30 YEARS | Australian Payments Network

AUSTRALIAN PAYMENT FRAUD 2022

Australian Payments Network (AusPayNet) collects payment fraud data from financial institutions and card schemes. We publish this report to highlight current fraud trends affecting the payments ecosystem. The data allows us to measure the success of industry mitigants, such as the Card-Not-Present (CNP) Fraud Mitigation Framework, and assists us in developing further response strategies, such as the banking and payments industry scams mitigation program.

SNAPSHOT

The 2021 economic recovery, following the height of the global pandemic, saw Australian card payments increase by 8.0% to $865 billion. Online retail spending grew by an estimated 8.2% to $53 billion. Card fraud increased by 5.7% to $495 million.

COMBATTING FRAUD

As the important work of the industry CNP Fraud Mitigation Framework continues, a decrease and stabilisation of the fraud rate has been observed. In 2021, the fraud rate was steady at 57.3 cents per $1,000 spent, compared to 58.6 cents in 2020.

RESPONDING TO SCAMS

The rate of scams continues to rise, and this is a focus for the recently established Economic Crime Forum (ECF). The Australian Bureau of Statistics (ABS) reported that 11.1 million Australians were exposed to a scam in 2021.

THE CNP FRAUD MITIGATION FRAMEWORK

This framework defines an approach to reduce online card fraud in Australia. It is also designed to build consumer trust and support continued growth in e-commerce.

THE ECONOMIC CRIME FORUM (ECF)

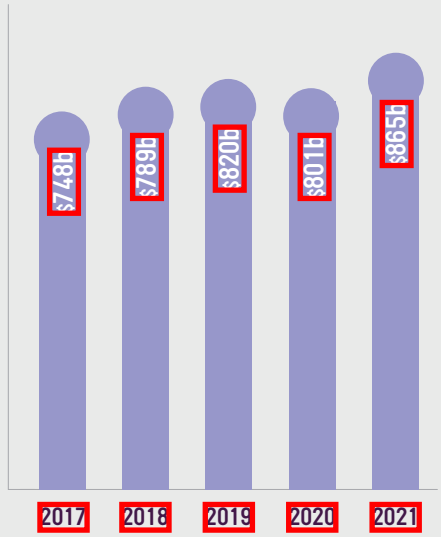
The ECF brings together a broad set of participants to target economic crime – scams, fraud, financial crime, and banking-related cyber incidents.

JANUARY – DECEMBER

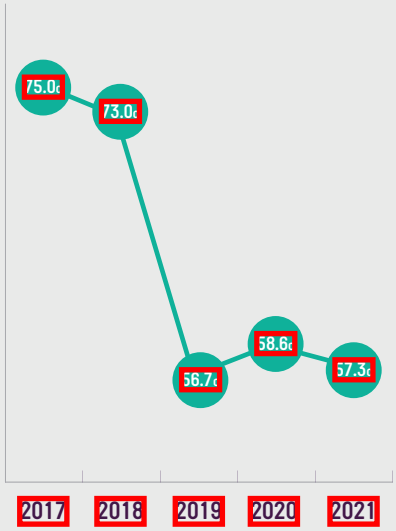
2021 DATA

Snapshot

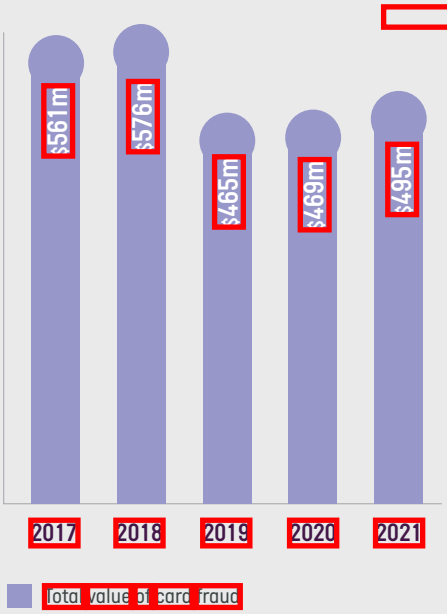
In 2021, the total value of card transactions **increased by 8.0%** to $865 billion. This followed a 2.3% decrease in 2020.



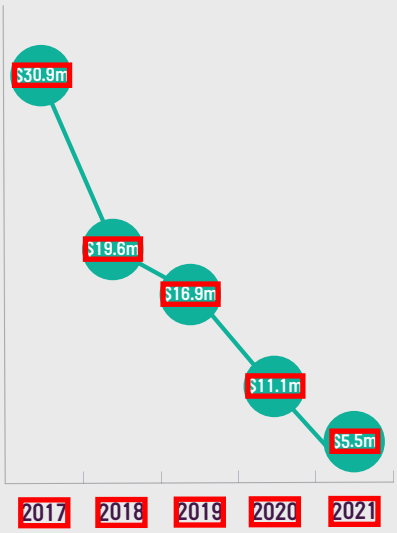
While the value of card fraud increased, the card fraud rate **fell in 2021**, to 57.3 fraud cents per $1,000 spent.



The total value of card fraud was **up 5.7%** in 2021.



