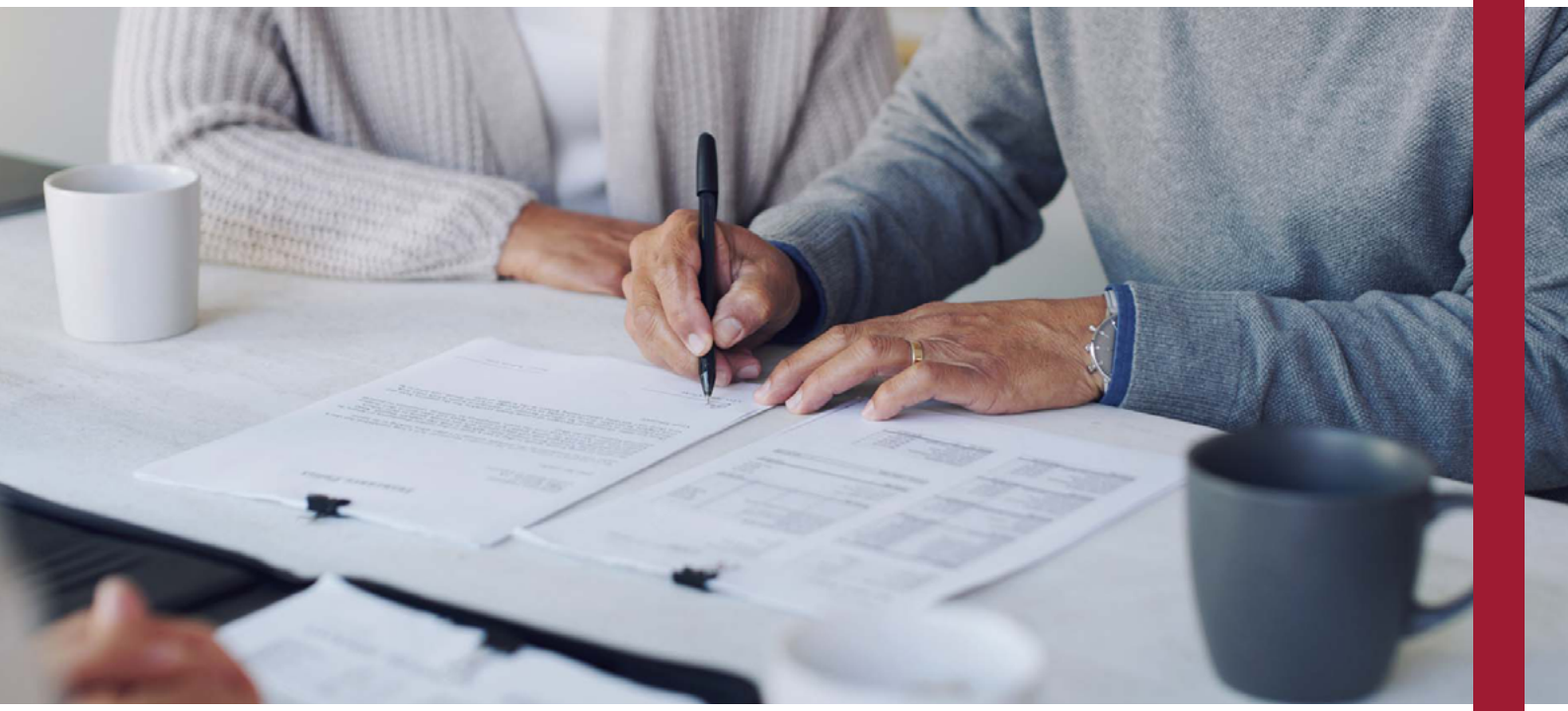
Fraud Index Report

2026

Contents



What is the Fraud Index Report?

The Fraud Index Report 2026 aggregates data from Equifax Identity and Fraud Digital Solutions, enriched with proprietary, public, and third-party sources. This data highlights shifting fraud trends by examining listings and volumes across types and credit/non-credit categories for the 2025 calendar year.

As the landscape of financial crime in Australia becomes increasingly complex, the Equifax Identity and Fraud Digital Solutions enable customers to share intelligence of confirmed fraud events, helping to identify threats before they can penetrate individual institutions. While this data represents a specific set of Australian organisations, it serves as a useful indicator of the evolving tactics used by bad actors.

Key Findings:

- **Credit Fraud returns to the forefront:** Fraud is now growing significantly faster among credit products than non-credit products, reversing a three-year trend as overall listings grew by 4%. Within that total, credit fraud listings jumped by 11.1%, while non-credit listings saw a slight dip of -1.1%.
- **Money muling surges:** This category saw an explosive surge in activity. The volume of money mule listings grew by a massive 90.9%, now accounting for 14.6% of all fraud listings.
- **Identity takeover declines:** While still a major threat, identity takeover dropped from 62.1% of listings in 2024 to 49.8% in 2025 as a ramp-up in money mule detection led to more distinct classification of fraudulent accounts.
- **First-party fraud accelerates while third-party fraud stabilises:** Fraud committed by the applicant grew to 31.6% of all listings, up from 26.2% in 2024. Third-party fraud saw a slight decline, representing 2.9% of listings, down from 3.2% in 2024.
- **Niche threats grow:** Smaller, high-impact categories like synthetic identities and bust-outs saw aggressive growth. The volume of fraud listings in this category surged by 96.5% compared with the previous year.

