Australian Payments Network
Connect Inspire Thrive

AUSTRALIAN PAYMENT FRAUD 2020

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

Fraud on Australian payment cards dropped by double digits for the first time ever in 2019. While spending on cards grew by 3.9% to more than $819 billion, fraud fell by 19.5% to $464 million.

COMBATTING FRAUD

The CNP Fraud Mitigation Framework took effect in July 2019. This industry initiative is targetting online card fraud alongside a range of fraud detection and prevention measures.

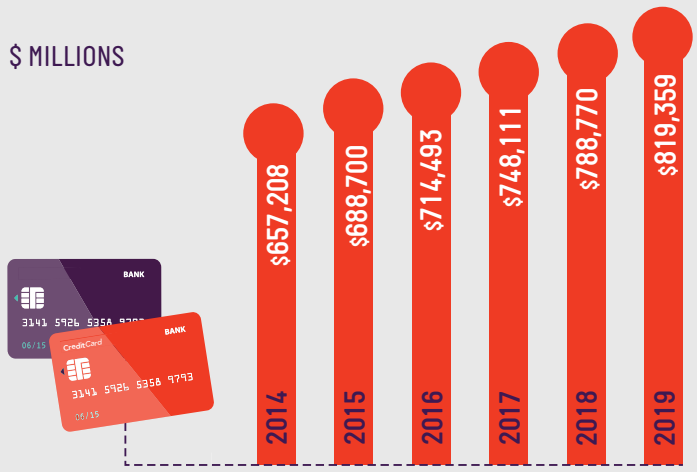
DATA AND TRENDS

The value of online card fraud fell by 17.7%, skimming/counterfeit fraud by 14.3% and fraud on lost/ stolen cards by 37%. While fraud on cards is dropping, scams are on the rise.

