
Australian
Payments
Network
AUSTRALIAN
PAYMENT FRAUD
2025
JANUARY – DECEMBER 2024 DATA

FOREWORD

Welcome to the 2025 *Australian Payment Fraud Report*, which covers current trends in card and cheque fraud, helps assess the impact of industry initiatives and guides our pursuit of new measures.

Payment fraud losses are often profound, extending beyond financial injury (which itself can be life-altering) to harmful effects on the mental health and wellbeing of victims. Too many Australians continue to be affected by these crimes.

Cybercriminals are evolving their methods, including by using agentic artificial intelligence, creating new threats. But as this occurs, Australian Payments Network (AusPayNet) remains committed to mitigating and preventing economic crime, including payment fraud.

Encouragingly, in 2024, the domestic card-not-present (CNP) fraud rate continued to decline to a record low of 97 cents per $1,000 spent. This decline suggests AusPayNet's CNP Fraud Mitigation Framework, established in 2019, is having an impact in its efforts to make domestic CNP fraud more difficult to perpetrate.

However, as we identified last year, overseas CNP fraud is a rising issue. In 2023, overseas CNP fraud overtook domestic CNP fraud for the first time and, in 2024, outpaced domestic CNP fraud by $92m. While only 3 per cent of the total card spend last year involved Australian cards used overseas, 50 per cent of all card fraud was attributable to overseas CNP fraud. In other words, overseas CNP fraud occurred at a rate more than 12 times higher than domestic CNP fraud.

Overseas CNP transactions typically lack the robust customer authentication controls applied to domestic CNP transactions, creating vulnerabilities that transnational criminals exploit to perpetrate payment fraud and execute higher-value scams. Stolen credentials are used to purchase digital services that enable broader scam infrastructure, including digital advertising and telecommunications services. These digital services are then used to facilitate the operations of scam compounds on an industrialised scale, often exploiting workers who are victims of human trafficking.

Successfully addressing this complex challenge requires a global, whole-of-ecosystem response. In Australia, we facilitate the Economic Crime Forum, bringing together our industry and law enforcement to share intelligence and develop tactical initiatives, including a National Day of Action that disrupted criminals using SIM boxes

Andy White, CEO

> “ Successfully addressing this complex challenge requires a global, whole-of-ecosystem response.

to scam Australians and obtain their card data. I also sit on the Advisory Board of the National Anti-Scam Centre (NASC), while our Head of Economic Crime participates in NASC's fusion cell and working groups, which successfully supported the expansion of website takedown services to include e-commence scam sites. The Australian Financial Crime Exchange's anti-scam intelligence loop is now in operation and enables industry to share malicious telephone numbers and websites that should be blocked or taken down. We have also become a supporting member of the Global Anti-Scam Alliance, where a key focus is targeting scam compounds that appear to be the source of card fraud and scams.

AusPayNet welcomes the recent passage of the *Scams Prevention Framework Act 2025*. This coordinated, cross-sectoral framework will ensure designated sectors adopt appropriate measures to prevent, detect, disrupt and respond to scams.

As I've said previously, in working to prevent economic crime we are better together. AusPayNet looks forward to continuing work on multiple fronts to protect payments system end-users against cybercriminals and to boost trust in the digital economy.

Andy White
Chief Executive Officer, AusPayNet

PAYMENT FRAUD IN 2024

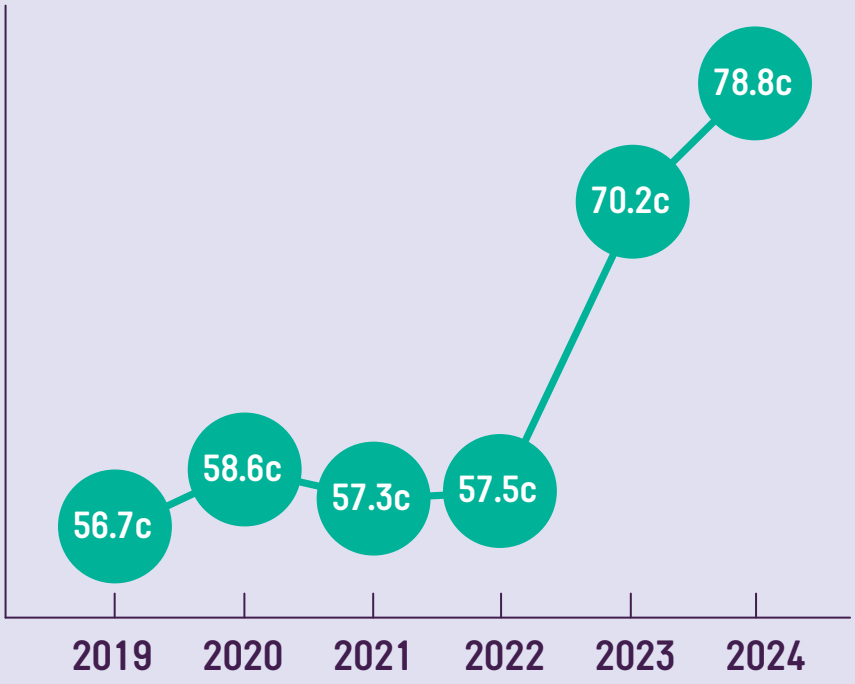
Total value of card transactions increased 7% to $1.16t; following an increase of 8% in 2023.

For Australian-issued cards:

- Total value of card fraud **increased by 20% to $913m**
- Card-not-present (CNP) fraud **rose 19% to $816m** after increasing 33% in 2023
- Lost/stolen card fraud was **up by 31% to $68m**, after increasing 24% in 2023
- Counterfeit/skimming **decreased by 20% to $6.2m** after increasing 8.5% in 2023
- Fraud involving cards never received increased **41% to $2.4m** but remains well below pre-pandemic levels
- After remaining steady for the past three years, fraudulent applications **increased 56% to $1.4m**
- 'Other' fraud **increased 63% to $18.7m**
- The use of cheques has continued to decline, **down by 32% to 15m**
- Value of fraudulent cheque transactions **dropped 44% to $2.7m**

CARD FRAUD RATE

The fraud rate on Australian-issued cards increased to **78.8 fraud cents per $1,000 spent**, a 12% year-on-year increase, driven by the growth in overseas CNP fraud.