Introduction

Fraud Growth

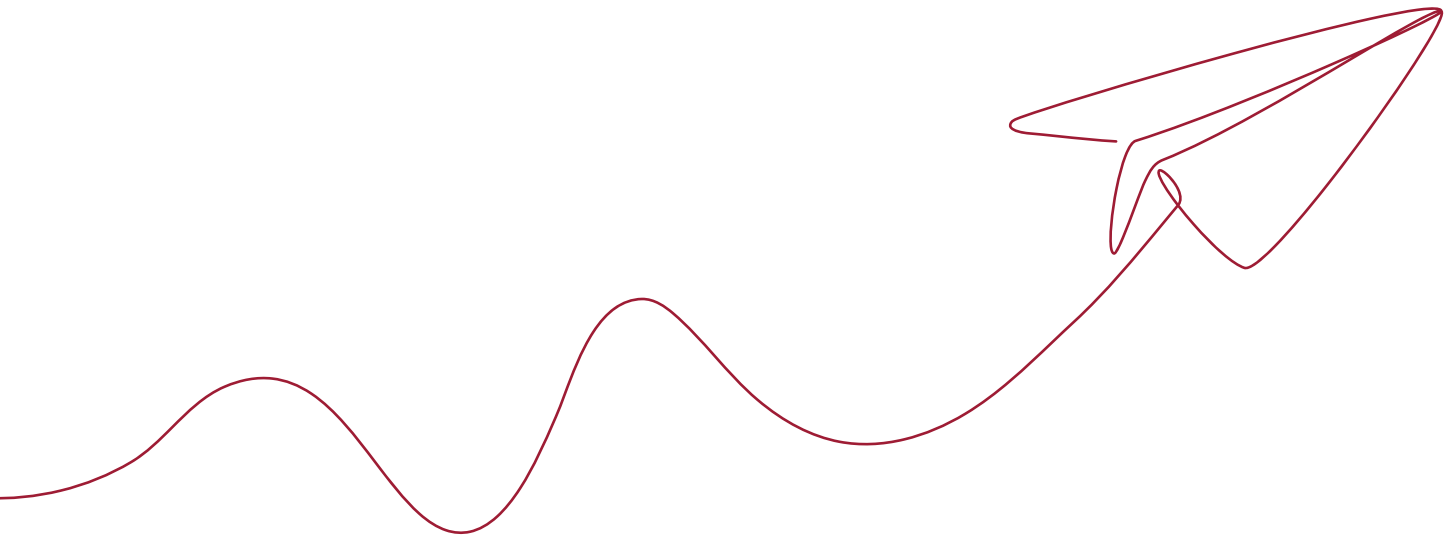
The 2025 calendar year was marked by a rise in fraudulent activity, with total fraud listings growing by 4.0%. Rising financial pressure has heightened consumer vulnerability, making individuals easier targets for scams and recruitment into money muling.

Fraudsters are also narrowing their focus to high-value targets. Auto loans are a primary target for identity takeover and synthetic identities, contributing to a 112% surge in fraud for big-ticket credit items like vehicles and commercial assets[1]. Non-credit products are often used to launder money (money muling) or to establish identities and build customer profiles for future credit fraud. Conversely, the high volume of documents required for mortgage applications creates significantly more opportunities for document fraud.

Because these targets involve significant capital, they represent a critical risk for financial loss. The use of highly convincing falsified documents, powered by GenAI, underscores a move toward quality as bad actors are becoming more sophisticated in their use of deepfake technology and automated document manipulation.

Despite this uptick in fraudulent activity, Equifax Identity and Fraud Digital solutions customers prevented over $1.5 billion of fraudulent activities before they occurred, emphasising the value of collaborative intelligence-sharing. This increase in reported listings can be attributed, in part, to the expanding membership of the Exchange and the enhanced operational capacity of our members to identify and contribute data.

Essentially, our collective ability to detect and report these threats is improving, allowing the industry to stay ahead of increasingly bold fraudulent tactics.



[1]Equifax Championing Digital Trust Report

Credit vs. Non-Credit Listings Shift

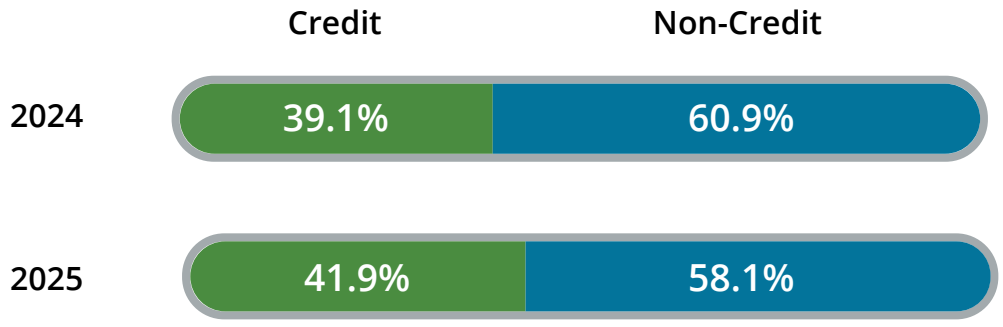
For the past three years, non-credit products dominated fraud listings. However, 2025 saw a significant shift in this long-term trend, with credit volume listings jumping by 11.1% while non-credit listings experienced a slight contraction of -1.1%.

The financial risk from credit fraud is immediate and direct, as financial institutions bear the risk of unrecovered principal, which can range from a $5,000 credit card limit to $1M+ for a mortgage.