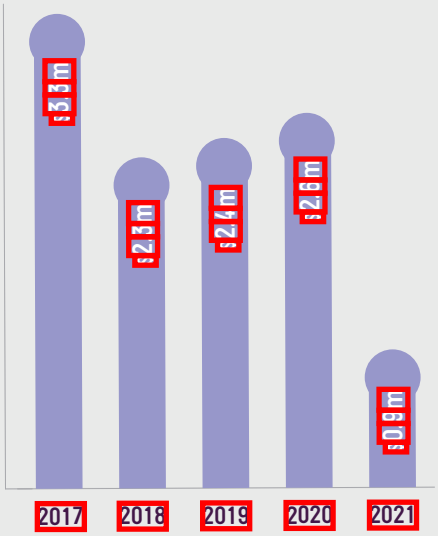
Counterfeit/skimming fraud **fell by more than 50%**, to a new record low.



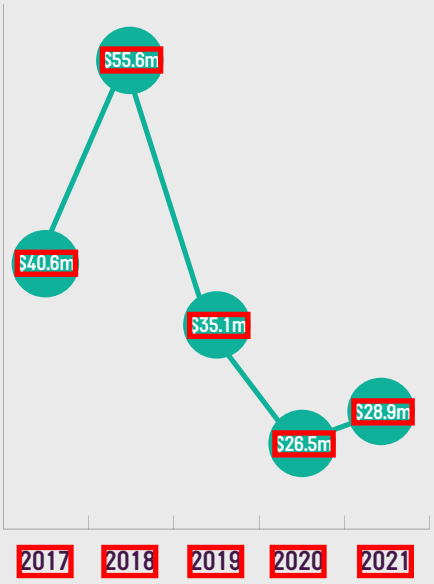
Sources: Reserve Bank of Australia and AusPayNet

Fraudsters continue making payments on cards that they have applied for, using another person's identity or other false information (fraudulent applications).

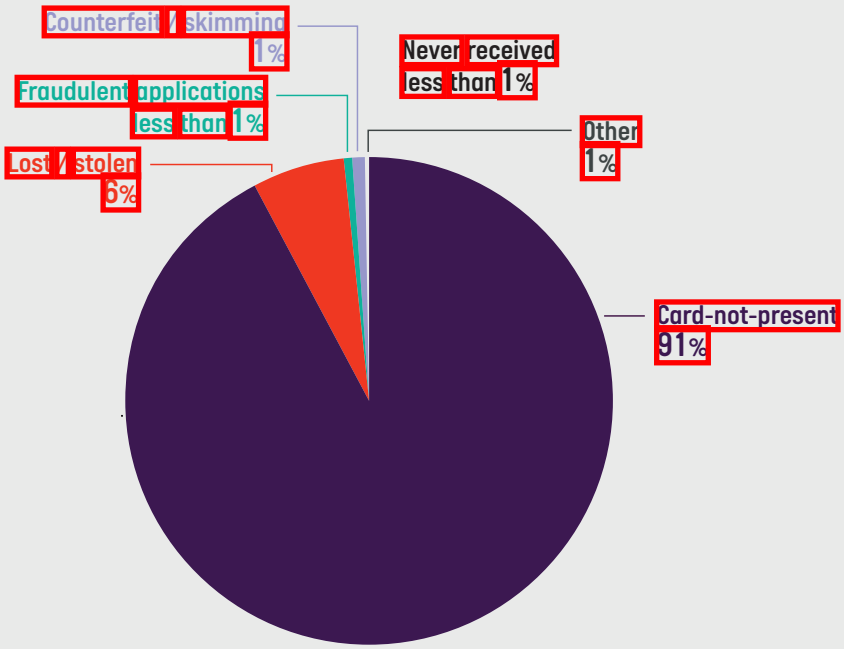
However, the total value of fraudulent applications **dropped by 65%** in 2021.



Lost/stolen card fraud **rose by 9.3%** in 2021 but remains well below the levels of previous years.



CNP now accounts for 91% of all card fraud, an **increase of 1%** in 2021.



Sources: Reserve Bank of Australia and AusPayNet

Payment Fraud

In 2021, as the economic recovery from the pandemic began, spending on Australian cards rose by 8% and the overall value of card fraud increased by 5.7%.

As the COVID-19 pandemic has progressed, more consumers have opted for digital payments, while cash and cheque use continues to decline. Around 75% of card payments are now made via debit cards, compared to 60% 10 years ago. Since the onset of the pandemic, the volume of online retail transactions has continued rising. NAB estimates[1] that in the 12 months to December 2021, Australians spent $53 billion on online retail, around 14.4% of total retail and almost 20% higher than the previous 12 months[1]. It is anticipated that the use of digital channels for payments will continue to grow, with Australians favouring the convenience of online shopping and mobile payment options.

In 2021, as the economic recovery from the pandemic began and lockdown restrictions were eased, the total amount spent on cards rose by 8.0% to $865 billion. Over the same period, overall card fraud increased by 5.7% to $495 million, while the fraud rate decreased to 57.3 cents per $1,000 spent.

Before the CNP Fraud Mitigation Framework (CNP framework) was established in 2019, the fraud rate averaged 74.3 fraud cents (between 2016 and 18). Since the introduction of the CNP framework, the fraud rate has averaged 57.5 fraud cents (between 2019 and 21).

As more transactions occur over online payment rails, fraud also continues to move online. Online card fraud, or the use of credit, debit or bank cards to make purchases without the account owner's permission, now accounts for 91% of all fraud on Australian cards. AusPayNet's CNP framework supports financial institutions' fraud detection and mitigation initiatives. Financial institutions have continued to update their fraud capabilities, including the use of technologies such as real-time monitoring, machine learning, tokenisation and Strong Customer Authentication (SCA).