** Detailed six-year statistics (sourced from the Reserve Bank of Australia and AusPayNet) are available from page 12 in this report.*

2024 SNAPSHOT

CARD USE AND FRAUD

$1.16T TOTAL CARD TRANSACTIONS

+7%

$913M CARD FRAUD VALUE (AUSTRALIAN-ISSUED CARDS)

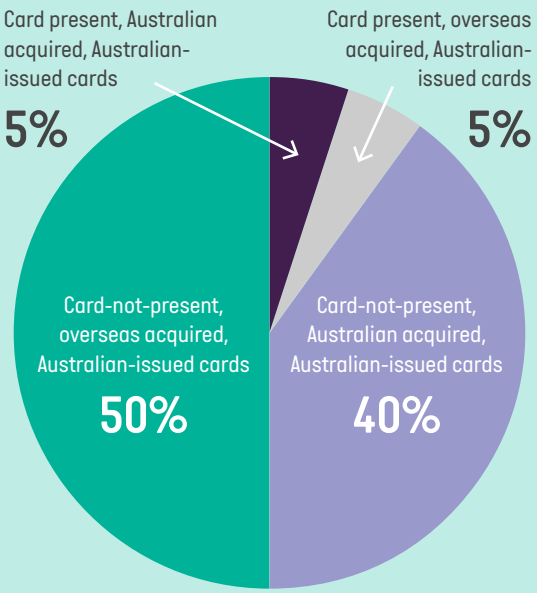
+20%

CARD FRAUD RATE

78.8c per $1,000 spent

+12%

CARD FRAUD CATEGORIES



*Card present fraud is the sum of:

- lost / stolen
- never received
- fraudulent application
- counterfeit / skimming

CHEQUE USE AND FRAUD

15M CHEQUES TRANSACTED

-32%

$194B VALUE OF CHEQUES

-24%

$2.7M FRAUDULENT CHEQUES

-44%

$816M
CARD-NOT-PRESENT
+19%

$6.2M
COUNTERFEIT / SKIMMING
-20%

$68M
LOST / STOLEN CARD
+31%

$2.4M
CARDS NEVER RECEIVED
+41%

$1.4M
FRAUDULENT APPLICATION
+56%

$18.7M
OTHER FRAUD
+63%

CARD FRAUD

Total spending on Australian cards rose 7 per cent in 2024 to $1.16 trillion. Total card fraud increased 20 per cent over the same period to $913 million, with the rate of increase slowing from 32 per cent in 2023. The overall fraud rate in 2024 was 78.8 cents per $1,000 spent compared to 70.2 cents in 2023, which is a 12 per cent increase year-on-year and the highest fraud rate since AusPayNet commenced publishing fraud statistics in 2012, driven by the increase in overseas CNP fraud.

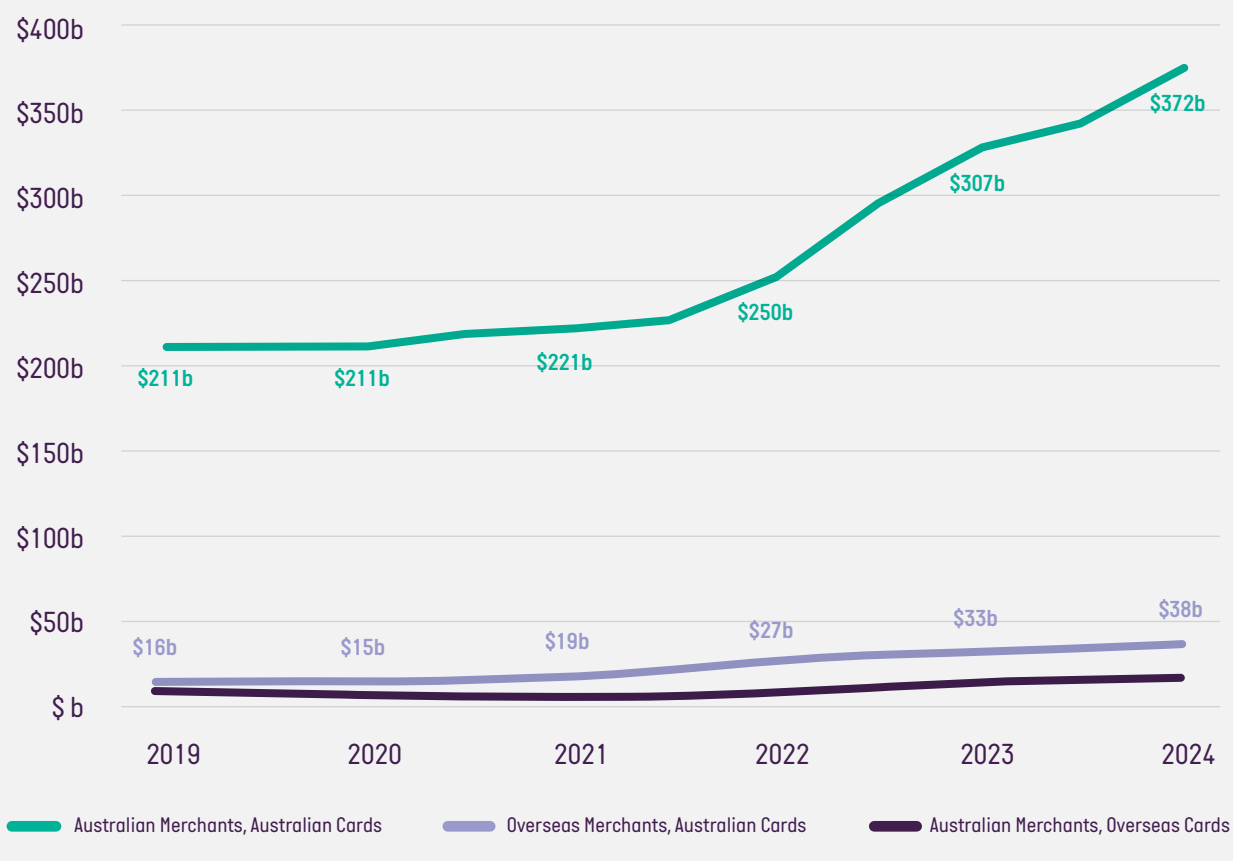
CARD-NOT-PRESENT (CNP) FRAUD TRENDS

Total CNP spending on Australian cards increased 20 per cent in 2024 to $410 billion, reflecting the ongoing rise in the popularity of e-commerce. The total value of CNP fraud on Australian-issued cards used either at Australian merchants or overseas merchants increased by 19 per cent to $816 million, continuing to account for approximately 90 per cent of all card fraud in Australia.

