EQUIFAX®

Championing Digital Trust

Strengthening Australia's digital economy against evolving fraud and identity threats.

Contents

03 Executive Summary

04 Introduction

05 **Digital Identity** The gateway to trust

07 **Digital Trust** Your frontline defence in the battle against fraud

10 **Hacking with AI** A new adversary

12 **Scams** The social impact of fraud

13 **Staying ahead of AML/CTF**

15 Your Partner in **Fraud Prevention and Digital Trust**

Executive Summary

The 'realness' of our digital world is increasingly under question. Online deception is rampant and it's reshaping trust, identity and safety.

Data from the Equifax Fraud Consortium shows that as economic pressures have intensified over the past three years, so has the incident of fraud. We've seen a 112% rise in fraud to secure big-ticket credit items like cars or commercial assets, while the opening of transaction accounts by **money mules** with the probable intent to launder money has surged by 438%.

With a 30-fold increase in **deepfakes** used in facial biometrics, AI is increasingly blurring the line between real and illusion. It's now enabling everything from fake voices and synthetic personas to automated scams. This changing face and pace of fraud means that an organisation's approach to identity verification and fraud prevention really matters.

For 25 years, Equifax has been helping businesses connect to trusted identities. Our goal is to enable you to move faster and become smarter by using our multisource, multidimensional data and technology capabilities to efficiently assess risk and act decisively.

Last year, we processed 97 million searches across our identity and fraud capabilities, helping to prevent $1.5 billion in attempted fraud and returning that saving to the Australian economy.

Beyond our technology, we are an extension of your team, providing actionable insights to help you better understand your customers from all angles. We believe in working with government, industry, customers, consumers, and partners to collaboratively build an ecosystem for a more secure digital world. By doing so, we create positive social impact and help innovate and future-proof our shared digital landscape against the threats of tomorrow.

Tehani Legeay

GM of Identity & Fraud Services
Equifax

Introduction

The Championing Digital Trust report sheds light on how businesses can foster digital trust by leveraging differentiated data, advanced analytics and technology to grow confidently, minimise risk and deliver exceptional and secure customer experiences.

The report leverages key insights from our Equifax Frontiers event, which brought together a range of industry leaders, including The Hon. Victor Dominello, Assistant Minister Matt Thistlethwaite and John Shepherd from the Department of Finance.

Neil Jeans from Grant Thornton, as well as partners like Marina Lee from IDVerse, a LexisNexis® Risk Solutions company, spoke of strengthening defences, ensuring regulatory compliance, and future-proofing operations.

We also heard from a former black-hat hacker, Bastien Treptel, on how AI has lowered the barrier to entry for cybercrime, and what you can do to protect your business.

The central theme is that 'digital trust' - meaning customer confidence and security in online business interactions - is no longer a peripheral concern. Instead, it's a foundational element for business resilience and growth.

DIGITAL IDENTITY
The gateway to trust

The shift from traditional paper identification like driver's licences and passports to digital identities (digital IDs) is well underway. These consumer-consented electronically issued identities include everything from personal data and biometrics to emails, PINs, security tokens and more.

As more transactions move to digital at a higher frequency, consumer relations are being tested with every interaction as the battle against fraud ramps up.

The legislative mandate for trust

The newly enacted Digital Identity Act 2024, which transforms Australia's Digital ID Framework, aims to restore trust and increase security in digital transactions. Equifax supports the framework and has actively contributed to the direction the legislation has taken, as we believe in working with government, industry, customers, consumers and partners to create a more secure digital world.

The Act establishes a whole-of-economy framework with strong privacy safeguards to foster trust and address the current inefficiencies and risks associated with manual identity checks and repeated sharing of personal information.

The Future Government Institute estimates that moving to digital identity could unlock between $19 billion to $32 billion in annual productivity dividends in Australia, says its CEO, the Hon Victor Dominello.