The data indicates that Australia's prevention initiatives are proving effective in stabilising the CNP fraud rate. In 2021, while CNP fraud increased by 7.6% to $452 million, this remains below the peaks in 2018 ($489 million) and 2017 ($476 million). As CNP transaction volumes continue to increase, combatting CNP fraud will remain a key priority for the payments industry.

In March 2022, the ABS published a survey of 28,386 Australians focusing on card fraud and scams. The survey estimates that 6.9% of Australians aged 15 and over (1.4 million) experienced card fraud between July 2020 and June 2021[1], a higher victimisation rate than for scams and identity theft.[1]

6.9% OF AUSTRALIANS AGED 15 AND OVER EXPERIENCED CARD FRAUD

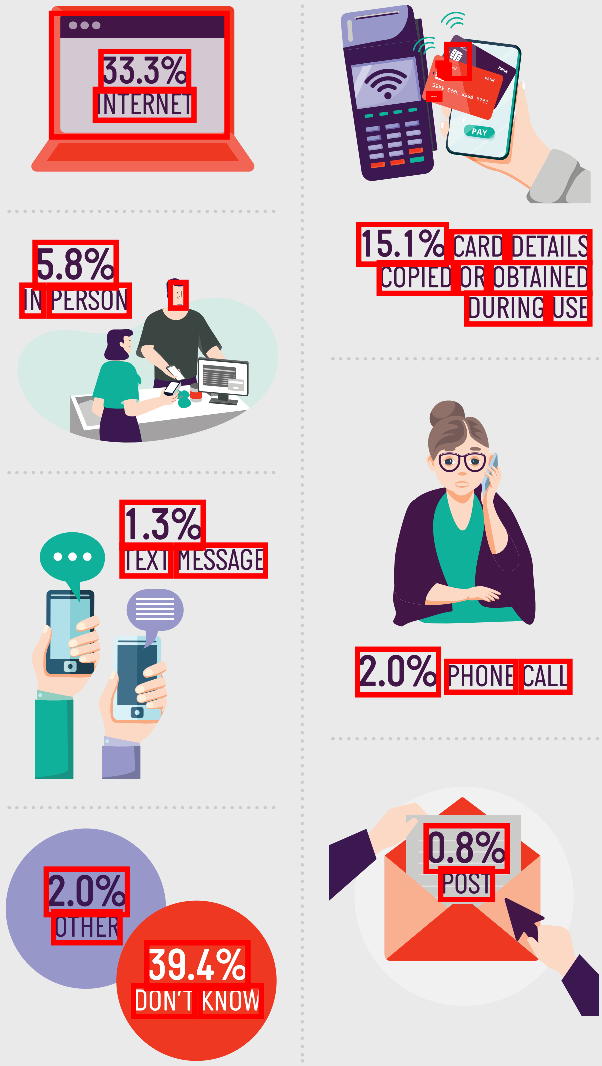
Source: ABS, Personal Fraud 2020-21

Card fraud is a crime, however the vast majority of victims (88.7%) report card fraud to their financial institutions rather than law enforcement authorities. Additionally, 5.1% don't report these incidents anywhere.

AusPayNet continues to engage with Australian law enforcement agencies on this issue via its ECF.

[1] https://business.nab.com.au/wp-content/uploads/2022/01/NAB-Online-Retail-Sales-Index-December-2021.pdf
[1] https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/2020-21

How were victims' card details obtained?



Most victims of card fraud (39.4%) did not know how fraudsters obtained their card details. Among victims able to identify how their details were obtained, most cited the internet (33.3%).

AusPayNet's data reveals that counterfeit/skimming fraud fell in 2021 by over 50%, to $5.5 million – another record low. After an increase in fraudulent applications between 2018 and 2020, persistent industry efforts contributed to a significant decrease of 55% last year. However, lost and stolen card fraud increased by 9.3%, to $23.9 million, which may be attributable to Australia's easing out of lockdown restrictions in many states, resulting in an increased likelihood of consumers losing cards and/or greater opportunities for theft.

As criminals adapt and evolve their methods to take advantage of the increasing amount of time Australians are spending online, payment scams are on the rise (these will be discussed later in the report). The following sections provide further information on card fraud trends and outline measures that consumers and businesses can take to actively mitigate risk.

Where was card fraud reported?

- 88.7% BANK OR FINANCIAL INSTITUTIONS
- 15.3% CREDIT CARD COMPANY
- 6.4% POLICE
- 3.8% SOMEONE ELSE
- 2.2% GOVERNMENT ORGANISATION OR DEPARTMENT
- 5.1% INCIDENT NOT REPORTED

Source: ABS, Personal Fraud 2020-21

Australian payments industry actions to further combat fraud

Work to prevent payment fraud requires coordination across the industry, from financial institutions and card schemes to merchants and consumers. AusPayNet continues to lead a number of industry-wide initiatives focused on enhancing the security and convenience of payments. Among these is the CNP framework.

CNP framework

The CNP framework is designed to reduce fraud in Australian online channels, while ensuring the continued growth of online transactions. The CNP framework outlines an approach to mitigating the impact of CNP payments fraud for merchants, consumers, issuers, acquirers, card schemes, payment gateways, payment service providers, and regulators. The CNP framework defines the minimum requirements for an issuer, acquirer or merchant to authenticate CNP transactions online, promoting multifactor authentication, encryption and tokenisation as best practice to reduce fraud in online CNP channels.

Our guiding principles are to:

- leverage off global standards and best practices in other jurisdictions
- consistently apply SCA
- be technology neutral to provide choice and ease of implementation
- review the scope and thresholds annually.

