

THE SCEÁWIAN AUSTRALIAN INVESTIGATION & FRAUD INDEX 2026

An intelligence-led analysis of published Australian data on scams,
deception and investigative risk.

THE TRUTH HAS A TRAIL.

28 SEPTEMBER 2026 / AUSTRALIA

The signal in the noise.

Australia recorded \$2.18 billion in combined reported scam losses in calendar 2025, up 7.8% from 2024, across five major reporting channels. Yet the ABS found a lower household scam victimisation rate in 2024-25. These series measure different populations, periods and events; together they point to a landscape in which fewer surveyed people may experience a scam while reported financial harm remains acute. [1][2]

\$2.18bn

combined reported scam losses, 2025

[1] NASC

10.4%

card fraud victimisation, 2024-25

[2] ABS

\$166.8m

payment redirection losses, 2025

[1] NASC

Six findings

- Investment scams remained the largest combined loss category at \$837.7 million; payment redirection rose to \$166.8 million. [1]
- The ABS estimated 596,600 people aged 15 and over experienced a scam in 2024-25; 2.3 million experienced card fraud. Categories can overlap. [2]
- Business email compromise remains a serious operational exposure: it represented 15% of self-reported business cybercrime threats to ReportCyber in 2024-25. [3]
- The OAIC received 1,205 eligible data breach notifications in 2025, 716 attributed to malicious or criminal activity. [5]
- Commonwealth entities recorded 14,323 internal fraud/corruption allegations in 2024-25; these are allegations, not proven incidents. [6]
- In a selected ASIC sample, 134 companies reported 8,095 whistleblower-channel disclosures in 2024-25. They were not all fraud or substantiated matters. [14]

The most consequential trail often runs through ordinary systems: a changed bank detail, an access log, a supplier record or a reused identity.

Four lenses. Four different denominators.

This publication is an editorial index of investigative signals, not a proprietary numerical score. It interprets published Australian sources available at 28 September 2026. None of the figures below should be added together to estimate total national fraud. [1]-[7][14]

01 REPORTED LOSS

NASC/ACCC collates reports to Scamwatch, ReportCyber, AFCX, IDCARE and ASIC. It describes known reported losses, after adjustments for duplicates and unreliable high losses. [1]

02 SURVEY EXPERIENCE

ABS interviews people in private dwellings; AIC surveys an online panel. Victimization percentages are not report counts or dollar losses. [2][4]

03 INCIDENT RESPONSE

ASD/ACSC describes reports made through cyber channels and costs self-reported by reporting businesses. Its denominator is reporters, not all businesses. [3]

04 ADMINISTRATIVE RECORD

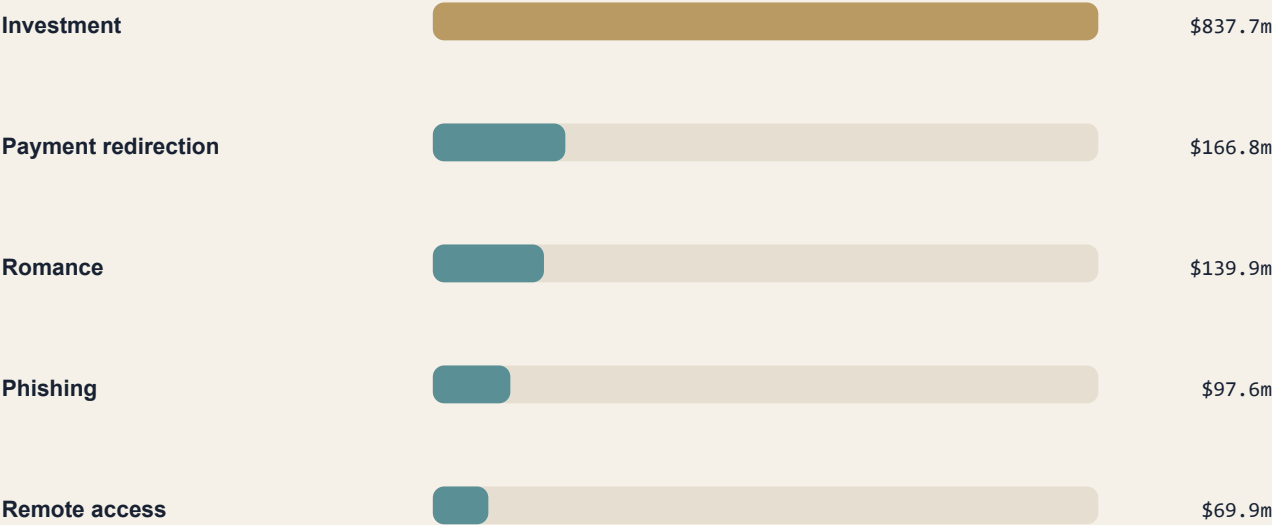
OAIC notifications and the AIC Commonwealth census describe their statutory/reporting populations, not every breach or fraud in Australia. [5][6]

