Australian
Payments Network
Connect Inspire Thrive

AUSTRALIAN PAYMENT FRAUD 2021

Australian Payments Network collects payment fraud data from financial institutions and card schemes. We publish this report to increase merchant and consumer awareness about fraud trends and prevention measures.

SNAPSHOT

In 2020, in the wake of the global pandemic, spending on Australian payment cards fell for the first time – down 2.2% to $801.7 billion. Card fraud increased by 0.6% to $468 million, driven by the accelerated shift to online payments.

COMBATTING FRAUD

While Australian online retail spending grew by an estimated 44%, online card fraud increased by 3.8% to $418.9 million. The industry CNP Fraud Mitigation Framework continues to support financial institutions' fraud detection and prevention initiatives.

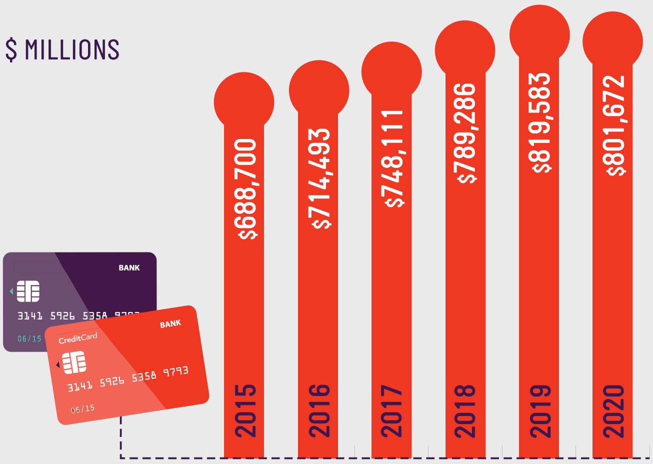
DATA AND TRENDS

As card fraud becomes more difficult to perpetrate, scams are on the rise. The ACCC reports that Australians lost over $850 million to scams in 2020 – up 34% on 2019, and almost twice the total value of card fraud. The industry's focus is on improving protection of susceptible customers.

JANUARY – DECEMBER 2020 DATA

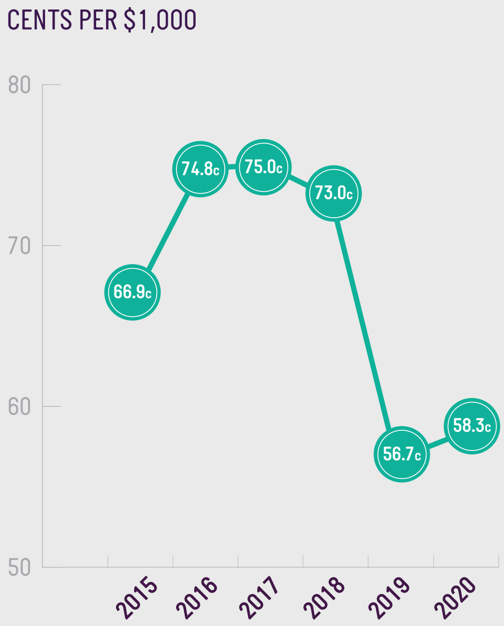
Snapshot

IN 2020, AS COVID-19 TOOK HOLD, THE TOTAL VALUE OF CARD PAYMENTS FELL FOR THE FIRST TIME – **DOWN 2.2%.**



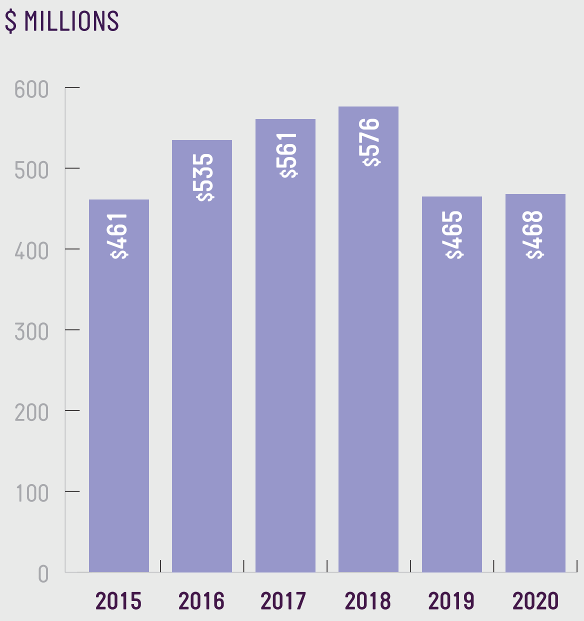
Source: Reserve Bank of Australia

THE CARD FRAUD RATE **ROSE SLIGHTLY** IN 2020 BUT REMAINS WELL BELOW LEVELS SEEN IN THE RECENT PAST.



