Australian Payments Network
Connect Inspire Thrive

AUSTRALIAN PAYMENT CARD FRAUD 2019

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

SNAPSHOT

Fraud is growing at a slower rate than overall spending on Australian cards. In 2018, card transactions grew by 5.4% to $788.6 billion; fraud was up 2.3% to $574.3 million.

COMBATTING FRAUD

The industry is committed to tackling fraud. Initiatives include the CNP Fraud Mitigation Framework, and fraud identification and prevention tools for merchants.

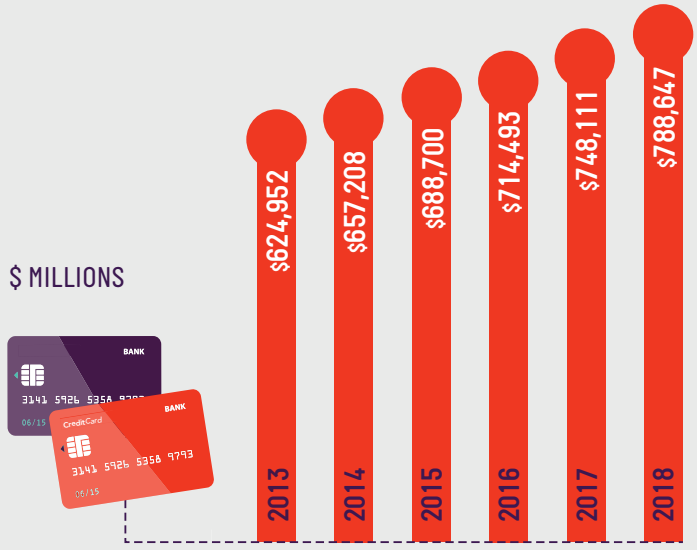
DATA AND TRENDS

Counterfeit/skimming fraud fell by 36.8% to a record low $19.5 million. This fact-base provides details and figures of fraud on Australian cards from 2013 to 2018.