A larger number can reflect a wider capture system. A smaller rate can reflect a different survey window. The source definition is part of the finding.

Financial harm concentrates in a few forms.

The National Anti-Scam Centre recorded 481,523 combined scam reports in 2025, 2.3% fewer than in 2024, while reported losses rose 7.8% to \$2.18 billion. Of the reports, 274,577 involved financial loss. The five largest loss categories accounted for 60% of the combined total. [1]

2025 COMBINED REPORTED LOSSES / A\$ MILLION



Source: NASC combined data, calendar 2025. Values are reported losses, not prevalence. [1]

Interpretation

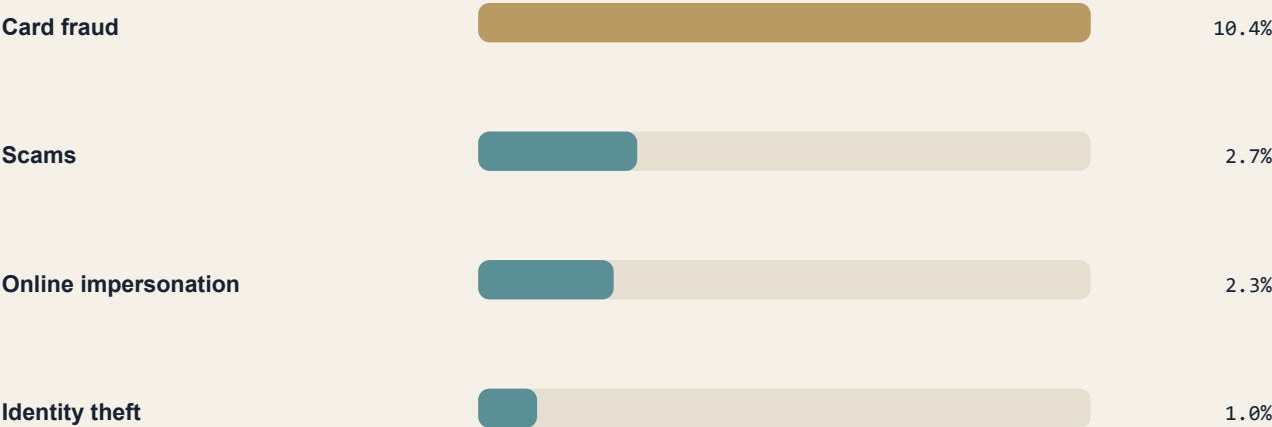
The investment category is still the largest loss pool, despite falling from \$945 million in 2024. Payment redirection rose from \$152.6 million to \$166.8 million. This is a published-category comparison, not a measure of all business invoice fraud. [1]

For investigators, follow the money and the authority trail together: who changed the destination, who approved it and what evidence was visible at the time?

The victimisation picture is broader than scams.