JANUARY – DECEMBER 2019 DATA

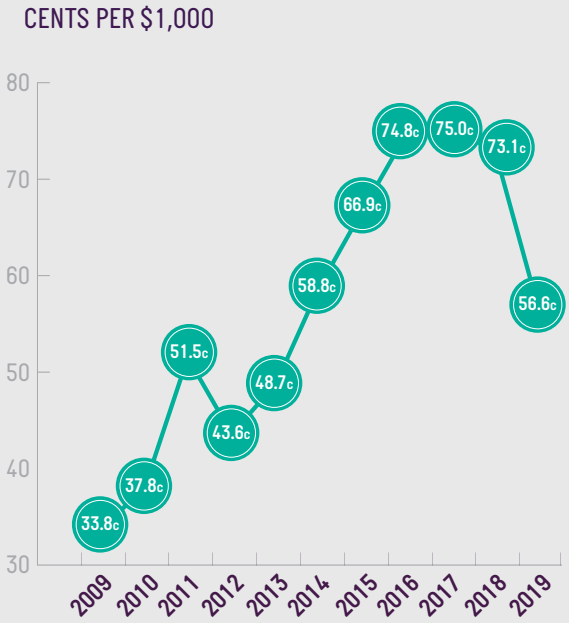
Snapshot

THE TOTAL VALUE OF CARD PAYMENTS **CONTINUED TO GROW IN 2019**



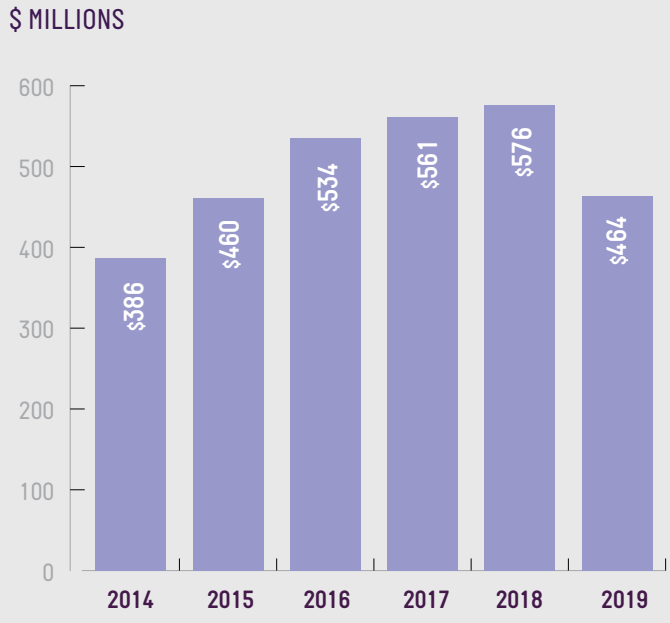
Source: Reserve Bank of Australia

THE CARD FRAUD RATE **DECLINED FOR THE SECOND YEAR IN A ROW**, AND IS NOW BELOW THAT LAST SEEN IN 2014



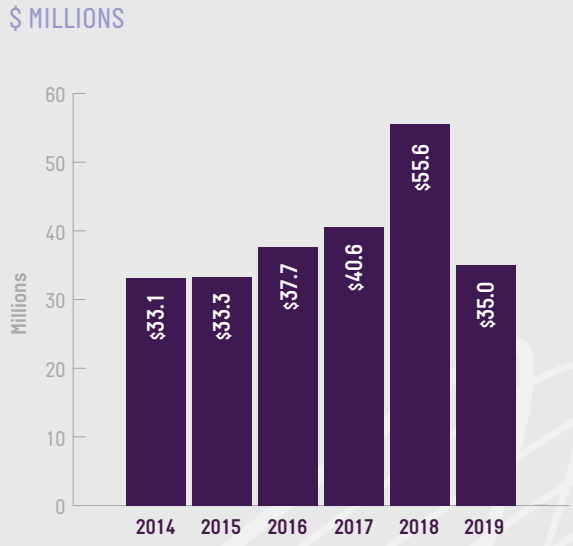
Source: Reserve Bank of Australia and AusPayNet

THE TOTAL VALUE OF CARD FRAUD **FELL STRONGLY**, DOWN BY NEARLY 20%



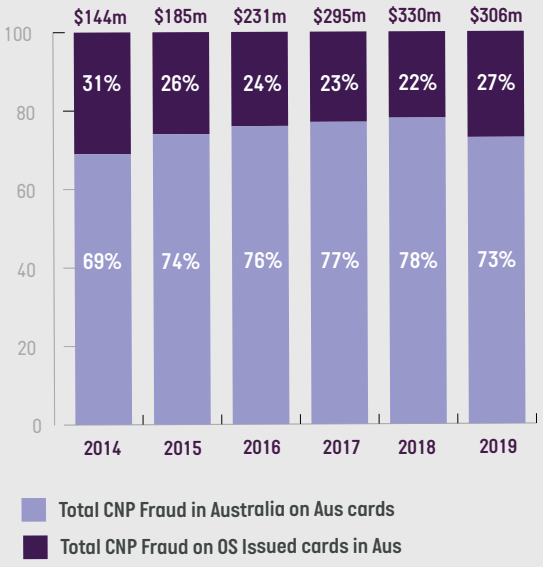
Source: AusPayNet

FRAUD ON LOST/STOLEN CARDS **FELL BY 37%**



Source: AusPayNet

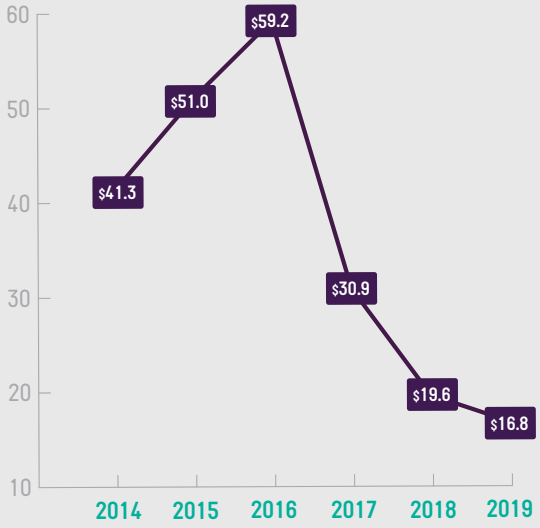
CARD-NOT-PRESENT FRAUD AT AUSTRALIAN ONLINE MERCHANTS, **HAS DECLINED FOR THE FIRST TIME**