JANUARY – DECEMBER 2018 DATA

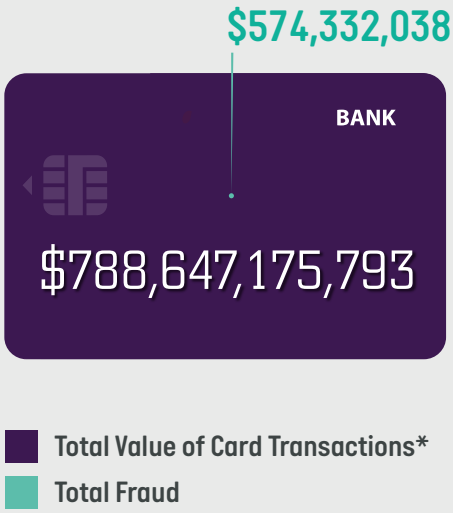
Snapshot

CARD USE CONTINUES TO GROW, WITH THE TOTAL VALUE OF TRANSACTIONS FOR THIS REPORTING PERIOD EXCEEDING PREVIOUS YEARS



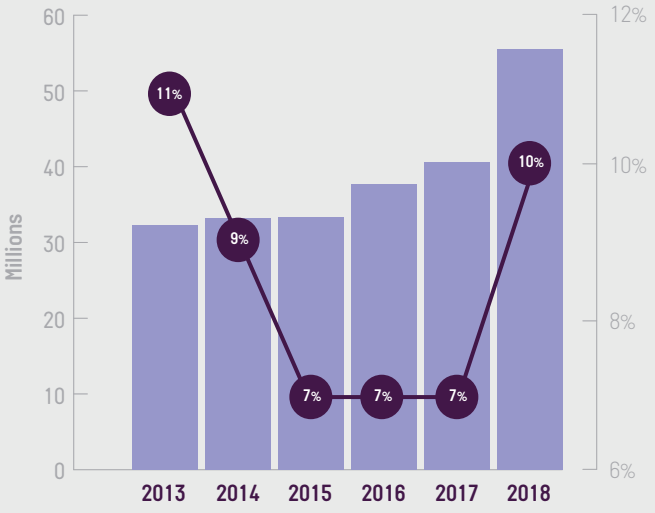
Source: Reserve Bank of Australia

FRAUD ($574 MLLION) AS A PERCENTAGE OF ALL TRANSACTIONS ($788 BILLION) IS LESS THAN 0.1%

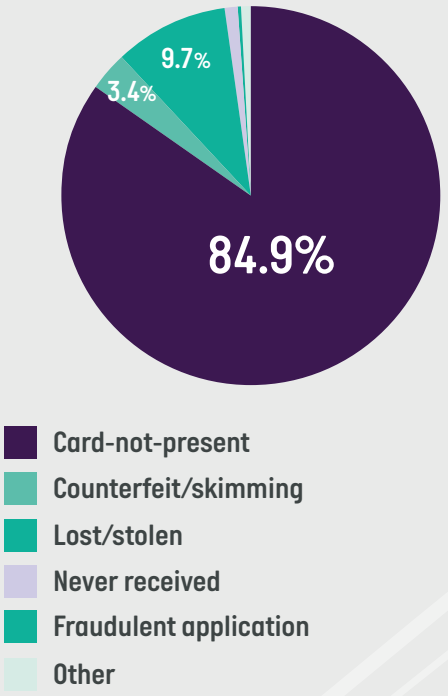


Source: Reserve Bank of Australia

LOST AND STOLEN FRAUD HAS INCREASED AND NOW REPRESENTS SOME 10% OF ALL CARD FRAUD

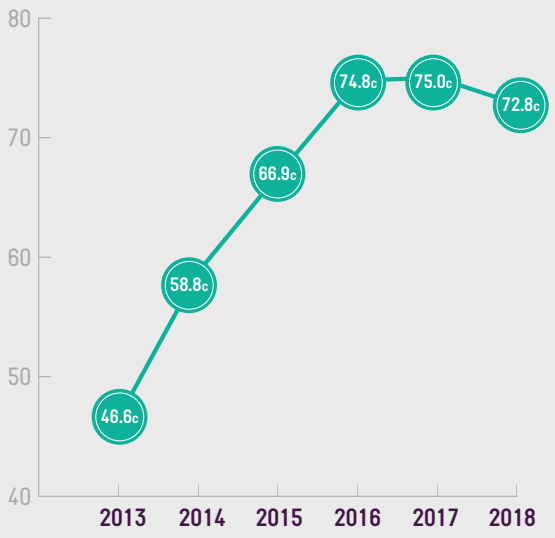


CARD-NOT-PRESENT FRAUD IS THE MOST PREVALENT TYPE OF FRAUD ON AUSTRALIAN CARDS



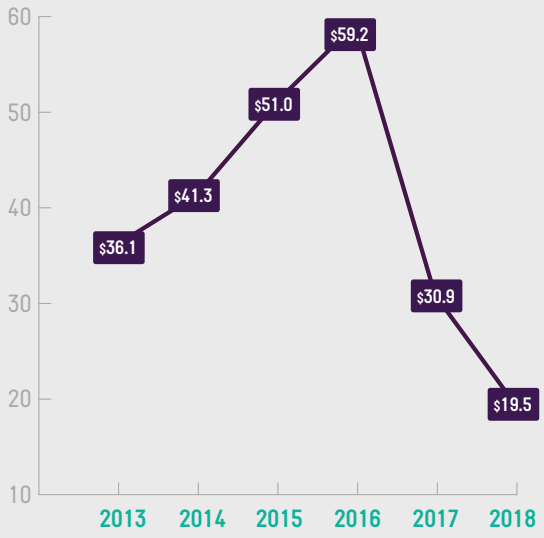
THE RATE OF FRAUD ON CARDS IS **DECLINING** FOR THE FIRST TIME EVER

FRAUD RATES - CENTS PER $1,000

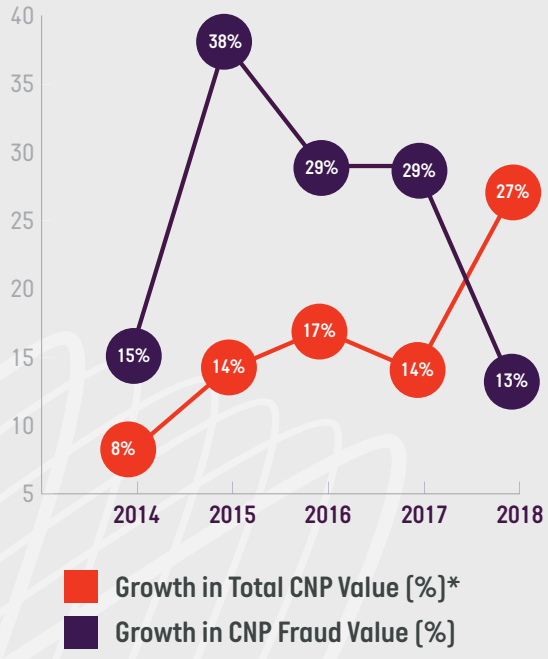


THE VALUE OF COUNTERFEIT/SKIMMING FRAUD CONTINUES TO **FALL TO RECORD LOWS**

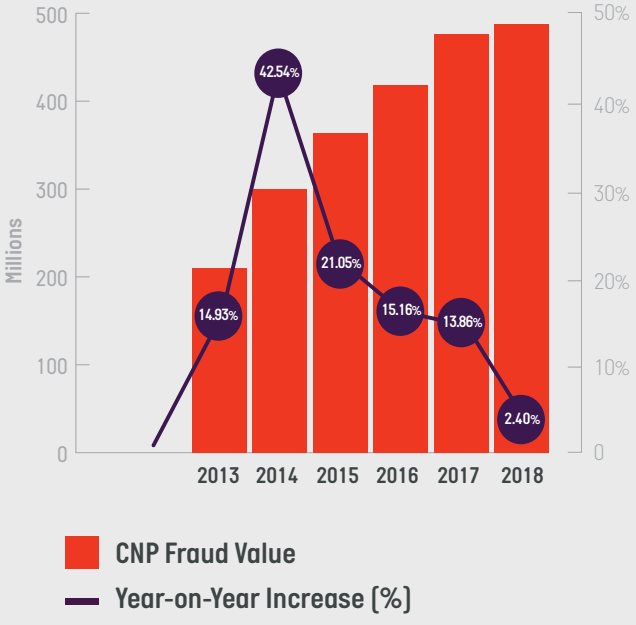
VALUE ($ MILLIONS)



THE **GROWTH IN CARD-NOT-PRESENT TRANSACTIONS** IN AUSTRALIA IS OUT STRIPPING THE RATE OF CNP FRAUD



CARD-NOT-PRESENT FRAUD IS GROWING, BUT THE RATE OF INCREASE HAS DECLINED TO **2.4% IN 2018**



Source: Reserve Bank of Australia

Australian industry initiatives to combat CNP fraud