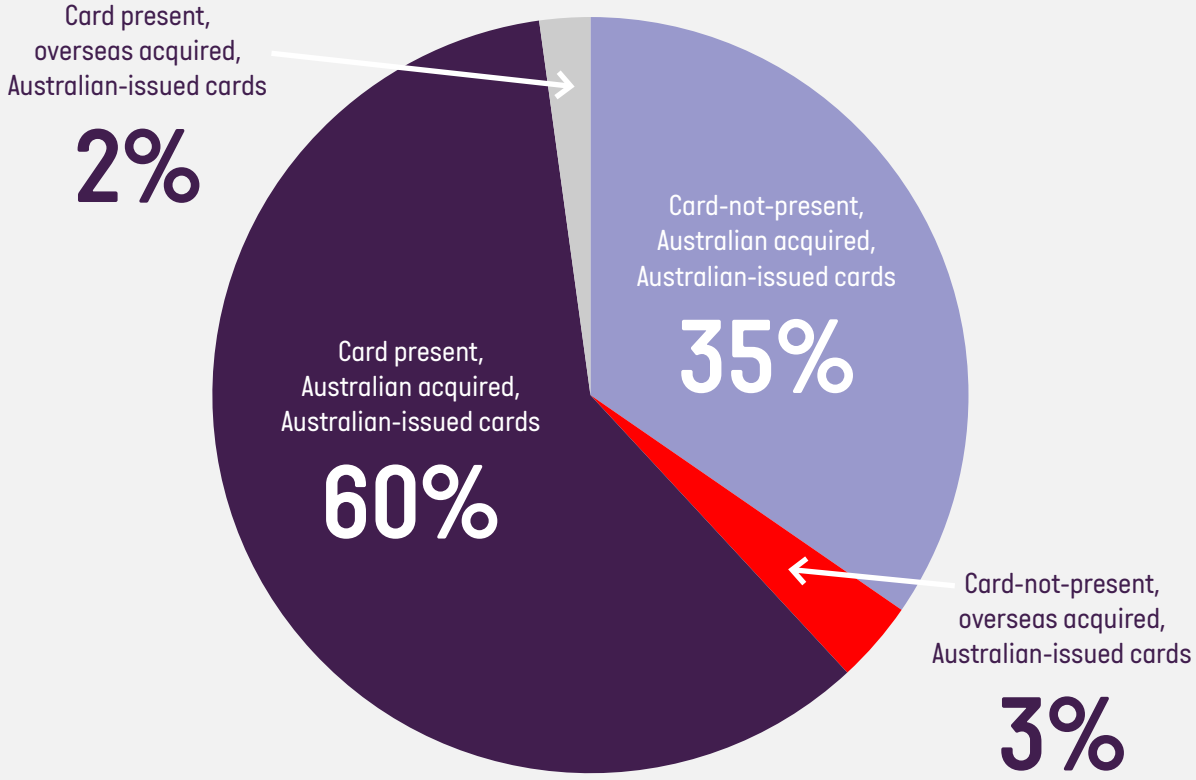
Last year's report showed a 33 per cent increase in CNP fraud losses, primarily driven by a 51 per cent rise in CNP fraud on Australian-issued cards used at overseas merchants. In 2024, that trend continued. Fraud losses in this category increased a further 25 per cent to $454 million, exceeding the 15 per cent growth in spending in this category over the same period ($38 billion). So, in 2024, while CNP transactions via overseas merchants made up only 3 per cent of the total value of all card transactions, 50 per cent of all card fraud involved transactions in this category. Overseas CNP fraud occurred at a rate of $12.08 per $1,000 spent. The suspected cause of this trend and the industry measures being implemented to address this challenge are outlined later in the report.

In contrast, CNP fraud on Australian cards used at Australian merchants increased 11 per cent to $362 million, but it was lower than the spending growth rate of 21 per cent, to $372 billion. This resulted in an 8 per cent decrease in the fraud rate for domestic CNP fraud, from $1.06 per $1,000 spend in 2023 to a record low of 97 cents per $1,000 spent in 2024.