Source: AusPayNet

COUNTERFEIT/SKIMMING FRAUD DROPPED TO ANOTHER **RECORD LOW**

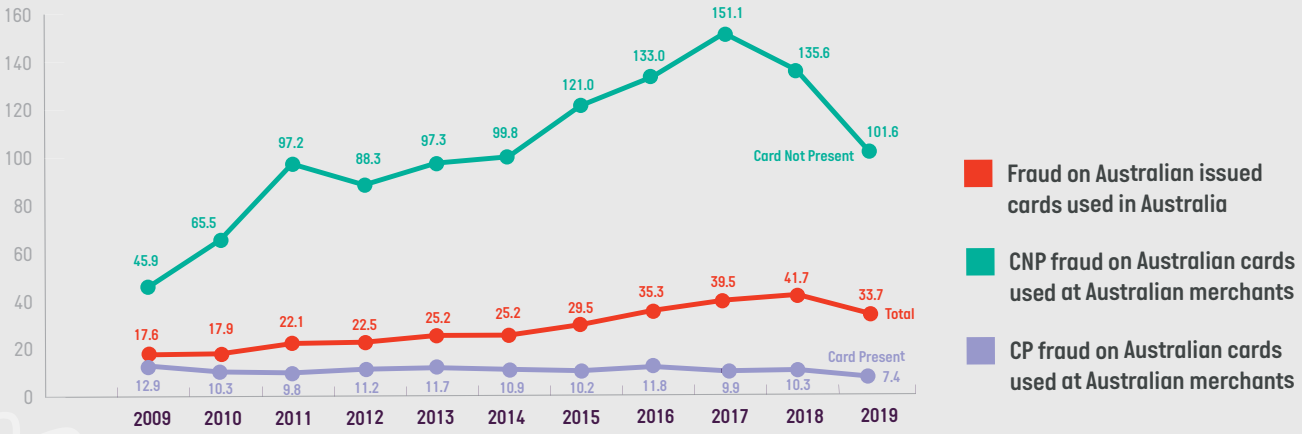
$ MILLIONS



Source: AusPayNet

FRAUD RATES ARE TRENDING DOWN AND REMAIN ESPECIALLY LOW FOR IN-PERSON CARD PAYMENTS WITHIN AUSTRALIA

CENTS PER $1,000



Source: Reserve Bank of Australia and AusPayNet

Payment Fraud

FRAUD ON AUSTRALIAN CARDS FELL BY DOUBLE DIGITS IN 2019 WHILE THE OVERALL SPEND ON CARDS REACHED A NEW RECORD HIGH

Fraud on Australian cards fell by double digits in 2019 while the overall spend on cards reached a new record high.

Consumers spent more than $819 billion on cards – up 3.9% on the previous year. Alongside this growth, card fraud fell by almost 20% to $464 million. This translates to a fraud rate of 56.6¢ per $1,000 spent, a significant drop from 73.1¢ per $1,000 in 2018 and 75.1¢ per $1,000 in 2017. The fraud rate on Australian cards is now back to the level last seen in 2014.

Card-not present (CNP) fraud continues to account for the vast majority of payments fraud. CNP fraud occurs when valid card details are stolen and used to make purchases or other payments without the card, usually online.

Online shopping and in-app purchases are increasingly popular. CNP transactions in Australia grew by 16% in 2019 to $220 billion. Over the same period, CNP fraud on Australian cards dropped by almost 18% to $403 million. The industry is committed to tackling CNP fraud, which accounts for 87% of all card fraud, and remains vigilant as e-commerce volumes increase during the COVID-19 pandemic.

In July 2019, AusPayNet launched the CNP Fraud Mitigation Framework, a whole-of-industry approach to tackling fraud, and a key step in further stimulating the uptake of secure technologies such as real-time monitoring, machine learning, tokenisation and strong customer authentication.

Building on this work, industry is now expanding its focus to address other areas such as identity fraud and push payment scams. Data relating to scams is covered in the "Spotlight" section of this report.

Preventing payment fraud continues to require coordination at every level, from financial institutions and card schemes through to merchants and consumers. The following sections provide further information on card fraud trends, as well as measures that consumers and businesses can take to mitigate risk.

Australian payments industry actions to further combat fraud

Committed to combatting all types of fraud, AusPayNet is leading industry wide initiatives designed to improve the security and convenience of payments. Two initiatives in particular are focus on the online environment.