The ABS Personal Fraud survey estimates that 15% of Australians aged 15 and over experienced at least one selected type of personal fraud in 2024-25. Its individual categories overlap. Scam victimisation fell from 3.1% in 2023-24 to 2.7% in 2024-25, while card fraud was broadly stable. [2]

VICTIMISATION RATE / PEOPLE AGED 15+



ABS 2024-25; category overlap means bars must not be summed. [2]

What the figures change

- A missing bank balance is not the only harm. Account access, document misuse and impersonation may precede or outlast a transfer. [2][4]
- Preserve the victim’s original messages and account history before changing devices, accounts or passwords where it is safe to do so. [13]
- Build a chronology of contact, credentials, payment instructions and remediation; record reimbursement separately from initial loss.

The payment instruction is an attack surface.

\$166.8m

payment redirection losses in combined 2025 scam data

[1] NASC

15%

business cybercrime threat reports: BEC with financial loss, FY2024-25

[3] ASD

ASD's ACSC received more than 84,700 cybercrime reports in 2024-25. For businesses reporting a cybercrime, the average self-reported cost per report was \$80,850, up 50% on the prior year. This is an average among reports and is vulnerable to outliers; it is not the average loss of an Australian business. [3]

A typical evidence trail

- Original invoice and purchase order
- Supplier master-record history
- Mailbox sign-in and forwarding rules
- Approval and callback records
- Bank account changes and transfer timing
- Subsequent recovery and bank contact

Control response

Separate the approval of a supplier bank-detail change from the person entering it. Verify changes through a previously established contact channel. Preserve the native email, headers and audit trail when a redirection is suspected. These are investigative and control implications drawn from the NASC and ASD threat patterns. [1][3][13]

The fraud may start with one email, but the answer usually sits across finance, identity and messaging systems.

Stolen data becomes a reusable credential.

The ABS estimated 220,400 people experienced identity theft and 500,000 experienced online impersonation in 2024-25. The AIC's 2025 online-panel survey found 20.6% of respondents experienced identity crime and misuse in the previous 12 months. These are different definitions and sampling frames; they should not be treated as directly comparable rates. [2][4]

1,205

eligible data breach notifications, calendar 2025

[5] OAIC

716

notifications attributed to malicious or criminal activity

[5] OAIC

The OAIC total was 8% higher than 2024. It covers entities subject to the Notifiable Data Breaches scheme and incidents likely to cause serious harm; it is not a count of every compromise or every person affected. Health service providers made 225 notifications, the largest sector count. [5]

Investigative implication

- Treat identity misuse as a possible sequence: acquisition, account access, impersonation, payment or document abuse, then re-use. [2][4][5]
- Preserve the breach and downstream fraud timelines separately. A breach does not by itself prove the later fraud came from it.
- Record what was verified independently and what remains an inference.

Convincing appearance is no longer proof.

The AIC's 2025 Australian Cybercrime Survey involved 10,593 online Australians. In that panel, 11.4% reported fraud and scams in the prior 12 months; the proportion increased from the 2024 survey. The AIC cautions that much cybercrime goes unreported to police and ReportCyber. [4]

ASIC warned in 2026 of deepfake endorsements, fabricated news pages and networks of spoof websites used to make investment scams appear legitimate. ASIC took down more than 19,400 online scam items in 2025-26, 182% more than the previous year. The takedown count reflects enforcement activity and detection as well as scam supply; it is not a prevalence estimate. [7]

Verification sequence

- Capture the page, URL, timestamp and referral path.
- Check the legal entity and licence in ASIC's independent registers.
- Verify claimed people and institutions through a separate, known channel.
- Preserve original media and metadata before re-encoding.
- Document what is authentic, altered or simply unverified.

What to avoid

A single screenshot, search result or AI detection score is a weak basis for an adverse finding. Investigators need provenance, corroboration and the native record where available. ASIC specifically warns that a quick search is insufficient to verify an investment. [7][13]

The more polished the impersonation, the more important an independent source becomes.

Allegation volume is a signal, not a verdict.

