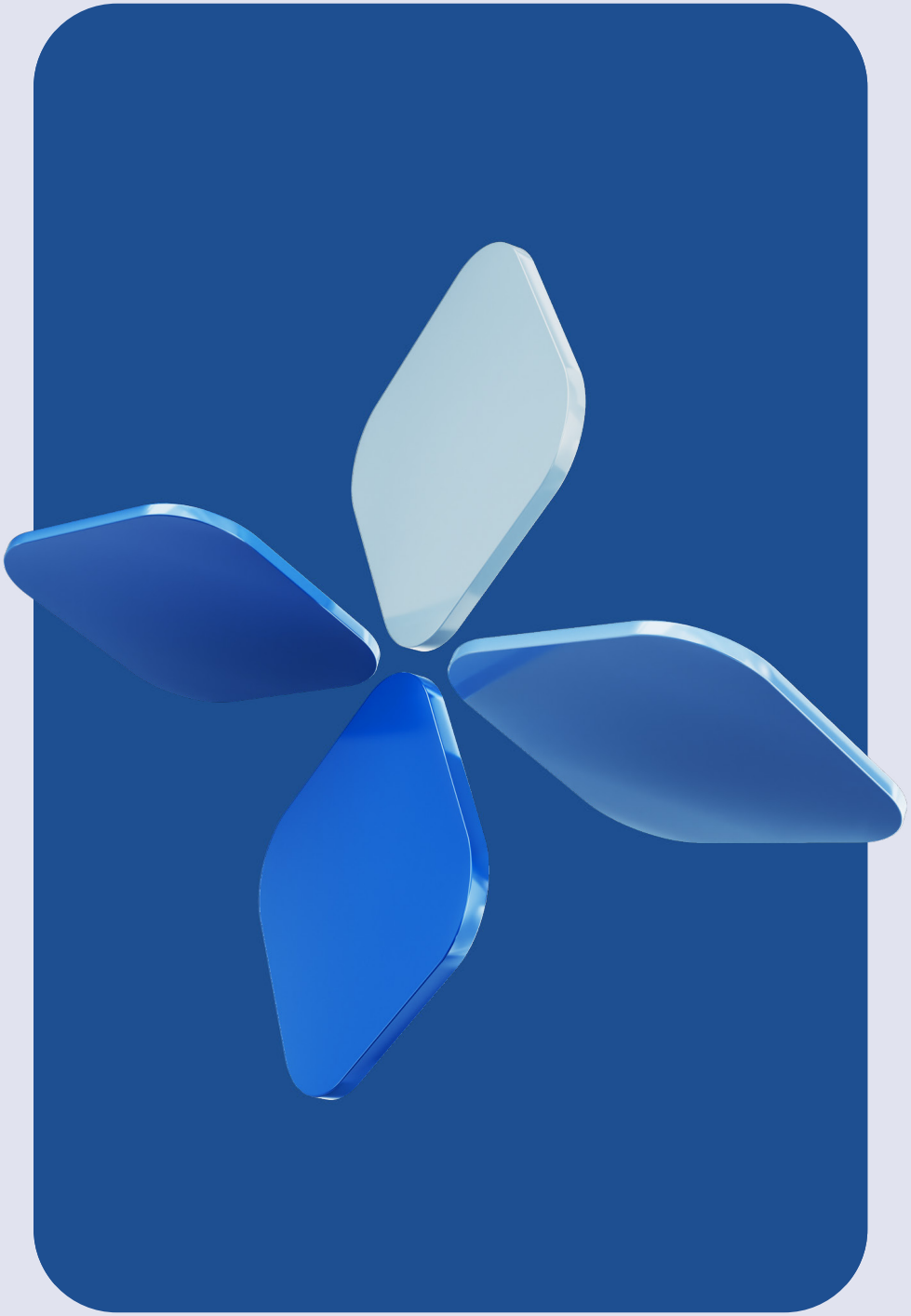
experian

Fraud in the Age of AI: Identity, Risk and Consumer Behaviour

Contents

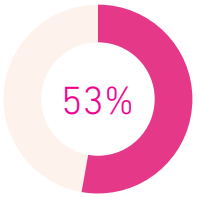


Executive summary

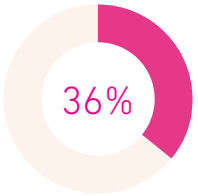
Fraud is evolving at unprecedented speed, driven by organised cybercrime networks, automation, and GenAI-powered attack methods. At the same time, digital adoption across banking, telco and e-commerce sectors has expanded the attack surface, placing identity at the centre of security risk.

Fraud in the Age of AI: Identity, Risk and Consumer Behaviour combines research conducted amongst Australian and New Zealand consumers with insights from decision-makers responsible for fraud across key industries and analysis of emerging fraud and AI-enabled threats.

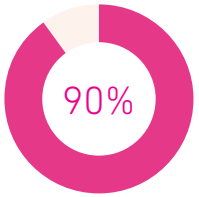
The purpose is to help organisations and consumers understand the changing fraud landscape and what protection requires in the AI era.