Notwithstanding the positive trend in 2018, which indicates a decline in the growth rate of card-not-present (CNP) fraud, tackling fraud in this channel remains a priority for the payments industry. Continued industry collaboration is required, and to this end, both Australian Payments Network and the Australian Payments Council are leading industry wide initiatives. These initiatives address different aspects of card fraud and are designed to improve the security and convenience of online payments.

AUSPAYNET CNP FRAUD MITIGATION FRAMEWORK

The industry CNP Fraud Mitigation Framework took effect on 1 July 2019. The Framework is the culmination of 18 months of deep industry engagement and collaboration, embodying the e-commerce community's common goal of reducing CNP fraud while ensuring that remote transactions continue to grow.

The Framework defines the minimum requirement for an issuer and merchant (or acquirer or payment gateway) to authenticate CNP transactions, and mandates Strong Customer Authentication (SCA) for those issuers and merchants whose fraud rate is consistently in breach of agreed industry thresholds. These thresholds were collaboratively set to ensure a targeted approach to minimising fraud, while also minimising the impact on smaller merchants.

Combining this approach with a comprehensive communications strategy and phased lead times for implementation, the Framework provides a clear runway to readiness for the wider payments community for reducing CNP fraud.

THE AUSTRALIAN PAYMENTS COUNCIL - CYBER SECURITY

Data breaches, resulting from cyber attacks, are a known cause of fraudulent use of card holder data.