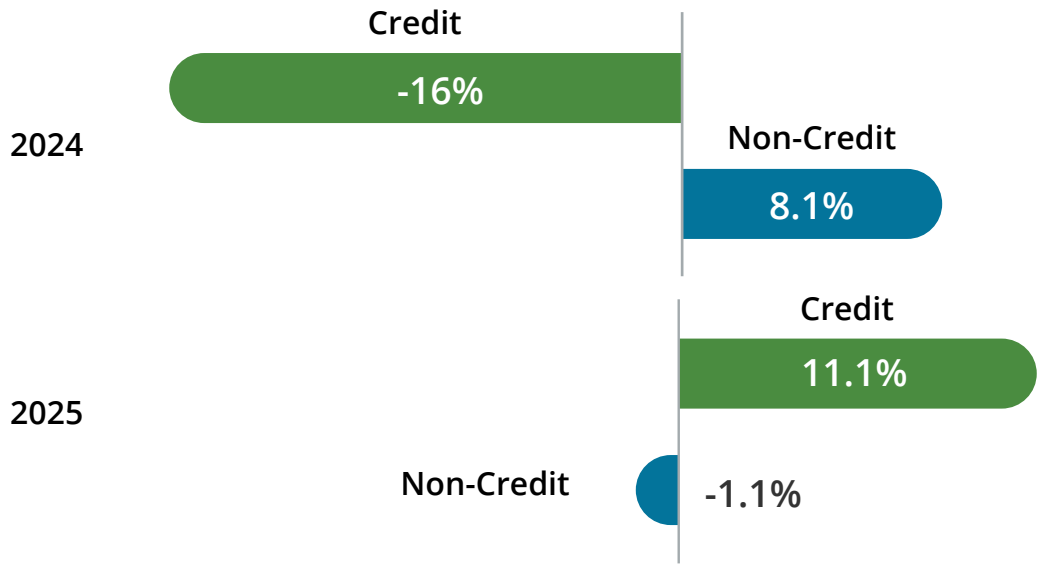
While non-credit listings still represent the majority of reports, fraud in this category – primarily via bank accounts and telco/utility applications – poses a different, systemic threat. Non-credit products can be used to launder money (money muling) or to establish identities and build customer profiles that can be leveraged for future credit fraud, often with fewer upfront document verification requirements.

While the immediate financial loss from non-credit fraud may be smaller, the long-term financial, regulatory, and reputational risk associated across multiple products remain a major concern. Consequently, this necessitates rigorous identity and document verification, as well as biometric solutions, across all product types.

Share of total listings



Year-on-year growth in credit volume listings



What drives credit and non-credit product fraud?

- **Baseline credit activity:** More Australians are seeking credit products, providing a larger pool for fraudulent attempts. The Equifax Market Pulse Report Q4 2025 shows a 6% overall rise in unsecured credit demand, with significant spikes in credit cards (15.5%) and personal loans (8.9%). Additionally, mortgage enquiries saw their strongest year-on-year growth since 2021, surging 12.3%.
- **Escalating financial pressure:** Market Pulse metrics indicate that Australians are attempting to 'bridge the gap' through credit document manipulation or by participating in illicit money muling networks to manage escalating arrears. Although hardship applications retreated in Q4 2025/26, the concentration of risk in higher-balance accounts suggests that those who are struggling are under significant pressure. This is particularly evident in Victoria, which leads late mortgage arrears growth at 16%.
- **Technological leverage:** Fraudsters are deploying GenAI to craft synthetic identities – Frankenstein profiles combining real and stolen data – to circumvent traditional Know Your Customer (KYC) checks. This is further amplified by the use of deepfake audio and video to impersonate trusted individuals or officials in real-time.

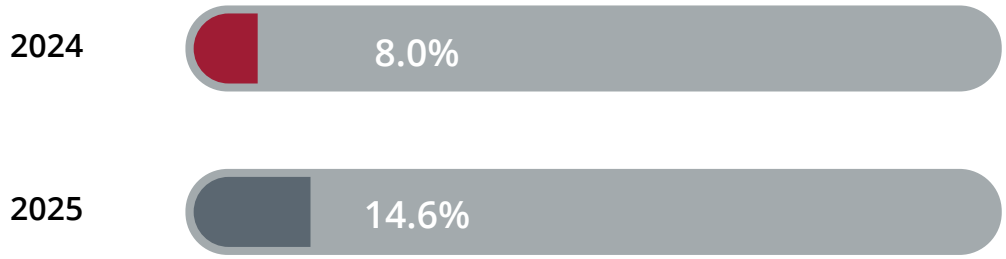
Money Muling Surges

Driven in part by rising economic hardship and social instability, the dramatic rise in money mule activity is the most significant shift observed in the 2025 fraud landscape. Money mule accounts have grown by over 90% compared to 2024 and have doubled their share of total listings.

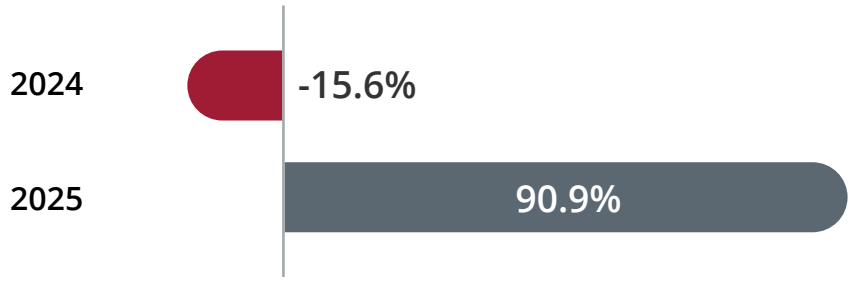
Money mules are individuals who transfer illicit funds on behalf of others, aiding in money laundering and obscuring the original source of the funds.This activity is enabled by non-credit products, primarily existing or newly opened bank accounts, through which they typically receive and subsequently transfer the funds to other accounts or withdraw them as cash.