Working with our members, we established industry level fraud thresholds, which are designed to encourage early intervention by issuers and acquirers. Quarterly reporting by our members allows us to track their progress and potential breaches of those thresholds. Recommendations are provided on proactive steps our members should take with their merchants and cardholders, with a view to taking action that will bring them back below the thresholds.

To date, the data indicates that of the merchants who have exceeded the agreed fraud threshold, the majority bring their fraud levels back below the threshold by the final quarter of the relevant reporting period. Evolving technologies to support customer experience and convenience, such as 'click and collect' and 'scan as you go', can create or lead to new fraud challenges. Acquirers are working closely with their merchants to reduce fraud, including implementing remediation plans.

We are working in a fast-paced environment in which risk and threats continue to evolve. An annual review of the CNP framework by AusPayNet members ensures it remains relevant. Workshops continue to address identified issues, and these broadly fall into two categories:

- ensuring the mitigants are relevant and achievable
- driving the correct behaviour via an appropriate sanctions and fines regime.

Combatting CNP fraud remains a priority for the payments industry, as e-commerce volumes rapidly rise and Australians' use of digital payment methods continues to increase. The CNP framework is supporting financial institutions' fraud detection and mitigation initiatives. Financial institutions have continued to update their fraud capabilities by using secure technologies, such as real-time monitoring, machine learning, tokenisation and SCA.

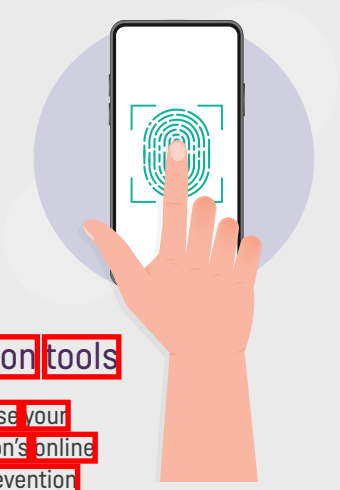
In 2021, while card fraud increased by 5.7%, to $495 million, the fraud rate decreased to 57.3 fraud cents per $1,000 spent. Prior to the CNP framework, the fraud rate averaged 74.3 fraud cents between 2016 and 2018. The introduction of the CNP framework and other mitigants implemented by the industry continue to assist in achieving a stabilisation of the fraud rate.

Further details are available at https://www.auspaynet.com.au/insights/initiatives/CNP-Fraud-Mitigation-Framework.

How consumers can reduce fraud risk

Australian consumers are not liable for fraud losses on payment cards and will be refunded provided they have taken due care with their confidential data. Consumers are also reminded to regularly check their account statements and immediately report any unusual transactions to their financial institution. The measures below remain practical ways for consumers to prevent card fraud.

Remote Payments – Card-Not-Present



Authentication tools

Register for and use your financial institution's online payment fraud prevention solutions whenever prompted.

Biometrics are increasingly used for transaction authorisation, both in-store and via remote channels.

In-app payments can improve convenience and security via biometric support (e.g. thumbprint or facial recognition).

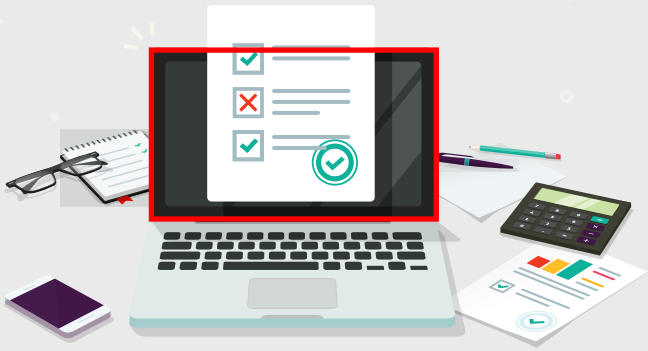
Know who you are dealing with

Take a few minutes to ensure that you are dealing with a legitimate merchant online. Do some checks before making a payment on a website for the first time.

Only provide card details on secure and trusted websites – look for a locked padlock icon in the toolbar and 'https' in the website's address.

Be suspicious of offers that look too good to be true – they probably are.

More information on Online Shopping Scams is available at ScamWatch.gov.au.



Be alert to phishing attacks

Be cautious when clicking on hyperlinks and email attachments or texts sent by an unknown contact.

As a general rule, do not provide your personal details to anyone you do not know or trust who makes contact with you, especially if it includes a proposition that involves payment.

Take time to install systems on your devices to protect against viruses and malicious software.

More information is available at ScamWatch.gov.au.

Face-to-face - Card Present

Protect against theft

Report any lost or stolen cards to your financial institution straight away. Similarly, tell your financial institution immediately if/when you change address.

To protect against mail theft, you should:

- Install a lockable mailbox and clear it daily
- During extended periods of absence, have mail held at the post office or collected by a friend
- Contact your financial institution if your new card has not arrived as expected

Protect your PIN & personal details

Consumers should keep their PIN secret, and always cover the PIN pad when entering PINs at point-of-sale terminals and ATMs.

Financial institutions will never ask their customers to divulge their card PIN over the phone, online or in an app.

Keep personal documents secure at home and shred any bills or statements before throwing them away.

Protect against skimming

The vast majority of payment terminals, ATMs and cards in Australia support chip transactions, which give strong protection against skimming fraud.

Always keep your card in sight when making a payment and do not hand your card to anyone else when making contactless payments. If you spot anything suspicious at an ATM or unattended terminal, do not use the machine and report it to your financial institution.