In order to improve cyber attack prevention and detection, the Australian Payments Council (APC) is working collaboratively with the Joint Cyber-Security Centre to identify ways in which the industry and Government can share actionable information on cyber-security.

Moreover, the focus on combatting financial crime is reflected in the APC's 2019 Strategic Agenda, *Payments in a Global, Digital World*. The agenda is outcome focused and outlines a two-pronged approach to combatting financial crime based on:

- Prevention and detection; and
- Customer protection

The APC's work will include auditing current national and international initiatives, distilling best practice from other jurisdictions and recommending collaborative action to prevent financial crime and ensure there are appropriate mechanisms to protect customers.

TRUSTID FRAMEWORK VERSION 1.0

The continued shift towards a digital economy means that both private and public sector entities are focused on improving online service delivery. This shift in turn increases the demand for better ways for individuals and organisations to identify themselves online.

In response to this demand, the APC led the development of the TrustID framework. TrustID aims to improve the security, privacy and convenience of online interactions which will lead to reduced fraud.

TrustID is an open, contestable framework; it establishes a set of principles as well as functional, operational and legal standards that guide the behaviour of participants in the framework.

TrustID is intended to stimulate market competition, provide choice to customers and solve the identity fragmentation that creates customer friction and security vulnerabilities.

The TrustID framework will be available through the AusPayNet and APC websites.

Global collaboration and alignment to reduce fraud

Online payments continue to account for a growing portion of retail sales and improving the security of this channel is a key focus for global bodies. The FIDO Alliance, EMVCo, and the World Wide Web Consortium (W3C) recently announced the creation of the Web Payment Security Interest Group. The group will "define areas of collaboration and identify gaps between existing technical specifications in order to increase compatibility among different technologies." [2]

EMVCO

EMVCo is a global technical body that develops specifications to facilitate the worldwide interoperability and acceptance of payment transactions.

Card Present Initiatives

The EMV Chip Specifications are global payment industry specifications for interoperability between chip-based payment applications. The specifications, managed by EMVCo, encompass both contact and contactless payments. They are designed to improve security for face-to-face payment transactions. In 2018, EMVCo reported that 73.6% of card transactions globally were EMV chip technology enabled, an increase from 63.7% in 2017.[3]

Card-Not-Present Initiatives

In 2018, EMVCo delivered a number of initiatives to improve ease of use and security for payments conducted using a device or online via a web browser. Key initiatives include:

- The Secure Remote Commerce (SRC) draft specification. SRC enables consumers to use their payment cards across browsers and devices more securely and easily.
- 3D Secure test platform to assist with the rollout of 3DS2.0 infrastructure across Australia. The 3D Secure protocol enables consumers to authenticate themselves to their card issuer during remote purchases.

EMVCo also published A guide for Payment Tokenisation Use Cases. Payment Tokenisation is the process of replacing the 16-digit Personal Account Number on a card with a unique digital identifier (a token).

W3C

W3C is an international community with a remit to develop Web standards.

W3C has established a Web Payments Working Group to develop protocols for handling remote payments.

In particular, the Payments Working Group is focused on improving the customer experience, enhancing security and trust, and lowering integration costs.

AusPayNet closely follows W3C developments, with the goal of ensuring national practices are aligned.

THE FIDO ALLIANCE

The FIDO (Fast IDentity Online) Alliance, formed in July 2012, is an industry association that creates open standards for authentication practices beyond passwords.

FIDO supports authentication practices that provide a simple user experience and are easy for service providers to deploy and manage.

AusPayNet is a Liaison Partner of the FIDO Alliance.

[2] https://www.w3.org/securepay/
[3] https://www.emvco.com/about/deployment-statistics/

Fraud prevention Consumers

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

Financial institutions have invested in technology and introduced a number of measures to manage 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
- Card activation processes to ensure the recipient of a new card is the account holder

Additionally, consumers are advised to regularly check 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 their card like their cash, keeping it safe at all times.