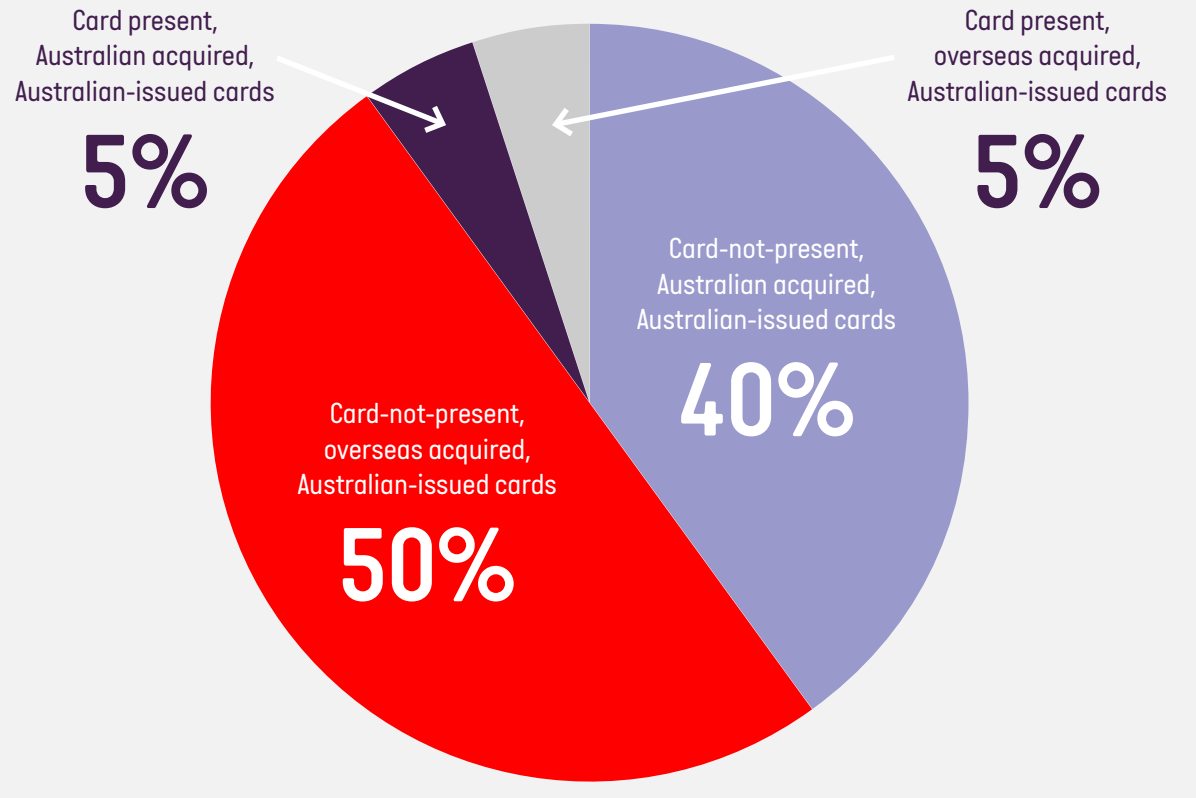
CNP SPEND BY CALENDAR YEAR



CARD SPEND 2024

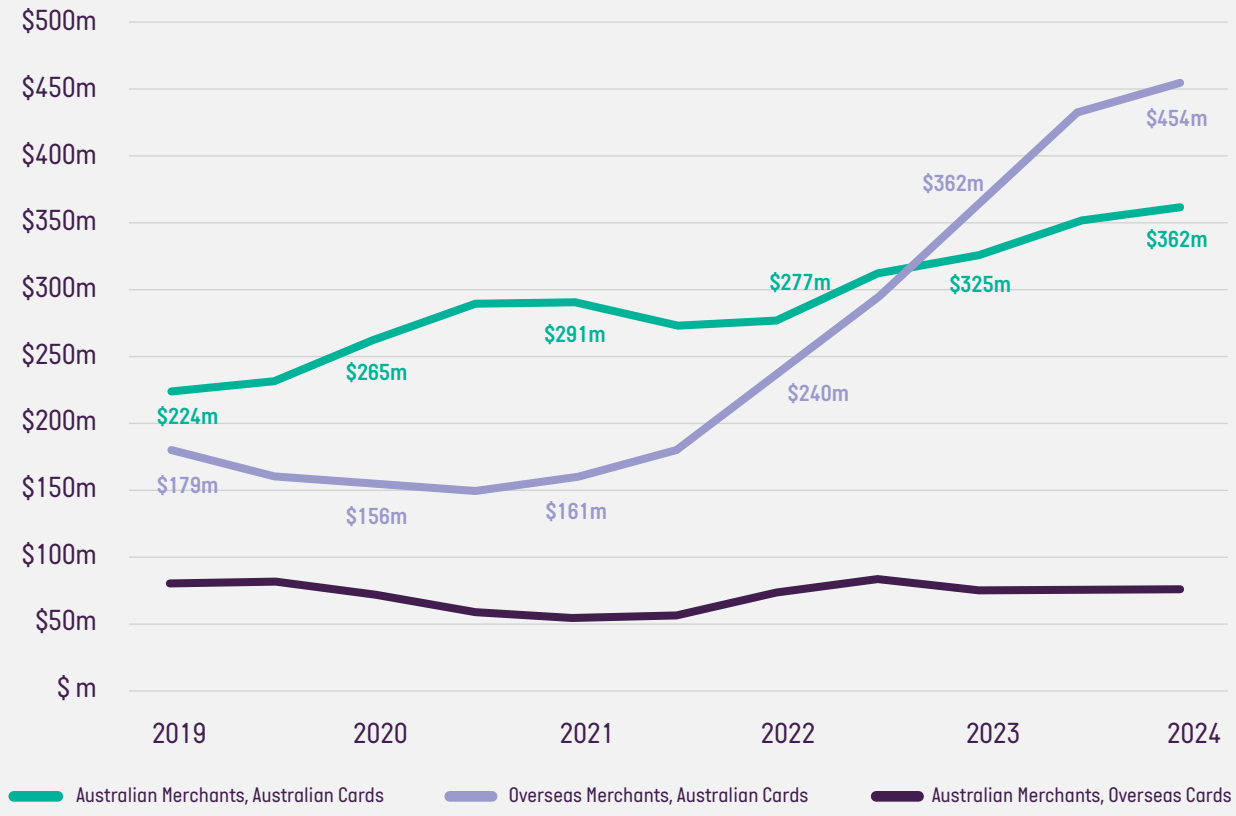


CARD FRAUD 2024

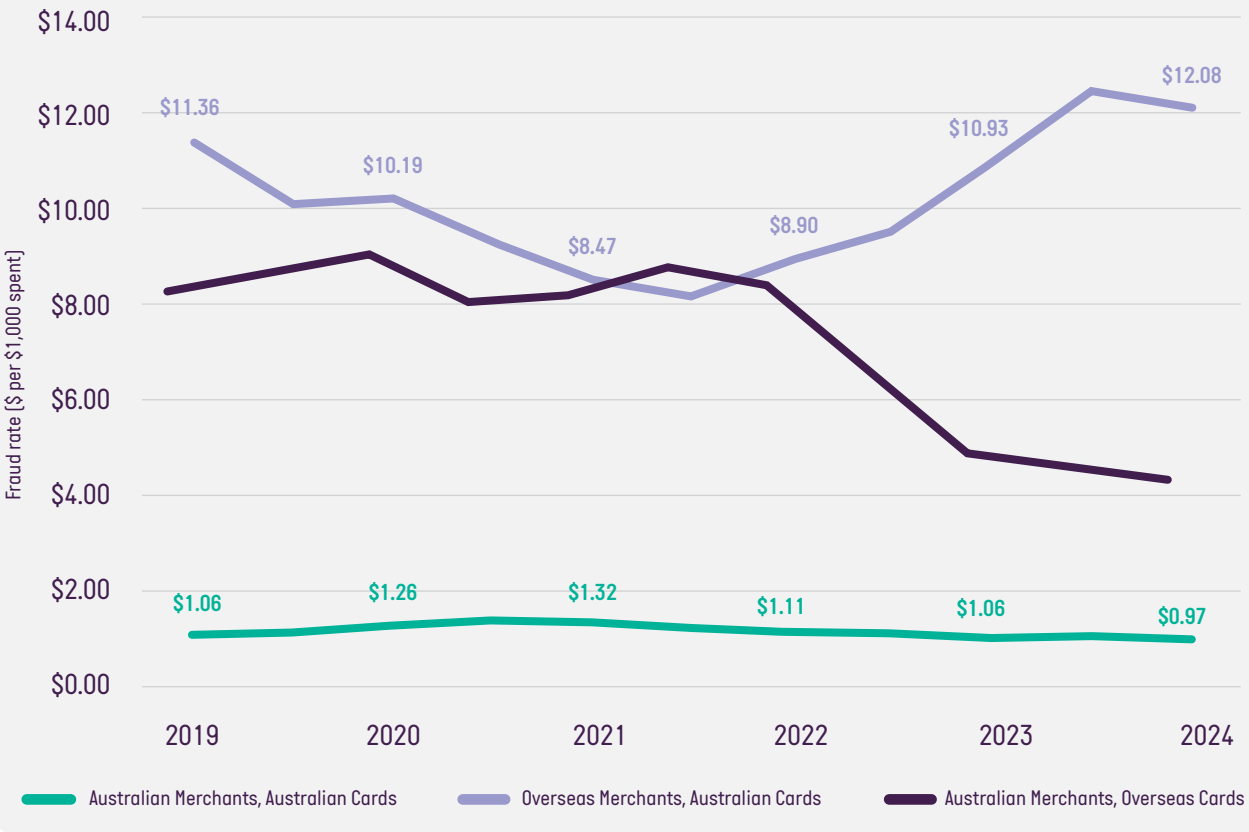


*Card present fraud is the sum of: - lost / stolen - never received - fraudulent application - counterfeit / skimming