Contactless payments using a mobile device can provide added protection through biometric authentication and tokenised card credentials.

How merchants can reduce fraud risk

Financial institutions, payment gateways, cyber and fraud management services and other payment service providers offer a range of solutions to mitigate payment fraud. Increasingly, fraud detection solutions are leveraging new technologies such as machine learning and artificial intelligence. Merchants should discuss options for securing their businesses directly with their service providers, to ensure solutions are tailored specifically to their business needs.

Remote Payments – Card-Not-Present

Payment Card Industry Data Security Standards (PCI DSS)

PCI DSS defines the minimum security controls required when cardholder data is stored, processed or transmitted. The goal is to increase security controls and minimise the card data compromised in the instance of an attack (such as a data breach).

Compliance with PCI DSS can be a significant undertaking and online merchants may wish to investigate the use of hosted solutions provided by a PCI DSS-compliant service provider.

Use tools that help authenticate customers

SCA should be used for transactions identified as higher risk (including high value transactions) to ensure the person requesting the transaction is the legitimate card owner.

In addition to other risk-based fraud controls used by merchants, the 3DS 2.0 protocol includes an ability to share greater data to inform a more assured risk-based decision by the card issuer and reduce declines.

Invest in tokenisation

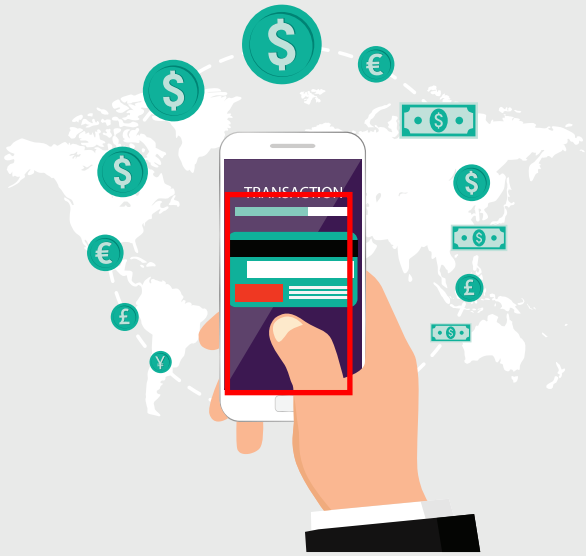
Merchants holding sensitive payment information can become targets for the theft of card data through hacking or other data breaches. Tokenisation replaces the original payment credential with a unique digital identifier (a token). This means that even if there is a data compromise of a merchant's systems, the card information cannot be misused.

The card schemes and financial institutions now offer tokenisation services based on the EMV Payment Token specification. Payment tokens offer an additional layer of security and deliver unique identifiers across different channels, linking back to the original 16-digit card Personal Account Number of the payment card.

Remote Payments – Card-Not-Present

MOTO transactions

Mail Order/Telephone Order (MOTO) transactions – in which the cardholder provides card details over the phone to the merchant – are susceptible to fraud, because it is difficult for the merchant to verify the identity of the cardholder. Merchants should be cautious processing MOTO transactions, especially where unusually large value items, or multiple duplicate orders for the same item, are concerned.



Overseas cards

It is possible to use fraud management selectively and apply rules to different transactions based on, for example, transaction value, product purchased and shipping destination. Rules can also be set on card issuing country, so that you can choose to evaluate overseas card transactions more thoroughly.

Face-to-face - Card Present

EMV chip technology

The global shift to EMV chip technology is proving effective in preventing face-to-face fraud.

A small number of cards (e.g. some overseas, prepaid) may not have chip. If a signature is required, check it carefully against the card signature.

Merchants should encourage cardholders to insert chip cards for contact transactions or tap cards for contactless transactions (with or without PIN).

Avoid refunds to alternative cards

The card schemes define the rules and processes for disputing a transaction.

All refunds should be processed onto the same card that was used to make the original purchase. Requesting a refund to a different card is a common fraudster tactic.

Data and Trends

All Australian Cards

Data in the tables below provide an overview of all transactions on Australian cards. The aggregated data includes:

- fraud on scheme credit, debit and charge cards as operated by American Express, Diners Club International, eftpos Payments Australia, Mastercard and Visa
- card payment statistics published by the Reserve Bank of Australia.

Trends on Australian-issued cards

In 2021, as the economic recovery from the global pandemic began, overall spending on Australian cards increased to $865 billion, an 8.0% increase on the previous year and a 21% increase since 2016. Fraud accounted for 0.057% of that total, a decrease from 0.059% in 2020. The number of fraudulent transactions on Australian cards increased by about 5%, to 4.27 million, but remained below the peak levels observed in 2018. The average value of fraud transactions was $116, well below the $188 average in 2016.

	2017	2018	2019	2020	2021
Value:					
All card transactions*	$748b	$789b	$820b	$801b	$865b
Fraudulent transactions	$561m	$576m	$465m	$469m	$495m
Fraud rate (cents per $1,000):	**75.0c**	**73.0c**	**56.7c**	**58.6c**	**57.3c**
Number:					
All card transactions*	8,965m	9,985m	11,000m	11,373m	12,528m
Fraudulent transactions	3,581,001	4,369,431	3,796,069	4,062,183	4,267,201
Fraud rate (as % of total no. of card transactions)	**0.040%**	**0.044%**	**0.035%**	**0.036%**	**0.034%**
Average value of fraudulent transactions	$157	$132	$122	$115	$116

*Source: Reserve Bank of Australia

Types of fraud occurring on Australian cards

The definitions of the different types of fraud are provided in the Glossary. In 2021, CNP fraud increased by 7.6% on the previous year, counterfeit/skimming fell by 50.8% to a record low, and fraudulent applications dropped significantly (65.6%), as a result of the technological and security mitigants adopted by industry. After a 24.6% fall in 2020, lost/stolen card fraud rose by 9.3%, which may be linked to increased opportunities for fraudsters associated with Australians having emerged from COVID-19 lockdowns.