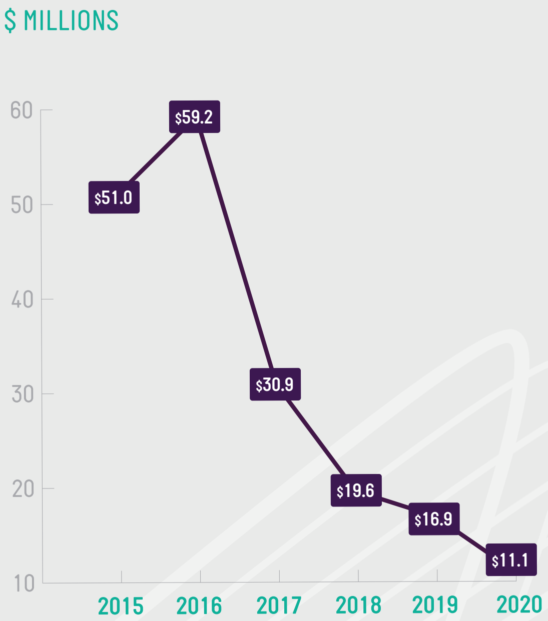
Source: Reserve Bank of Australia and AusPayNet

THE TOTAL VALUE OF CARD FRAUD **REMAINED LARGELY UNCHANGED** – UP 0.6% ON 2019.



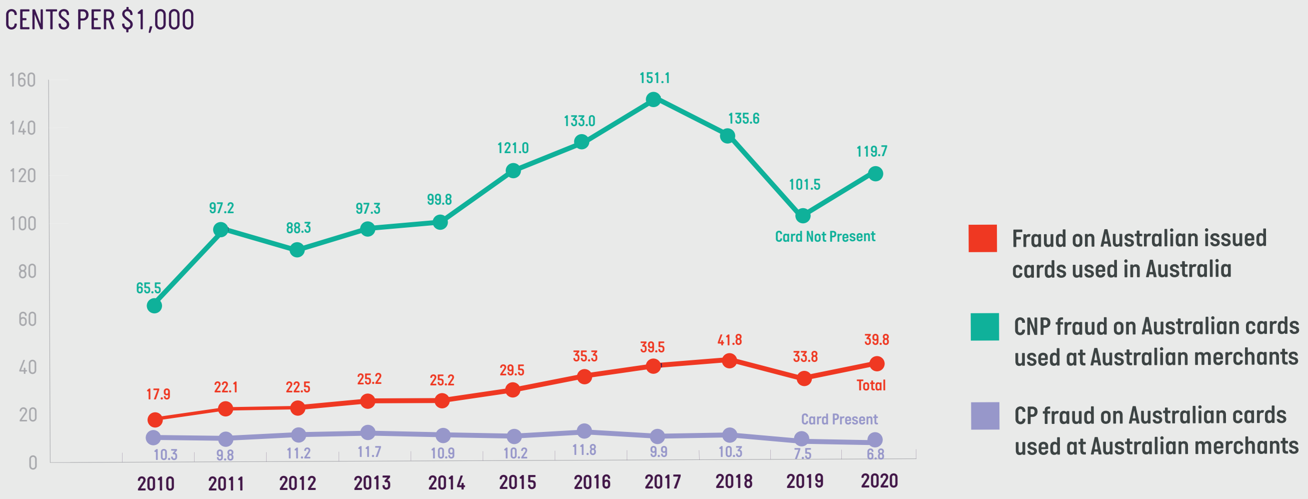
Source: AusPayNet

COUNTERFEIT/SKIMMING FRAUD **FELL 34%** TO REACH ANOTHER RECORD LOW.