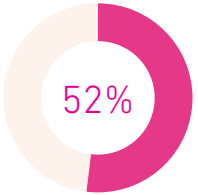
53% of consumers across Australia and New Zealand have experienced fraud, with card fraud, purchase scams and social media scams being the most common



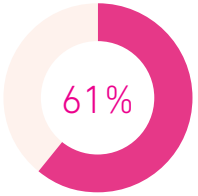
36% of respondents have experienced identity theft or account takeover, with nearly 1 in 3 fraud victims reporting diminished trust in digital platforms



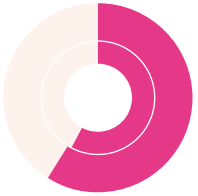
90% of Australian and New Zealand consumers are concerned about someone stealing their identity and using it to commit fraud online



52% of consumers report having abandoned an online sign-up or verification process because it felt too intrusive



61% of fraud decision-makers identify AI generated fraud as the greatest future threat



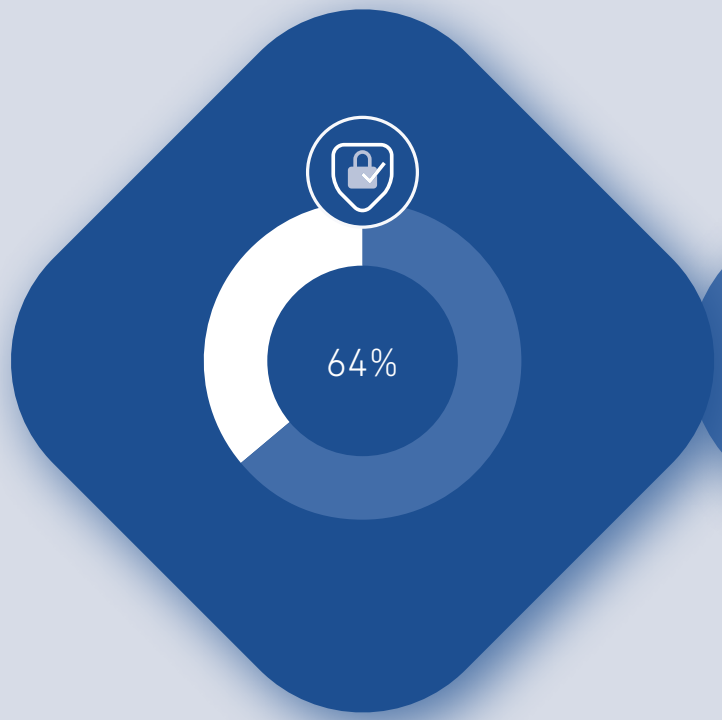
Fraud decision makers in Australia **(59%)** and New Zealand **(58%)** state their existing Know Your Customer (KYC) and identity verification checks are not equipped to detect GenAI-generated documents

The new fraud landscape

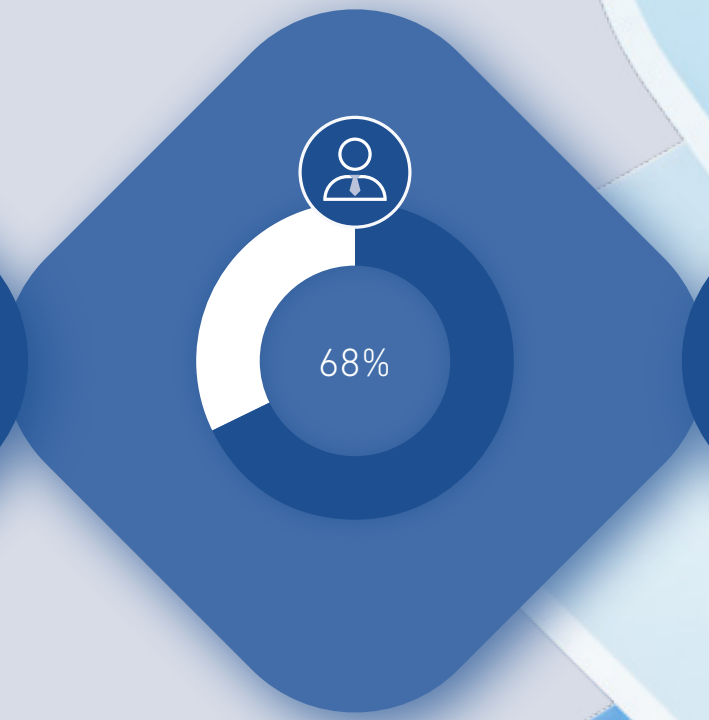
Fraud is becoming more complex, organised and technologically sophisticated and it's having a negative impact on organisations. Nearly two-thirds (64%) of businesses report a surge in fraud-related losses over the past year, with 68% of business leaders admitting that their current security tools are no longer robust enough to combat increasingly sophisticated fraud and identity theft attempts.

AI technologies are central to this shift. Deepfakes and AI-generated identities enable fraudsters to impersonate individuals and bypass traditional security measures. Fraudsters also exploit dark web AI tools to create synthetic identities, making it harder to distinguish between legitimate transactions and fraud. According to Experian research conducted by Forrester Consulting, 61% of fraud decision-makers identify AI-driven fraud as the greatest future threat.