The private sector can apply to join the Australian Government Digital ID System (AGDIS) from **December 2026**

Economic and social dividends

Digital identity, and mechanisms such as Consumer Data Rights (CDR), can create new revenue streams for business, transforming the identity process from a burdensome task into a streamlined, secure operation that enhances consumer experience.

The success of initiatives like the NSW Digital Driver's Licence, which The Future Government Institute reported as achieving an 85% voluntary adoption rate and 93% satisfaction, demonstrates that convenience and usability are key drivers for widespread acceptance.

Beyond economic gains, these systems build a foundation of user-centric trust. Trust isn't built by preventing every failure, but by building systems resilient enough to recover quickly when an inevitable failure like a data breach occurs.

> "Digital identity is now a strategic enabler for trust, consumer experience, and growth, extending beyond mere compliance."
>
> **Hosay Mangal,**
> **Head of Product Development,**
> **Digital Identity, Equifax**

Digital identity helps businesses reduce data proliferation and mitigate risk by reducing the need to collect and store sensitive customer identity documents. Maintaining your customer's trust is closely linked to protecting their data. Unauthorised disclosure of personal information can severely undermine consumer confidence in your organisation's reliability. With cyberattacks happening every six minutes across Australia[1], the threat of a **data breach** is an ever-present danger.

Verifiable credentials (e.g., digital driver licences) and partnerships with accredited identity service providers are now critical to combating increasingly sophisticated, AI-driven fraud, by enabling real-time, trusted verification.

[1] ASD Annual Cyber Threat Report 2023-24

DIGITAL TRUST

Your frontline defence in the battle against fraud

While digital interactions are at an all-time high, so are the threats to their integrity. Data insights from the **Equifax Fraud Consortium** tell the story of an evolving and escalating battle against fraud.

Global e-commerce has grown by **75%** in the last three years.

Fraud for big-ticket credit items is up by **12%**.

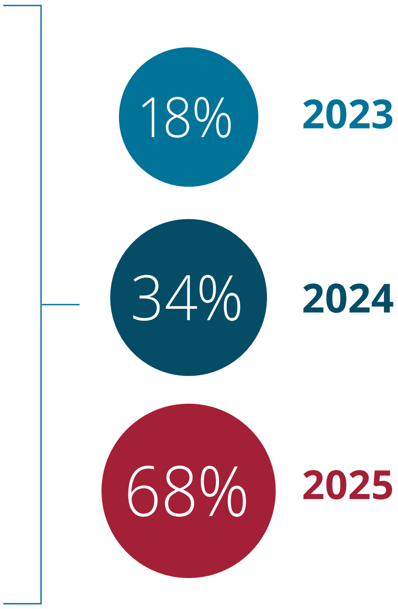
The number of suspected **money mule accounts** has surged by **438%**.

Deepfakes in facial biometrics have increased **30-fold**.

In 2023, **$2 billion** was lost to scams in Australia alone.

Equifax helped prevent **$1.5 billion** in attempted fraud in 2024.

GenAI is a powerful tool for fraudsters, making sophisticated crimes like fake documents and **deepfakes** accessible to everyone. The fakes are so realistic that the human eye can no longer be relied on for detection. Equifax IDVerse data shows that as of May 2025, 68% of attempted fraud is digitally generated/edited artefacts, up 100% from 2024.



What is digital trust?

At its essence, digital trust is about having confidence that:

1
The people accessing your services are who they say they are

2
Their intentions are what they say they are.

Being able to trust consumer identities as they're presented in real-time across any digital interaction helps strengthen and protect the entire customer journey - from account generation and login to payments and disputes. In turn, this can help increase approval rates, and ultimately, revenue, while reducing manual reviews, false positives and chargebacks.

Digital trust helps ensure the user trying to log into a banking app is an authorised account holder, not a fraudster who hacked or stole the information. Or, say a retail customer is attempting to checkout online as a "guest". Identity trust comprehensively cross-references and validates their identity, including their device information, in real time, without adding friction that might cause a legitimate customer to abandon their cart.