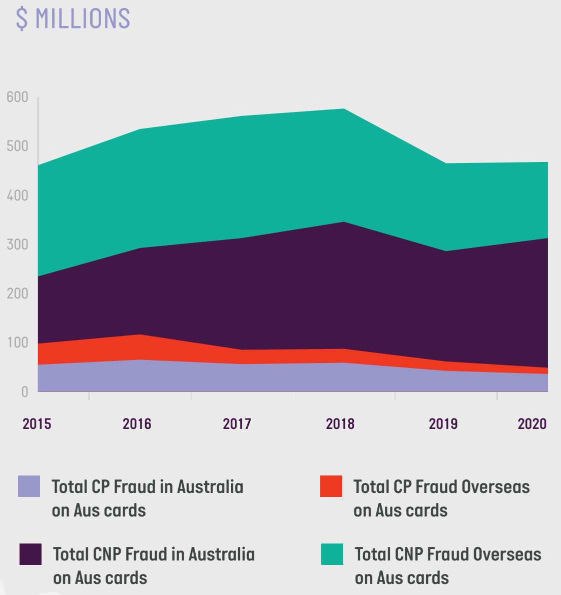
Source: AusPayNet

WITH ONLINE SPENDING UP AN ESTIMATED 44%*, THE **CNP FRAUD RATE HAD AN UPTICK.**



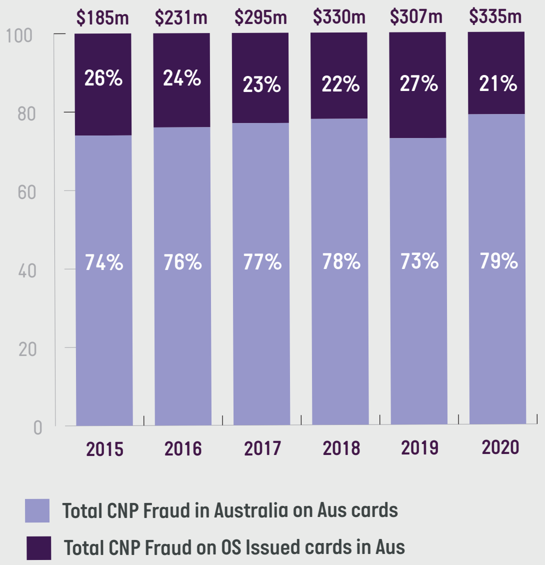
Source: Reserve Bank of Australia and AusPayNet
* NAB Online Retail Sales Index

ALONG WITH THE UPTICK IN CNP FRAUD, **ALL OTHER TYPES OF CARD FRAUD FELL.**



Source: AusPayNet analysis

CNP FRAUD AT AUSTRALIAN ONLINE MERCHANTS **INCREASED BY 9% ON 2019 AND 1.5% ON 2018.**



Source: AusPayNet

Payment Fraud

IN 2020, IN THE WAKE OF THE GLOBAL PANDEMIC, SPENDING ON AUSTRALIAN CARDS DROPPED BY 2.2% AND THE OVERALL VALUE OF CARD FRAUD REMAINED LARGELY UNCHANGED - UP BY 0.6%.

The COVID-19 pandemic has reinforced the strong customer preference for digital payments and sparked a significant surge in the adoption of e-commerce[1]. Changing habits due to restrictions and lockdowns accelerated the pre-existing shift to online channels. With more transactions occurring in the online space, fraud continues to move online.

In 2020, spending on Australian cards dropped for the first time to total $801.7 billion – down 2.2% on the previous year. Against this drop, the NAB Online Retail Sales Index estimates that online retail spending grew by 44%[2]. Similarly, data from the Australian Bureau of Statistics shows that from March 2020 to January 2021, total online sales have averaged an annual rise of 65%[3].

While overall card fraud remained largely unchanged in 2020 - up 0.6% to $467.6 million - card-not-present (CNP) fraud, which occurs mainly online, increased by 3.8% to $418.9 million. Over the same period, card-present (CP) fraud continued to fall. Counterfeit/skimming fraud dropped by 34.1% to $11.1 million, reaching another record low - and lost and stolen card fraud dropped by 24.9% to $26.3 million, the lowest total since 2012. Chip technology continues to provide strong protection against counterfeit/skimming protection. Similarly, contactless payments using a mobile phone or device are highly secure.

As face-to-face transactions decreased during the pandemic and online shopping continued to accelerate, there was an uptick in CNP fraud.

Online card fraud now accounts for 90% of all fraud on Australian cards – up from 87% in 2019. Combatting CNP fraud remains a priority and the payments industry continues to be vigilant as e-commerce volumes rapidly increase during the pandemic. The CNP Fraud Mitigation Framework introduced by AusPayNet in July 2019 is supporting financial institutions' fraud detection and mitigation initiatives. Financial institutions have continued to update their fraud capabilities including use of secure technologies such as real-time monitoring, machine learning, tokenisation and strong customer authentication. The application of these tools has helped CNP fraud remain below the peak levels of 2018 ($489.9 million) and 2017 ($476.1 million) during the pandemic.

The following sections provide further information on card fraud trends, as well as measures that consumers and businesses can take to actively mitigate risk.

As criminals adapt and evolve their methods to take advantage of people spending more time online, payment scams are on the rise. Data relating to scams are included in this report.