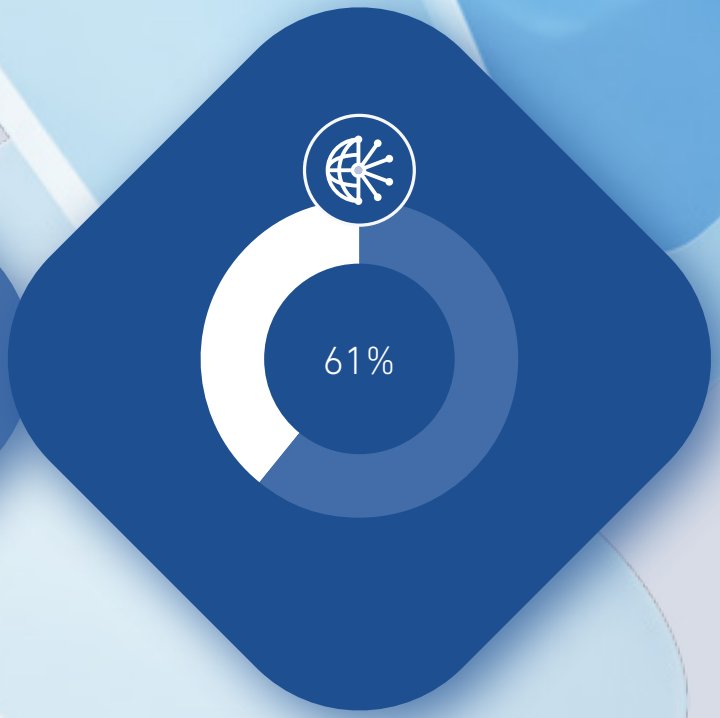
How fraud is impacting business



of businesses reported a surge in fraud-related losses over the past year



of business leaders admit that their current security tools are no longer adequate



of fraud decision-makers identify AI-driven fraud as the greatest future threat

Identity: The new security perimeter

With the rise of AI-powered fraud, traditional fraud detection methods are being put under increasing pressure. Fraud decision makers in Australia (59%) and New Zealand (58%) state their existing KYC and identity verification checks are not equipped to detect GenAI-generated documents. This gap between evolving fraud techniques and existing verification systems is increasing the risk of identity compromise for both organisations and their customers. Consumer led research highlights this growing challenge: 36% of respondents have experienced identity theft or account takeovers, and nearly 1 in 3 fraud victims report reduced trust in online services. As digital interactions increase, protecting identities has become fundamental to maintaining consumer confidence.

Securing digital identities

To address these evolving threats, businesses need robust and user-friendly identity verification solutions that can verify customer identities in real time while maintaining seamless digital experiences. Key protection solutions include:

Biometric verification
(e.g. facial recognition)

Device fingerprinting and
device intelligence

Document authentication

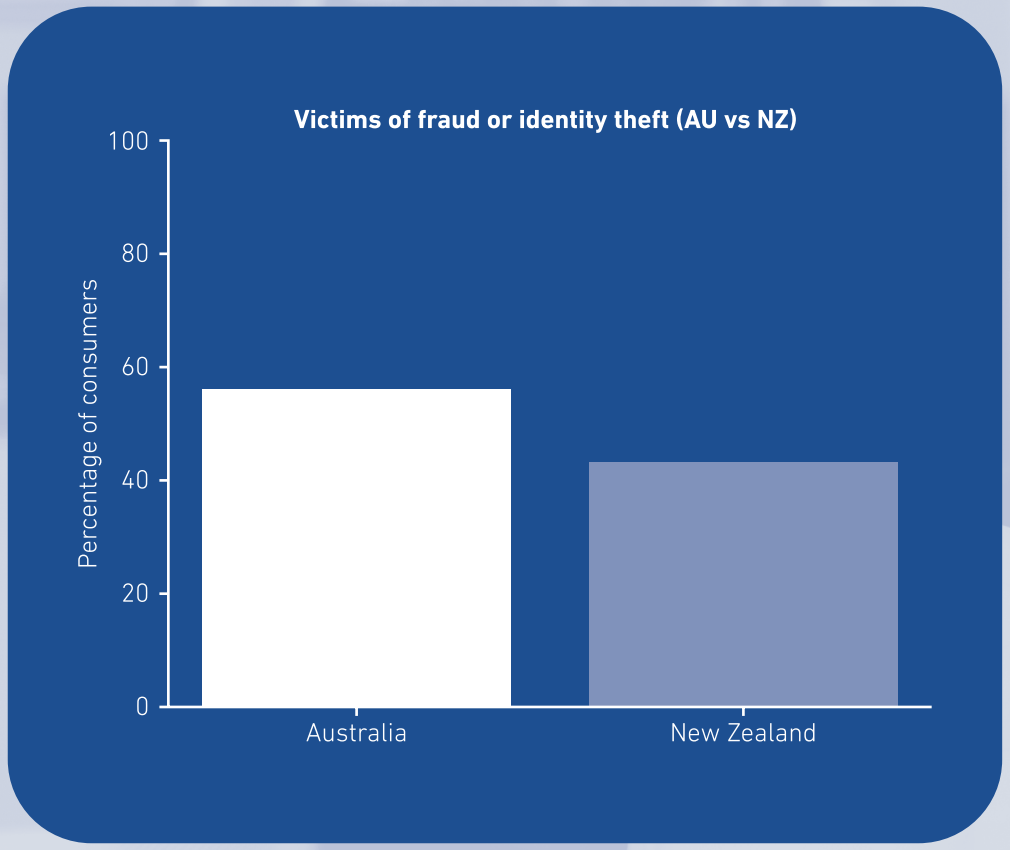
Identity verification

Combining AI, identity data and advanced analytics strengthens fraud detection while minimising friction for legitimate customers.