While some mules are aware of their role in criminal activity, others are recruited via social media and remain unaware they are breaking the law. These unwitting participants are often manipulated by criminal networks into using their personal bank accounts to launder stolen funds under the guise of seemingly legitimate work-from-home opportunities.

Share of total listings



Year-on-year growth in money mules listings



What drives money muling?

- **Rising economic and social vulnerability:** Individuals experiencing financial hardship or social instability may be more susceptible to recruitment, often lured by the promise of quick financial gain[2]. Times of inflation, rising income inequality or economic downturn increase the supply of vulnerable people who are less likely to question dubious income opportunities.
- **Growth in criminal proceeds:** Increased profits from illegal activities heighten the demand for money laundering services, driving the recruitment of money mules. Money mules are essential for 'cashing out' proceeds from other crimes.
- **Criminal evasion tactics:** As financial institutions get better at blocking suspicious payments, criminals are forced to open a higher volume of disposable accounts to circumvent these controls, which contributes to the rapid growth in mule activity.
- **Targeting of temporary residents:** International students and non-permanent residents can be attractive targets for recruiters due to their potential unfamiliarity with local laws and financial systems[3].
- **Detection capabilities:** This growth is partly driven by the deployment of better market solutions for the detection of muling activity, allowing Equifax Identity and Fraud Digital Solutions members to identify and report these accounts more frequently.

[2] Detecting Money Mules to Protect Your Business, Equifax Knowledge Hub

[3] https://www.austrac.gov.au/sites/default/files/2024-06/2024_AUSTRAC_FCG_StudentMoneyMules.pdf

Spotlight: Money Muling

Rising Financial and Social Pressures increase Vulnerability to Exploitation

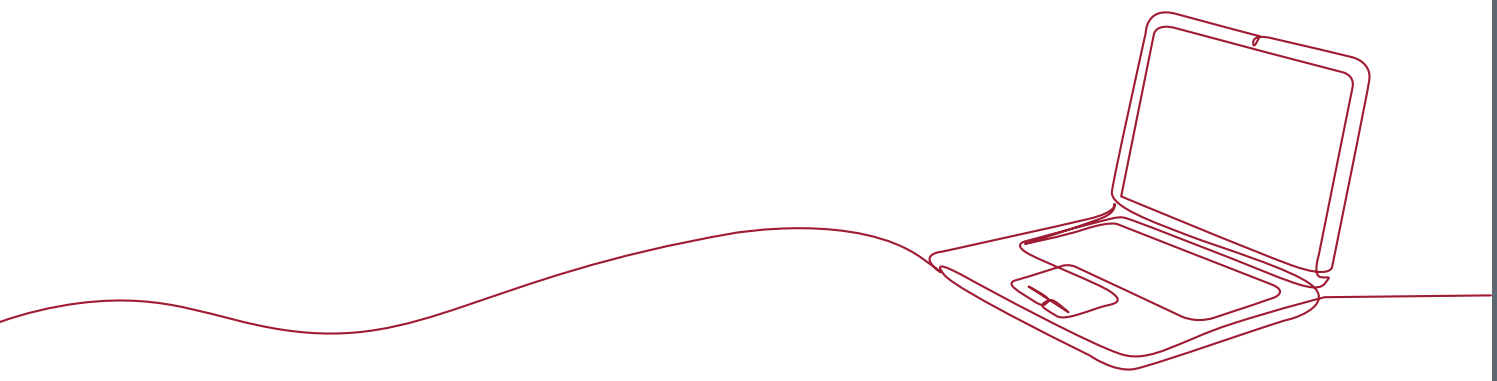
The 90.9% surge in money mule listings identified from our Equifax Known Fraud Exchange reporting may be just the tip of the iceberg. Many millions in illicit funds are possibly moving through accounts that remain unnoticed or unrecorded by institutions operating outside our collaborative network.

As economic pressures like inflation and income inequality persist, the supply of potential mules may grow as more people become susceptible to dubious income opportunities. Not all recruits even realise their job is to clean money for criminals. Beyond financial lures, syndicates often employ social engineering, such as romance scams and social networking, to exploit and recruit unsuspecting participants.

The financial and reputational risks

The threat of money muling is a significant and growing risk for financial institutions and SMEs across all sectors, leaving businesses vulnerable to escalating fraud losses, reputational risk, regulatory penalties and operational inefficiency.

- **Syndicate attraction**
  Muling is frequently linked to broader identity theft schemes. Individuals involved may use stolen credentials to gain unauthorised access to your services, potentially attracting organised crime syndicates operating identity theft schemes such as ID Takeover.
- **SME targeting**
  Fraudsters often target smaller entities on the assumption that they lack the sophisticated detection systems of larger enterprises.
- **Revenue disruption**
  If your services are paid for with funds from a compromised or mule account, your business faces the risk of chargebacks, which can disrupt revenue streams and operational efficiency.



Spotlight: Money Muling cont.

Rising Financial Stress & Fraud Risk

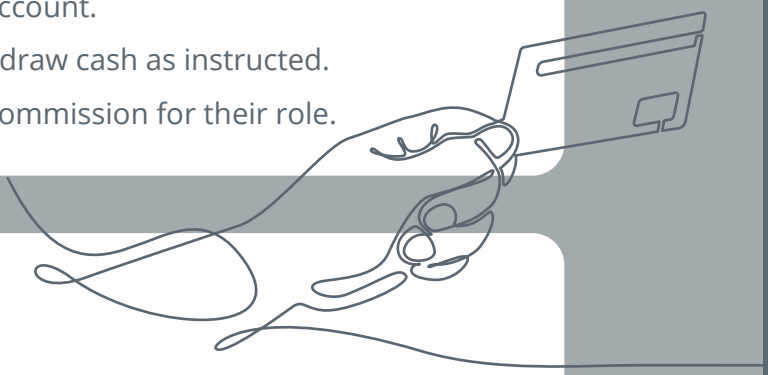
Equifax Market Pulse Q4 2025 metrics highlight the affordability gap helping to drive fraud trends.