To protect against mail theft, cardholders should:

- Install a lockable mailbox
- Clear mail daily
- During extended periods of absence, have mail held at the post office or collected by a friend

PROTECT AGAINST SKIMMING

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

Cardholders are encouraged to always keep their card in sight when making a payment.

PROTECT YOUR PIN

Consumers should keep their PIN secret and always use their hand to cover their PIN entry 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.

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.

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.

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.

More information on Online Shopping Scams is available at ScamWatch.

BE ALERT TO PHISHING ATTACKS

Be cautious when clicking on hyperlinks in emails sent by an unknown contact.

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

More information on Phishing Scams is available at ScamWatch.

Fraud prevention Merchants

Financial institutions, gateways and other payment service providers offer a range of solutions to mitigate card fraud. Merchants should discuss mechanisms to secure their business directly with their service provider to ensure the 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 and PIN has been mandated in Australia at point-of-sale since 2014.

Merchants should encourage cardholders to insert chip cards for contact transactions or tap cards for contactless transactions.

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.

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 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 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) tools should be used for transactions identified as higher risk, to ensure the person requesting the transaction is authorised.

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.

INVEST IN TOKENISATION

Merchants holding sensitive account holder information can become targets for the theft of card data. Tokenisation replaces this information with a unique digital identifier (a token). This means that even if there is a data compromise of merchant systems, the information cannot be misused.

The card schemes 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.

MAIL ORDER/TELEPHONE ORDER (MOTO) TRANSACTIONS

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 card holder.

Merchants should be cautious processing MOTO transactions, especially where unusually large items, or multiple duplicate orders for the same item are concerned.

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 card. Financial institutions report card fraud data as gross actual losses.

All Australian Cards

Data in the tables below provide an overview of all transactions on Australian-issued cards[4]:

- Scheme credit, debit and charge cards: operated by MasterCard, Visa, American Express, and Diners.
- Proprietary debit cards: operated by eftpos Payments Australia

OVERVIEW OF TRENDS ON AUSTRALIAN ISSUED CARDS

More than $788.6 billion was transacted on Australian cards in 2018 – up 5% on 2017. Fraud accounted for 0.073% of that total, increasing by 2.3% to $574.3 million. The average value of a fraudulent transaction decreased from $157 in 2017 to $132 in 2018.

	2013	2014	2015	2016	2017	2018
Value ($ millions):						
All card transactions*	$624,952	$657,208	$688,700	$714,493	$748,111	$788,647
Fraudulent transactions	$291	$386	$461	$535	$561	$574
Fraud rate (cents per $1,000):	**46.6**	**58.8**	**66.9**	**74.8**	**75.0**	**72.8**
Number:						
All card transactions*	6,141m	6,670m	7,292m	8,051m	8,965m	9,988m
Fraudulent transactions	1,415,487	1,733,821	2,191,082	2,848,033	3,581,001	4,345,243
Fraud rate (as % of total no. of card transactions)	**0.023%**	**0.026%**	**0.030%**	**0.035%**	**0.040%**	**0.044%**
Average value of fraudulent transactions	$206	$223	$210	$188	$157	$132

*Source: Reserve Bank of Australia

TYPES OF FRAUD OCCURRING ON AUSTRALIAN CARDS

Fraud value ($m)	2013	2014	2015	2016	2017	2018
Card-not-present	$210.4	$300.0	$363.1	$418.1	$476.1	$487.5
Counterfeit / skimming	$36.1	$41.3	$51.0	$59.2	$30.9	$19.5
Lost / stolen	$32.3	$33.1	$33.3	$37.7	$40.6	$55.5
Never received	$9.1	$8.6	$9.1	$10.3	$7.9	$6.1
Fraudulent application	$1.5	$1.2	$1.3	$3.7	$3.3	$2.2
Other	$2.0	$2.3	$3.1	$5.5	$2.5	$3.5
TOTAL	**$291.4**	**$386.5**	**$460.9**	**$534.7**	**$561.3**	**$574.3**

[4] Some figures have been revised since earlier publication. Full details are available on www.auspaynet.com.au.
Where totals do not add up, the diference is due to rounding.

TRENDS

Card-not-present (CNP) fraud accounts for 84.9% of all fraud perpetrated on Australian-issued cards, reflecting a global trend of growing online card fraud and cybercrime in general. The key reasons for this trend 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.