[1] https://www.rba.gov.au/publications/annual-reports/psb/2020/trends-in-payments-clearing-and-settlement-systems.html
[2] https://business.nab.com.au/wp-content/uploads/2021/02/NAB-Online-Retail-Sales-Index-December-2020.pdf
[3] https://www.abs.gov.au/articles/online-sales-january-2021-supplementary-covid-19-analysis

Australian payments industry actions to further combat fraud

Preventing payment fraud requires coordination at every level, from financial institutions and card schemes through to merchants and consumers. AusPayNet is leading a number of industry wide initiatives aimed at increasing the security and convenience of payments. The following two initiatives in particular are focused on the online environment.

CNP FRAUD MITIGATION FRAMEWORK

At the end of 2020, the industry CNP Fraud Mitigation Framework had been in operation for 18 months and is being widely used across the industry. The Framework is designed to reduce fraud in Australian online channels while at the same time ensuring remote transactions continue to grow. It provides a mechanism for managing fraud thresholds that all merchants and issuers must remain below.

The NAB Online Retail Sales Index estimates that Australian online retail spending grew by 44% in 2020. In this context, the rate of online card fraud increased by 17% to 119.7 cents per $1,000 spent, up from 101.5 cents in 2019, but still held well below the peak of 151.1 cents in 2017. Indeed, CNP fraud rates had started to decline by the latter stages of 2020 as more merchants implemented strong customer authentication (SCA) in their online shopping environments. Under the Framework, SCA is a requirement for those merchants whose fraud rates consistently exceed the agreed thresholds.

To date, of the merchants who have exceeded the agreed fraud threshold, around 60% have brought their fraud levels back below the threshold in the following quarter and a further 10% within subsequent quarters. The remaining 30% of merchants, those with newly reported breaches or complex payment ecosystems, are working closely with their acquirers to reduce fraud.

With the full benefits of the Framework to be realised in coming years, the e-commerce community remains vigilant as online volumes rapidly increase during the pandemic.

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

TRUSTID FRAMEWORK

The accelerated shift to the use of electronic payment channels fuelled by the pandemic has further reinforced the need for individuals and organisations to have better mechanisms for building trust online. Indeed, in 2020, IDCARE (Australia and New Zealand's not-for-profit national identity and cyber support service) witnessed a 76% jump in demand for its services from Australians who have experienced identity theft, scams and cybercrimes.

To promote the effective development of the digital economy, the Australian Payments Council (APC) led the creation of the Trust ID framework . The framework addresses security vulnerabilities and related problems by reducing the requirement for sharing personally identifiable information. It presents a series of rules and guidelines for organisations to adhere to in their design, manufacture and operation of products and services.

During the last 12 months, industry has been focused on developing solutions that will offer interoperable services to consumers and businesses under the framework. In parallel, AusPayNet has led work with members on topics of branding and framework governance. The outcomes from these work streams will be announced later in 2021.

Importantly, the potential role that the TrustID Framework could play in securing the data economy was acknowledged in the report of the Inquiry into the Future Directions for the Consumer Data Right (CDR) .

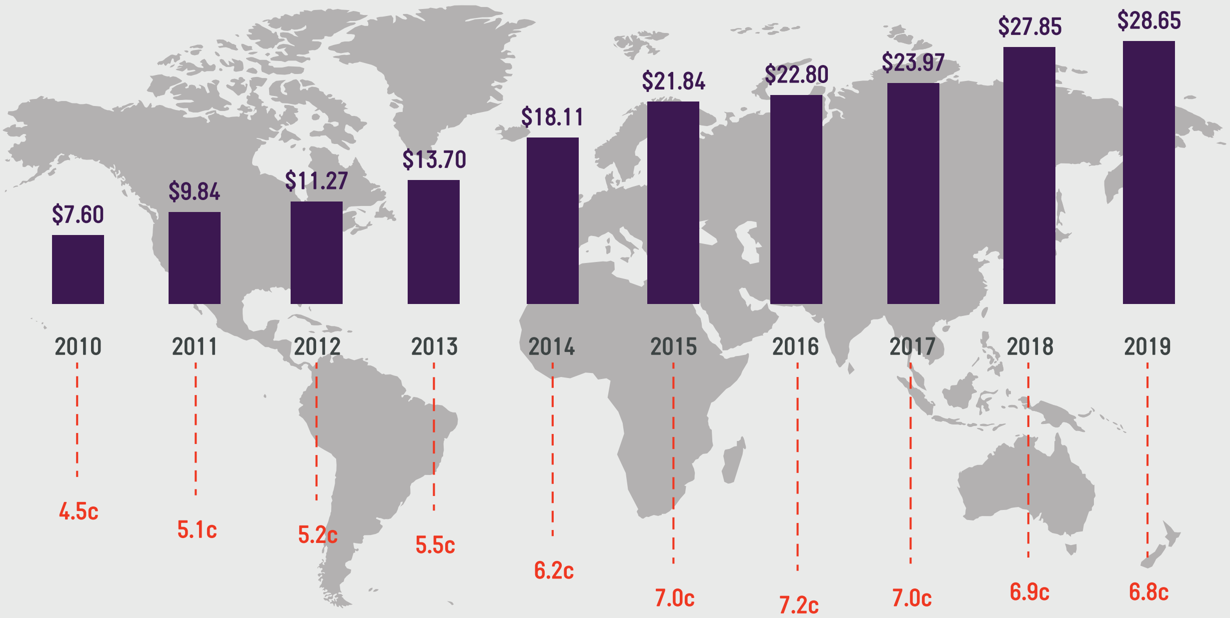
It is anticipated that, in due course, a number of interoperable Digital Identity services will become available in the Australian market. Further details are available at https://www.auspaynet.com.au/insights/Trust-ID.