In the AIC's 2024-25 census, 162 Commonwealth entities responded. Sixty-four entities received or detected 14,323 allegations of internal fraud and corruption; 58 entities recorded 348,072 external fraud allegations. Reported losses were \$2.41 million internal and \$110.70 million external. The census covers Commonwealth entities, and allegations are not findings. [6]

14,323

**internal fraud/corruption allegations in
Commonwealth entities**

[6] AIC

\$110.7m

**reported external fraud losses at Commonwealth
entities**

[6] AIC

The AIC found program information was the principal target in substantiated internal matters, while program payments were the principal target in substantiated external matters. This makes records, permissions and approval paths central evidence. [6]

Procurement is a process trail

The Commonwealth Fraud Prevention Centre identifies risk across the procurement lifecycle. NSW ICAC's 2026 Operation Tivoli found false qualifications, an undeclared family conflict and unauthorised secondary employment in a public-sector matter. This is a case illustration, not a prevalence estimate. [8][10]

- Preserve tender versions, evaluation scores, conflict declarations and approval records.
- Test relationships and qualifications against independent records.
- Keep the allegation, evidence, response and finding distinct.

Inside the organisation: what the record shows.

ASIC surveyed 134 selected Australian companies about their whistleblower programs. They reported 8,095 disclosures through designated channels between July 2024 and June 2025. This is a window into internal reporting and investigation, not a national count of corporate fraud. ASIC says the company responses were self-reported and not independently verified; the sample was not designed to be statistically representative. [14]

8,095

disclosures through designated channels

[14] ASIC

39%

average share assessed as in scope

[14] ASIC

24%

average share of investigated in-scope matters substantiated

[14] ASIC

The denominator changes at each step

The 8,095 includes grievances and other reports made through whistleblower channels. ASIC says companies assessed around 39% of disclosures, on average, as within the legal whistleblower framework. They then substantiated an average of 24% of investigated in-scope disclosures. These percentages are averages across companies, not a single national funnel; multiplying them would invent a result ASIC did not report. [14]

ASIC asked each company to nominate its single most common reported wrongdoing. Five per cent nominated fraud and 3% nominated theft or misappropriation of assets. Those shares describe companies' nominations, not the proportion of all 8,095 disclosures involving fraud. [14]

A speak-up channel measures what people report and what a company recognises. It does not measure all misconduct inside the business.

Six internal pathways to investigate.

The following are investigative typologies, not estimates of how often each scheme occurs in Australia. A concern becomes a finding only after records, alternative explanations and the affected person's response have been tested. ASIC's review establishes the relevance of internal disclosure and substantiation; it does not supply a national prevalence rate for these mechanisms. [14]

01 SUPPLIER & INVOICE

A fabricated or altered supplier, duplicate invoice or changed bank detail can turn an authorised purchase into an improper payment. Preserve supplier-master changes, invoice originals, receipts, approvals and beneficiary records.

02 PROCUREMENT & CONFLICT

An undisclosed relationship can influence specifications, quotes, evaluation or variation approvals. Compare tender versions, scoring, declarations, related parties and the timing of decisions.

03 PAYROLL & TIME

Ghost employees, altered hours, allowances or diverted pay require a joined view of employment records, rosters, access logs, payroll changes and bank-account history.

04 EXPENSES & CARDS

Personal expenditure may be disguised as a business expense or split below approval thresholds. Test receipts, merchant data, travel purpose, policy exceptions and approving relationships.

05 STOCK & ASSETS

Inventory diversion can hide behind write-offs, returns, damaged goods or manual adjustments. Reconcile stock movements, custody, access, disposal and physical counts.

06 FINANCIAL REPORTING

Management override can shift entries, classifications or timing to alter a reported result. Trace journal permissions, supporting contracts, reconciliations and review evidence.

Typology and record tests: Sceáwian investigative analysis. No prevalence or national loss estimate is implied. [14]

The reporting system is part of the evidence.

