

Payment Fraud Statistics - Summary of Results
Fraud Perpetrated on Australian Cheques and Cards
1 January 2015 - 31 December 2015 (Revised December 2016)

	Fraud Transactions		Total Transactions		Fraud Rates	
	number	\$	number (millions)	\$ (millions)	as % of total no. of transactions	as % of total value (\$) of transactions
Cheques	1,160	\$8,389,133	140	\$1,228,424	0.0008%	0.0007%
Australian-issued cards	2,191,082 r	\$460,885,995 r	7,292 r	\$688,701 r	0.0300%	0.0669%
- Proprietary debit cards	63,074	\$22,909,985	N/A	N/A	N/A	N/A
- Scheme credit, debit and charge cards	2,128,008	\$437,976,010	N/A	N/A	N/A	N/A
Total	2,192,242	\$469,275,128	7,431	\$1,917,125	0.0295%	0.0245%

Note:

1. Data for the total number and total value of all transactions is from the RBA's Payment Data. The data for cheques is sourced from Table C6 and for cards from Tables C1, C4 and C5.
2. A break in the series occurred at the end of 2012 as a result of a change in the data available in Table C5. The RBA no longer publishes debit card data by card types but provides aggregated data for all cards. Therefore APCA is no longer able to calculate fraud rates for proprietary debit cards and scheme credit, debit and charge cards separately.
3. For cards 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.

r = Figures have been revised.

Cheque Fraud Perpetrated in Australia

1 January 2015 - 31 December 2015

	Category	Actual		Exposure		Recoveries *
		Transactions	Value (\$)	Transactions	Value (\$)	Value (\$)
On-Us Fraud	Valueless	7	738,435	436	28,460,226	766,590
	Fraudulently Altered	360	3,556,966	566	7,389,473	919,045
	Stolen Blank Cheque / Book	441	1,754,667	1,155	9,047,294	201,635
	Originated Counterfeit Cheques	263	1,179,176	264	4,054,221	130,743
	Non-Originated Counterfeit Cheques	49	652,085	118	3,676,750	14,256
	Breach of Mandate	21	288,912	25	889,737	20,680
	On-Us Total	1,141	8,170,241	2,564	53,517,701	2,052,949
Deposit Fraud	Valueless	4	29,059	217	43,822,601	27,211
	Valueless - Kite Flying	1	3,000	22	2,863,354	2,625
	Third Party Conversion	14	186,833	32	774,929	74,378
	Deposit Total	19	218,892	271	47,460,884	104,214
Total	1,160	8,389,133	2,835	100,978,585	2,157,163	

* 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.

Explanation of Cheque Fraud Categories

On-us Fraud

On-us cheque fraud includes cheques issued by Financial Institution X and deposited back into Financial Institution X. Categories for On-Us Fraud include:

- Valueless - Covers cheques drawn on an account where there appears to be suspicious circumstances or where it is thought that the Cheque is stolen or forged or in any other way is fraudulently issued and action is taken in terms of Rule 4.4 in Schedule 10.
- Fraudulently Altered Cheques :
 - Payee Only - cheques that have been altered to show payee details other than those originally authorized by the drawer and where no other area of the cheque has been altered.
 - Amount Only - cheques that have been altered to show \$-amount details other than those originally authorized by the drawer and where no other area of the cheque has been altered.
 - Both Payee AND Amount - Cheques that have been altered to show payee details AND \$-amount details other than those originally authorized by the drawer and where no other area of the cheque has been altered.

Note: Fraudulently altered cheques do not include cheques with forged signatures. These are included in Stolen Blank Cheque/Book and Originated or Non-Originated Counterfeit Cheques.

Where alterations are made to the MICR line, items are included in the counterfeit category

- Stolen Blank Cheque/Book - this includes original stolen blank cheques that are written or marked in order to be passed off as if by the legitimate signatory. Includes forged makers mark.
- Originated Counterfeit Cheques - originated counterfeit cheques are produced using the paper of the original cheque to create a new, unauthorized cheque. Techniques used in this process include washing, laser printing, scanning and desk-top publishing.
- Non-originated Counterfeit Cheques - non-originated counterfeit cheques made on new paper to create a new, unauthorized cheque. Techniques used in this process include laser printing, photocopying, scanning and desk-top publishing. This category also includes items where the MICR line has been altered.
- Breach of Mandate – this involves payment of cheques which do not follow the original instructions or arrangements set up. That is, the cheque may require two signatories but the financial institution, through error, allows only one signatory. Other examples include a cheque drawn by a designated authority such as Financial Officer or Accountant and used for fraudulent purposes.

Deposit Fraud

- Valueless - Covers cheques deposited to an account knowing that these cheques should not be honoured on presentation by the drawee financial institution as they are valueless (lack of funds), counterfeit, reported stolen, have been fraudulently altered or are in breach of mandate (e.g. do not contain required number of signatures).

Note: This category excludes customer cheques dishonoured or returned for lack of funds where cheques were drawn in error, that is, there was no intent to defraud.