How does Australia compare?

Fraud rates are the most common measure used by the industry to monitor movement in fraud activity. In 2020, overall spending on Australian cards dopped by 2.2% while card fraud increased by 0.6%. This translated to a card fraud rate of 5.8 cents per $100 spent – up from 5.7 cents per $100 in 2019, and well below 7.3 cents per $100 in 2018.

Recently published 2019 fraud data of comparable geographic markets show that Australia's prevention initiatives are proving effective.

Global Fraud Losses on Cards in USD Billions: 2010-2019



Cents per $100: Of Total Value

Source: The Nilson Report November 2019

2019	Australia[8]	UK[9]	Germany[10]	France[11]	USA[12]
CNP Fraud (% of CNP spend)	0.102%	-	0.165%	0.231%	-
All Card Fraud (% of all card spend)	0.057%	0.075%	0.033%	0.067%	0.103%
2020	**Australia**	**UK**			
All Card Fraud (% of all card spend)	0.058%	0.072%	0.032%	0.071%	
CNP Fraud (% of all card fraud)	89.6%	78.8%	90.9%	78.0%	

[8] Source: RBA payment statistics and AusPayNet analysis

[9] Source: UK Finance

[10] Source: ECB and FICO (https://www.fico.com/europeanfraud/)

[11] Source: ECB and FICO (https://www.fico.com/europeanfraud/)

[12] Source: The Nilson Report

How consumers can reduce fraud risk

Australian consumers are not liable for fraud losses on payment cards, and will be refunded, as long as they have taken due care with their confidential data.

Financial institutions continue to invest in technology and introduce numerous measures to manage fraud risks. These include:

- Self-service systems allowing cardholders to remotely lock their card or place limits on transactions;
- Biometric access authentication to mobile banking apps and payments;
- Card activation processes to ensure the recipient of a new card is the account holder;
- Fraud detection systems to track customer card activity and identify unusual spending patterns;
- PIN verification for cash withdrawals at ATMs and point-of-sale terminals;
- Limits on the value of contactless purchases and mandatory PIN verification for transactions above those limits;
- Detection to stop payments on cards that have been reported lost or stolen:
- Using dynamic Card Verification Codes which are CVVs that are changed regularly by the issuer for use online.

Additionally, consumers are 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 & FRAUD DETECTION TOOLS

Register for and use your financial institution's online payment fraud prevention solutions whenever prompted. Enrol in push notifications so you receive an alert each time a transaction is made on your account.

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.

For example, 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

Do not be tricked into giving fraudsters access to your personal or financial information, and 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 on Phishing Scams is available at ScamWatch.gov.au.

Face-to-face - Card Present

PROTECT AGAINST THEFT

Cardholders are reminded to treat a card like cash, keeping it safe at all times.

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

PROTECT AGAINST SKIMMING

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

Always keep your card in sight when making a payment, and do not hand your card over 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.

PROTECT YOUR PIN & 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.

How merchants can reduce fraud risk

Financial institutions, epayment gateways, cyber & 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 level of security controls required when cardholder data is stored, processed or transmitted. The goal of PCI DSS 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, in order to reduce the scope of their PCI DSS obligations.

USE TOOLS THAT HELP YOU AUTHENTICATE YOUR CUSTOMERS

Merchants are strongly encouraged to use risk-based authentication tools in the first instance to assess the level of risk associated with a particular transaction. Strong Customer Authentication (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. For example, the 3DS 2.0 protocol, which is being rolled-out in Australia, provides enhancements on the original version, including 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 can provide merchants with an additional layer of security, while also delivering unique identifiers across different channels, linking back to the original 16-digit card Personal Account Number of the payment card.

