AUSTRALIAN PAYMENT FRAUD 2024

JANUARY – DECEMBER 2023 DATA

Australian Payments Network

FOREWORD

For several years, ameliorating payment fraud has been a key focus for Australian Payments Network (AusPayNet), the payments industry self-regulatory body, in creating confidence in payments and reducing the economic cost of fraud. Published annually, the Australian Payment Fraud Report highlights current trends and allows us to measure the success of existing, and develop further, industry mitigants.

In positive news, the latest data show that, despite the increase in e-commerce spending since the pandemic, domestic card-not-present (CNP) fraud has decreased by almost a quarter since the introduction of our CNP Fraud Mitigation Framework (CNP Framework) in 2019.

However, overseas CNP fraud is an increasing concern, overtaking domestic fraud for the first time, with a fraud rate 10 times higher than domestically, and having grown over 50 per cent in the last year. The nexus between fraud, scams, and cybercrime makes this challenging. For example, the ACCC's *Targeting Scams* Report showed online shopping scams to be the third most reported, while intelligence from AusPayNet's Economic Crime Forum revealed that international criminal groups use card data stolen in cyber-attacks in fraud and higher-value scams, including bank impersonation scams.

AusPayNet will continue to engage with Australian issuers and acquirers to review potential mitigants to overseas CNP fraud. The National Anti-Scam Centre (NASC) – on whose Advisory Board I have the honour of sitting – is also expanding website takedowns to include online shopping.

On scams more broadly, the establishment of the NASC and upcoming introduction of Mandatory Industry Scam Codes are important in promoting cross-sectoral collaboration. By working with the telecommunications and digital communications industries, we can make Australia a hard target for scams.

In addition to card fraud, AusPayNet collects cheque fraud data. Since 2018, cheque use has declined 70 per cent, but cheque fraud has increased 61 per cent.

> “Domestic CNP fraud has decreased by almost a quarter since the introduction of our CNP Framework in 2019

Government's *Strategic Plan for Australia's Payments System* proposed that the cheques system be wound down by 2030. AusPayNet stands ready to lead a coordinated transition to more modern (and less fraud prone) payment methods.

Finally, on broader payments security, AusPayNet is leading an industry migration of the Australian card payments system to the Advanced Encryption Standard (AES). This will ensure card payment data continues to be protected from cyber-attacks and data breaches.

In working to prevent economic crime we are better together. AusPayNet looks forward to working with its stakeholders to optimise the protection of end-users against the illicit activities of criminals.

Andy White
Chief Executive Officer, AusPayNet

PAYMENT FRAUD IN 2023

Total value of card transactions **increased 8% to $1.1t**; following an increase of 16% in 2022

Total value of card fraud **increased by 32% to $762m**

Card-not-present (CNP) fraud **rose 33%** to **$688m** after increasing 14.4% in 2022

Lost/stolen card fraud was **up by 24% to $52m**, returning to pre-pandemic levels

Counterfeit/skimming **increased by 8.5% to $7.7m** but remains well below pre-pandemic levels

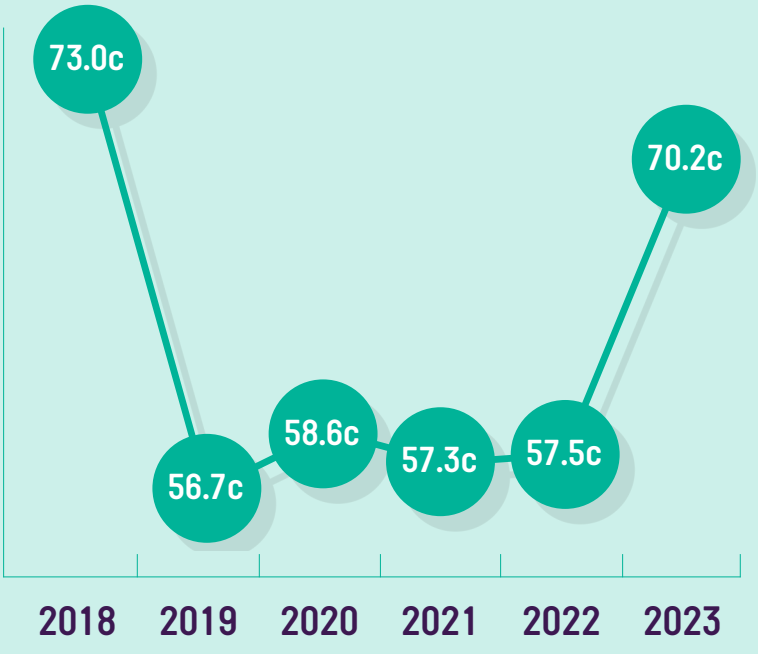
Fraud involving cards never received **increased slightly to $1.7m** but remains well below pre-pandemic levels

The use of cheques **continues to decline.** There were **22m** cheques transacted with a value of **$254b** (**-20%**). In 2023, the Government announced that cheques are to be phased out by 2030

Fraudulent cheque transactions were valued at $4.8m, an **increase of 97%**

CARD FRAUD RATE

The rate increased to **70.2 fraud cents per $1,000 spent**, a 22% year-on-year increase and the highest level since 2018.