The e-commerce community is committed to combatting CNP fraud. While CNP fraud is continuing to rise, the rate of increase has slowed, reflecting the progressive uptake of prevention measures.

Chip technology is providing strong protection against card fraud in face-to-face environments. Counterfeit/skimming fraud fell to a record low for the second year in a row, down to $19.5 million in 2018 – a 67% drop from $59.3 million in 2016. This type of fraud now represents 3.4% of all fraud on Australian cards.

As chip technology and enhanced detection tools make fraud more difficult, criminals are reverting to simpler, more opportunistic methods. In 2018, fraud on lost and stolen cards increased to $55.5 million from $40.6m in 2017, representing 10% of all fraud on Australian cards. Close cooperation between financial institutions and law enforcement through AusPayNet's Fraud in Banking Forum helps build an intelligence-led response to gangs operating in Australia.

The following section provides further information on fraud by card type.

Proprietary Debit Cards

Data in this table cover proprietary debit cards fraud data including:

- All fraud occurring on debit cards operated by eftpos Payments Australia.
- Most fraud occurring at ATMs in Australia (including on scheme credit, debit and charge cards).

Fraud ($m)	2013	2014	2015	2016	2017	2018
Counterfeit / skimming	$13.6	$17.0	$16.5	$18.5	$11.9	$6.3
Lost / stolen	$2.7	$3.1	$3.5	$2.4	$2.6	$3.9
Never received	$1.3	$1.4	$1.6	$2.1	$1.5	$1.4
Other	$0.8	$1.5	$1.4	$0.7	$0.9	$1.8
TOTAL	$18.4	$23.0	$23.0	$23.7	$16.9	$13.4

KEY TREND

Fraud perpetrated on proprietary cards continues to decline. The total amount of fraud on proprietary debit cards dropped 21% in 2018 to $13.4 million. Counterfeit/skimming fraud dropped 47% to $6.3 million, following the transition to chip-reading ATMs in Australia in 2016 and the roll-out of chip technology on proprietary debit cards.

Scheme Credit, Debit and Charge Cards

Data in the table below cover fraud on scheme credit, debit, and charge cards issued by the international card schemes (Visa, MasterCard, Amex and Diners) and carried over their respective networks.

The data includes all fraud occurring:

- Over the internet, telephone, or by mail order (card-not-present).
- Where the 'credit' option is chosen at the point-of-sale device.
- On all Australian cards used overseas (including at ATMs).

FRAUD PERPETRATED IN AUSTRALIA

Fraud ($m)	2013	2014	2015	2016	2017	2018
Card-not-present	$85.9	$99.1	$136.8	$175.8	$227.4	$257.9
Counterfeit / skimming	$9.7	$8.4	$6.4	$7.3	$4.6	$5.1
Lost / stolen	$18.5	$16.8	$17.0	$21.4	$24.7	$32.9
Never received	$7.3	$6.7	$6.9	$7.6	$6.2	$4.4
Fraudulent application	$1.4	$1.0	$0.8	$2.4	$2.8	$1.8
Other	$0.8	$0.6	$0.9	$2.6	$0.9	$1.1
TOTAL	$123.6	$132.6	$168.8	$217.1	$266.6	$303.2

KEY TREND

CNP fraud accounts for 85% of all fraud perpetrated in Australia on Australian-issued scheme credit, debit and charge cards. Reducing CNP fraud takes a co-ordinated approach across the entire e-commerce network. Throughout 2018, the e-commerce community came together to develop the CNP Fraud Mitigation Framework (See "Industry Initiatives to combat card-not-present fraud"). The increasing uptake of fraud prevention measures by both merchants and consumers is having a positive effect, with the 27% increase in overall CNP value outstripping the 13% increase in CNP fraud in 2018.