- Late-stage delinquency values are surging for personal Loans (10%), BNPL (7.4%) and mortgages (6.8%), indicating higher financial stakes per at-risk account.
- Credit card arrears for 18–25 year olds have jumped 28.8% year-on-year
- The average loan amount in late arrears is up 8.4%, with Victoria seeing the highest growth in stress at 16%.
- While the number of personal loan arrears has dipped, the total financial value of those in late-stage delinquency has escalated by 10%.

The Mule Cycle

The 4-Step Muling Sequence

1. **Recruitment:** Criminals recruit mules via fake job ads, romance scams, online chat rooms and social networking.
2. **Deposit:** Illicit funds enter the mule's account.
3. **Layering:** Mules transfer funds or withdraw cash as instructed.
4. **Pay-off:** The mule typically receives a commission for their role.



How to identify money mules?

Red flags to watch for:

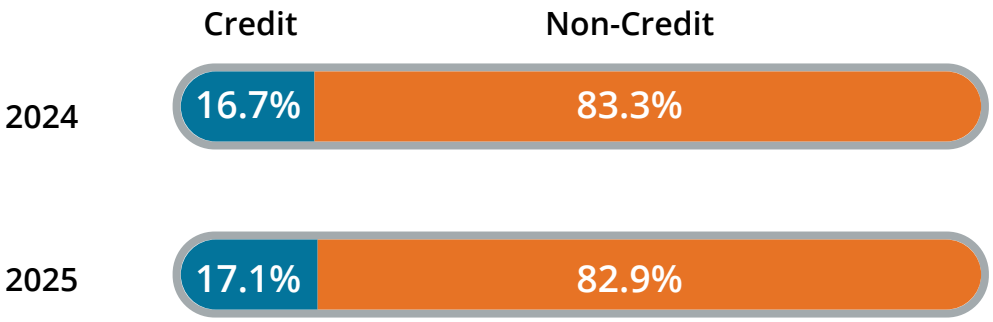
- Sudden large deposits that appear inconsistent with the account's history.
- High transaction volumes with no clear commercial purpose.
- Transfers to or from jurisdictions that do not align with the customer profile.
- Frequent changes to contact information, which can sometimes precede a spike in muling activity.
- Repeated log-in issues suggesting ID Takeover attempts.

Identity Takeover Declines

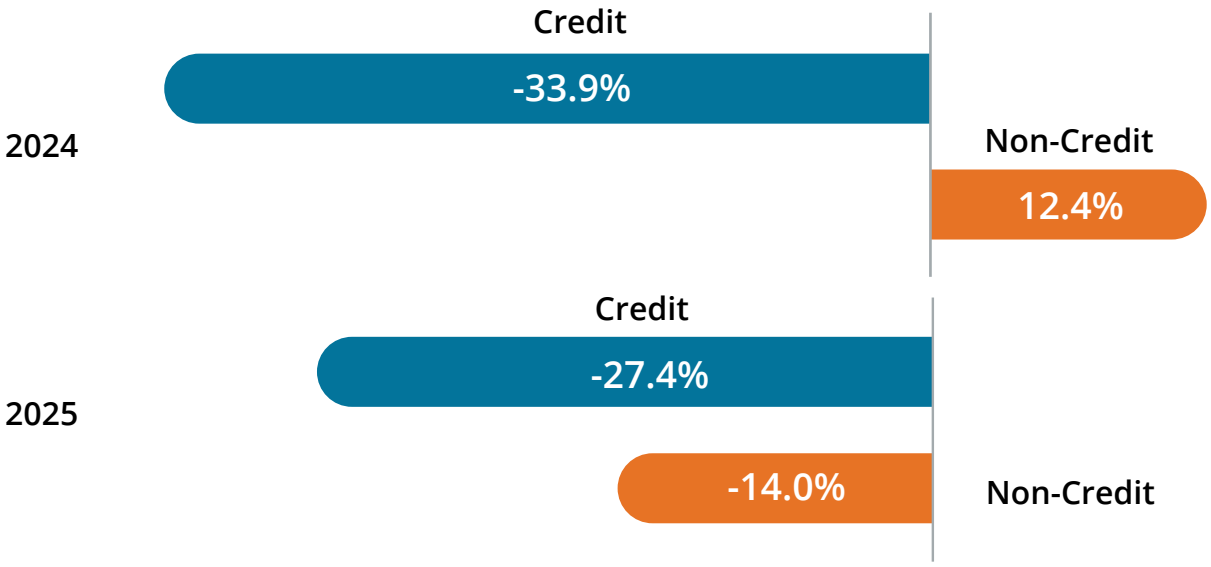
Identity takeover remains the most common category of fraud, but we have seen its share of total listings fall to 49.8%, down from 62.1% in 2024. This is supported by a -16.6% decline in volume listings, suggesting that our collective understanding of fraud is becoming more nuanced and specific. For example, accounts that were previously classified broadly as identity takeover are now being reported as money mule activity.

In this report, identity takeover refers to the unauthorised use of a real person's personally identifiable information, such as name, date of birth, and driver's licence number, regardless of whether the individual is living or deceased. This form of identity fraud allows criminals to circumvent identity verification processes, gaining access to existing accounts or opening new ones. The costs for financial institutions rise with each fraudulent application.