** Detailed six-year statistics (sourced from the Reserve Bank of Australia and AusPayNet) are available from page 11 in this report.*

SNAPSHOT

CARD USE AND FRAUD

$1.1T TOTAL CARD TRANSACTIONS

+8%

$762M CARD FRAUD VALUE

+32%

$688M
CARD-NOT-PRESENT
+33%

$7.7M
COUNTERFEIT/SKIMMING
+8.5%

$52M
LOST/STOLEN CARD
+24%

$1.7M
CARDS NEVER RECEIVED
+6.3%

CHEQUE USE AND FRAUD

22M CHEQUES TRANSACTED

-18.5%

$254B VALUE OF CHEQUES

-20%

$4.8M
FRAUDULENT CHEQUES
+97%

CARD FRAUD

Total spending on Australian cards rose 8 per cent in 2023 to $1.1 trillion, however card fraud increased 32 per cent over the same period to $762 million. The overall fraud rate in 2023 was 70.2 cents per $1,000 spent compared to 57.5 cents in 2022, a 22 per cent increase year-on-year and at a level not seen since 2018.

CARD-NOT-PRESENT (CNP) FRAUD TRENDS

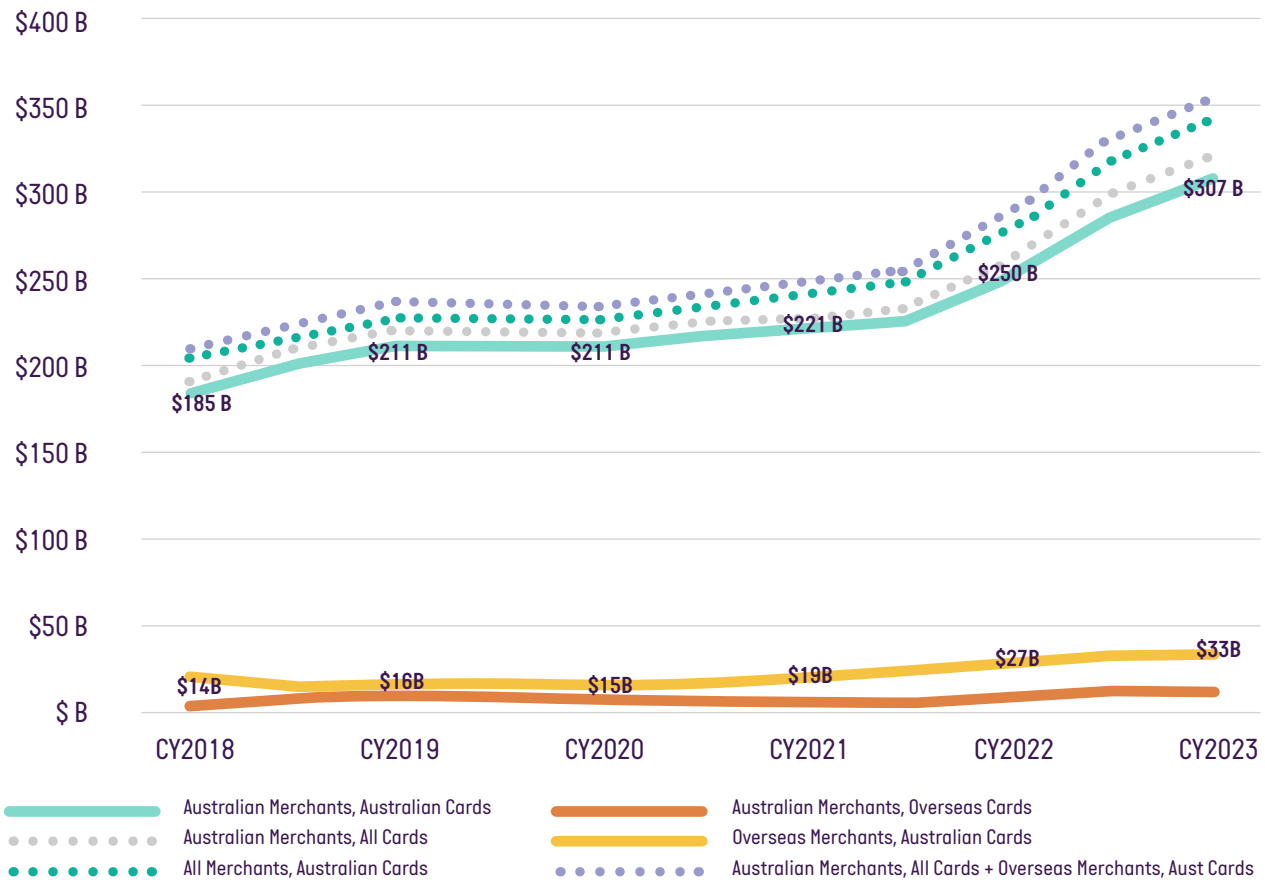
Total CNP spending on Australian cards increased 24 per cent in 2023 to $320 billion, reflecting the ongoing surge in e-commerce since the pandemic. The total value of CNP fraud on Australian-issued cards used at Australian merchants and at overseas merchants increased 33 per cent to $688 million, accounting for over 90 per cent of all card fraud in Australia.