Consumer reality: Fraud in everyday life

Fraud is no longer an abstract risk for consumers across Australia and New Zealand - 90% say they are concerned about someone stealing their identity and using it to commit fraud online, highlighting how fraud anxiety has become embedded in everyday digital behaviour.

Across Australia and New Zealand, more than half of respondents (52%) report experiencing fraud or identity theft. The frequency is notably higher in Australia, where 56% report becoming victim, compared with 43% in New Zealand.



Consumer snapshot: The cautious digital consumer

Sarah, 34, represents a growing group of digitally active consumers who rely heavily on online banking, shopping and mobile apps, but feel increasingly exposed to scams and fraud.

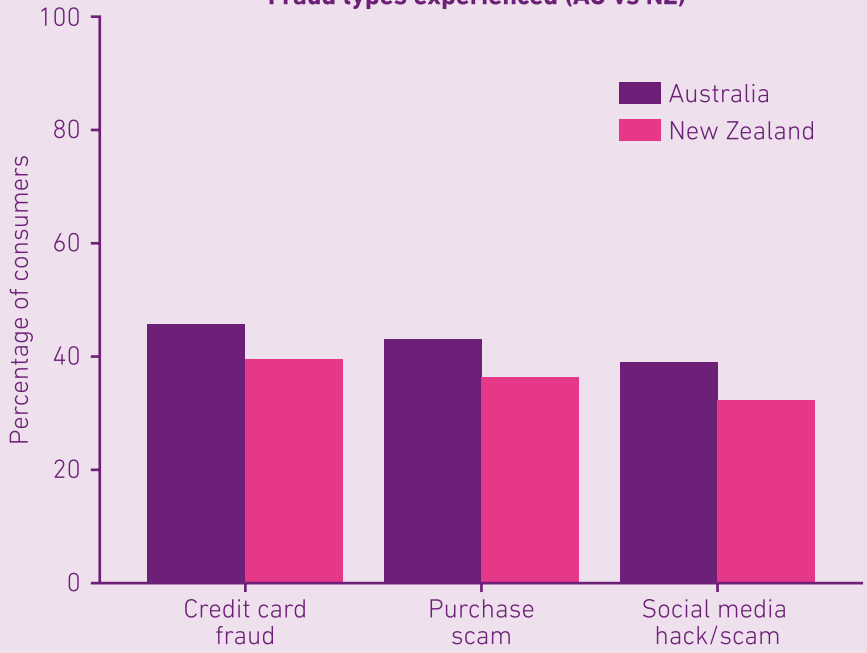
Recently, she received a convincing delivery-scam text and has had multiple login attempts flagged on her bank account. Experiences like these are becoming more common, which helps explain why 9 in 10 consumers across Australia and New Zealand say they are worried about identity theft.

While Sarah takes steps to protect herself, enabling fraud alerts and real-time notifications, navigating digital security can feel overwhelming. Like many consumers, she avoids sign-ups that feel intrusive and sometimes reuses passwords because stronger security measures feel difficult to manage.

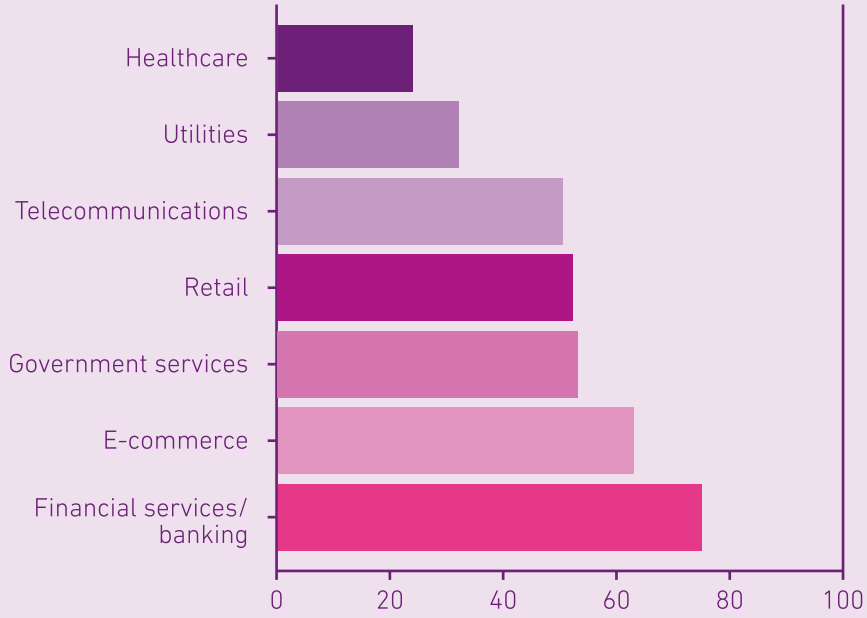
These concerns are also changing how she behaves online. She has abandoned online purchases when something feels suspicious and is increasingly cautious about apps requesting document uploads or biometric verification.

For consumers like Sarah, trust in digital services is becoming more conditional. What they expect from businesses is clear: transparent explanations of how personal data is used, simple and secure verification processes, and fraud protection that works seamlessly in the background without creating unnecessary friction.

Fraud types experienced (AU vs NZ)



Sectors where consumers report encountering fraud (AU + NZ)



What's really hitting consumers? The fraud threats shaping everyday life

Across Australia and New Zealand, consumers are encountering a wide range of fraud types as scams and identity-based attacks become increasingly common.