Credit vs Non-Credit share of total listings



Credit vs Non-Credit year-on-year growth in credit volume listings



What drives identity takeover?

- **Data breaches:** Unauthorised access, disclosure, or loss of personal information increases the availability of identity data for fraudulent use[4]. Malicious attacks were the leading cause (59%) of data breach notifications to the Office of the Australian Information Commissioner (OAIC) Jan-June 2025. This period also saw a significant jump in human error breaches, which rose to 37% (up from 29%)[5].
- **Successful scams:** Scams that deceive individuals into divulging personal information fuel the supply of identity data. Australians reported over $318,000 in total losses to ScamWatch during the first nine months of 2025, an increase of 16%[6].
- **Identity-centric cyberattacks:** Increased digitisation expands opportunities for successful cyberattacks targeting individuals' identities, such as phishing and credential stuffing, further contributing to the pool of data available to fraudsters[7].
- **Technological advancements:** agentic AI is now automating the planning and execution of new app fraud attacks. As of early 2026, fraudsters are deploying autonomous AI agents that can, with minimal human intervention, research targets, create synthetic identities, forge documentation, and submit applications at industrial scale.[8].
- **Lack of consumer awareness:** Better understanding of data security practices among individuals will reduce the supply of identity data that fuels identity takeover[9].

Useful reading:

- Infographic: Identity Takeover
- 9 Practical Measures to Reduce the Impact of a Data Breach
- Security Breaches: Types Common in the Workplace
- Protecting Financial Institutions Against Identity Theft

[5] https://www.oaic.gov.au/news/blog/latest-notifiable-data-breach-statistics-for-january-to-june-2025
[6] https://www.accc.gov.au/media-release/australians-report-nearly-260m-in-losses-as-shopping-scams-surge
[7] https://www.proofpoint.com/au/blog/identity-threat-defense/rise-in-identity-threats
[8] https://www.ey.com/en_ca/insights/banking-capital-markets/the-rise-of-agentic-ai-transforming-fraud-risk-management
[9] https://www.scamwatch.gov.au/types-of-scams/account-or-identity-takeover-scams

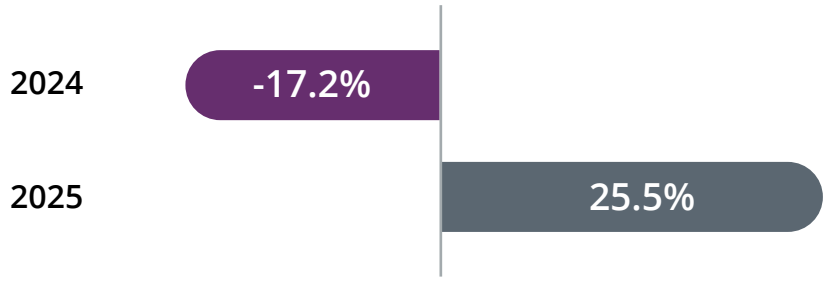
First-Party Fraud Accelerates while Third-Party Fraud Stabilises

First-party fraud or 'loan manipulation' – where a genuine applicant provides false or conflicting information – continues to climb, with volume listings growing by 25.5%. Perpetrators typically provide false information on their credit application or use counterfeit documents. For instance, opening credit card or loan accounts and placing charges against them with no intention of repayment.

Third-party fraud – perpetrated by someone other than the applicant, like a broker, accountant, or dealer – saw a decline, with volume listings dropping by -4.6% compared with strong 16.0% growth in 2024. In these cases, the third party may falsify documentation or identity details with or without the applicant's knowledge, such as through fabricated bank statements or residency status to influence credit decisions. Third-party fraud remains a smaller portion of the overall landscape, accounting for 2.9% of all listings (vs 3.2% in 2024).

First party fraud share of total listings

First party fraud year-on-year growth in credit volume listings



What drives first-party fraud?

- **Document manipulation:** This is a primary driver of accelerating first-party fraud, evidenced by a 14.3% surge in false document credit listings (following almost no growth last year) and a renewed upward trend in non-credit listings.
- **Technological accessibility:** GenAI tools and online tutorials have significantly lowered the barrier to entry for creating high-quality, falsified financial documents like payslips and bank statements. We are seeing a move away from identity theft toward identity manipulation, as the ease of using GenAI for first-party fraud likely reduces the need for external criminal assistance, potentially accounting for the decline in third-party fraud.
- **Product targets:** This type of fraud is most prevalent in personal loans, mortgages and auto finance, where higher limits provide a greater incentive for dishonesty.