CNP FRAUD VALUE BY CALENDAR YEAR



CNP FRAUD RATE BY CALENDAR YEAR



HOW CNP FRAUD IS PERPETRATED

CNP fraud typically occurs in one of two scenarios:

- when criminals steal valid card details and then use those details to make purchases or other payments via a remote channel without the physical card being seen by the merchant, mainly online via a web browser or by phone; or
- when a cardholder fraudulently disputes a legitimate transaction in the hopes of obtaining both the goods/service and recovering the money (first-party misuse).

Criminals can steal valid card details using several methods, including:

- **Bank Identification Number (BIN) attacks:** criminals take the BIN (the first six digits of a card number) and use computer software to generate the remaining sequence of numbers. The card numbers generated are verified (by completing payment transactions for small amounts on websites) and then used to complete larger transactions.
- **Data breaches and cyberattacks on e-commerce platforms:** an organisation's website is compromised, enabling criminals to access customers' personal information (including card details) stored in that website's database.
- **Insecure transactions:** criminals intercept card details when a cardholder makes a payment on an unsecured website or by using a public Wi-Fi network.
- **Malware:** criminals infect a cardholder's computer system using software (including viruses, worms and spyware) to obtain card details.
- **Skimming:** criminals steal card numbers and PINs by attaching small electronic devices to ATMs or point-of-sale (POS) terminals.
- **Phishing scams:** Criminals may trick cardholders into sharing their card details as part of a scam, such as online shopping, buying and selling, or false billing.

CARD PRESENT FRAUD TRENDS

Lost and stolen card fraud refers to unauthorised transactions on cards that have been reported by the cardholder as lost or stolen. Fraud on Australian cards rose 31 per cent from last year to $68 million, with losses split relatively evenly between cards lost or stolen domestically and overseas. This marks a shift from the previous two years, when growth was driven primarily by overseas incidents. In Australia, criminals exploit found or stolen cards at POS terminals for purchases under the contactless threshold — where neither a PIN nor signature is required — before cardholders report the theft or fraud detection systems block the transactions.

Counterfeit/skimming fraud was down 20 per cent in 2024 to $6.2 million, after increasing 8.5 per cent in 2023. The reduction in this category coincides with Australian and international law enforcement disrupting foreign organised crime syndicates travelling to Australia to perpetrate ATM skimming activities[1].

Counterfeit/skimming fraud occurs when details from a card's magnetic stripe are skimmed at an ATM, POS terminal, or through a standalone skimming device, and used to create a counterfeit card. Criminals use the counterfeit card to purchase goods for resale or, if the PIN has also been captured, to withdraw cash from an ATM.

Fraud involving cards never received increased 41 per cent to $2.4 million. Never received fraud occurs when transactions are made on a card that was stolen before it was received by the owner. Feedback from law enforcement partners indicates some criminals still pursue this type of crime via mail theft.

Fraud involving fraudulent applications occurs when transactions are made on a card where the account was established using someone else's identity or other false information. After remaining flat for the past three years, fraudulent applications increased 56 per cent to $1.4 million. In the wake of recent data breaches, the industry has been increasing the sophistication of its customer verification processes, including ongoing enhanced customer due diligence and biometric verification for new accounts.

Other card fraud increased by 63 per cent to $18.7 million. This category covers fraudulent transactions that cannot be categorised as any of the common fraud types listed above, including account takeover fraud and malicious activity by a merchant (such as duplicate charging, misrepresentation of purchase and manipulation of the cardholder). Engagement with Members has identified three potential reasons for this increase: card scams involving criminals tricking a victim into providing their strong customer authentication one-time-pin to unknowingly authorise a transaction; criminals leveraging tap-to-pay technology to trick a victim to unknowingly authorise a transaction[2]; and some occurrences of first party misuse that, while typically classified as CNP fraud, were categorised here due to definitional ambiguity.

Account takeover — also known as identity takeover — fraud describes malicious actors using stolen card details or credentials to access an account. They can then remotely provision a virtual card onto their mobile device for device-present payments.

1. AFP (Australian Federal Police) (2025), 'Romanian nationals charged over alleged ATM skimming scheme in NSW', Media Release, 23 May; AFP (2023), 'Five foreign nationals charged with defrauding Australians', Media Release, 5 September.
2. Jabbara M (2025), 'Relaying the message on relay fraud'. Available at <https://corporate.visa.com/en/sites/visa-perspectives/security-trust/relaying-the-message-on-relay-fraud.html>.

COMBATTING CARD FRAUD

CNP FRAUD MITIGATION FRAMEWORK (CNP FRAMEWORK)

To address the rising rates of CNP fraud, AusPayNet established the CNP Framework, which was implemented on 1 July 2019. Currently, CNP fraud accounts for approximately 90 per cent of all card fraud in Australia. The CNP Framework is designed by industry to reduce fraud on Australian cards used at Australian merchants in online channels, while enabling the continued growth of online transactions. The Framework defines the minimum requirements for an issuer, merchant, acquirer or payment gateway to authenticate CNP transactions online, establishing authentication as best practice to reduce fraud in online channels. It also encourages secure merchant technologies including real-time monitoring, machine learning and tokenisation.

The CNP Framework is enforced through AusPayNet's Issuers and Acquirers Community (IAC) Code Set. It defines fraudulent transaction value and volume thresholds that all merchants and issuers must remain below. Breaches of these thresholds trigger obligations for acquirers or issuers to take corrective action, and if these breaches are not resolved within a specified period, they can be referred to the Sanctions Tribunal, which determines whether penalties should be imposed and the size of those penalties.

Since the implementation of the CNP Framework in 2019, quarterly figures have shown a downward trend in the domestic CNP fraud rate, despite continued growth in the volume of CNP transactions. The domestic CNP fraud rate has decreased from $1.26 per $1,000 spent in 2020 to a record low of $0.97 per $1,000 in 2024.