- Valueless: Kite Flying - the activity of depositing valueless cheques and making withdrawals against those valueless cheques, between accounts owned by the same person. Also called round robin transactions.
- Third Party Conversion - this category includes unaltered cheques which have been deposited to an account other than the payee. This arises where the financial institution has made insufficient enquiry or verification of the depositor regarding their title to the cheque. It also includes cheques where there are two payees but the financial institution has allowed one payee to deposit the amount into their personal account without authority from the other payee.

Proprietary Debit Cards Fraud Perpetrated in Australia

1 January 2015 - 31 December 2015

Category		Transactions	Value (\$)
Debit Card Fraud - PIN Used	Lost / Stolen	13,642	3,430,563
	Never Received	3,658	1,606,635
	Counterfeit / Skimming	40,723	16,423,221
	Other	4,096	1,372,790
	PIN Used Total	62,119	22,833,209
Debit Card Fraud - PIN Not Used	Lost / Stolen	763	52,369
	Never Received	5	67
	Counterfeit / Skimming	174	22,930
	Other	13	1,410
	PIN Not Used Total	955	76,776
Total Debit Card Fraud		63,074	22,909,985

Note: For fraudulent transactions initiated at ATMs, POS terminals and other devices, the above statistics incorporate all transactions where either "cheque" or "savings" was selected, regardless of the type of card used (that is debit card, 'combo' card, scheme card etc). 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.

Explanation of Proprietary Debit Cards Fraud Categories

- Lost/Stolen - fraud resulting from the loss or theft of an existing card and a fraudulent transaction has taken place.
- Card Never Received - fraud where a card has been intercepted (stolen) during delivery to the customer and used before it was received by the customer.
- Counterfeit/Skimming - the use of altered or illegally reproduced cards including the replication/alteration of the magnetic stripe and/or changes to the details on the face of the card with intent to defraud. Skimming is a form of magnetic-stripe counterfeiting in which criminals are able to copy magnetic stripe track information (including Card Verification Value - CVV) from a valid card. Information is then encoded on a counterfeit or stolen card and then used fraudulently.
- Other - fraud that cannot be categorized under any of the other fraud type categories. This includes identity takeover and false applications etc.

Scheme Credit, Debit and Charge Card Fraud Perpetrated in Australia and Overseas on Australia-issued Cards

1 January 2015 - 31 December 2015 (Revised December 2016)

Category	In Australia		Overseas		Total	
	Transactions	Value (\$)	Transactions	Value (\$)	Transactions	Value (\$)
Lost / Stolen	211,671	17,002,315	42,095	12,837,511	253,766	29,839,825
Never Received	66,234	6,861,624	2,188	630,225	68,422	7,491,849
Fraudulent Application	3,590	839,553	2,195	451,256	5,785	1,290,810
Counterfeit / Skimming	15,586	6,406,258	71,289	28,149,280	86,875	34,555,537
Card Not Present (CNP)	597,648	136,767,066	1,102,124	226,316,732	1,699,772	363,083,798
Other	6,268	930,206	7,120	783,985	13,388	1,714,191
Total	900,997	168,807,022	1,227,011	269,168,988	2,128,008	437,976,010

Fraud Perpetrated in Australia on Cards Issued Overseas

Category	Transactions	Value (\$)
Lost / Stolen	15,331	2,987,209
Never Received	855	117,929
Fraudulent Application	393	72,258
Counterfeit / Skimming	47,541	7,998,900
Card Not Present (CNP)	181,229	47,852,921
Other	1,151	571,836
Total	246,500	59,601,053

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.

Explanation of Scheme Credit, Debit and Charge Cards Fraud Categories

- **Lost/Stolen Card** - fraud resulting from the loss or theft of an existing card and a transaction has taken place without the cardholder's consent or authority.
- **Card Never Received** - fraud where a card has been intercepted (stolen) during delivery to the customer and used before it was received by the customer.
- **Fraudulent Application** - fraudulent applications are applications for card accounts using a fictitious identity, using someone else's identity or providing false information during the application process.
- **Counterfeit/Skimming** - the use of altered or illegally reproduced cards including the replication/alteration of the magnetic stripe and changes to the details on the face of the card with intent to defraud. Skimming is a form of magnetic stripe counterfeiting in which criminals are able to copy magnetic stripe track information (including Card Verification Value - CVV) from a valid card. Information is then encoded on a counterfeit or stolen card and used fraudulently.
- **Card Not Present (CNP)** - the use of account information including pseudo account information without the physical card being involved, via the phone, mail, Internet etc. without the authority of the cardholder. This category also includes fraud where a card should normally be present (eg: in a retail transaction) but a merchant has chosen to accept the transaction based on a card number only and it turns out to be a fraudulent transaction.
- **Other** - fraud that cannot be categorised under any of the other Fraud Type categories. For example fraud using imprints of cards at merchants, or use of an existing account without the authority of the cardholder by a person who gains access to and use of the account through an unauthorized means, such as a fraudulent change of address or request for re-issuance of cards (but not lost or stolen cards).