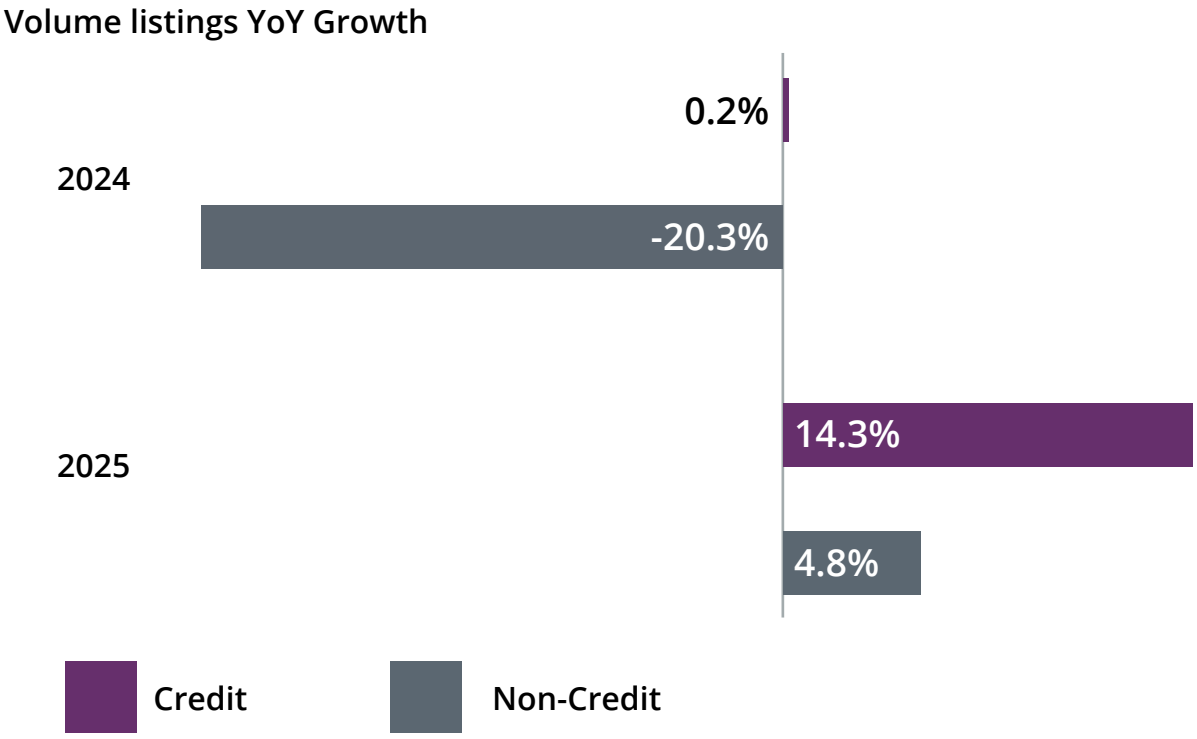
Types of first-party and third-party fraud

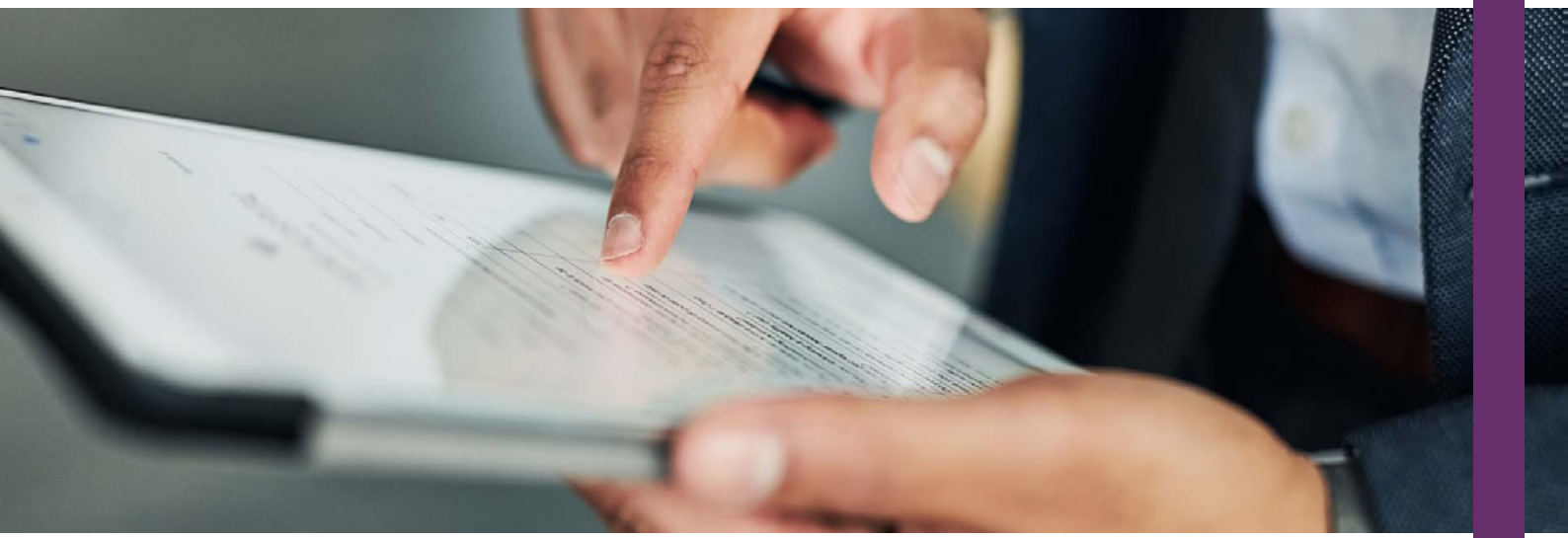
Document fraud

Advances in technology have made document fraud increasingly easier and more prevalent. It involves individuals (first-party) or intermediaries like brokers, agents, or dealers (third-party) submitting false documents during the application process. This can include altering existing documents, creating entirely fake documents, or fabricating aspects of an identity.

Common types of document fraud include document forgery, document alteration, synthetic identity fraud and document image fraud.

First and third party false documents





What drives document fraud?

- **Financial pressures:** Individuals facing economic hardship may be more inclined to engage in document fraud for financial gain.
- **Coercion and exploitation:** Some individuals may be pressured or manipulated into falsifying documents by first or third parties.
- **Technological accessibility:** The availability of sophisticated yet affordable technology enables the creation of high-quality fraudulent documents and lowers the economic barrier for sophisticated fraud. This increases the confidence of bad actors that the forgeries will pass verification, encouraging their use.
- **Increased online activity:** The shift towards online platforms and transactions has created more opportunities for fraudsters to exploit personal information[10].
- **Prevalence of scams:** The rise in scams has fueled the demand for forged documents, which are used to deceive victims and facilitate fraudulent activities.