FRAUD PERPETRATED OVERSEAS

Fraud ($m)	2013	2014	2015	2016	2017	2018
Card-not-present	$124.5	$200.9	$226.3	$242.3	$248.7	$229.6
Counterfeit / skimming	$12.8	$15.9	$28.2	$33.5	$14.4	$8.1
Lost / stolen	$11.1	$13.3	$12.8	$13.9	$13.4	$18.7
Never received	$0.5	$0.5	$0.6	$0.6	$0.3	$0.4
Fraudulent application	$0.1	$0.2	$0.5	$1.3	$0.6	$0.4
Other	$0.4	$0.3	$0.8	$2.2	$0.6	$0.6
TOTAL	$149.4	$231.1	$269.2	$293.8	$277.9	$257.8

KEY TREND

Similar to when used in Australia, the majority of fraud on Australian-issued scheme credit, debit and charge cards used overseas occurs online. While CNP fraud dropped for the first time in 2018 – down by 8% to $229.6 million- it accounted for 89% of all fraud perpetrated overseas on these types of cards.

Fraud Perpetrated in Australia on Overseas Cards

When international visitors use their cards at Australian ATMs or point-of-sale terminals, the transactions are processed by the international card schemes.

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

Fraud value ($m)	2013	2014	2015	2016	2017	2018
Card-not-present	$33.6	$44.8	$47.9	$55.0	$67.3	$71.2
Counterfeit / skimming	$11.1	$9.3	$8.0	$8.8	$7.6	$5.8
Lost / stolen	$4.4	$2.8	$3.0	$2.9	$3.4	$3.3
Never received	$0.1	$0.0	$0.1	$0.1	$0.1	$0.1
Fraudulent application	$0.1	$0.1	$0.1	$0.1	$0.1	$0.1
Other	$0.5	$0.5	$0.6	$0.9	$0.8	$1.5
TOTAL	**$49.8**	**$57.6**	**$59.6**	**$67.7**	**$79.4**	**$82.0**

KEY TRENDS

CNP fraud accounts for 87% of all fraud perpetrated in Australia on cards issued overseas. Australian merchants play an important role in minimising this type of fraud. For more information, merchants should refer to the section on fraud prevention for remote payments.

Glossary

The Australian Payments Council is the strategic coordination body for the Australian payments industry. It engages directly with the Reserve Bank of Australia's Payments System Board.

Types of Fraud

Card-not-present (CNP) fraud: occurs when valid card details are stolen and then used to make purchases or other payments without the card via a remote channel, mainly online via a web browser or by phone. The key drivers that cause the global growth in card-not-present fraud continue to be:

- Chip and PIN deployments migrating fraud from in-person to remote channels.
- Large scale data-breaches, which capture cards from international jurisdictions
- Identity theft, where card-not-present fraud is one of the resulting crimes.

Card present fraud: occurs when a 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 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.

Proprietary debit cards: operated by eftpos Payments Australia Limited as well as cards used to make transactions at Australian ATMs.

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.

Appendix - Cheque Fraud Perpetrated in Australia

AusPayNet also collects cheque fraud data. The cheque fraud data cover fraud occurring on Australian 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 include Australian personal cheques, financial institution cheques, and drafts in Australian dollars.

Fraud ($m)	2013	2014	2015	2016	2017	2018
On us fraud:						
Breach of mandate	$0.9	$0.4	$0.3	$0.9	$0.4	$0.4
Fraudulently altered	$1.2	$1.7	$3.6	$2.1	$2.4	$1.2
Stolen blank cheque / book	$4.0	$1.7	$1.8	$2.2	$2.3	$1.5
Originated counterfeit cheques	$0.7	$1.1	$1.2	$0.4	$0.3	$0.2
Non originated counterfeit cheques	$0.2	$0.6	$0.7	$0.6	$0.3	$0.1
Valueless	$0.0	$0.9	$0.7	$0.0	$0.0	$0.3
ON-US TOTAL	**$7.0**	**$6.3**	**$8.2**	**$6.2**	**$5.7**	**$3.7**
Deposit Fraud	$0.2	$0.2	$0.2	$0.2	$0.2	$0.6
TOTAL ALL CHEQUES FRAUD	**$7.1**	**$6.5**	**$8.4**	**$6.4**	**$5.9**	**$4.4**

* Data on the 'transactions' of recoveries is not collected.

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

About this Report

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 major card schemes[1] – 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

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