Fraud value ($m)	2017	2018	2019	2020	2021
Card-not-present	$476.1	$489.0	$403.4	$420.1	$451.8
Counterfeit / skimming	$30.9	$19.6	$16.9	$11.1	$5.5
Lost / stolen	$40.6	$55.6	$35.1	$26.4	$28.9
Never received	$7.9	$6.1	$3.0	$3.1	$2.0
Fraudulent application	$3.3	$2.3	$2.4	$2.6	$0.9
Other	$2.5	$3.5	$4.2	$5.6	$6.4
TOTAL	**$561.3**	**$576.2**	**$465.0**	**$469.0**	**$495.5**

Trends

There was a 7.6% increase in card-not-present (CNP) fraud in 2021 to $452 million. This coincides with an 8.2% increase in online retail spending, to $53 billion, reflecting Australians' growing preference for the convenience of digital channels and online shopping post the COVID-19 pandemic. CNP fraud now accounts for 91% of all Australian card fraud, which is in line with the global trend of growing online card fraud and cybercrime in general. The following are key reasons for global growth:

- Migration from card-present channels – with the rapid shift towards online transactions, and with EMV chip technology providing strong protection for face-to-face transactions, fraud is migrating online.
- Large scale data breaches – sensitive card data is captured and used to perform fraudulent transactions.
- Identity theft – fraudsters assume the identity of another individual and perform transactions under a false identity.

Chip technology continues to be effective in combatting fraud on Australian cards. Counterfeit/skimming fraud fell for the fifth consecutive year, down to $5.5 million in 2021 – a 90.7% drop from a peak of $59.2 million in 2016. As card fraud becomes more difficult for criminals to perpetrate, there is a shift towards scams and buy-now-pay-later (BNPL) fraud. Additionally, friendly/first party fraud occurs when customers dishonestly claim to have not received goods or, during a returns dispute with a merchant, claim the transaction is fraudulent. Industry reports that friendly/first party fraud is becoming a greater issue. AusPayNet is working with industry to obtain further insights and mitigate these threats.

Australian Cards

Fraud perpetrated in Australia

Fraud perpetrated on Australian-issued cards within Australia rose by 9% in 2021 to $315.7 million. Card-Not-Present (CNP) fraud was up by 10% to $291.0 million and accounted for 92% of the fraud perpetrated in Australia. Significant falls were observed in both the counterfeit/skimming and fraudulent application categories. Counterfeit/skimming fell by more than 49% to $1.6 million and fraudulent applications by around 65% to $810,000.

Fraud ($m)	2017	2018	2019	2020	2021
Card-not-present	$227.4	$258.6	$224.5	$264.6	$291.0
Counterfeit / skimming	$4.6	$5.1	$4.5	$3.2	$1.6
Lost / stolen	$24.7	$33.0	$19.0	$16.6	$19.4
Never received	$6.1	$4.4	$1.9	$1.9	$1.2
Fraudulent application	$2.8	$1.9	$2.0	$2.3	$0.8
Other	$0.9	$1.1	$1.0	$1.2	$1.7
TOTAL	$266.5	$304.1	$252.9	$289.7	$315.7

NOTE: The number of fraud transactions does not represent the number of cards or consumers affected. Typically, multiple fraud transactions are made on a single compromised payment credential. Financial institutions report card fraud as gross actual losses.

Fraud perpetrated overseas

Fraud on Australian cards transacting in overseas locations fell by 15% in 2020, to $168.3 million, the fourth year of decline. In 2021, this rate remained stable, at $169 million. Most fraud perpetrated overseas on Australia cards continues to be in the CNP category. Card details are often obtained through data breaches that have occurred onshore in Australia. In 2021, CNP fraud at overseas online merchants rose 3.4%, to $160.8 million. In all other categories, fraud on Australian cards transacting in overseas locations fell in 2021.

Fraud ($m)	2017	2018	2019	2020	2021
Card-not-present	$248.7	$230.5	$178.9	$155.5	$160.8
Counterfeit / skimming	$14.4	$8.1	$6.3	$5.1	$1.5
Lost / stolen	$13.4	$18.8	$11.5	$5.5	$5.5
Never received	$0.3	$0.4	$0.1	$0.2	$0.1
Fraudulent application	$0.6	$0.4	$0.5	$0.3	$0.1
Other	$0.6	$0.6	$0.7	$1.6	$1.1
TOTAL	$277.9	$258.8	$198.1	$168.3	$169.0

Overseas Cards

Fraud perpetrated in Australia

When international visitors use their cards at Australian ATMs or point-of-sale (POS) terminals or on Australian websites, the payment transactions are processed by the international card schemes. With Australia's borders closed for most of 2021 due to the COVID-19 pandemic, fraudsters with overseas cards were largely limited to online transactions. Indeed, fraud perpetrated in Australia using cards issued overseas continued to decline, by 24% to $61.7 million. All categories of fraud declined or remained stable, including CNP fraud, which was down 23.6% to $54.8 million.