Conflicting information fraud

Conflicting information fraud occurs when individuals (first-party) or intermediaries (third-party) provide false or inaccurate information on credit applications, significantly impacting a lender's decision-making process.

What drives conflicting information fraud?

- **Financial pressure:** Individuals facing economic hardship may misrepresent their financial situation to improve their chances of approval.
- **Coercion or pressure:** Applicants or third parties may be pressured to provide false information.
- **Inadequate controls:** Weaknesses in the application process, such as insufficient verification or incentives to overlook inconsistencies, can enable this type of fraud.
- **Lack of scrutiny:** Failure to thoroughly examine application details, such as inconsistencies in addresses, employment history, or income, can allow conflicting information to go undetected.

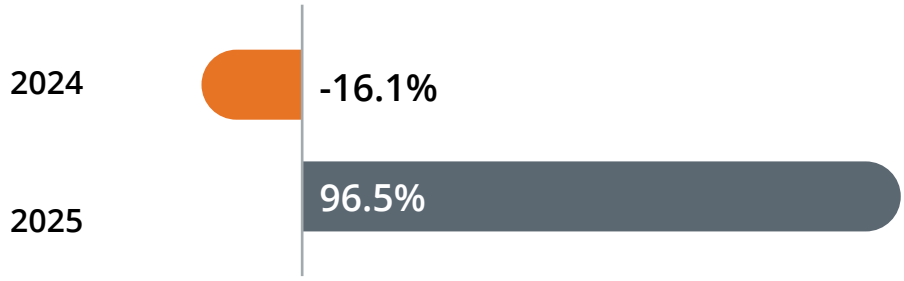
[10] https://www.redflagreporting.com/document-fraud-is-on-the-rise-what-you-should-know/

Niche Threats Grow

The most aggressive growth in 2025 was seen in specialised categories, with smaller, high-impact fraud like synthetic identities and bust-outs surging by 96.5%. While this group still only represents 1.1% of total listings it has nearly doubled its share of listings from 2024.

Share of total listings

Year-on-year growth in credit volume listings



Fraud types within this category:

- **Synthetic identities:** These involve the creation of fabricated personas by combining real and fake information like name, date of birth and drivers licence. These identities are notoriously difficult to detect as they bypass traditional verification and can remain dormant or appear legitimate for extended periods.
- **Bust-out (Never Pay) fraud:** Characterised by an intent to defraud from the outset. Bad actors obtain credit with no intention of repayment, often showing a pattern of zero payments or multiple missed payments within the first 90 days of account opening.
- **False fraud claims:** This involves genuine individuals submitting fraudulent claims – such as false financial hardship or unauthorised transaction claims – to gain a financial benefit or avoid repayment obligations.
- **Merchant fraud:** Occurs when a merchant knowingly processes unauthorised transactions or steals card information for financial gain.

Drivers of Growth:

- **AI and deepfakes:** Generative AI has made fabricated identities increasingly convincing, blurring the lines between real and deepfakes and allowing these threats to bypass automated security.

Useful reading:

- Championing Digital Trust
- What is synthetic identity theft?
- eCommerce Fraud Prevention and Detection Best Practices for Businesses

Global Fraud Spotlight

To provide broader context on the shifting threat landscape, we have curated a snapshot of recent fraud metrics from other Equifax regions. These insights highlight universal challenges and unique variations in global financial crime.

Canada

Canadian trends demonstrate how fraud adapts to economic and demographic changes, mirroring several shifts observed in the Australian market.

- **Synthetic identity surge:** Synthetic identity fraud more than doubled over a two-year period, frequently targeting younger consumers who typically have more data available online that can be used to create fake identities.
- **Mortgage misrepresentation:** Over 95% of fraudulent mortgage applications involved falsifying financial information to secure better terms.
- **Auto fraud vulnerability:** New to Credit/Canada consumers experience auto application fraud at more than double the rate of established consumers (0.51% versus 0.22%).
- **First party fraud:** The majority of first party fraud is conducted by consumers aged 26 to 35 with credit scores of 650-749.

Brazil

Data from Brazil reveals a rapid escalation in attempt volumes and an aggressive pivot toward advanced technical methods.

- **Explosive attempt volume:** Fraud attempts surged by 117.5% in Q1 2025 compared to the previous year.
- **Loss prevention:** The average value of blocked fraud attempts rose by 143.9% year-over-year, reaching an average of R$2,231.30 ($616.51 AUD).
- **AI-enabled tactics:** Scammers are increasingly adopting AI, reflecting a global shift toward more technical, automated fraud methods.
- **Prevention efficacy:** While suspected cases rose by 41.5%, confirmed fraud cases actually fell by 3.4%, demonstrating the vital importance of real-time anti-fraud technology.

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 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:** We 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

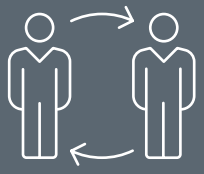
Verify customers in real-time and meet AML/CTF screening requirements.

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.

Identity Verification and Fraud Prevention

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

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.

Fraud Check: A members-only collaborative knowledge-sharing service designed to stop fraudsters with unparalleled access to fraudulent information in Australia.

Global Screening: 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 defense.

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 us to learn how our leading fraud and ID solutions can help protect your business.

EQUIFAX®