To ensure the Framework remains fit for purpose, AusPayNet Members undertake an annual review of the CNP Framework with representatives from a diverse range of participants in the payments industry. The latest review of the Framework in 2025:

- Provided a more robust pathway for merchants to identify first-party misuse.
- Evaluated the current thresholds and fine structure, and determined that no changes are necessary at this time.
- Considered whether greater enforcement of the Card Security Code could assist in combatting CNP Fraud.
- Highlighted the issue of overseas CNP Fraud and convened a follow-up workshop to develop insights and potential mitigants.
- Explored opportunities to reduce the timeline and burden of the reporting and compliance obligations related to the Framework.

Further details on the CNP Framework are available at AusPayNet's website.

FIRST-PARTY MISUSE

First-party misuse (FPM) occurs in a few scenarios, including but not limited to:

- Transaction confusion, where consumers do not recall or recognise a transaction made. This is especially common with annual subscriptions.
- A household member or additional card holder making a transaction of which the primary card holder is unaware.
- Deliberate, fraudulent chargebacks, where a consumer receives the goods or service, but raises a dispute, attempting to get their money back.

Where the merchant, seeing what they consider to be a 'safe' transaction from a known customer, elects not to require enhanced security such as strong customer authentication, liability for fraud defaults to the merchant. While a merchant can contest a dispute as being genuine, therefore making the consumer liable, the success rate for these challenges across the Australian ecosystem is low, and many merchants do not see the commercial case for vigorous pursuit of these actions.

Visa and Mastercard have recognised this challenge and have responded with their Compelling Evidence and First Party Trust programs, respectively. These programs aim to provide additional merchant safeguards by using additional transactional data (such as previous and non-disputed transactions from the same card/device/user account) to prevent FPM disputes from being successful. These programs are in the early phase of being adopted by Australian merchants and therefore the full benefits have likely not yet been realised.

AusPayNet recognises that first-party fraud presents a significant challenge for some merchants and recently conducted a comprehensive review of this issue.

The review revealed that, while the programs described above have delivered some positive outcomes, not all FPM transactions contain the necessary information required for processing under these programs. The review further concluded that establishing a single standard for what constitutes reasonable evidence of FPM is challenging, given the substantial variations in merchants' processes and data sources.

In response to these findings, AusPayNet has provided enhanced guidance to the Sanctions Tribunal established under the CNP Framework and strengthened the CNP data reporting process. These improvements enable AusPayNet to evaluate any merchant's claim of being significantly impacted by FPM on a case-by-case basis and to provide comprehensive analysis of such claims as part of the Sanctions Tribunal process.

FIGHTING OVERSEAS CNP FRAUD AND SCAMS

The growing challenge

The figures in this report suggest that the CNP Framework continues to positively influence the level of domestic CNP fraud. However, overseas CNP fraud targeting Australian cardholders has become a critical concern, surpassing domestic CNP fraud levels since 2023.

Australian-issued cards used at overseas merchants face significant vulnerabilities. Online shopping scams, data theft, and sophisticated phishing attacks are driving this surge in overseas CNP fraud. These transactions operate outside of Australia's regulatory framework, as overseas merchants and acquirers are not subject to the CNP Framework, which requires protective measures such as Strong Customer Authentication (SCA).

The scam ecosystem connection

The rise in overseas CNP fraud coincides with the proliferation of scam compounds across Southeast Asia. According to the United Nations Office on Drugs and Crime (UNODC), many of these operations have expanded into e-commerce fraud and credit card schemes, employing tactics such as SMS SIM box phishing to harvest card details.[3]

The fraud typically follows a pattern. Consumers are initially deceived into authorising transactions, after which criminals use the stolen credentials for additional purchases via international merchants that lack SCA requirements. These fraudulently obtained goods and digital subscriptions are then resold, while the unauthorised transactions serve as stepping stones to higher-value scams, including remote access and bank impersonation scams. Evidence suggests stolen card credentials also finance scam infrastructure, including advertisements on digital platforms and telecommunications services that enable broader criminal operations.

Regulatory response and industry action

Scams Prevention Framework

The Scams Prevention Framework Act 2025, which passed in February, will establish obligations on designated sectors to prevent, detect, disrupt, and respond to scams. The Australian Government has indicated that the first tranche of designated sectors will be banks, telecommunications providers, and digital platforms[4]. The supporting industry-specific codes will be developed throughout 2025 and 2026. Given the impact of card fraud and its nexus to scams, AusPayNet anticipates that the Scams Prevention Framework and codes will assist to address CNP fraud across the scam lifecycle not only within the payments sector, but importantly by mitigating phishing scams via telecommunications and digital platforms.

Collaborative initiatives

AusPayNet facilitates the Economic Crime Forum (ECF), bringing together law enforcement, regulators, and the payments industry. Through coordinated action, including National Days of Action, members have worked with Australian law enforcement to disrupt criminal networks using SIM boxes to target Australian consumers with card phishing scams.[5] These operations generated strategic intelligence for the National Anti-Scam Centre (NASC) and telecommunications sector to address system vulnerabilities within that sector that are enabling card fraud.

AusPayNet recently joined the Global Anti-Scam Alliance (GASA) as a supporting member. Our Head of Economic Crime, Toby Evans, serves on the Board of the Oceania Chapter and participates in international workgroups focused on dismantling the scam compounds responsible for SIM box phishing scams.

AusPayNet's CEO, Andy White, serves on the NASC Advisory Board, while our Head of Economic Crime participates in fusion cell activities and working groups. AusPayNet highlighted the impact of CNP fraud and the

3. UNODC (United Nations Office on Drugs and Crime) (2024), 'Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape', UNODC Report.
4. The Treasury (2025), 'Parliament passes world-leading scams prevention framework', Media Release, 13 February.
5. AFP (2024), 'Nationwide policing operation targets widespread SIM box fraud', Media Release, 19 July.

nexus to scams, and supported the NASC expanding website takedown services to include e-commerce scams. We also supported the roll out of the Australian Financial Crimes Exchange's (AFCX) open intelligence loop, which allowed banks to share data with the telecommunications and digital platforms industry to block malicious telephone numbers and fraudulent online advertisements.

Industry engagement and future actions

AusPayNet has raised the challenge of overseas CNP fraud through our Issuers and Acquirers Forum (IAF) and continues to engage in the implementation of the Scams Prevention Framework. While overseas merchants and acquirers operate beyond AusPayNet's direct regulatory influence, we will continue to explore approaches to protect Australian cardholders through targeted workshops, industry forums, and international collaboration focused on identifying and implementing effective mitigation strategies.