The most common fraud types across Australia & New Zealand include:

40% report experiencing credit card fraud

40% report hacks or scams on their social media accounts

39% report purchase scams

Some differences also emerge between markets. Credit card fraud is reported by 42% of consumers in Australia, compared with 36% in New Zealand.

Fraud hotspots across everyday services

Fraud also spans multiple sectors. Across Australia and New Zealand, financial services and banking are the sectors where consumers most often report fraud (74%), followed by e-commerce platforms (63%) and government services (53%).

Other sectors where fraud is commonly reported include:

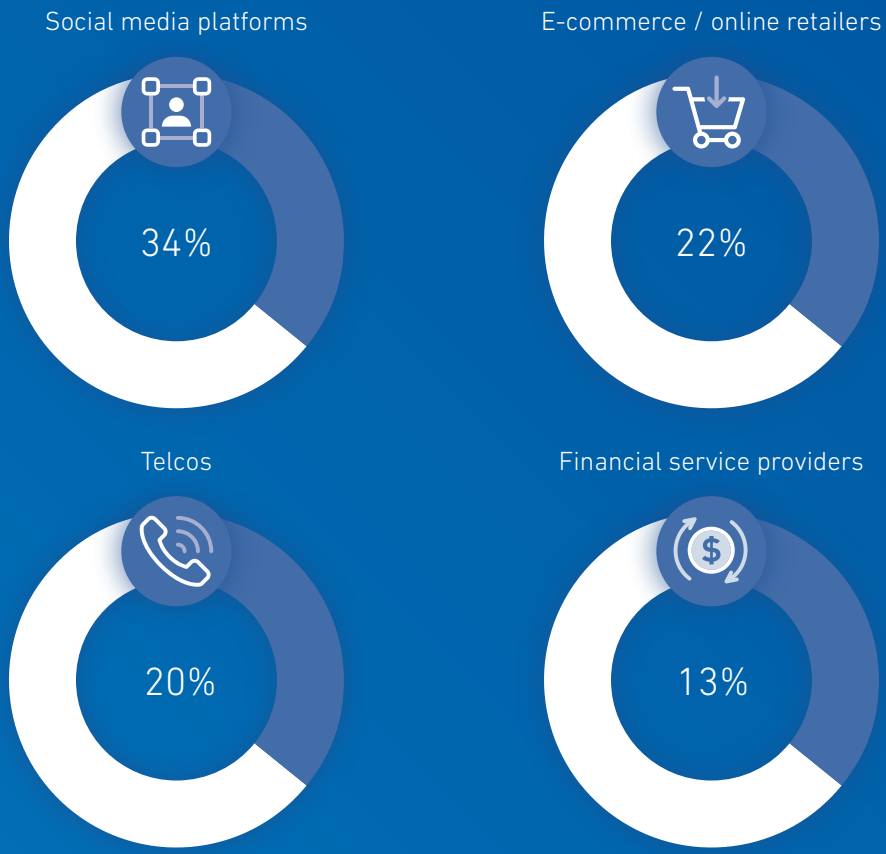
Retail	Telco	Utilities	Healthcare
52%	50%	32%	24%

How is fraud changing trust and behaviour?

Fraud doesn't just cause financial loss; it also erodes confidence in online purchasing capabilities. Social media platforms appear most distrusted, with 34% of consumers across Australia and New Zealand reporting that their trust has declined due to fraud concerns. This is followed by e-commerce / online retailers (22%), telco providers (20%), and financial service providers (13%).

More broadly, 1 in 3 say that experiencing fraud significantly reduced their trust in online services overall, highlighting the wider reputational impact fraud can have on digital platforms and transactions.

Most distrusted digital services due to worries about fraud or identity theft



How consumers are currently defending their identity:

As fraud risk grows, consumers are increasingly turning to tools that help them monitor and protect their identities. According to research, 54% of consumers use real-time notifications, and 40% set up fraud alerts to monitor activity on their accounts. These tools are viewed as essential for giving consumers more control over their personal information. However, nearly a third of consumers are dissatisfied with these tools, indicating a need for ongoing improvement and better education on how to use these tools effectively.

Consumers rely on alerts and monitoring tools to feel in control; however businesses must ensure these tools are effective, easy to use, and capable of providing accurate alerts to protect consumers from emerging fraud risks.

AI, deepfakes and the next fraud frontier

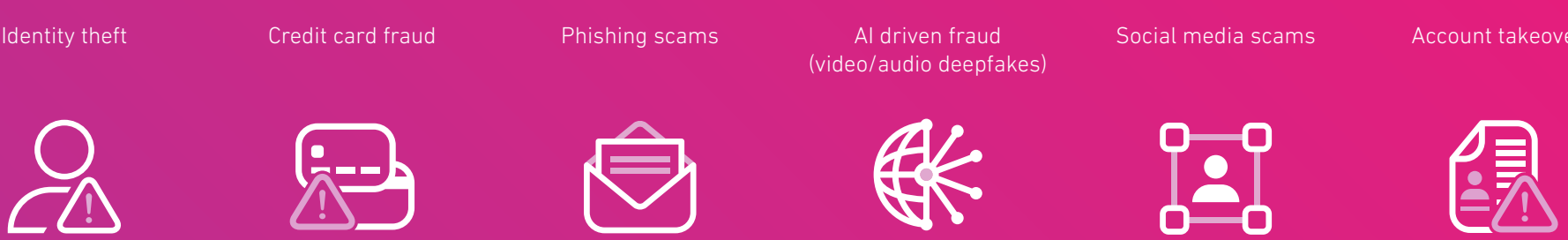
AI is rapidly becoming both a tool for fraudsters and a key line of defence in the fight against digital fraud. While AI-powered technologies are enabling fraudsters to carry out increasingly sophisticated fraud attacks, AI is also helping businesses improve fraud detection capabilities.