ASIC's selected company sample reported an average of 49 days to complete a whistleblower investigation. Twenty-two per cent of surveyed companies recorded no disclosures. A zero count can reflect several circumstances, including a genuinely lower volume of reportable matters; ASIC recommends testing awareness, trust and accessibility before drawing a conclusion. [14]

PROGRAMME SIGNALS IN ASIC'S 134-COMPANY REVIEW

58%

had not sought employee feedback on the programme

30%

did not regularly review programme effectiveness

25%

did not provide regular staff training

22%

recorded zero disclosures

Source: ASIC REP 827, July 2024-June 2025. Selected, self-reported company sample; not national prevalence. [14]

How an internal matter moves

- Intake: preserve the original disclosure, establish confidentiality needs and separate personal grievances from potentially protected disclosures.
- Triage: define the alleged conduct, people, period, systems, potential conflicts and immediate evidence-retention needs.
- Investigation: use a written mandate, restricted access, a chronology and an independent reviewer where conflicts or seniority require it.
- Outcome: distinguish unsubstantiated from disproven, document the standard used, offer procedural fairness and track remediation separately from disciplinary action.

A board-level response to internal fraud.

The internal-fraud question for a board is not simply how many complaints arrived. It is whether staff can raise concerns safely, whether the organisation can preserve a transaction trail, and whether material allegations are tested without management interference. ASIC observed wide variation in whistleblower practice among its 134 selected companies. [14]

01 VISIBILITY

Track the nature, source, status, age and outcome of matters separately. A larger disclosure count may reflect better access to reporting channels, not more misconduct.

02 INDEPENDENCE

Route allegations involving an executive, investigator or approving manager outside the ordinary reporting line. Record recusals, the investigator's mandate and oversight.

03 CONTROL TESTING

Look for recurring exceptions: repeated manual journals, supplier changes before payment, split approvals, unusual write-offs and override permissions. Treat anomalies as leads.

04 EVIDENCE & FAIRNESS

Issue proportionate preservation instructions early. Retain native records and access logs, test innocent explanations, and put material adverse evidence to the person affected.

05 REMEDIATION

Separate recovery, control repair, employment action and referral decisions. Assign owners and deadlines, then test whether the weakness was actually closed.

An internal allegation is a starting point. The defensible outcome is a documented trail from report to evidence, response, finding and control repair.

Where the public record cannot support a rate.

Insurance fraud

The Insurance Council of Australia describes fraud spanning exaggerated claims, misrepresentation and fabricated losses. In November 2025 it announced an industry collaboration to build a shared fraud detection and investigation platform, initially focused on motor claims. These sources establish the risk and response, but do not provide a current, comparable national insurance-fraud loss series. We do not publish an unsupported dollar estimate. [11][12]

Geography

The ABS provides state and territory survey tables, but the national figures used here, combined scam reports, cybercrime reports, privacy notifications and Commonwealth entity allegations have different denominators and reporting pathways. Raw report counts cannot rank the risk of Sydney, Melbourne, Brisbane or any state. No cross-jurisdiction league table is included. [1]-[6]

A missing denominator is itself a finding. Without it, a map can look authoritative while saying very little about comparative risk.

What would close the gaps

- Consistent, de-duplicated incident definitions across reporting systems.
- Population or transaction-based denominators for meaningful geographic comparisons.
- Public insurance claims-fraud series with clear detection and loss definitions.
- Repeatable measures of investigative outcomes and recovery, not only initial reports.

Find the trail. Preserve its context.

Open-source intelligence (OSINT) can identify leads, relationships and contradictions, but a public profile or search result is not proof of identity or misconduct. Digital evidence needs a collection record, time zone, source, access history and preserved original. ASD's incident-response guidance calls for documented collection and handling, including dates, people, locations and hash values where applicable. [13]

01**DEFINE**

Frame the allegation and rival explanations.

02**PRESERVE**

Secure native files, logs, devices and transaction records.

03**TRIANGULATE**

Compare independent people, systems and documents.

04**TEST**

Put material inconsistencies to the relevant person fairly.

05**EXPLAIN**

Separate observation, inference and conclusion.

An investigation is defensible when another reader can retrace how each finding was reached.