CARD PRESENT FRAUD PREVENTION

Device approval process

AusPayNet maintains a governance framework for card present payment acceptance solutions deployed in Australia, with the goal of delivering an efficient, cost effective and appropriately secure service for participants, merchants and consumers.

Within this framework, a device approval process has been established for these solutions. Solutions which are approved and listed by the Payment Card Industry (PCI) can be deployed in Australia (subject to any applicable AusPayNet operating conditions) without the requirement to be registered with AusPayNet. For non-standard technology solutions which have not been approved by PCI, AusPayNet undertakes an assessment of these solutions to ensure appropriate security is in place for these to be deployed in the Australian card payments system.

The benefits of this framework are alignment to PCI security for standard solutions and a rigorous security risk assessment of non-standard solutions, helping to contribute to an overall reduction in fraud and scams while supporting innovation for the payments industry.

Migration to the Advanced Encryption Standard

As a result of advances in classical and quantum computing, there is a material risk that current methods used to encrypt card payments may be compromised. The current encryption standard, Triple Data Encryption Standard (TDES), is considered vulnerable - IBM Quantum quotes research that suggests a 50 per cent likelihood that TDES may be compromised by 2031. Compromise of this encryption method will undermine the integrity of the card payments system, risking exposure of sensitive consumer cardholder data.

Migration to the Advanced Encryption Standard (AES) (which is widely recognised as quantum safe) is the proposed solution to these risks. AusPayNet is leading an industry-wide program to migrate the Australian card payments system to the AES encryption standard. The program involves upgrading over 970,000 point-of-sale terminals and 25,200 ATMs across 55 issuers and 25 acquirers, as well as upgrades to the interchange links, switches and card schemes that interconnect them.

The program is expected to be completed in 2030/31, subject to the necessary regulatory approvals.

More details about the AES Migration Program and its progress are available on AusPayNet's website.

CARD FRAUD DATA

AUSTRALIAN CARDS - FRAUD RATES AND TOTALS

	2019	2020	2021	2022	2023	2024
Value ($m):						
All card transactions	$819,583	$800,920	$864,727	$1,003,698	$1,085,284	$1,157,677
Fraudulent transactions	$465	$469	$495	$577	$762	$913
FRAUD RATE (CENTS PER $1,000)	**56.7**	**58.6**	**57.3**	**57.5**	**70.2**	**78.8**
Number:						
All card transactions (m)	11,000	11,373	12,528	13,989	15,057	15,929
Fraudulent transactions (k)	3,796	4,062	4,267	4,597	5,771	6,320
Fraud rate (as % of total no. of card transactions)	**0.035%**	**0.036%**	**0.034%**	**0.033%**	**0.038%**	**0.040%**
Average value of fraudulent transactions	$122	$115	$116	$126	$132	$144

AUSTRALIAN CARDS - FRAUD VALUE AND PERCENTAGE BY TYPE

Fraud ($m)	2019	2020	2021	2022	2023	2024
Card-not-present	$403	$420	$452	$517	$688	$816
Counterfeit / skimming	$16.9	$11.1	$5.5	$7.1	$7.7	$6.2
Lost / stolen	$35	$26	$29	$42	$52	$68
Never received	$3.0	$3.1	$2.0	$1.6	$1.7	$2.4
Fraudulent application	$2.4	$2.6	$0.9	$0.9	$0.9	$1.4
Other	$4.2	$5.6	$6.4	$9.2	$11.5	$18.7
Total	**$465**	**$469**	**$495**	**$577**	**$762**	**$913**
Fraud (%)						
Card-not-present	86.8%	89.6%	91.2%	89.5%	90.3%	89.4%
Counterfeit / skimming	3.6%	2.4%	1.1%	1.2%	1.0%	0.7%
Lost / stolen	7.5%	5.6%	5.8%	7.2%	6.8%	7.4%
Never received	0.6%	0.7%	0.4%	0.3%	0.2%	0.2%
Fraudulent application	0.5%	0.6%	0.2%	0.1%	0.1%	0.1%
Other	0.9%	1.2%	1.3%	1.6%	1.5%	2.0%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

SCHEME CREDIT, DEBIT AND CHARGE CARDS – FRAUD VALUE BY TYPE

Fraud ($m)		2019	2020	2021	2022	2023	2024
Fraud perpetrated in Australia	Card-not-present	$224	$265	$291	$277	$325	$362
	Counterfeit / skimming	$4.5	$3.2	$1.6	$2.0	$1.1	$1.8
	Lost / stolen	$19	$17	$19	$24	$25	$31
	Never received	$1.9	$1.9	$1.2	$1.0	$1.1	$1.3
	Fraudulent application	$2.0	$2.3	$0.8	$0.7	$0.7	$1.2
	Other	$1.0	$1.2	$1.7	$3.9	$3.8	$6.04
	TOTAL	**$253**	**$290**	**$315**	**$308**	**$357**	**$404**
Fraud perpetrated overseas	Card-not-present	$179	$156	$167	$240	$362	$454
	Counterfeit / skimming	$6.3	$5.1	$1.5	$2.0	$2.5	$2.8
	Lost / stolen	$12	$5	$5	$13	$23	$31
	Never received	$0.1	$0.2	$0.1	$0.1	$0.1	$0.2
	Fraudulent application	$0.5	$0.3	$0.1	$0.2	$0.2	$0.2
	Other	$0.7	$1.7	$1.11	$2.4	$4.7	$6.7
	TOTAL	**$198**	**$168**	**$169**	**$257**	**$393**	**$495**
TOTAL OF ALL SCHEME CREDIT, DEBIT AND CHARGE CARDS		**$451**	**$458**	**$484**	**$565**	**$750**	**$899**

PROPRIETARY DEBIT CARDS – TOTAL FRAUD

Fraud	2019	2020	2021	2022	2023	2024
Value ($m)	$14	$11	$11	$12	$12	$14
Transactions	76,068	66,047	65,235	73,872	89,013	104,183
Average value ($)	$185	$168	$165	$158	$138	$132

PROPRIETARY DEBIT CARDS – FRAUD VALUE BY TYPE

Fraud ($m)	2019	2020	2021	2022	2023	2024
Lost / stolen	$4.5	$4.4	$4.1	$5.0	$4.7	$5.3
Counterfeit / skimming	$6.0	$2.8	$2.4	$3.2	$4.1	$1.6
Never received	$0.9	$1.0	$0.7	$0.5	$0.5	$0.9
Other	$2.6	$2.8	$3.6	$3.0	$3.0	$6.0
TOTAL	**$14**	**$11**	**$11**	**$12**	**$12**	**$14**