The marked increase in CNP fraud losses was primarily driven by a significant rise in CNP fraud on Australian cards used at overseas merchants. Fraud losses in this category increased 51 per cent in 2023 to $362 million, far surpassing the 23 per cent spending growth in this category over the same period ($33 billion). Put another way, 53 per cent of CNP fraud in 2023 was perpetrated on 10 per cent of the CNP spend, at an alarming fraud rate of $10.93 per $1,000 spent.

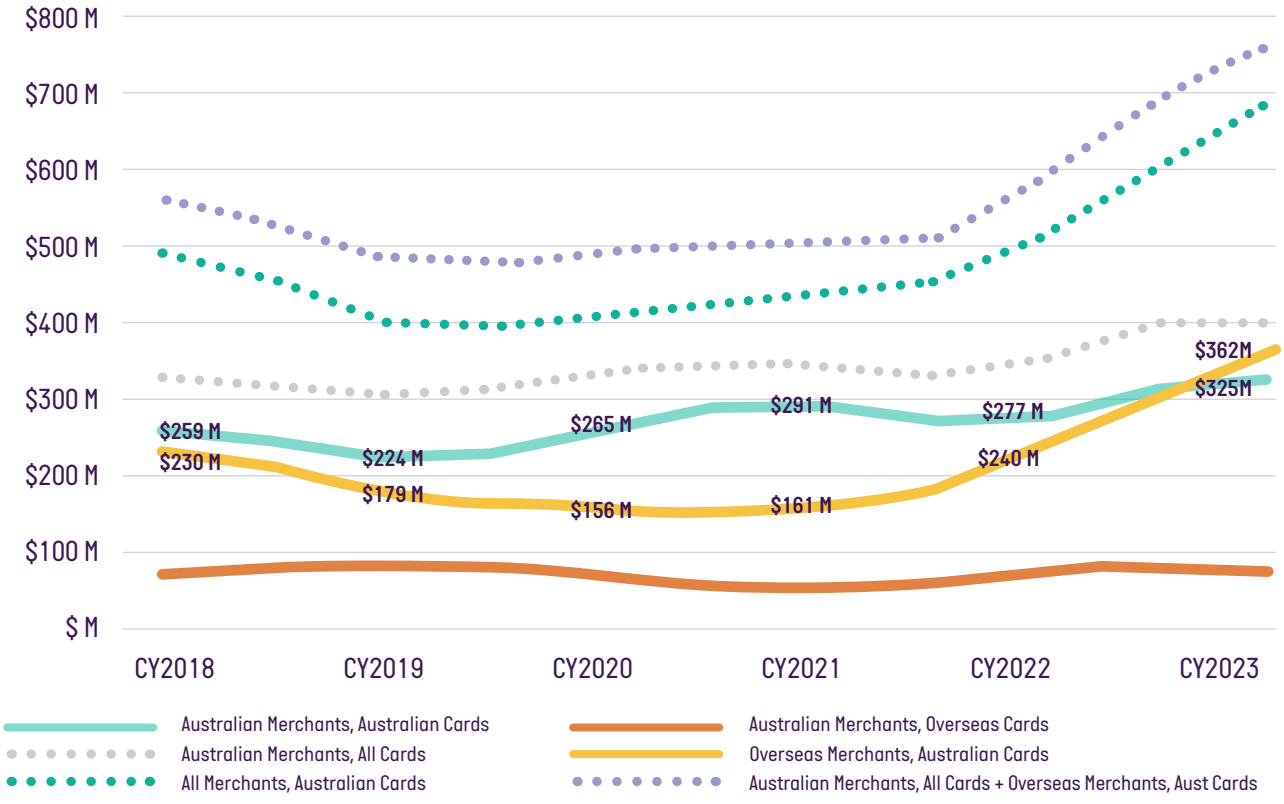
In contrast, CNP fraud on Australian cards used at Australian merchants increased 17.5 per cent in 2023 to $325 million, at a lower rate than the spending growth rate of 24 per cent to $307 billion. This resulted in a 5 per cent decrease in the fraud rate for domestic CNP fraud, from $1.11 per $1,000 spent in 2022 to $1.06 in 2023.