Australian merchants play a significant role in identifying and addressing fraud on overseas-issued cards. Security features on these cards vary by the country of origin.

Fraud ($m)	2017	2018	2019	2020	2021
Card-not-present	$67.3	$71.5	$82.6	$71.8	$54.8
Counterfeit / skimming	$7.6	$5.8	$7.3	$4.8	$3.2
Lost / stolen	$3.4	$3.3	$4.5	$3.3	$2.5
Never received	$0.1	$0.1	$0.2	$0.1	$0.1
Fraudulent application	$0.1	$0.1	$0.1	$0.1	$0.1
Other	$0.8	$1.4	$0.9	$0.9	$1.0
TOTAL	$79.4	$82.3	$95.6	$81.0	$61.7

Cheque Fraud Perpetrated in Australia

AusPayNet also collects cheque fraud data, which covers fraud occurring on Australian issued cheques in Australia and overseas. The figures represent the losses written off by financial institutions during a given year, although the fraud may have occurred sometime before. Cheque data includes Australian personal cheques, financial institution cheques and drafts in Australian dollars.

In 2021, consumers' continued shift towards digital payments was also reflected in the further decline in the use of cheques, with the value transacted dropping 8.7%, to $371 million. Fraud losses on cheques declined by 20%, to $3.2 million, and the fraud rate decreased to 0.9 cents per $1,000 transacted.

	2017	2018	2019	2020	2021
Value:					
Cheque transactions*	$1b	$885m	$602m	$407m	$371m
Fraudulent transactions	$5.9m	$4.4m	$4.8m	$4.0m	$3.2m
Fraud rate (cents per $1,000):	**0.5c**	**0.5c**	**0.8c**	**1.0c**	**0.9c**
Number:					
Cheque transactions*	90m	72m	57m	41m	33m
Fraudulent transactions	727	591	680	652	494
Fraud rate (as % total no. of transactions)	0.0008%	0.0008%	0.0012%	0.0016%	0.0015%
AVERAGE VALUE OF FRAUDULENT TRANSACTIONS	$8,123	$7,402	$7,106	$6,153	$6,503

*Source: Reserve Bank of Australia

Fraud ($m)	2017	2018	2019	2020	2021
On us fraud:					
Breach of mandate	$0.4	$0.4	$0.0	$0.0	$0.2
Fraudulently altered	$2.4	$1.2	$1.5	$1.1	$0.9
Stolen blank cheque / book	$2.3	$1.5	$1.9	$1.2	$1.3
Originated counterfeit cheques	$0.3	$0.2	$0.4	$0.4	$0.4
Non originated counterfeit cheques	$0.3	$0.1	$0.6	$1.2	$0.3
Valueless	$0.0	$0.3	$0.0	$0.0	$0.0
ON-US TOTAL	$5.7	$3.7	$4.4	$3.9	$3.1
Deposit Fraud	$0.2	$0.7	$0.4	$0.1	$0.1
TOTAL ALL CHEQUES FRAUD	$5.9	$4.4	$4.8	$4.0	$3.2

'Actual' losses can relate to 'Exposure' during an earlier period. This explains why in some reporting periods, actual losses may exceed exposure.

Scams

Fraud or Scam – What's the difference?

Fraud is commonly defined as an unauthorised payment made from an account without the permission of the account holder. Scams occur when an account holder is tricked into authorising a payment from their account or sharing information that enables the scammer to authorise a payment by impersonating the account holder.

Because payment fraud is becoming more difficult to perpetrate, criminal groups are turning their attention to other kinds of activities, a shift that is reflected in an increase in scams. In 2021, Australians lost over $2 billion to scams, according to a report by the Australian Competition and Consumer Commission (ACCC).[3] Scams are on the rise and IDCARE, who provide victim support services, reported a 43% surge in demand for their services in 2021, compared to 2020.[4]

Additionally, the ABS reported that 55% of Australians aged 15 and over (11.1 million Australians) were exposed to a scam during the 2020-21 survey period, while 723,000 (3.6%) responded to a scam. The survey revealed that only 50% of those targeted by a scam actually reported it to an authority, most people instead only reporting it to their financial institution.

The ABS survey revealed that Australians were targeted by scammers outside of the payments system. Most commonly, their exposure to a scam was via telephone (38.3% or 7.8 million Australians) or email (32.2% or 6.5 million Australians). Similarly, IDCARE attributes the heightened demand for their services to scam activities targeting Australians via telephone and text messages.

ABS data highlights the elaborate lengths scammers go to to identify and engineer victims via telecommunications, email and online platforms. Using these platforms, scammers trick their victims into authorising payments.

The ABS survey suggested a significant underreporting of scam offences to law enforcement bodies. Underreporting is a global trend and is attributed to embarrassment, concerns about reputational damage, confusion over multiple avenues of reporting and expectations of a limited response from law enforcement and regulatory authorities.[5]

How were victims exposed to scams?

38.3% PHONE CALL

32.2% EMAIL

23.4% TEXT MESSAGE

20.2% ONLINE

0.6% OTHER

1.3% LETTER

Source: ABS, Personal Fraud 2020-21

Australian Communication and Media Authority (ACMA) consumer research from 2021 indicated that approximately 98% of Australian adults received scam calls or texts.[6]

In 2020, the Reducing Scams Call Code was introduced and since then, the payments industry and organisations such as the Australian Financial Crime Exchange provide information that has contributed to more than 549 million unsolicited scam communications being blocked.[7] Similarly, the introduction of the *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020* has been linked to a significant reduction in mobile porting scams. And effective 30 June 2022, new rules introduced by ACMA require telcos to use multi-factor ID checks for transactions commonly targeted by scammers.[8]

Financial institutions are dedicating significant resources and technology to the detection and prevention of scams, and the education of end users.

