



Payment Fraud Statistics - Summary of Results

Fraud Perpetrated on Australian Issued Payment Instruments						
1 January 2007 - 31 December 2007 (revised June 2010)						
Instrument	No. of Fraud Transactions	Value (\$) of Fraud Transactions	Total No. of all Transactions <i>(thousands)</i>	Total Value (\$) of all Transactions <i>(\$ millions)</i>	Fraud as % of Total No. of Transactions	Fraud as % of total value (\$) of Transactions
Cheque	1,561	14,312,072	418,103	1,839,498	0.0004%	0.0008%
Debit Card	44,826	14,389,124	1,990,946	203,660	0.0023%	0.0071%
Credit / Charge	337,911 ^r	113,245,136 ^r	1,758,296	250,626	0.0192%	0.0452%
Total	384,298	141,946,332	4,167,345	2,293,784	0.0092%	0.0062%

Data for total number of all transactions and total value of all transaction is sourced from data published in the RBA Bulletin. The data is sourced from Table C6 for Cheques, Table C4 and C5 for the Debit Card (ATM-POS) Category and Table C1 and C5 for Credit/Charge Cards Category

As the Reserve Bank tables do not differentiate between scheme debit and proprietary debit transactions for the reporting period, the figures in tables C1, C4 and C5 have been adjusted according to data supplied by the Card Schemes to provide a true comparison with the fraud data collected by APCA.

Note: ^r = figures have been revised.

Cheque Fraud Perpetrated in Australia					
1 January 2007 - 31 December 2007 (revised June 2010)					
Category	Actual		Exposure		Recoveries*
<i>On-Us Fraud</i>	<i>Number</i>	<i>Value (\$)</i>	<i>Number</i>	<i>Value (\$)</i>	<i>Value (\$)</i>
Fraudulently Altered	518	4,724,650	946	12,488,082	547,478
Stolen Blank Cheque / Book	710	3,029,897	1,238	9,707,386	421,718
Originated Counterfeit Cheques	112	724,308	284	3,277,603	105,053
Non-Originated Counterfeit Cheques	57	435,991	262	6,254,970	140,491
Breach of Mandate	59	3,323,685	81	1,583,226	5,237,102
<i>On-Us Total</i>	1,456	12,238,531	2,811	33,311,267	6,451,842
<i>Deposit Fraud</i>					
Valueless	35	1,315,388	1,624	40,340,806	974,055
Valueless - Kite Flying	20	65,660	176	508,184,980	24,703
Third Party Conversion	50	692,493	113	3,428,746	21,547
<i>Deposit Total</i>	105	2,073,541	1,913	551,954,532	1,020,305
<i>Total</i>	1,561	14,312,072	4,724	585,265,799	7,472,147

* Data on the 'number' 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:

- **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.

Debit Card Fraud Perpetrated in Australia		
1 January 2007 - 31 December 2007 (revised June 2010)		
Category	Number	Value (\$)
<i>Debit Card Fraud - PIN Used:</i>		
Lost / Stolen	8,308	2,819,993
Never Received	1,665	910,579
Counterfeit / Skimming	11,370	4,147,849
Other	5,168	1,978,323
<i>PIN Used Total</i>	26,511	9,856,744
<i>Debit Card Fraud - PIN Not Used:</i>		
Lost / Stolen	6,065	1,398,342
Never Received	738	148,654
Counterfeit / Skimming	2,816	1,156,457
Other	8,696	1,828,927
<i>PIN Not Used Total</i>	18,315	4,532,380
<i>Total Debit Card Fraud</i>	44,826	14,389,124

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).

Explanation of Debit Card 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.

Credit Card and Charge Card Fraud Perpetrated in Australia and Overseas on Australian-issued Cards						
1 January 2007 - 31 December 2007 (revised June 2010)						
	In Australia		Overseas		Total	
Category	Number	Value (\$)	Number	Value (\$)	Number	Value (\$)
Lost / Stolen	46,976	12,029,793	14,617	5,545,864	61,593	17,575,657
Never Received	10,194	2,939,639	973	246,117	11,167	3,185,756
Fraudulent Application	5,550	2,824,338	637	254,860	6,187	3,079,198
Counterfeit / Skimming	24,919	14,734,419	27,767	18,168,889	52,686	32,903,308
Card Not Present (CNP)	61,129	20,475,536	135,578	34,113,723	196,707	54,589,259
Other	7,791	1,551,081	1,780	360,878	9,571	1,911,959
Total	156,559	54,554,805	181,352	58,690,331	337,911	113,245,136

Fraud Perpetrated in Australia on Cards Issued Overseas		
Category	Number	Value (\$)
Lost / Stolen	26,935	9,380,811
Never Received	2,161	536,475
Fraudulent Application	1,058	381,454
Counterfeit / Skimming	134,527	60,528,343
Card Not Present (CNP)	72,862	22,766,977
Other	2,250	712,058
Total	239,793	94,306,118

Credit/Charge Card figures have been revised



Explanation of Credit Card and Charge Card 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).