In absolute terms, CNP fraud on transactions involving Australian cards used at overseas merchants has overtaken domestic CNP fraud in 2023 for the first time since 2017.

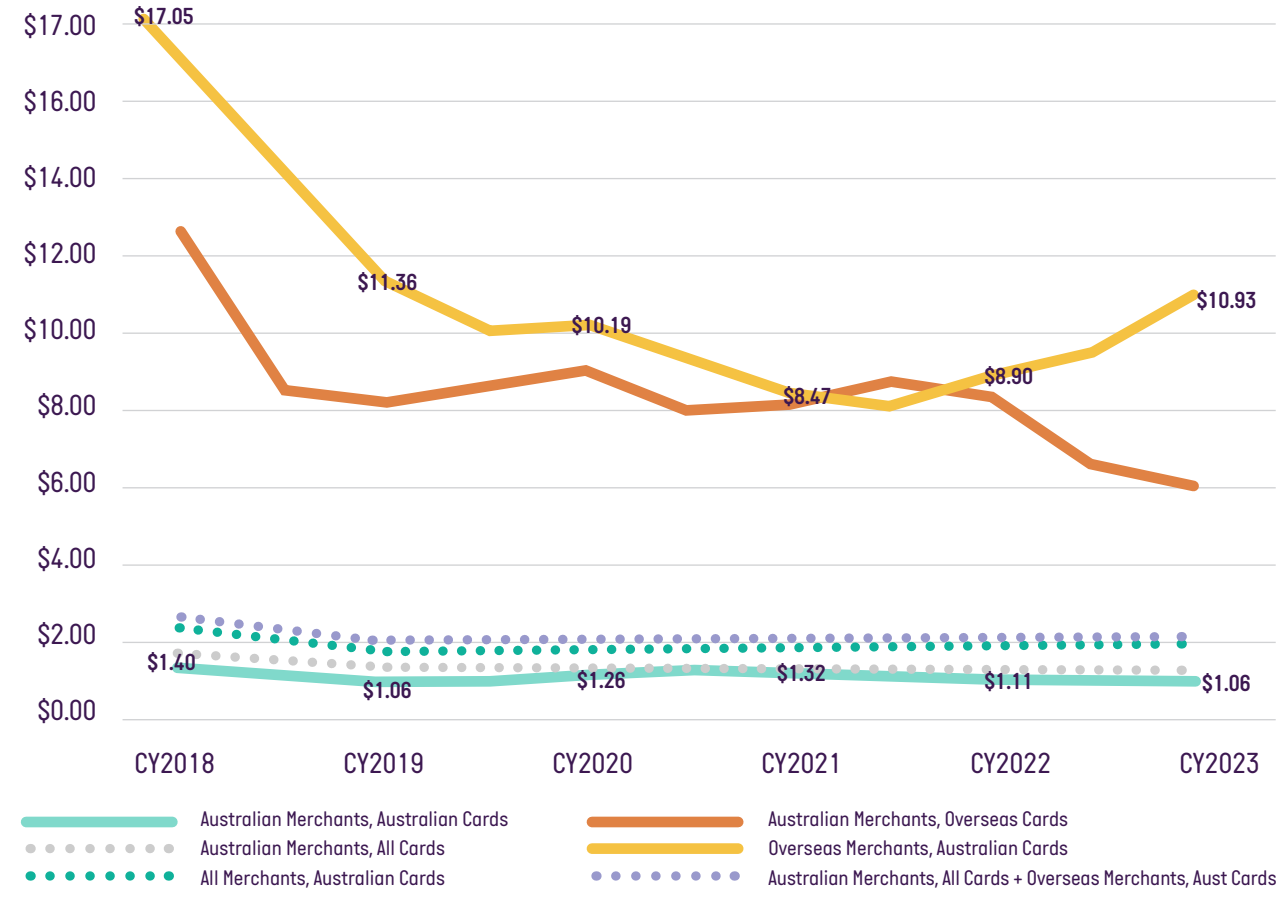
CNP SPEND



CNP FRAUD VALUE



CNP FRAUD RATE



HOW CNP FRAUD IS PERPETRATED

CNP fraud occurs when valid card details are stolen by criminals and then used 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.