The AI threat: Deepfakes and synthetic identities

AI's ability to create deepfakes – manipulated audio, video and images that convincingly mimic real people – has become a significant risk for businesses. Consumers are also increasingly worried about the potential for AI-powered fraud.

In our research, AI-driven fraud, including deepfakes and synthetic identities, was highlighted as a major concern for consumers, particularly in relation to identity theft and account takeovers. When asked about the most worrying types of fraud, identity theft (e.g. stolen personal details) was ranked as the most concerning, followed closely by credit card fraud, phishing scams and AI-driven fraud tactics like deepfakes.

Types of fraud consumers are most worried about

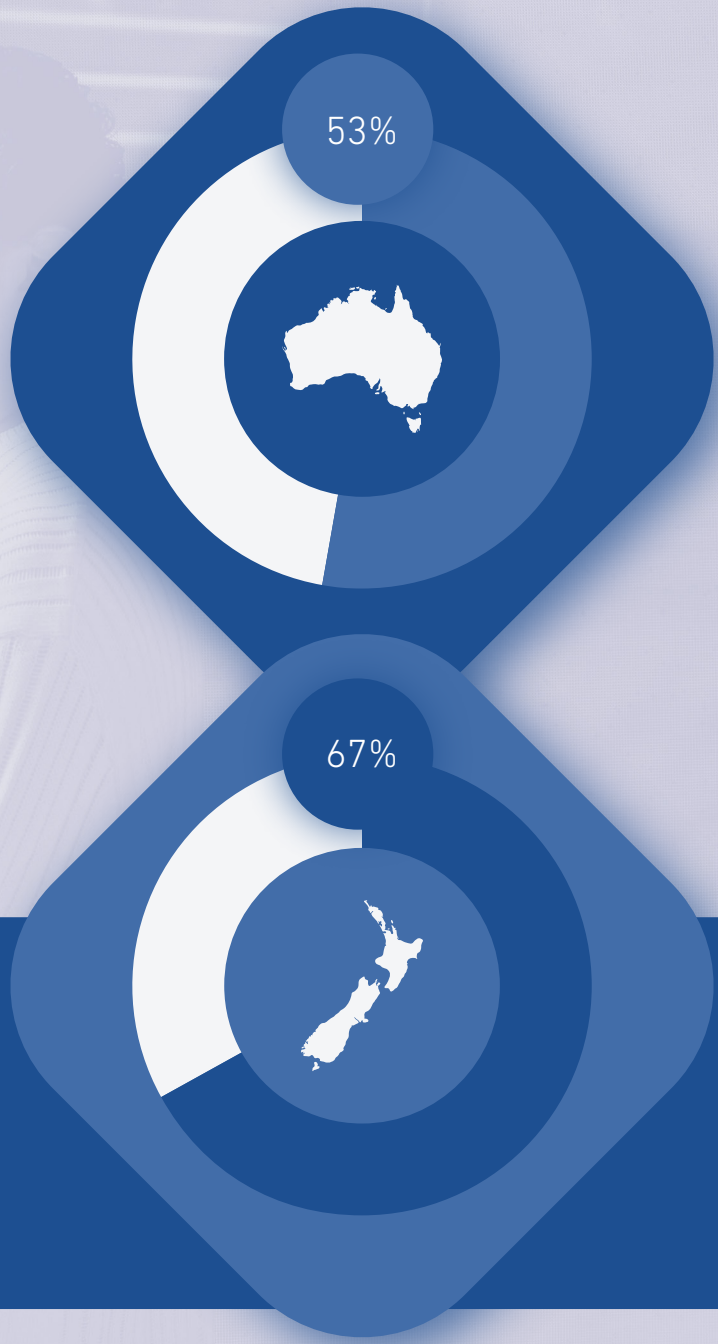


How AI is becoming the frontline in organisations' fight against fraud

To better detect and prevent fraud in real time, businesses are increasingly adopting AI-powered fraud detection technologies. These tools allow businesses to identify unusual activity and fraudulent behaviour more quickly than traditional methods. According to research, 67% of fraud leaders in New Zealand and over half (53%) of fraud leaders in Australia are incorporating AI into their fraud detection systems to stay ahead of emerging threats.

However, while AI enables more advanced fraud detection, businesses must ensure transparency and security in the use of these technologies to maintain consumer trust. As fraudsters evolve their methods, organisations must adapt by integrating AI-driven fraud prevention systems that not only improve security but also address consumer concerns around privacy and data misuse.

Fraud leaders incorporating AI into fraud detection systems



Machine learning adoption in fraud prevention

Machine learning (ML) is now central to fraud detection across both Australia and New Zealand.

67% of fraud leaders in Australia and 60% of fraud leaders in New Zealand report a measurable improvement in the accuracy of their fraud detection since implementing ML technologies. Additionally, 66% (Australia) and 59% (New Zealand) agree that ML allows them to better prioritise manual review cases, significantly improving fraud analysts' productivity.