In late 2021, AusPayNet established the Economic Crime Forum (ECF), which expanded on the Fraud in Banking Forum's existing role. The ECF brings together a broad set of participants to coordinate a joint response to all economic crime – scams, fraud, financial crime, and banking-related cyber incidents – and share intelligence on emerging threats. The ECF has representatives from AusPayNet's 150+ members and includes Australia's State and Federal policing agencies, intelligence agencies and regulators.

The ECF allows AusPayNet members to:

- share data to develop insights, priorities and appropriate response strategies
- provide referrals to law enforcement, intelligence agencies or regulators to disrupt economic crime
- identify and develop community awareness prevention initiatives
- allow industry to share best practice technological and procedural risk mitigants.

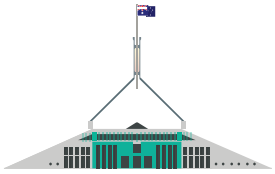
The ECF's current priorities are addressing investment, romance and remote access scams, which account for approximately 80% of scams (in terms of value and volume), according to industry data.

In 2021, AusPayNet also developed a scams mitigation program with the Australian Banking Association (ABA), Australian Financial Crime Exchange (AFCX) and IDCARE. Via collaboration, the program seeks to make Australia a hard target for scams, with the objective of achieving reduction in occurrences and losses. The program includes the following five key pillars of work:

1. **Data and Insights:** Via the AFCX, use data to drive insights and response strategies to reduce scams.
2. **Fusion and Response:** Via the ECF, connect law enforcement and industry to drive response, community awareness and prevention strategies.
3. **End User Education:** Develop and implement an industry-driven end user awareness and prevention program to increase customer awareness and reduce the likelihood of scams. IDCARE highlights that Australians need to take more collective responsibility to fight against scammers by emphasising one of our core cultural values – looking out for your mates. Family members and friends are a key disrupter to scammers.
4. **Policy:** Contribute to public policy to ensure the most effective strategies to reduce the impact of scams on consumers and make Australia hostile to scammers.
5. **Industry Standards:** Review the AusPayNet and IDCARE identity theft and scam industry standards and guidelines, to ensure consistent industry standards and minimise the impact of scams on payment end users and our financial system.

Scams were reported to...

27.3% BANK OR FINANCIAL INSTITUTION



8.4% GOVERNMENT ORGANISATION OR DEPARTMENT

9.8% OTHER

8.7% SOCIAL MEDIA OR SELLING SITE

8.2% POLICE

50.3% INCIDENT NOT REPORTED

Source: ABS, Personal Fraud 2020-21

*Figures reflect that scams may have been reported to more than one authority

[1] Targeting scams: report of the ACCC on scams activity 2021" released July 2022
[2] IDCARE is Australia and New Zealand's national identity and cyber support service that helps individuals and organisations reduce the harm they experience from the compromise and misuse of their identity information by providing effective response and mitigation.
www.idcare.org
[3] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime Cross C, Richards K & Smith R 2016, The reporting experiences and support needs of victims of online fraud, Trends & Issues in crime and criminal justice no. 518, Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi518
[4] Australian Communications and Media Authority, "Unsolicited communications in Australia: Consumer experience research 2021" released January 2022
[5] https://www.accc.gov.au/speech/acccs-priorities-and-approach-to-regulating-the-financial-services-sector
[6] Scams targeting multicultural communities are on the rise – CHOICE
https://www.acma.gov.au/articles/2022-07/new-rules-fight-sms-scams

Glossary - Card Fraud

Types of Fraud

Card-Not-Present (CNP) fraud: occurs when valid card details are stolen 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.

Card Present fraud: occurs when a physical card is used fraudulently at ATMs or point-of-sale devices. The various types of card present fraud are:

Counterfeit / skimming: 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.

Lost / stolen: Lost and stolen 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.

Never received: refers to unauthorised transactions on cards that were stolen before they were received by the owners.

Fraudulent application: transactions made on a card where the account was established using someone else's identity or other false information.

Friendly/first party fraud: occurs when customers dishonestly claim that they have not received goods. Alternatively, it describes where, during a returns dispute with a merchant, a customer claims the transaction is fraudulent.

Other: covers fraudulent transactions that cannot be categorised under any of the common fraud types above. For example, identity or account takeover.

Types of Cards

Scheme credit, debit and charge cards: operated by international card schemes – Mastercard, Visa, American Express, and Diners – and domestic debit scheme, eftpos Payments Australia Limited.

Key Terms

Payment Card Industry Data Security Standard: PCI DSS is a security standard mandated by the international card schemes to ensure sensitive card data is held securely.

About Us

Australian Payments Network (AusPayNet) is the self-regulatory body for Australia's payments industry. We enable the efficiency, resilience, adaptability, and accessibility of Australia's payments system. We have more than 150 members and participants, including Australia's leading financial institutions, major retailers, payments system operators – such as the major card schemes – and other payments service providers. Through our network, we deliver on our purpose to promote confidence in payments and to ensure the payments system continues to meet the evolving needs of end users.

30 YEARS

Australian Payments Network

Australian Payments Network Limited
ABN 12 055 136 519

Level 23, Tower 3, International Towers Sydney
300 Barangaroo Avenue 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
[illegible] www.auspaynet.com.au