Valid card details are stolen by criminals in several ways[1], 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.
- **Scams**: Criminals may also trick cardholders into sharing their card details as part of a scam, such as online shopping, buying and selling, false billing and other phishing scams.

CARD PRESENT FRAUD TRENDS

Lost and stolen card fraud increased by 24 per cent to $52 million, returning to pre-pandemic levels. However, the most substantial increase in this category was in fraud outside the country, with a 76.5 per cent increase in fraud involving Australian cards lost or stolen overseas. This is likely attributable to Australians returning to pre-pandemic levels of international travel, and that many destination countries for Australians do not have the same level of mobile wallet payments (which come with added security benefits and reduce the need to carry physical cards).

Lost and stolen card fraud refers to unauthorised transactions on cards that have been reported by the cardholder as lost or stolen. Unless the PIN has also been captured, criminals may use these cards – or duplicates of these cards – at point-of-sale by forging the signature where accepted, or for purchases where neither a PIN nor signature is required.

Counterfeit/skimming fraud increased by 8.5 per cent to $7.7 million but remains well below the $19.6 million pre-pandemic level in 2018. The number of counterfeit/skimming transactions decreased by 41 per cent, resulting in an increase in the fraud value per transaction from $190 to $350. The increase in counterfeit/skimming fraud is also likely attributable to the reopening of international borders, which enabled the re-entry of transnational organised criminals.

Counterfeit/skimming fraud occurs when details from a card's magnetic stripe are skimmed at an ATM, point-of-sale 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 slightly to $1.7 million but remains well below pre-pandemic levels. Never received fraud occurs when transactions are made on a card that was stolen before it was received by the owner.

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. In 2023, fraud involving fraudulent applications remained flat at $0.9 million.

Other card fraud increased by 24.5 per cent to $11.5 million. This category covers fraudulent transactions that cannot be categorised under any of the common fraud types above, including account takeover and first-party fraud. Account takeover — also known as identity takeover — 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. First-party fraud, also known as friendly fraud or chargeback fraud, refers to a situation where a cardholder or a family member of the cardholder makes a purchase online with their card and then disputes the charge with their card issuer, fraudulently claiming that the transaction was unauthorised or that they did not receive the purchased goods or services.

1. Moneysmart, Banking and credit scams (webpage) https://moneysmart.gov.au/financial-scams/banking-and-credit-scams; Commonwealth Bank of Australia, Card fraud (webpage) https://www.commbank.com.au/support/security/card-fraud.html; Westpac, 10 things you can do to avoid credit card fraud (webpage) https://www.westpac.com.au/personal-banking/solutions/staying-credit-smart/understanding-credit-cards/avoiding-credit-card-fraud/ (accessed 25 June 2024).

COMBATTING CARD FRAUD

Combatting card fraud has long been an area of focus for AusPayNet. We publish the *Australian Payment Fraud Report* annually to highlight current fraud trends affecting the payments ecosystem. The data allows us to measure the success of industry mitigants and assists us in developing further response strategies.

The Australian card system moved to Europay, Mastercard and Visa (EMV) chip technology in 2014, which made it incredibly difficult to perpetrate traditional forms of physical card fraud. With that avenue seriously constrained, criminal groups have shifted their focus to online card transactions. Online card transactions have also become a more attractive target for CNP fraud due to the surge in e-commerce in recent years, particularly since the pandemic. As highlighted earlier in this report, CNP fraud now accounts for over 90 per cent of all card fraud in Australia.

CNP FRAUD MITIGATION FRAMEWORK (CNP FRAMEWORK)

AusPayNet introduced the CNP Framework to counteract rising rates of this type of fraud. The Framework is designed by industry to reduce fraud on Australian cards at Australian merchants in online channels, while enabling the continued growth of online transactions. Implemented on 1 July 2019, 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 rate of CNP transactions, pointing to its impact. The domestic CNP fraud rate has decreased from $1.26 per $1,000 spent in 2020 to $1.06 in 2023.

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 review this year will consider the trends highlighted in this report and related mitigants for their effectiveness to determine if there is a need to strengthen any of the controls, including the fraud thresholds that apply to issuers and acquirers.

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

FIGHTING OVERSEAS CNP FRAUD AND SCAMS

While the figures illustrate the continuing positive impact of the CNP Framework on domestic CNP fraud, overseas fraud has become increasingly concerning, overtaking domestic card fraud in 2023 for the first time since 2017.