CNP FRAUD MITIGATION FRAMEWORK

The industry CNP Fraud Mitigation Framework took effect on 1 July 2019. The Framework, developed through significant industry engagement and collaboration, embodies the eCommerce community's common goal of reducing CNP fraud while ensuring that remote transactions continue to grow. Key elements include the setting of targets for card issuers to reduce CNP fraud, and the implementation of strong customer authentication for merchants who exceed the set fraud threshold for more than two consecutive quarters. To date, of the merchants who have exceeded the fraud threshold, some 66% brought their fraud back below the threshold in the following quarter. The remaining third, mostly with complex payment ecosystems and in higher-fraud market segments, are working closely with acquirers to reduce fraud. These efforts are having an impact on reducing CNP fraud, however, the e-commerce community needs to remain vigilant as volumes increase during the COVID pandemic. The full benefits of the Framework are expected to be realised in coming years.

TRUSTID FRAMEWORK VERSION 1.0

A successful digital economy demands convenient, secure and privacy-enhancing ways for people and businesses to build trust online. The payments industry is at the forefront of the digital economy and in reviewing its responsibility to engender confidence in the payments system, the Australian Payments Council (APC) led the creation of the Trust ID framework .

The Trust ID framework is not a digital identification solution in and of itself; it comprises a series of rules and guidelines for organisations to adhere to in their design, build and operation of products and services. These rules and guidelines are intended to improve the efficiency, security, privacy and convenience of online service delivery. Participation in the framework is open to all parties that meet the accreditation requirements.

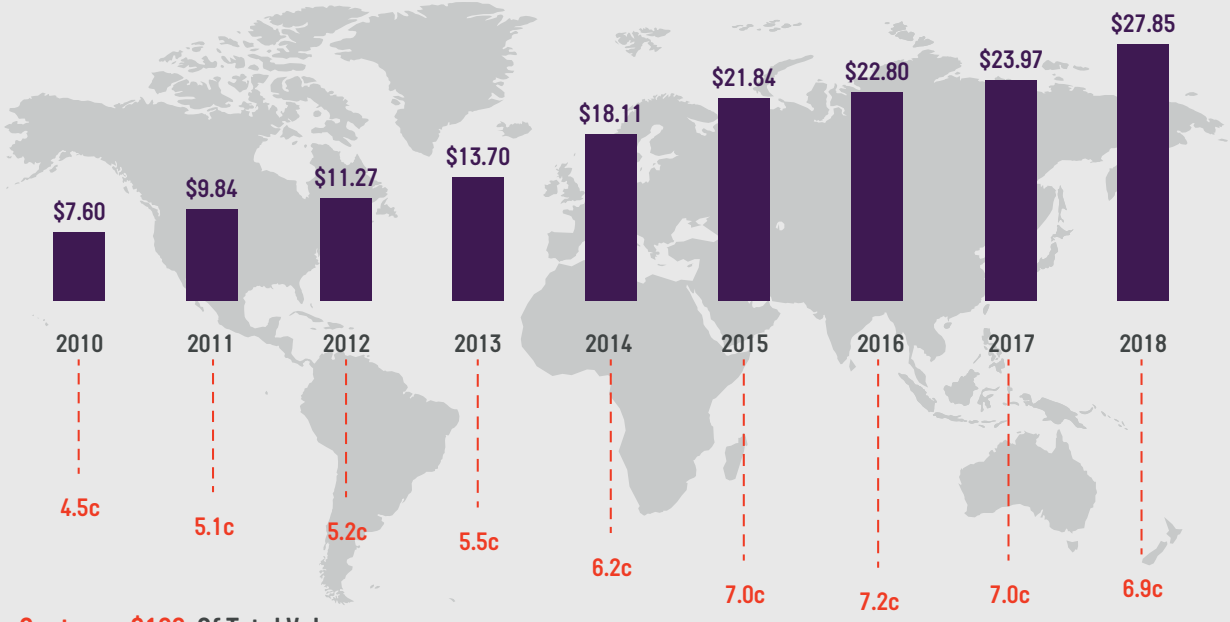
The framework has the potential to benefit many industries, including health, energy, telecommunications, and financial services with applications ranging from authentication (to access a service) to digital signature of contracts. Moreover, it is anticipated that services offered under the framework will help reduce the duplicative costs of AML/CTF (Know Your Customer) processes and help to address the growing problem of identity theft.

AusPayNet is currently managing three work streams designed to support the operation of services under the framework: a governance structure for the framework, accreditation, and a trust mark. A range of service providers are participating in these work streams, from financial institutions to technology providers.

How does Australia compare?

Fraud rates are the most common measure used by the industry to monitor movement in fraud activity. Recently published 2018 fraud data of comparable geographic markets show that Australia's prevention initiatives are proving effective.