MOTO TRANSACTIONS

Mail Order / Telephone Order (MOTO) transactions – in which the cardholder provides card details over the phone to the merchant – are processed as Card-Not-Present transactions. This channel is 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

CHIP TECHNOLOGY

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

Chip & PIN has been mandated in Australia at point-of-sale since August 2014. 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

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.

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.

OVERVIEW OF TRENDS ON AUSTRALIAN ISSUED CARDS

In the wake of the global pandemic, the overall value of spending on Australian cards dropped in 2020 to $801.6 billion, a 2.2% drop on the previous year. Fraud accounted for 0.058% of that total, slightly up from 0.057% in 2019. Fraud on Australian cards increased by 0.6% to $467.6 million, but remained below the peak levels of 2018 and 2017. The average value of fraud transactions was $116, continuing a long-term downward trend.

	2015	2016	2017	2018	2019	2020
Value ($ millions):						
All card transactions*	$688,700	$714,493	$748,111	$789,286	$819,583	$801,672
Fraudulent transactions	$461	$535	$561	$576	$465	$468
Fraud rate (cents per $1,000):	**66.9**	**74.8**	**75.0**	**73.0**	**56.7**	**58.3**
Number:						
All card transactions*	7,292m	8,051m	8,965m	9,985m	11,000m	11,388m
Fraudulent transactions	2,191,082	2,848,033	3,581,001	4,369,431	3,796,069	4,046,988
Fraud rate (as % of total no. of card transactions)	**0.030%**	**0.035%**	**0.040%**	**0.044%**	**0.035%**	**0.036%**
Average value of fraudulent transactions	$210	$188	$157	$132	$122	$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 2020, amongst the three most prevalent types of card fraud, only CNP fraud increased – up 3.8% on the previous year. Counterfeit/skimming fell by 34.1% to a record low and lost/stolen card fraud dropped by 24.9%, declining for a second year in a row.

Fraud value ($m)	2015	2016	2017	2018	2019	2020
Card-not-present	$363.1	$418.1	$476.1	$489.0	$403.4	$418.9
Counterfeit / skimming	$51.0	$59.2	$30.9	$19.6	$16.9	$11.1
Lost / stolen	$33.3	$37.7	$40.6	$55.6	$35.1	$26.3
Never received	$9.1	$10.3	$7.9	$6.1	$3.0	$3.1
Fraudulent application	$1.3	$3.7	$3.3	$2.3	$2.4	$2.6
Other	$3.1	$5.5	$2.5	$3.5	$4.2	$5.6
TOTAL	**$460.9**	**$534.7**	**$561.3**	**$576.2**	**$465.0**	**$467.6**

TRENDS

Card-Not-Present (CNP) fraud rose in 2020, by 3.8% to $418.9 million. This is likely due to the increased reliance on digital channels due to the lockdowns and work-at-home orders arising from the COVID-19 pandemic, and the accelerated shift to online shopping. CNP fraud now accounts for 90% of all Australian card fraud, reflecting the global trend of growing online card fraud and cybercrime in general. Key reasons for the global growth include:

- Migration from card-present channels – with the rapid shift towards online transactions, and with 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 is proving effective in combatting fraud on Australian cards. Counterfeit/skimming fraud fell for the fourth year in a row, down to $11.1 million in 2020 – an 81% drop from a peak of $59.2 million in 2016. This type of fraud now represents only 2.4% of all fraud on Australian cards, compared to 11.1% in 2016.

Australian Cards

FRAUD PERPETRATED IN AUSTRALIA

Fraud perpetrated within Australia on Australian issued cards rose by 12% in 2020, to $299.8 million. Card-Not-Present (CNP) fraud, primarily occurring online, increased by 18%, to $263.8 million and accounts for 88% of the fraud perpetrated in Australia. Fraud data for contactless or Tap'n'Go cards (with no PIN required) is captured in the Lost /Stolen and Never Received categories. The combined fraud value in these categories declined further in 2020, with Lost/Stolen card fraud dropping 11% to $20.9 million. Counterfeit/Skimming fraud dropped 42.9% to $6 million.

Fraud ($m)	2015	2016	2017	2018	2019	2020
Card-not-present	$136.8	$175.8	$227.4	$258.6	$224.5	$263.8
Counterfeit / skimming	$22.9	$25.8	$16.5	$11.5	$10.5	$6.0
Lost / stolen	$20.5	$23.8	$27.2	$36.9	$23.6	$20.9
Never received	$8.5	$9.7	$7.6	$5.7	$2.8	$2.9
Fraudulent application	$2.2	$3.1	$3.7	$3.7	$4.5	$5.1
Other	$0.9	$2.6	$0.9	$1.1	$1.0	$1.1
TOTAL	$191.7	$240.9	$283.4	$317.4	$266.9	$299.8

FRAUD PERPETRATED OVERSEAS

Fraud on Australian cards transacting in overseas locations fell by 15% in 2020 to $167.8 million, the fourth year of decline. With international borders closed due to the COVID-19 pandemic, there was a significant drop in Australian card spend overseas. Most fraud perpetrated overseas occurs in the CNP category, with the card details often being obtained by data breaches that have occurred onshore in Australia. Nonetheless, CNP fraud at overseas online merchants dropped for the third year running to $155.1 million – down 13%. This type of fraud represents over 92% of the total fraud perpetrated overseas on Australia cards.