Online shopping scams, data theft and other forms of phishing are contributing to the rise in CNP fraud on Australian cards used at overseas merchants. These transactions are not subject to strong customer authentication controls that are applied to domestic CNP spend through the CNP Framework. AusPayNet is working with its Members to consider if industry collaboration on mitigants and potential technical standards can help combat this adverse trend.

The ACCC's *Targeting Scams* Report highlighted the prevalence of online shopping scams, which ranked as the third most reported type of scam and seventh in terms of financial losses incurred. This is linked to transnational organised crime groups targeting Australians, with the stolen card details used to perpetrate higher-value fraud at overseas merchants and enabling social engineering of card fraud victims into higher value scams such as bank impersonation scams.

AusPayNet is working closely with the Government, ACCC, law enforcement and private sector experts to prevent scams. This includes:

- Actively participating in the ACCC's National Anti-Scam Centre (NASC) program of work, which includes the expansion of website takedown services to include online shopping and data sharing between the NASC and the Australian Financial Crime Exchange (AFCX) anti-scam intelligence loop to block online advertisements. The AusPayNet CEO also serves as a member of the Advisory Board to the NASC.

- Working with the Australian Government on the legislative framework for combatting scams and the introduction of mandatory industry codes for scams. The codes will prescribe responsibilities for specific industries – including banks, digital communications platforms, and telecommunications providers - for disrupting scam activity. By working with the telecommunications industry and digital communications platforms, banks can disrupt phishing attacks and online shopping scams that contribute to CNP fraud. AusPayNet has also offered its support in the development of any technical standards for the payments industry that might be required to assist in the implementation of the mandatory industry codes.

- The facilitation of the Economic Crime Forum, which brings together law enforcement, regulators, and the payments industry, we continue to support public-private partnerships domestically and internationally to tackle scams and other cyber-enabled crime.

CARD PRESENT FRAUD PREVENTION

The industry has undergone a period of rapid technological advancements, including modern payment acceptance solutions, fuelled by the evolution of mobile, cloud, low-cost hardware and contactless adoption. The distinction between face-to-face (card present) and online transactions (card-not-present) have blurred. Mobile devices used for online transactions can provide strong user authentication and EMVCo compliant transactions, features traditionally only available for face-to-face transactions. Innovation has evolved authentication, security and fraud mitigation in card-present transactions, especially given the shift to mobile and biometrics.

AusPayNet has established 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 the industry. Within this framework, a device approval process has been established. Devices and solutions meeting an approved standard, and which have been approved by Payments Card Industry (PCI) can be readily deployed. For non-standard solutions which have not been validated by a PCI program, a structured risk assessment is undertaken to ensure appropriate security protections. For traceability purposes, AusPayNet manages a listing of approved standard and non-standard solutions for Australia.

With regard to fraudulent applications, 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.

FIRST-PARTY FRAUD

First-party fraud 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 house-hold member or additional card holder making a transaction of which the primary card holder is not aware.

- 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 a 'safe' transaction from a known customer, elects not to require enhanced security such as 3D Secure, the liability for fraud defaults to the merchant. While a merchant can contest a dispute as being genuine, and therefore the consumer is liable, the success rate for these across the Australian ecosystem is low, and many merchants do not see the commercial case for vigorous pursuit of these defences.

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 is a significant challenge for some merchants and is currently reviewing how best to manage first-party fraud within the CNP Framework. This review will complete in early 2025.

MIGRATION TO ADVANCED ENCRYPTION STANDARDS

Advances in classical and quantum computing present a material risk that the methods used to encrypt card payments data today may be compromised. The current encryption method, Triple Data Encryption Standard (TDES), is considered vulnerable, with IBM Quantum quoting research that suggests a 50 per cent chance 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 cardholder data.

A long-term solution is required to address these long-term risks. Migrating to a quantum-safe encryption method, Advanced Encryption Standard (AES), is the proposed solution. AusPayNet is leading an industry-wide migration to AES for Australia, requiring the upgrade of over 970,000 point-of-sale terminals and 25,200 ATMs across 55 issuers and 25 acquirers, together with upgrades to the interchange links, switches and card schemes that interconnect them.

The migration is underway and, if it proceeds as planned, is expected to be completed in 2030-2031.