Identity trust decisions are complex, drawing on a multitude of intelligent data, behavior patterns and signals. The process is dynamic and multifaceted, as it's designed to present a 360-degree view of risk, in seconds.

Start building digital trust today

Managing identity and fraud risk requires unwavering focus and effort across an organisation. For businesses looking to modernise their approach, the first place to start is by establishing digital trust at the point of contact for every consumer interaction. This helps mitigate risk before it enters the business, while at the same time facilitating growth through improved operational performance and efficiency, faster account approvals and a better consumer experience.

Here are some thoughts to get you started:

Collaboration and data sharing strengthens defences

Shared industry intelligence is key to strengthening defences. The **Equifax Fraud Consortium** shares confirmed fraud data and knowledge across 150 multi-industry organisations. Our Modern FraudCheck service helps businesses quickly distinguish good customers from fraudsters at the point of application and the new Equifax Exchange will extend this protection to scam data.

The future is a Global Fraud Risk Score

Equifax is building a world where businesses can access a global fraud network through a single interface. This allows customers to select tailored data sources, enabling real-time threat detection throughout the lifecycle of their consumers. Our Global Fraud Risk Score will provide continuous fraud monitoring for both businesses and consumers.

Technological investment and innovation are key

As fraudsters use advanced tech, businesses must too. A layered, multi-pronged approach is essential. Equifax's fraud and identity tools use AI, multiple data points, and powerful trust signals to assess risk and flag fraud, all operating seamlessly behind the scenes.

Equifax is innovating and future-proofing a digital identity solution that lets consumers update and verify their personal information from their phone. Consumers can manage their identity as they get new qualifications or apply for jobs and finance, with continuous fraud monitoring for protection.

HACKING WITH AI

A new adversary

AI has “completely destroyed the barrier to entry” for hacking, and we must recognise this as the new normal, says Bastien Treptel, former black-hat hacker and founder of Ironclad ID. The digital security landscape has shifted dramatically, and traditional defences are no longer enough.

Criminal syndicates are leveraging AI more effectively than many corporations. They use AI to:

- **Craft convincing social engineering scams**, including **deepfakes** and real-time voice cloning that manipulate employees and bypass security.
- **Develop new exploits at a staggering pace**, generating new vulnerabilities in minutes instead of months.
- **Exploit compromised credentials**, with billions of leaked passwords from past data breaches available on the dark web.
- **Compromise critical infrastructure**, which remains alarmingly susceptible to attacks that could cause long-term, widespread disruption.

The uncomfortable truth

Humans are the weakest link
It’s far easier to exploit human psychology than to breach a corporate firewall.

No silver bullets
Relying on a single solution is no longer enough.

Identity is a high-value target
A personal social media account, which many people don’t think is important, can be leveraged by a hacker to steal millions

Defence in layers

To protect your business, you need a new approach that uses layers upon layers of controls that combine human vigilance, AI-driven tools, and robust processes.

1. **Human awareness**
   Never underestimate the power of social engineering. Train your staff to be a critical part of your defence.

2. **Multisource, multidimensional data**
   The importance of data diversity cannot be understated. To build a fast-moving, 'all-angles' view of fraud risk, you need access to multiple data sources. It helps fill gaps in identity assessments and reduce uncertainty around the identity, therefore reducing risk.

3. **AI and machine learning technology**
   The analytic models created to fight fraud today must be equally - if not more - innovative and iterative than fraudsters themselves. This makes machine learning models, both supervised and unsupervised, ideal for fraud mitigation. When appropriately designed and trained, these models will continually learn and adapt to fast-moving fraud patterns, with little to no human intervention.

4. **Credential monitoring**
   Actively monitor for compromised corporate credentials on the dark web and enforce immediate access revocation.

5. **Secure foundations**
   Ensure your critical infrastructure and supply chain are secured with reputable suppliers and robust systems that eliminate vulnerabilities.

SCAMS

The social impact of fraud

The industrialisation of deceit

Scams are no longer the work of isolated individuals. They are part of a global, industrialised criminal complex. These sophisticated syndicates operate with a clear strategy, using a "spray and pray" approach to cast a wide net and then elevating promising targets to specialised teams.