Fraud ($m)	2015	2016	2017	2018	2019	2020
Card-not-present	$226.3	$242.3	$248.7	$230.5	$178.9	$155.1
Counterfeit / skimming	$28.1	$33.5	$14.4	$8.1	$6.3	$5.1
Lost / stolen	$12.8	$13.9	$13.4	$18.8	$11.5	$5.5
Never received	$0.6	$0.6	$0.3	$0.4	$0.1	$0.2
Fraudulent application	$0.5	$1.3	$0.5	$0.4	$0.5	$0.3
Other	$0.8	$2.2	$0.6	$0.6	$0.7	$1.6
TOTAL	$269.2	$293.8	$277.9	$258.8	$198.1	$167.8

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 due to the COVID-19 pandemic, fraudsters with overseas cards were primarily limited to online transactions. Indeed, fraud perpetrated in Australia using cards issued overseas reduced for the first time, by 16% to $80.7 million. All categories of fraud declined, including CNP fraud which reduced by 13% to $71.5 million.

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

Fraud ($m)	2015	2016	2017	2018	2019	2020
Card-not-present	$47.9	$55.0	$67.3	$71.5	$82.6	$71.5
Counterfeit / skimming	$8.0	$8.8	$7.6	$5.8	$7.3	$4.8
Lost / stolen	$3.0	$2.8	$3.4	$3.3	$4.5	$3.3
Never received	$0.1	$0.1	$0.1	$0.1	$0.2	$0.1
Fraudulent application	$0.1	$0.1	$0.1	$0.1	$0.1	$0.1
Other	$0.6	$0.9	$0.8	$1.4	$0.9	$0.9
TOTAL	$59.6	$67.7	$79.4	$82.3	$95.6	$80.7

Scams
Data and trends

As payment fraud becomes harder to perpetrate, criminal groups turn their attention to other areas, as is now evident in the rise in scams. The Australian Competition and Consumer Commission (ACCC) reports that Australians lost $851 million to scams in 2020[13]. This represents an increase of 34% on the $634 million scam losses in 2019. The industry is responding to the rise in scams on a number of fronts, including working in close collaboration with law enforcement, and providing a strong focus on victim support.

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.

Scams that dominated 2020

Criminals are using increasingly sophisticated methods to exploit susceptible individuals and businesses online. Across the combined industry reporting, the top three scams causing the most financial harm to Australians in 2020 were: investment scams ($328m), romance scams ($131m) and business email compromise ($128m). The tables below from the ACCC provide a more detailed view of attacks and losses as reported to its Scamwatch.

Table 1[14]

Top 10 scams by reports

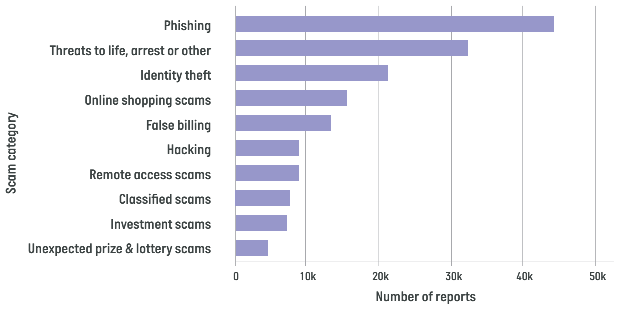
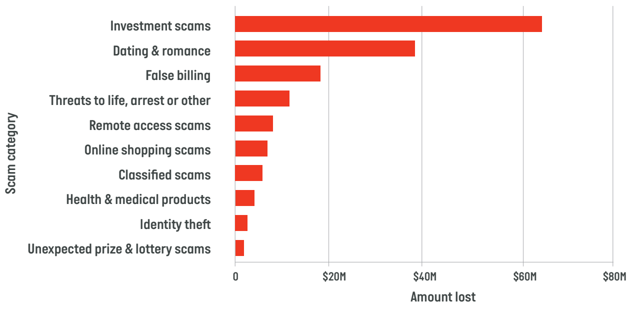


Table 2[15]

Top 10 scams by amount lost



New scam techniques employed during the year, included those related to "Health and Medical Products" (likely to include scams related to COVID-19 cures and vaccination) and mis-directed superannuation withdrawals.