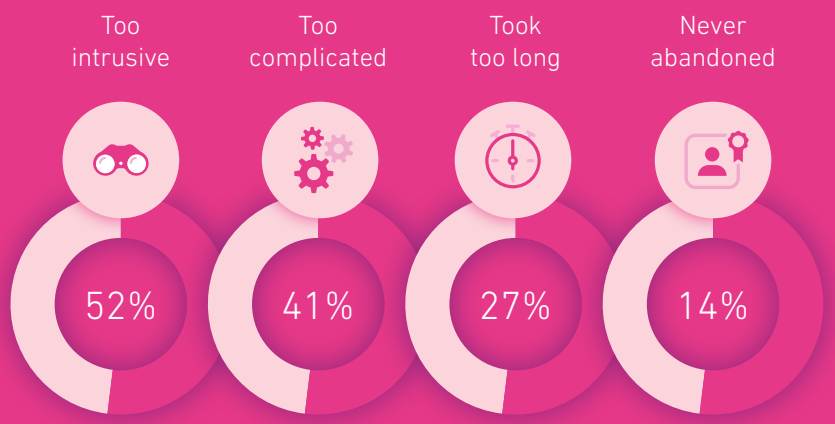
Friction vs protection – Designing safer experiences

So, how does an organisation's response to detecting AI driven fraud threats sit with customers? As businesses integrate AI-driven fraud prevention tools, the challenge becomes balancing strong fraud protection with seamless user experience, particularly when verification processes become too complex or intrusive.

The impact of complex verification processes

Complex verification processes are a major barrier to trust and completion rates. Over half of consumers (53%) have abandoned an online sign-up or verification process because it felt too intrusive. Furthermore, 38% of consumers stated they are less likely to trust a service if their sign up/verification process seemed complicated or outdated.

Reasons for abandonment during sign up or verification



Consumer snapshot: The privacy-conscious Gen Z consumer

Josh, 23, represents a growing group of digitally active Gen Z consumers who rely heavily on apps for banking, shopping, entertainment and everyday services, but are increasingly cautious about how much personal information they are asked to share online.

Recently, he attempted to sign up for an online platform but abandoned the process when it required uploading identity documents and completing additional verification steps that felt overly intrusive for a simple registration. Experiences like this are becoming more common, which helps explain why many younger consumers are becoming more selective about the platforms they engage with. Our research shows **59% of Gen Z consumers have abandoned an online sign-up or verification process because it felt too intrusive,** highlighting the higher sensitivity younger users have to requests for personal data.

While Josh understands that verification processes are designed to improve security and reduce fraud, navigating these checks can sometimes feel excessive. Like many consumers, he is comfortable using digital services but becomes wary when platforms request more personal information than he believes is necessary.

Transparency on data use is key

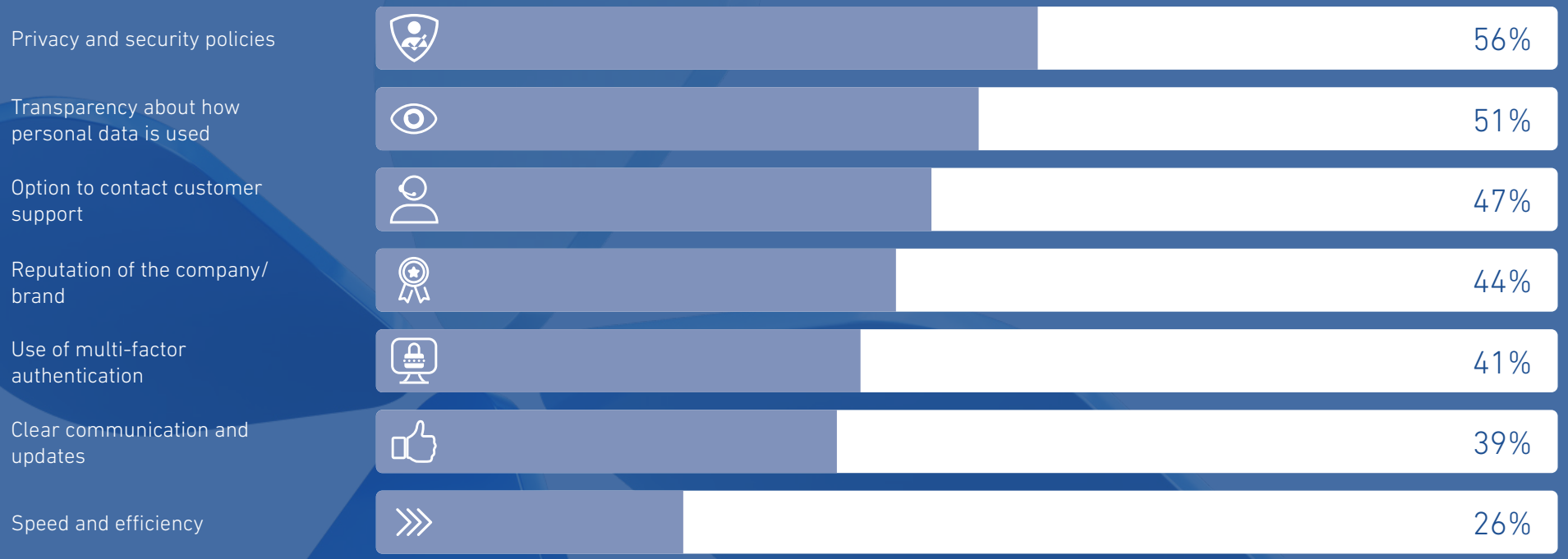
As consumers grow more concerned about how their data is used, transparency is becoming critical to maintaining trust. 54% of consumers expect businesses to provide full or moderate transparency on how their data is used for fraud prevention. Other factors highlighted as being important for trust in a sign up or verification process include privacy and security policies (56%) and an option to contact customer support (47%).

