



Payment Fraud Statistics - Summary of Results

Fraud Perpetrated on Australian Issued Payment Instruments						
1 January 2009 - 31 December 2009						
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	1,488	18,643,194	333,006	1,500,225	0.0004%	0.0012%
Debit Card	63,894	24,471,348	2,509,411	259,520	0.0025%	0.0094%
Credit / Charge	593,819	145,854,208	1,845,183	255,235	0.0322%	0.0571%
Total	659,201	188,968,749	4,687,600	2,014,980	0.0141%	0.0094%

Note: 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.

Cheque Fraud Perpetrated in Australia					
1 January 2009 - 31 December 2009					
Category	Actual		Exposure		Recoveries*
<i>On-Us Fraud</i>	<i>Number</i>	<i>Value (\$)</i>	<i>Number</i>	<i>Value (\$)</i>	<i>Value (\$)</i>
Valueless	11	1,289,347	158	9,201,566	58
Fraudulently Altered	576	6,126,456	990	16,019,800	1,854,801
Stolen Blank Cheque / Book	503	2,682,630	861	13,429,349	164,486
Originated Counterfeit Cheques	158	1,346,637	318	2,841,326	220,144
Non-Originated Counterfeit Cheques	54	597,249	356	15,308,801	78,085
Breach of Mandate	33	1,002,762	125	2,371,184	121,441
<i>On-Us Total</i>	1,335	13,045,081	2,808	59,172,026	2,439,015
<i>Deposit Fraud</i>					
Valueless	65	720,863	1,565	16,895,837	139,595
Valueless - Kite Flying	37	4,264,568	130	13,195,286	2,030
Third Party Conversion	51	612,682	76	1,042,593	14,635
<i>Deposit Total</i>	153	5,598,113	1,771	31,133,716	156,260
<i>Total</i>	1,488	18,643,194	4,579	90,305,742	2,595,275

* 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:

- *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.

Debit Card Fraud Perpetrated in Australia

1 January 2009 - 31 December 2009		
Category	Number	Value (\$)
Debit Card Fraud - PIN Used:		
Lost / Stolen	8,993	3,082,485
Never Received	2,517	1,159,502
Counterfeit / Skimming	45,917	17,585,337
Other	5,118	2,336,238
PIN Used Total	62,545	24,163,562
Debit Card Fraud - PIN Not Used:		
Lost / Stolen	661	147,740
Never Received	16	9,300
Counterfeit / Skimming	72	33,684
Other	600	117,062
PIN Not Used Total	1,349	307,786
Total Debit Card Fraud	63,894	24,471,348

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 2009 - 31 December 2009						
	In Australia		Overseas		Total	
Category	Number	Value (\$)	Number	Value (\$)	Number	Value (\$)
Lost / Stolen	36,689	7,565,237	26,009	5,514,849	62,698	13,080,086
Never Received	10,507	2,741,708	998	290,171	11,505	3,031,879
Fraudulent Application	2,686	1,534,863	1,033	154,622	3,719	1,689,485
Counterfeit / Skimming	29,670	14,985,351	43,388	22,539,755	73,058	37,525,105
Card Not Present (CNP)	114,914	31,471,427	322,664	57,250,045	437,578	88,721,472
Other	4,318	1,533,784	943	272,396	5,261	1,806,180
Total	198,784	59,832,370	395,035	86,021,838	593,819	145,854,208

Fraud Perpetrated in Australia on Cards Issued Overseas		
Category	Number	Value (\$)
Lost / Stolen	28,333	7,966,323
Never Received	2,131	604,609
Fraudulent Application	624	221,971
Counterfeit / Skimming	109,228	40,563,240
Card Not Present (CNP)	90,014	24,085,177
Other	3,602	762,852
Total	233,932	74,204,171



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).