[13] Australian Competition & Consumer Commission report "Targeting Scams: Report of the ACCC on scams activity 2020", released June 2021

[14] https://www.scamwatch.gov.au/scam-statistics

[15] https://www.scamwatch.gov.au/scam-statistics

The industry is increasing defences

Financial institutions continue to take a proactive approach to reducing the impact on customers, including by:

- working in close collaboration with law enforcement to ensure perpetrators of scams are apprehended;
- increasing education and awareness, through targeted campaigns and internet banking messaging, to help susceptible customers
- monitoring unusual transaction activity, and requesting further confirmation of abnormal or large transfers of funds;
- introducing new payment methods that are inherently more secure. For example, payers can ask the person they are about to pay for their PayID, which has a confirmation step, so the payer can be sure they are about to pay the right person.
- identifying account takeovers (where a scammer gains access to an online banking account through phishing personal details), and closing accounts set up in fake names; and
- extending information sharing capabilities to ensure strong coordination and collaboration across the financial services industry and most importantly with other industries.

Scams and identity theft have also been a focus for AusPayNet's Fraud in Banking Forum. In early 2020, a working group chaired by IDCARE finalised the Identity Theft and Scam Response Standard and Guidelines. These provide practical guidance to financial institution staff on supporting victims, including best practice communications and response processes.

Building on significant efforts already underway, AusPayNet has established the Economic Crime Forum, which will take over from and expand on the Fraud in Banking Forum's existing role. The new forum will bring 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.

Education and awareness

Governments and financial institutions are educating consumers and businesses on the types of scams and the circumstances scammers are exploiting to trick account holders. As the shift to digital payments accelerates, consumers and businesses need to be wary of unsolicited contact online and try to keep personal information private. Always be alert to scams, especially if a proposition involves payment, and there is a sense of urgency in the request. Immediately report any suspicious activity to your financial institution and Scamwatch. Further information is available at Scamwatch.

Cheque Fraud Perpetrated in Australia

AusPayNet also collects cheque fraud data; this data 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.

The usage of cheques continues to decline in Australia, with the value transacted dropping 32% to $407 billion in 2020. Fraud losses on cheques remain low, both in absolute dollars at $4.0 million and in fraud rate at 1¢ per $1,000 transacted.

	2015	2016	2017	2018	2019	2020
Value ($ millions):						
Cheque transactions*	$1,228,426	$1,154,864	$1,110,711	$885,147	$602,094	$407,096
Fraudulent transactions	$8.4	$6.4	$5.9	$4.4	$4.8	$4.0
Fraud rate (cents per $1,000):	**0.7**	**0.6**	**0.5**	**0.5**	**0.8**	**1.0**
Number:						
Cheque transactions*	140m	112m	90m	72m	57m	41m
Fraudulent transactions	1,160	904	727	591	680	652
Fraud rate (as % total no. of transactions)	0.0008%	0.0008%	0.0008%	0.0008%	0.0012%	0.0016%
AVERAGE VALUE OF FRAUDULENT TRANSACTIONS	**$7,232**	**$7,087**	**$8,123**	**$7,402**	**$7,106**	**$6,153**

*Source: Reserve Bank of Australia

Fraud ($m)	2015	2016	2017	2018	2019	2020
On us fraud:						
Breach of mandate	$0.3	$0.9	$0.4	$0.4	$0.0	$0.0
Fraudulently altered	$3.6	$2.1	$2.4	$1.2	$1.5	$1.1
Stolen blank cheque / book	$1.8	$2.2	$2.3	$1.5	$1.9	$1.2
Originated counterfeit cheques	$1.2	$0.4	$0.3	$0.2	$0.4	$0.4
Non originated counterfeit cheques	$0.7	$0.6	$0.3	$0.1	$0.6	$1.2
Valueless	$0.7	$0.0	$0.0	$0.3	$0.0	$0.0
ON-US TOTAL	**$8.2**	**$6.2**	**$5.7**	**$3.7**	**$4.4**	**$3.9**
Deposit Fraud	$0.2	$0.2	$0.2	$0.6	$0.4	$0.2
TOTAL ALL CHEQUES FRAUD	**$8.4**	**$6.4**	**$5.9**	**$4.4**	**$4.8**	**$4.0**

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

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: transactions made on a card that was stolen before it was received by the owner.

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

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 is the self-regulatory body for Australia's payments industry. We have more than 140 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.

Australian
Payments
Network
Connect Inspire Thrive

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.
Full details are available on www.auspaynet.com.au