PROPRIETARY DEBIT CARDS - FRAUD VALUE BY PIN USAGE

Fraud ($m)	2019	2020	2021	2022	2023	2024
PIN used	$12.1	$9.0	$8.2	$8.4	$8.9	$10.1
PIN not used	$2.0	$2.1	$2.6	$3.2	$3.4	$3.6
Total	**$14**	**$11**	**$11**	**$12**	**$12**	**$14**

OVERSEAS CARDS IN AUSTRALIA - FRAUD VALUE BY TYPE

Fraud value ($m)	2019	2020	2021	2022	2023	2024
Card-not-present	$83	$72	$55	$76	$75	$76
Counterfeit / skimming	$7.3	$4.9	$3.2	$5.2	$5.1	$4.6
Lost / stolen	$4.6	$3.3	$2.5	$2.8	$3.3	$3.4
Never received	$0.2	$0.1	$0.1	$0.2	$0.2	$0.2
Fraudulent application	$0.1	$0.1	$0.1	$0.1	$0.2	$0.1
Other	$0.9	$0.9	$1.0	$1.5	$1.8	$2.7
Total	**$96**	**$81**	**$62**	**$85**	**$85**	**$87**

CHEQUE FRAUD

For the past several years, digital and mobile payments have continued to grow in popularity, and there has been a significant and sustained decline in cheque use. Cheques account for less than 0.1 per cent of retail payments in Australia.[6]

In 2024, Australia's use of cheques declined 24 per cent in value from the previous year, with 15 million cheques processed for $194 billion. Compared to 2019, annual cheque values are now down 68 per cent and transactions down 74 per cent. In 2023, there was a 97 per cent increase in fraud to $4.8 million. However, this trend reversed in 2024, returning to $2.7 million (slightly higher than the 2022 level). A close examination of the figures reveals that the significant increase observed in 2023 was due to three discrete, one-off events involving three financial institutions. The total value of cheque fraud is now so small that even a single high-value cheque being fraudulently honoured can make a significant statistical difference to the overall values.

In November 2024, the Government announced its plan to ensure an orderly phase-out of cheques as part of a strategy to modernise Australia's payments system. As part of its plan, cheques will cease being issued by financial institutions by 30 June 2028 and will cease being accepted by them on 30 September 2029[7]. AusPayNet is leading the industry-wide coordination of the Cheques Transition Program, which has been authorised by the ACCC[8].

CHEQUE FRAUD VALUES AND TRANSACTIONS

Fraud	2019	2020	2021	2022	2023	2024
Value ($m)	$4.8	$4.0	$3.2	$2.4	$4.8	$2.7
Transactions	680	652	494	410	952	545
Average value ($)	$7,106	$6,153	$6,503	$5,953	$5,059	$4,961
All cheque transactions						
Value ($m)	$602,094	$407,096	$371,480	$317,435	$253,971	$194,448
Transactions (m)	57	41	33	27	22	15
Average value ($)	$10,577	$9,810	$11,391	$11,921	$11,750	$12,945
FRAUD RATE (CENTS PER $1,000)	0.8	1	0.9	0.8	1.9	1.4

6. The Treasury (2024), 'Cheques Transition Plan: Winding down Australia's cheques system', Australian Government Paper.
7. See The Treasury (2024)
8. ACCC (2025), 'ACCC authorises Australian Payments Network Limited for conduct to wind down Australia's cheques system', Media Release, 2 July.

CHEQUE FRAUD BY CATEGORY

Fraud ($m)	2019	2020	2021	2022	2023	2024
On-us fraud:						
Stolen blank cheque / book	$1.9	$1.2	$1.3	$1.1	$1.8	$1.6
Fraudulently altered	$1.5	$1.1	$0.9	$0.5	$0.5	$0.5
Originated counterfeit cheques	$0.4	$0.4	$0.4	$0.6	$0.5	$0.2
Non originated counterfeit cheques	$0.6	$1.1	$0.3	$0.1	$0.2	$0.2
Valueless	$0.0	$0.0	$0.0	$0.1	$0.8	$0.0
Breach of mandate	$0.0	$0.0	$0.2	$0.0	$0.0	$0.0
On-us total	**$4.4**	**$3.8**	**$3.1**	**$2.4**	**$3.8**	**$2.5**
Deposit fraud	$0.4	$0.2	$0.1	$0.0	$1.0	$0.2
Total all cheques fraud	**$4.8**	**$4.0**	**$3.2**	**$2.4**	**$4.8**	**$2.7**

On-us fraud covers fraud involving cheques deposited back into the same financial institution that the cheque is drawn on.

Types of on us fraud include:

- **Stolen blank cheque / book** – original blank cheques are stolen and passed off as if they were written by the account holder
- **Fraudulently altered** – payee and/or dollar amount details are altered to be different than originally written
- **Originated counterfeit cheques** – a counterfeit cheque is produced using the paper of the original cheque
- **Non originated counterfeit cheques** – a counterfeit cheque is produced on new paper using techniques such as laser printing and desktop publishing
- **Valueless** – cheques are deposited into an account where there appears to be suspicious circumstances or where it is thought that the cheque is stolen or forged or in any other way is fraudulently issued
- **Breach of mandate** – payment is made without the correct authority through error by the financial institution; for example, the cheque may require two signatories, but is cleared with only one.

Deposit fraud covers fraud involving cheques deposited into a financial institution that is different to the financial institution that the cheque is drawn on.

Types of deposit fraud include:

- **Valueless** – covers cheques deposited to an account knowing that these cheques should not be honoured on presentation by the drawee financial institution as they are valueless (lack of funds), counterfeit, reported stolen, have been fraudulently altered or are in breach of mandate (e.g. do not contain required number of signatures). It also includes the activity of depositing valueless cheques and making withdrawals against those valueless cheques, between accounts owned by the same person. Also called round robin transactions.
- **Third party conversion** – this category includes unaltered cheques which have been deposited to an account other than the payee. This arises where the financial institution has made insufficient enquiry or verification of the depositor regarding their title to the cheque. It also includes cheques where there are two payees but the financial institution has allowed one payee to deposit the amount into their personal account without authority from the other payee.

Australian Payments Network

Australian Payments Network Limited
ABN 12 055 136 519

Suite 2, Level 17, Grosvenor Place
225 George Street, Sydney NSW 2000

Email info@auspaynet.com.au

www.auspaynet.com.au

Historical data may be subject to revision in RBA reports where they receive late filings. To maintain consistency in our report, the data for 2019 to 2023 is the same as was published in the AusPayNet Fraud Report last year.