Global Fraud Losses on Cards in USD Billions: 2010-2018



Cents per $100: Of Total Value

Source: The Nilson Report November 2019

2018	Australia	UK	Germany	France	USA
CNP Fraud (% of CNP spend)	0.171%	0.131%	-	0.173%	-
All Card Fraud (% of all card spend)	0.073%	0.084%	0.029% Predominantly a debit market	0.062%	0.108%
2019	**Australia**	**UK**			
All Card Fraud (% of all card spend)	0.057%	0.075%			
Card Fraud as % of all payment fraud	92%	75%			
CNP Fraud as % of all card fraud	87%	76%			

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:

- 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
- Fraud detection systems to track customer card activity and identify unusual spending patterns
- Self-service systems allowing cardholders to remotely lock their card or place limits on transactions
- Card activation processes to ensure the recipient of a new card is the account holder.

Additionally, consumers are advised to regularly check their account statements and report any unusual transactions to their financial institution immediately. The measures below are also offered as practical guidance for preventing card fraud.

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 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 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 don't 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.

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.

Remote Payments – Card-Not-Present

AUTHENTICATION TOOLS

Register for & 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.

Many mobile wallets offer biometric support such as thumbprint or facial recognition, which improves both convenience and security.

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.

BE ALERT TO PHISHING ATTACKS

Don't be tricked into giving fraudsters access to your personal or financial information. Be cautious when clicking on hyperlinks in emails 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.

How merchants can reduce fraud risk

Financial institutions, epayment gateways, cyber and fraud management services and other payment service providers offer a range of solutions to mitigate payment fraud. Merchants should discuss mechanisms to secure their businesses directly with their service providers, to ensure the relevant solutions are tailored to their business needs.

Face-to-face - Card Present

EMV CHIP TECHNOLOGY

The global shift to EMV 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 a 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 to the same card that was used to make the original purchase. Requesting a refund to a different card is a common fraudster tactic.

Remote Payments – Card-Not-Present

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCIDSS)

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

Compliance with PCIDSS can be significant and online merchants may wish to investigate the use of hosted solutions provided by a PCIDSS compliant service provider to reduce the scope of their PCIDSS 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, 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.

INVEST IN TOKENISATION

Merchants holding sensitive payment information can become targets for the theft of card data. Tokenisation replaces the payment credential with a unique digital identifier (a token). This means that even if there is a data compromise of merchant 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 tools selectively and apply rules to different transactions, based on for example transaction value, product purchased and shipping destination. Rules can be set on card issuing country, so that you can choose to evaluate overseas card transactions more thoroughly.

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

Over $819 billion was transacted on Australian cards in 2019, an increase of 3.9% on the prior year. Fraud accounted for 0.057% of that total, down from 0.073% in 2018. The value of fraud dropped by 19% to $464 million – the first annual decline ever. The average value of fraud transactions was $123, down 44.8% on the 2014 peak.

	2014	2015	2016	2017	2018	2019
Value ($ millions):						
All card transactions*	$657,208	$688,700	$714,493	$748,111	$788,647	$819,157
Fraudulent transactions	$386	$461	$535	$561	$576	$464
Fraud rate (cents per $1,000):	**58.8**	**66.9**	**74.8**	**75.0**	**73.1**	**56.6**
Number:						
All card transactions*	6,670m	7,292m	8,051m	8,965m	9,988m	11,010m
Fraudulent transactions	1,733,821	2,191,082	2,848,033	3,581,001	4,369,431	3,785,118
Fraud rate (as % of total no. of card transactions)	**0.026%**	**0.030%**	**0.035%**	**0.040%**	**0.044%**	**0.034%**
Average value of fraudulent transactions	$223	$210	$188	$157	$132	$123

*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 2019, the three most prevalent types of card fraud all declined by double-digits.