The scale is staggering, with the national cyber support service IDCare supporting over 100,000 scam victims in the last 12 months, with financial losses exceeding $585 million.

> "I didn't lose the money. He stole it from me through sophisticated deceit."
>
> **Tracy Hall**
> **Consumer advocate**

Under-reporting of fraud

The most insidious aspect of this crime is the pervasive victim-blaming. Unlike other serious crimes, financial fraud is often discussed in a way that places responsibility on the victim. Consumer advocate Tracy Hall recalls the negative media reporting directed at her when she became the victim of fraud. She believes it's one of the reasons behind the significant under-reporting of fraud.

What can organisations do to support scam victims?

Education

Simple, practical education is key. We cannot assume consumers understand concepts like multi-factor authentication or reverse image searches. The message needs to be simple, hard-hitting, and empowering.

The pause

Experts advocate for the simple but powerful act of 'just stop, just pause'. Encouraging people to take a moment and talk to someone else before acting on a request. This can disrupt a scammer's momentum.

Support

Offer a clear, supportive pathway for victims. This includes providing the right language and resources to help them navigate the aftermath and restore their sense of security.

Australians lost over $2billion to scams last year, with social media being the most reported contact method leading to financial loss[1].

[1] National Anti-Scam Centre Targeting Scams Report 2024

STAYING AHEAD OF AML/CTF

Amendments to Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) regulations and the expansion to Tranche 2 entities will reshape the landscape for both financial and non-financial sectors.

The new legislation, effective March 2026, includes new requirements for enhanced due diligence, rigorous consumer verification and advanced technology to detect and prevent financial crime. To comply, institutions must bolster their AML risk management strategies to effectively identify and mitigate potential threats.

A new focus on harm prevention

A significant change is the move away from prescriptive rules to a more dynamic risk-based approach focused on harm prevention and outcomes. This means AUSTRAC will assess businesses on whether they've effectively detected and disrupted criminal activity, not just on whether they've completed a set of tasks. The new rules also significantly increase the amount of information required for due diligence, particularly for non-individual entities, including extensive information on ownership and control structures.

> "This is a rear-view mirror assessment. It's 'did you prevent harm?' That's how you'll be judged."
>
> **Neil Jeans**
>
> **Grant Thornton partner and risk management expert**

The challenge of scale

Tranche 2 will cause the number of reporting entities to surge to around 90,000, extending the regime to sectors like **real estate**, **legal** and **accounting professionals** and **Virtual Asset Service Providers (VASPs)**.

This expansion presents significant challenges:

Sevenfold increase in PEPs

The new rules are expected to lead to a roughly sevenfold increase in the number of Politically Exposed Persons (PEPs) that need to be screened, according to the Equifax Frontiers event panelists.

Compliance talent shortage

The demand for experienced AML/CTF professionals will stretch the talent pool, forcing businesses to consider new resourcing and change management strategies.

Inter-business coordination

Processes like property transactions, which involve multiple businesses (lawyers, real estate agents, banks), will require a coordinated approach to avoid duplicating efforts.

Embracing technology for a smoother transition

The complexities of the AML/CTF reforms are challenging, but they are also an opportunity to build a more resilient and efficient business. Effective risk management and a proactive approach are key.

Start with a comprehensive risk assessment to pinpoint potential vulnerabilities and develop a clearer understanding of your risk exposure. Then map new requirements to your existing processes and rewrite your AML/CTF program, rather than starting with a generic program and trying to fit your business into it.

Technology is your ally in this process. It allows for a more intelligent, dynamic business logic during onboarding, **tailoring checks to the risk level of each customer**. This means you can meet your obligations without creating unnecessary friction.