AI in fraud prevention: Customer comfort depends on the situation

While consumers are generally supportive of AI-driven fraud prevention tools, their comfort with these technologies varies widely depending on the application. 52% of consumers are most comfortable with AI for behavioural analysis to detect fraud, which operates in the background to identify suspicious patterns.

However, comfort levels drop significantly when AI is used for more intrusive methods, such as facial recognition or AI agents making decisions autonomously. Only 19% of consumers are very comfortable with facial recognition, and only 9% feel comfortable with AI agents making decisions like authorising payments or applying for services. This highlights the importance of transparency in how AI-driven fraud detection is used and the need for clear communication with consumers regarding how their personal data is being processed and protected.

Most important factors for trust in a sign up / verification process



What this means for organisations

The research shows that businesses must balance strong fraud protection with seamless customer experiences. Complexity in identity verification processes leads to higher abandonment rates, with over half of consumers abandoning sign-up processes due to complexity. To maintain trust, businesses need to adopt more transparent, user-friendly verification methods while providing robust security measures.

As fraud accelerates, organisations must stay ahead by embracing AI-driven fraud detection technologies and offering clear communication about how customer data is used. Transparency and consumer control will be key to maintaining trust as AI continues to play a critical role in the fight against fraud.

Richard Atkinson, Head of Fraud and ID, Experian A/NZ said:

"At Experian, we support clients with real-time identity verification and fraud solutions that help build trust while delivering seamless digital experiences.

"Our research solidifies that consumers are increasingly expecting transparency around how their personal data is used, with trust declining significantly once they've experienced fraud. Complex or intrusive verification processes are also leading to application abandonment, highlighting the need for solutions that protect customers without adding unnecessary friction.

"By combining advanced identity, data and analytics capabilities, organisations can strengthen fraud prevention while giving consumers greater confidence and control over how their data and identity are protected."

Experian continually invests in developing data, analytics and technology solutions that strengthens fraud prevention and identity protection for our clients and their customers. With advanced identity verification and fraud detection solutions, including biometric verification and document authentication, device intelligence and real-time fraud analytics, we support organisations to verify identities, detect suspicious activity and protect customers throughout the digital journey.

Looking ahead

Fraud across Australia and New Zealand is becoming more sophisticated, driven by organised cybercrime, automation and AI-enabled attack methods such as deepfakes and synthetic identities. As digital adoption expands, identity has become the new security perimeter, yet many organisations' existing fraud and verification tools are struggling to keep pace. At the same time, fraud is becoming a mainstream consumer experience, eroding trust in digital services and changing how people behave online.

For organisations, the challenge is no longer just stopping fraud but doing so in a way that maintains trust. Consumers want stronger protection, but they also expect verification to be seamless, transparent and not overly intrusive. As AI becomes a more important tool in fraud prevention, the organisations best positioned to respond will be those that combine advanced identity verification, AI-driven detection and low-friction customer experiences.

Key takeaways

Fraud is now a mainstream risk

More than half of consumers across Australia and New Zealand report experiencing fraud, while over a third have faced identity theft or account takeover.

Identity is the new security perimeter

Deepfakes and synthetic identities are increasing pressure on traditional KYC and identity verification systems.

AI is both a threat and a defence

AI-powered tools are enabling more sophisticated fraud attacks while also improving real-time fraud detection.

Trust is shaping digital behaviour

Fraud experiences are reducing trust in online platforms and changing how consumers engage with digital services.

Security must be balanced with user experience

Over half of consumers abandon sign-ups when verification processes feel intrusive.

Transparency underpins digital trust

Consumers expect clear communication about how their personal data is used in fraud detection and identity verification.

Methodology

Conducted in February 2026, Experian's consumer research engaged 1,300 consumers across Australia and New Zealand. The survey was distributed through independent research platform, Pollfish.

Experian's fraud report is based on a survey of 979 senior fraud decision-makers in Financial Services, Telcos and eCommerce across nine countries: Australia, Denmark, Germany, India, Italy, New Zealand, Norway, South Africa and Spain. The research was conducted by Forrester Consulting in July 2025 to understand the big trends impacting fraud prevention.

About Experian

Experian is a global data and technology company, powering opportunities for people and businesses around the world. We help to redefine lending practices, uncover and prevent fraud, simplify healthcare, deliver digital marketing solutions, and gain deeper insights into the automotive market, all using our unique combination of data, analytics and software. We also assist millions of people to realise their financial goals and help them to save time and money.

We operate across a range of markets, from financial services to healthcare, automotive, agrifinance, insurance, and many more industry segments.

We invest in talented people and new advanced technologies to unlock the power of data and to innovate. A FTSE 100 Index company listed on the London Stock Exchange (EXPN), we have a team of 25,100 people across 33 countries. Our corporate headquarters are in Dublin, Ireland. Learn more at experianplc.com.


experian