Fraud value ($m)	2014	2015	2016	2017	2018	2019
Card-not-present	$300.0	$363.1	$418.1	$476.1	$489.0	$402.6
Counterfeit / skimming	$41.3	$51.0	$59.2	$30.9	$19.6	$16.8
Lost / stolen	$33.1	$33.3	$37.7	$40.6	$55.6	$35.0
Never received	$8.6	$9.1	$10.3	$7.9	$6.1	$2.9
Fraudulent application	$1.2	$1.3	$3.7	$3.3	$2.3	$2.4
Other	$2.3	$3.1	$5.5	$2.5	$3.5	$4.2
TOTAL	**$386.5**	**$460.9**	**$534.7**	**$561.3**	**$576.2**	**$464.0**

TRENDS

Card-Not-Present (CNP) fraud dropped strongly in 2019, down by 18% to $402.6 million. This is likely due to increased awareness of on-line fraud as part of the CNP Fraud Mitigation Framework implemented on 1 July 2019. CNP fraud accounts for 87% 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 - EMV chip is already used in many countries and the roll-out across the globe continues. 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 third year in a row, down to $16.8 million in 2019 – a 72% drop from a peak of $59.2 million in 2016. This type of fraud now represents 3.6% of all fraud on Australian cards.

As chip technology and enhanced detection tools make fraud more difficult, criminals typically revert to simpler, more opportunistic methods. This has been reflected in a steady increase in fraud on lost and stolen cards since 2014, however, the trend appears to be changing. Lost and stolen card fraud dropped by 37% to $35.0 million in 2019.

Australian Cards

FRAUD PERPETRATED IN AUSTRALIA

Fraud perpetrated within Australia on Australian issued cards fell by 16% in 2019, to $266.4 million. Card-Not-Present (CNP) fraud, primarily occurring online, reduced by 13%, to $224.0 million at Australian merchants. Fraud through the use of contactless or Tap'n'Go cards (with no PIN required) is not collected separately, but captured in the Lost /Stolen and Never Received categories. Fraud values in both these categories declined in 2019, with Lost/Stolen card fraud dropping 36% to $23.5 million.

Fraud ($m)	2014	2015	2016	2017	2018	2019
Card-not-present	$99.1	$136.8	$175.8	$227.4	$258.6	$224.0
Counterfeit / skimming	$25.4	$22.9	$25.8	$16.5	$11.5	$10.5
Lost / stolen	$19.8	$20.5	$23.8	$27.2	$36.9	$23.5
Never received	$8.0	$8.5	$9.7	$7.6	$5.7	$2.8
Fraudulent application	$1.0	$0.8	$2.4	$2.8	$1.9	$1.9
Other	$2.0	$2.3	$3.3	$1.9	$2.9	$3.5
TOTAL	$155.4	$191.7	$240.9	$283.4	$317.4	$266.4

FRAUD PERPETRATED OVERSEAS

Fraud on Australian cards when used overseas fell by 24% in 2019 to $197.7 million. CNP fraud at overseas websites dropped by 23% to $178.6 million. This type of fraud represents over 90% of the total fraud perpetrated overseas on Australia cards.

Fraud ($m)	2014	2015	2016	2017	2018	2019
Card-not-present	$200.9	$226.3	$242.3	$248.7	$230.5	$178.6
Counterfeit / skimming	$15.9	$28.1	$33.5	$14.4	$8.1	$6.3
Lost / stolen	$13.3	$12.8	$13.9	$13.4	$18.8	$11.5
Never received	$0.5	$0.6	$0.6	$0.3	$0.4	$0.1
Fraudulent application	$0.2	$0.5	$1.3	$0.5	$0.4	$0.5
Other	$0.3	$0.8	$2.2	$0.6	$0.6	$0.7
TOTAL	$231.0	$269.2	$293.8	$277.9	$258.8	$197.7

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. Fraud perpetrated in Australia using cards issued overseas increased by 16% to $95.4 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)	2014	2015	2016	2017	2018	2019
Card-not-present	$44.8	$47.9	$55.0	$67.3	$71.5	$82.4
Counterfeit / skimming	$9.3	$8.0	$8.8	$7.6	$5.8	$7.3
Lost / stolen	$2.8	$3.0	$2.8	$3.4	$3.3	$4.5
Never received	$0.0	$0.1	$0.1	$0.1	$0.1	$0.2
Fraudulent application	$0.1	$0.1	$0.1	$0.1	$0.1	$0.1
Other	$0.5	$0.6	$0.9	$0.8	$1.4	$0.9
TOTAL	$57.4	$59.6	$67.7	$79.4	$82.3	$95.4

Spotlight on Scams

While card fraud has dropped in 2019, losses through scams have risen sharply. Moreover, many scams go unreported often because victims are embarrassed.

Scams and payments fraud – recognising the difference

Payments fraud is commonly defined as an unauthorised payment made from an account without the permission of the account holder.