Challenge	Technology-enabled solution
Increased due diligence	**Biometric verification** Seamlessly integrate biometrics into the onboarding process to efficiently verify individuals and ensure compliance.
Complex workflows	**Self-service processes** For non-individual entities (e.g. trusts, self-managed super funds), which involve multiple individuals and beneficial owners, use technology to engage each individual in the structure, allowing them to provide their own consent and complete the verification process.
Financial inclusion	**Dual processes** Implement both a digital, streamlined process and a manual or alternative pathway to serve a population that is not technologically literate.

YOUR PARTNER IN
Fraud prevention and digital trust

As a key partner with a unique view of Australia's digital landscape, Equifax builds the trust that allows businesses and government to prevent risk, protect customers and consumers, and grow with confidence.

Key benefits of partnering with Equifax:

- ✓ **Protect your business and customers**

  Our solutions are designed to secure online interactions, help prevent financial losses and mitigate reputational damage.

- ✓ **Move faster**

  We help you streamline onboarding and verification processes, enabling you to acquire good customers quickly and securely.

- ✓ **Become smarter**

  Our advanced analytics provide a single, clear view of risk, allowing you to make more informed decisions.

- ✓ **Innovate and future-proof**

  You can leverage our knowledge and expertise, market scanning and insights, as well as advanced technologies like GenAI to anticipate and address future challenges.

- ✓ **Collaborate for a secure ecosystem**

  We work with government, industry, and partners to create a more secure digital world for everyone.

Leading fraud detection and prevention solutions

We're here 24/7 to help businesses protect themselves and make the smart decisions that give good consumers easy and safe digital access to services.

Identity Verification

Verify customers in real-time and meet AML/CTF screening requirements.

Fraud Assessment

Screen for known fraud indicators during identity verification.

Biometrics

Determine if an individual is genuinely who they claim to be.

Fraud Data Consortium

Collaborate with other members to proactively manage fraud end-to-end.

PEP, sanctions & adverse media screening

Identify accounts for closer monitoring and further investigation.

Payments Fraud

Improve your defence against payments fraud and better manage chargebacks.

Comprehensive Solutions Overview

Equifax offers a robust portfolio designed to secure every customer interaction with less friction, leveraging multiple data points, powerful trust signals, and Artificial Intelligence.

Identity Verification & Fraud Prevention

IDMatrix: Detect and Stop Fraud with an advanced single view platform.
Australia's most comprehensive electronic verification solution, accurately verifying individuals' identities and detecting fraud.

- **Biometrics:** Facial matching, liveness detection, and document fraud analysis to confirm identity.
- **FraudCheck:** A members-only collaborative knowledge-sharing service designed to stop fraudsters with unparalleled access to fraudulent information in Australia.
- **GlobalScreening:** Locally hosted and customisable solution for checking watchlists and identifying Politically Exposed Persons (PEP) worldwide.
- **Device Intelligence:** Tracks customers doing business on stolen and fraudulent devices — a critical first line of defence.
- **Email Risk Search:** Validates identity and assesses risk using email address metadata for a seamless customer experience.
- **Visa Checks via VEVO:** Validates your customer's residency status with speed and efficiency.
- **Australian Death Check:** Australia's only official up-to-date source of death data for maintaining accurate customer data and preventing identity crime.
- **KOUNT Australia:** A leading fraud solution that protects your business against digital fraud and provides a frictionless customer journey from login to payment.
- **Equifax Protect:** Respond fast and help your customers take control in the event of a data breach.
- **Document Verification Service (DVS):** The DVS offers a reliable means of matching document data with key Government issued documents.
- **Super & Payroll Search:** Identity verification based on identity information from Superannuation and Payroll data sources.
- **Credit & Identity Health:** Help your customers to safeguard their identity by enabling them to monitor key personal information, receive alerts, and access their credit scores and reports.

Contact Equifax

The content of this document is provided for information purposes only. It does not constitute legal or compliance advice and should not be used as such. Further, the information in this document is provided on the basis that all persons accessing it undertake responsibility for assessing the relevance and accuracy of its content. Should you consider it necessary, please seek your own legal or compliance advice for application of any this information to your own circumstances.