CARD FRAUD DATA

AUSTRALIAN CARDS - FRAUD RATES AND TOTALS

	2018	2019	2020	2021	2022	2023
Value ($m):						
All card transactions	$789,286	$819,583	$800,920	$864,727	$1,003,698	$1,085,284
Fraudulent transactions	$576	$465	$469	$495	$577	$762
FRAUD RATE (CENTS PER $1,000):	**73.0**	**56.7**	**58.6**	**57.3**	**57.5**	**70.2**
Number:						
All card transactions (m)	9,985	11,000	11,373	12,528	13,989	15,057
Fraudulent transactions (k)	4,369	3,796	4,062	4,267	4,597	5,771
Fraud rate (as % of total no. of card transactions)	**0.044%**	**0.035%**	**0.036%**	**0.034%**	**0.033%**	**0.038%**
Average value of fraudulent transactions	$132	$122	$115	$116	$126	$132

AUSTRALIAN CARDS - FRAUD VALUE AND PERCENTAGE BY TYPE

Fraud ($m)	2018	2019	2020	2021	2022	2023
Card-not-present	$489	$403	$420	$452	$517	$688
Lost / stolen	$56	$35	$26	$29	$42	$52
Counterfeit / skimming	$19.6	$16.9	$11.1	$5.5	$7.1	$7.7
Never received	$6.1	$3.0	$3.1	$2.0	$1.6	$1.7
Fraudulent application	$2.3	$2.4	$2.6	$0.9	$0.9	$0.9
Other	$3.5	$4.2	$5.6	$6.4	$9.2	$11.5
Total	**$576**	**$465**	**$469**	**$495**	**$577**	**$762**

Fraud (%)	2018	2019	2020	2021	2022	2023
Card-not-present	84.9%	86.8%	89.6%	91.2%	89.5%	90.3%
Lost / stolen	9.7%	7.5%	5.6%	5.8%	7.2%	6.8%
Counterfeit / skimming	3.4%	3.6%	2.4%	1.1%	1.2%	1.0%
Never received	1.1%	0.6%	0.7%	0.4%	0.3%	0.2%
Fraudulent application	0.4%	0.5%	0.6%	0.2%	0.1%	0.1%
Other	0.6%	0.9%	1.2%	1.3%	1.6%	1.5%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

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

Fraud ($m)		2018	2019	2020	2021	2022	2023
Fraud perpetrated in Australia	Card-not-present	$259	$224	$265	$291	$277	$325
	Lost / stolen	$33	$19	$17	$19	$24	$25
	Counterfeit / skimming	$5.1	$4.5	$3.2	$1.6	$2.0	$1.1
	Never received	$4.4	$1.9	$1.9	$1.2	$1.0	$1.1
	Fraudulent application	$1.9	$2.0	$2.3	$0.8	$0.7	$0.7
	Other	$1.1	$1.0	$1.2	$1.7	$3.9	$3.8
	TOTAL	$304	$253	$290	$315	$308	$357
Fraud perpetrated overseas	Card-not-present	$230	$179	$156	$161	$240	$362
	Lost / stolen	$19	$12	$5	$5	$13	$23
	Counterfeit / skimming	$8.1	$6.3	$5.1	$1.5	$2.0	$2.5
	Never received	$0.4	$0.1	$0.2	$0.1	$0.1	$0.1
	Fraudulent application	$0.4	$0.5	$0.3	$0.1	$0.2	$0.2
	Other	$0.6	$0.7	$1.7	$1.1	$2.4	$4.7
	TOTAL	$259	$198	$168	$169	$257	$393
TOTAL OF ALL SCHEME CREDIT, DEBIT AND CHARGE CARDS		$563	$451	$458	$484	$565	$750

PROPRIETARY DEBIT CARDS – TOTAL FRAUD

Fraud	2018	2019	2020	2021	2022	2023
Value ($m)	$13	$14	$11	$11	$12	$12
Transactions	52,398	76,068	66,047	65,235	73,872	89,013
Average value ($)	$256	$185	$168	$165	$158	$138

PROPRIETARY DEBIT CARDS – FRAUD VALUE BY TYPE

Fraud ($m)	2018	2019	2020	2021	2022	2023
Lost / stolen	$3.9	$4.5	$4.4	$4.1	$5.0	$4.7
Counterfeit / skimming	$6.3	$6.0	$2.8	$2.4	$3.2	$4.1
Never received	$1.4	$0.9	$1.0	$0.7	$0.5	$0.5
Other	$1.8	$2.6	$2.8	$3.6	$3.0	$3.0
TOTAL	$13	$14	$11	$11	$12	$12

PROPRIETARY DEBIT CARDS - FRAUD VALUE BY PIN USAGE

Fraud ($m)	2018	2019	2020	2021	2022	2023
PIN Used	$12.4	$12.1	$9.0	$8.2	$8.4	$8.9
PIN Not Used	$1.0	$2.0	$2.1	$2.6	$3.2	$3.4
Total	**$13**	**$14**	**$11**	**$11**	**$12**	**$12**