A **payments scam** occurs 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. Both are payment scams; the first is authorised by the account holder, who believes payment is being made to a legitimate person or company, whereas the latter payment is authorised by the scammer without the account holder's permission.

Definitions – an inexact science

Table 1 below from ACCC Scamwatch[1] shows the top 10 types of scam reported by scam victims during 2019. Phishing and identity theft are in the top 3; these scams enable the scammer to obtain information to impersonate the account holder. During 2019, 11.8% of reported scams resulted in actual financial loss.

Table 1

Top 10 scams by reports

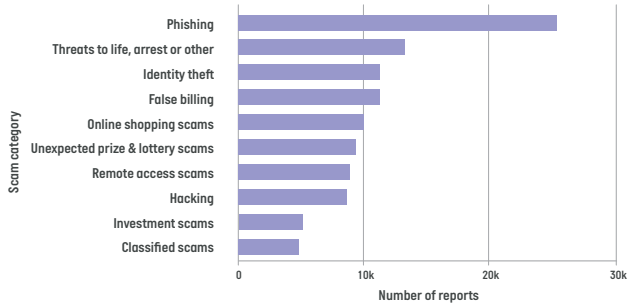
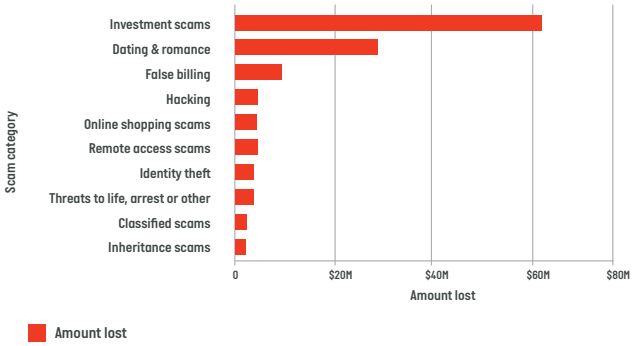


Table 2

Top 10 scams by amount lost



Scams – by numbers

The ACCC Scamwatch service publishes financial loss data for reported scams. The data shows that losses increased by 34% in 2019 to $143 million.

Of the cases reported to the ACCC over the last 3 years:

- the proportion of scams which have involved financial loss has increased by 51%
- the average loss in each incident has increased by 15%, from $6,462 to $7,449
- the total reported loss has increased by ~60% from $90.8m in 2017 to $143 million in 2019

Consumers and businesses also report scams to financial institutions and other entities as shown over the page.
In 2019, their combined reported scam losses amounted to $634 million.

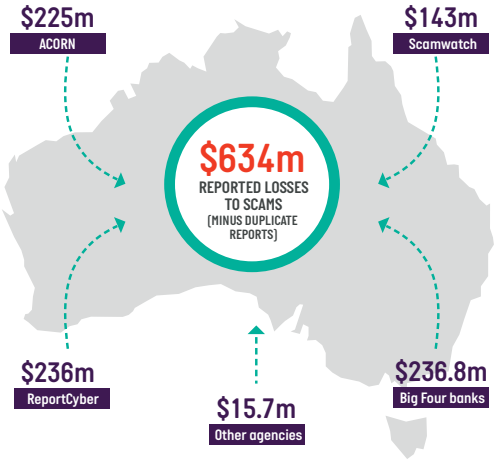
[1] https://www.scamwatch.gov.au/scam-statistics?scamid=all&date=2019

Is Australia unique?

Scams are a growing global problem with many methods used across multiple jurisdictions. In the UK, the value of scam losses rose by 29% in 2019 compared to the previous year, with reported cases up 45% over the same period.[2]

The table to the right shows the scam activity experienced in the USA in 2019, where the losses increased by 28%.[3] The top method for scammers contacting consumers was via phone[4]; in Australia, the most common contact method is email, but scams via phone result in the most financial loss.

In New Zealand, while the value of scam related losses remained unchanged in 2019, the number of scams resulting in financial loss almost doubled on the previous year.[5]

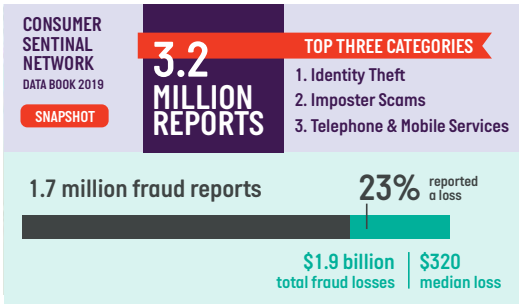


Source: ACCC

What the future may hold

Scammers are becoming increasingly sophisticated as they look for new opportunities.