Five developments to test, not forecast.

The following are Sceáwian's forward-looking risk judgements based on the cited 2025-26 evidence. They are scenarios for monitoring, not predictions or measured 2027 outcomes. [1][3][5][7][11]

01 SYNTHETIC AUTHORITY

Voice/video impersonation paired with spoof news, registers or company pages. Test independent verification and original-media provenance. [7]

02 SUPPLIER-CHANNEL CAPTURE

Compromised mailboxes or altered master data redirect legitimate payments. Monitor bank-detail changes, approvals and callback failures. [1][3]

03 IDENTITY REUSE AFTER BREACH

One data exposure can support later impersonation, account access and tailored contact. Watch for linked identifiers and time gaps. [2][4][5]

04 CONNECTED PROCUREMENT MISCONDUCT

Conflict, false credentials and record manipulation can cross recruitment, contracts and secondary employment. Link registers and decision trails. [8][10]

05 NETWORKED CLAIMS ANOMALIES

The ICA's planned shared detection capability points to cross-insurer pattern analysis. Treat alerts as leads requiring validation. [11]

What leaders can change now.

BOARD / EXECUTIVE

Track losses, control failures, disclosures and unresolved allegations separately. Require independent handling for matters involving senior decision-makers. [14]

FINANCE / PROCUREMENT

Use independent supplier callbacks, dual control for bank changes and retrievable approval/audit logs.

LEGAL / PEOPLE

Set the mandate early; protect disclosers, preserve volatile material, manage conflicts and give a fair opportunity to answer adverse evidence. [14]

CYBER / PRIVACY

Keep time-synchronised logs, access records and breach decisions. Join technical and financial chronologies without collapsing them.

INSURER / INVESTIGATOR

Treat anomaly scores and OSINT as leads. Keep native evidence and a documented chain of handling.

These actions are Sceáwian analysis of the risks documented in sources [1]-[14]; they are not a substitute for matter-specific legal advice.

Findings ready to quote.

- 01 “Australia’s reported scam losses rose to \$2.18 billion in 2025 even as the latest ABS household survey recorded a lower scam victimisation rate. The two measures tell different parts of the story.” [1][2]
- 02 “Payment redirection is a business-process crime as much as a cybercrime. The decisive evidence may be in a supplier change log, an approval trail or a mailbox rule.” [1][3]
- 03 “ASIC’s 134-company review recorded 8,095 whistleblower-channel disclosures. That is a view of internal reporting, not a count of proven corporate fraud.” [14]
- 04 “The public data does not justify a city-by-city fraud league table. A convincing map without comparable denominators would mislead readers.” [1]-[6]
- 05 “AI-generated credibility cues make independent verification and original evidence more important, not less.” [7][13]

Scope, safeguards and limitations.

Selection and cutoff

Sources were selected for primary collection, institutional authority, explicit definitions and availability by 28 September 2026. The principal reporting windows are calendar 2025 or financial year 2024-25; ASIC enforcement covers FY2025-26. ASIC's corporate whistleblower review covers July 2024-June 2025. [1]-[7][14]

No numerical score

"Index" is an editorial frame for a structured evidence review. Sceáwian did not conduct its own survey, audit a national case sample, estimate dark figures or create a composite risk score. Figures remain attributed to their publishers.

Editorial verification

All material figures are tied to source numbers in the text and full source notes on the following pages. Calculated comparisons are identified in prose. Forward-looking watchlist items are expressly analytical. Case examples are identified as cases, not prevalence. Recheck source pages before reuse after this edition date.

Suggested citation: Sceáwian Intelligence Group (2026), The Sceáwian Australian Investigation & Fraud Index 2026, public research edition, 28 September 2026.