OVERSEAS CARDS IN AUSTRALIA - FRAUD VALUE BY TYPE

Fraud ($m)	2018	2019	2020	2021	2022	2023
Card-not-present	$71	$83	$72	$55	$76	$75
Counterfeit / skimming	$5.8	$7.3	$4.9	$3.2	$5.2	$5.1
Lost / stolen	$3.3	$4.6	$3.3	$2.5	$2.8	$3.3
Never received	$0.1	$0.2	$0.1	$0.1	$0.2	$0.2
Fraudulent application	$0.2	$0.1	$0.1	$0.1	$0.1	$0.2
Other	$1.5	$0.9	$0.9	$1.0	$1.5	$1.8
Total	**$82**	**$96**	**$81**	**$62**	**$85**	**$85**

CHEQUE FRAUD

Consistent with the global trend towards digital and mobile payments, there has been a significant and sustained decline in cheque use in Australia. In the past 10 years, cheque use in Australia has declined by almost 90 per cent[1]. In 2022/23, cheque payments accounted for 0.1 per cent of the number of all non-cash retail payments, representing an average of less than one cheque transaction per person[2].

Australia's use of cheques declined another 20 per cent in 2023, with 22 million cheques processed for $254 billion of value. However, there was a 97 per cent increase in fraud to $4.8 million, driven by deposit fraud, stolen cheque books and valueless fraud.

In its *Strategic Plan for Australia's Payments System*, the Government recognised that greater security in the payments system will be achieved through an orderly wind down of the cheques system. While this will require supporting remaining cheque users to shift to and get the benefits of more secure and digital payment methods, it will also eliminate this legacy avenue for fraudsters. AusPayNet is working closely with the Government, RBA, and all participants of the Australian cheque system on this important industry initiative.

1. The Treasury, *Winding Down Australia's Cheques System* (Consultation Paper, December 2023) https://treasury.gov.au/sites/default/files/2023-12/c2023-471331-cp.pdf ('*Treasury Consultation Paper*').

2. Reserve Bank of Australia, *Payment System Board Annual Report* (Annual Report, 15 September 2023) https://www.rba.gov.au/publications/annual-reports/psb/2023/pdf/psb-annual-report-2023.pdf ('*RBA PSB 2023 Annual Report*')

CHEQUE FRAUD VALUES AND TRANSACTIONS

Fraud	2018	2019	2020	2021	2022	2023
Value ($m)	$4.4	$4.8	$4.0	$3.2	$2.4	$4.8
Transactions	591	680	652	494	410	952
Average value ($)	$7,402	$7,106	$6,153	$6,503	$5,953	$5,059
All cheque transactions						
Value ($m)	$885,147	$602,094	$407,096	$371,480	$317,435	$253,971
Transactions (m)	72	57	41	33	27	22
Average value ($)	$12,342	$10,577	$9,810	$11,391	$11,921	$11,750
FRAUD RATE (CENTS PER $1,000)	**0.5**	**0.8**	**1**	**0.9**	**0.8**	**1.9**

CHEQUE FRAUD BY CATEGORY

Fraud ($m)	2018	2019	2020	2021	2022	2023
On us fraud:						
Stolen blank cheque / book	$1.5	$1.9	$1.2	$1.3	$1.1	$1.8
Fraudulently altered	$1.2	$1.5	$1.1	$0.9	$0.5	$0.5
Originated counterfeit cheques	$0.2	$0.4	$0.4	$0.4	$0.6	$0.5
Non originated counterfeit cheques	$0.1	$0.6	$1.1	$0.3	$0.1	$0.2
Valueless	$0.3	$0.0	$0.0	$0.0	$0.1	$0.8
Breach of mandate	$0.4	$0.0	$0.0	$0.2	$0.0	$0.0
On-us total	**$3.7**	**$4.4**	**$3.8**	**$3.1**	**$2.4**	**$3.8**
Deposit Fraud	$0.7	$0.4	$0.2	$0.1	$0.0	$1.0
Total all cheques fraud	**$4.4**	**$4.8**	**$4.0**	**$3.2**	**$2.4**	**$4.8**

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.

ABOUT US

AusPayNet is the industry association and self-regulatory body for the Australian payments industry. We manage and develop procedures, policies and standards governing payments in Australia. We enable the efficiency, resilience, adaptability, and accessibility of Australia's payments system. AusPayNet currently has over 150 members, including financial institutions, payment system operators, major retailers and financial technology companies.

Australian Payments Network

Australian Payments Network Limited
ABN 12 055 136 519

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

Telephone +61 2 9216 4888

Email info@auspaynet.com.au

www.auspaynet.com.au

Some figures may have been revised since earlier publication.
Full details are available on www.auspaynet.com.au