Table 3 shows that in the UK, where requirements for strong customer authentication are in force for card-not-present fraud, "Authorised Push Payments" or scams comprise 36% of total financial fraud losses. This may be an indicator of the likely changing fraud trends in Australia.[6]



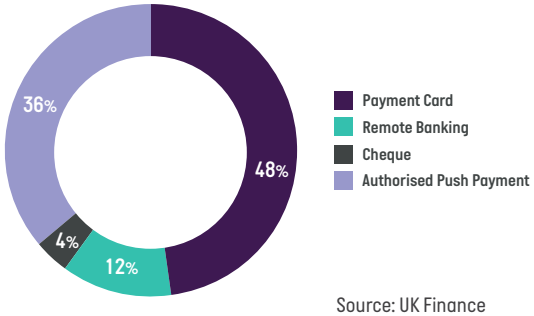
The action plan: Education, Awareness, Tracking

Governments and financial institutions are educating consumers and businesses on the types of scams and the circumstances scammers are exploiting to trick account holders. Financial institutions are working to identify account takeovers (where a scammer gains unauthorised access to an online banking account) and shut down accounts in fake names.

As the shift to digital payments accelerates, consumers and businesses need to be wary of unsolicited contact online especially if it includes a proposition that involves payment, and immediately report any suspicious activity to their financial institution.

Table 3

Total 2019 financial fraud losses by type



Source: UK Finance

[2] https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-14-May.pdf
[3] https://www.consumer.ftc.gov/blog/2019/02/top-frauds-2018
[4] https://www.usa.gov/common-scams-frauds
[5] https://www.netsafe.org.nz annual reports 2017-2018 and 2018-2019
[6] https://www.scamwatch.gov.au/scam-statistics?scamid=all&date=2020

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 34% to $544 billion in 2019. Fraud losses on cheques remain low, both in absolute dollars at $4.8 million and in fraud rate at 0.9¢ per $1,000 transacted, although the fraud rate lifted significantly in 2019 from the prior two year level of 0.5¢.

	2014	2015	2016	2017	2018	2019
Value ($ millions):						
Cheque transactions*	$1,228,513	$1,228,426	$1,154,864	$1,110,711	$824,209	$544,054
Fraudulent transactions	$6.5	$8.4	$6.4	$5.9	$4.4	$4.8
Fraud rate (cents per $1,000):	**0.5**	**0.7**	**0.6**	**0.5**	**0.5**	**0.9**
Number:						
Cheque transactions*	167m	140m	112m	90m	70m	55m
Fraudulent transactions	1,029	1,160	904	727	591	680
Fraud rate (as % total no. of transactions)	0.0006%	0.0008%	0.0008%	0.0008%	0.0008%	0.0012%
AVERAGE VALUE OF FRAUDULENT TRANSACTIONS	**$6,294**	**$7,232**	**$7,087**	**$8,123**	**$7,402**	**$7,106**

*Source: Reserve Bank of Australia

Fraud ($m)	2014	2015	2016	2017	2018	2019
On us fraud:						
Breach of mandate	$0.4	$0.3	$0.9	$0.4	$0.4	$0.0
Fraudulently altered	$1.7	$3.6	$2.1	$2.4	$1.2	$1.5
Stolen blank cheque / book	$1.7	$1.8	$2.2	$2.3	$1.5	$1.9
Originated counterfeit cheques	$1.1	$1.2	$0.4	$0.3	$0.2	$0.4
Non originated counterfeit cheques	$0.6	$0.7	$0.6	$0.3	$0.1	$0.6
Valueless	$0.9	$0.7	$0.0	$0.0	$0.3	$0.0
ON-US TOTAL	**$6.3**	**$8.2**	**$6.2**	**$5.7**	**$3.7**	**$4.4**
Deposit Fraud	$0.2	$0.2	$0.2	$0.2	$0.6	$0.4
TOTAL ALL CHEQUES FRAUD	**$6.5**	**$8.4**	**$6.4**	**$5.9**	**$4.4**	**$4.8**

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

Glossary

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.

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 unauthorized 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 130 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