Comparability

Reporting channels, surveys, administrative notifications and entity censuses have different units. Some reports can overlap across systems even after source adjustments. Under-reporting, detection effort, changing definitions and sampling error affect interpretation. No totals are summed across series. [1]-[6]

Coverage boundaries

Consumer, business, Commonwealth and insurer examples are not a complete national fraud census. ASIC's 134-company whistleblower sample is self-reported, includes some non-Australian employee data and is not statistically representative. The Commonwealth census excludes private-sector internal fraud. The insurance section omits a national fraud-loss estimate. [6][11][12][14]

Primary record and reading notes.

Source numbers in the body refer to the records below. Links are active in this PDF. Source pages were checked for this edition on 28 September 2026.

[1] NATIONAL ANTI-SCAM CENTRE / ACCC

Targeting scams: report on scams data and activity 2025, 30 March 2026. Combined report and loss data, categories and methodology.

[Open primary source on `accc.gov.au`](#)

[2] AUSTRALIAN BUREAU OF STATISTICS

Personal Fraud, 2024-25 financial year, released 12 March 2026. Household survey, national rates and methodology.

[Open primary source on `abs.gov.au`](#)

[3] AUSTRALIAN SIGNALS DIRECTORATE / ACSC

Annual Cyber Threat Report 2024-25, 14 October 2025. ReportCyber and business cost measures.

[Open primary source on `cyber.gov.au`](#)

[4] AUSTRALIAN INSTITUTE OF CRIMINOLOGY

Cybercrime in Australia 2025, Statistical Report 59, 30 June 2026. Online-panel survey.

[Open primary source on `aic.gov.au`](#)

[5] OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER

2025 Notifiable Data Breaches statistics, 6 July 2026. Notification totals and cause/sector breakdown.

[Open primary source on `oaic.gov.au`](#)

[6] AUSTRALIAN INSTITUTE OF CRIMINOLOGY

Fraud and corruption against the Commonwealth 2024-25, Statistical Report 61, 11 June 2026. Census of 162 entities.

[Open primary source on `aic.gov.au`](#)

[7] AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION

ASIC warns scammers are using AI to spin vast webs of deception, 2026 media release 26-195MR.

[Open primary source on `asic.gov.au`](#)

Primary record and reading notes.

Source numbers in the body refer to the records below. Links are active in this PDF. Source pages were checked for this edition on 28 September 2026.

[8] COMMONWEALTH FRAUD PREVENTION CENTRE

Procurement Administration Counter Fraud Toolkit, October 2024. Procurement lifecycle risk guidance.

[Open primary source on counterfraud.gov.au](#)

[9] NATIONAL ANTI-CORRUPTION COMMISSION

Annual Report 2024-25. Procurement case illustration and strategic priority.

[Open primary source on nacc.gov.au](#)

[10] NSW INDEPENDENT COMMISSION AGAINST CORRUPTION

Operation Tivoli media release, 2026. Findings on qualifications, conflicts and secondary employment.

[Open primary source on icac.nsw.gov.au](#)

[11] INSURANCE COUNCIL OF AUSTRALIA

ICA, EXL and Shift launch insurance fraud detection collaboration, 20 November 2025.

[Open primary source on insurancecouncil.com.au](#)

[12] INSURANCE COUNCIL OF AUSTRALIA

Insurance fraud: consumer information and fraud typology.

[Open primary source on insurancecouncil.com.au](#)

[13] AUSTRALIAN SIGNALS DIRECTORATE / ACSC

Cyber security incident response planning: practitioner guidance. Evidence collection and preservation.

[Open primary source on cyber.gov.au](#)

[14] AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION

REP 827, Insights from the ASIC whistleblower questionnaire: July 2024 to June 2025, published 4 December 2025. Selected 134-company self-reported review.

[Open primary source on download.asic.gov.au](#)

The truth has a trail.

The figures in this edition describe harm, exposure, reporting and institutional response from different angles. The investigative task is to trace a specific matter through original evidence, test alternative explanations and explain the result without exceeding what the record can support.

Evidence earns trust when its path is visible.

Sceáwian Intelligence Group / Australia

sceawian.com.au

Public research edition, 28 September 2026. Published Australian data; Sceáwian analysis. © Sceáwian Intelligence Group 2026.