Australian Payments
Clearing Association

Payment Fraud Statistics

Methodology Paper

CONTENTS

1. Introduction

APCA has been publishing cheque and card fraud[1] statistics since November 2006 based on information collected from APCA's member institutions as well as the major card schemes operating in Australia. This data provides consumers with information as to how fraud occurs so that they can take steps to minimise the risks when using cheques and cards as well as assisting the industry and APCA's members in monitoring fraud trends and developing targeted mitigating strategies.

Since 2006 the card landscape in Australia has changed markedly. The number and value of transactions carried out using scheme debit cards (those issued by MasterCard and Visa) has become significant (the RBA began publishing separate statistics for these transactions from March 2008). A commercial company, EFTPOS Payments Australia Limited, was formed in 2009 to take over the running of Australia's proprietary debit system.

2. Identification of Payments Fraud

Nearly all fraud data is identified in one of two ways:

1. *Direct reporting of fraudulent transactions by the customer* – customers who experience fraud make direct contact with their financial institution.

2. *Detection of fraudulent transactions by financial institutions* - fraudulent transactions are identified by financial institutions through their internal fraud detection systems.

4. Fraud Data Collections

The fraud data collections which are administered by APCA are:

1) card fraud data, made up of:
   a) scheme credit, debit and charge cards fraud data, and
   b) proprietary debit cards fraud data; and
2) cheque fraud data

5. Scope, Coverage and Data Collection

Scope, coverage and data collection for each of the collections is outlined below:

[1] **Fraud is defined in the Oxford Dictionary as: …** ***wrongful or criminal deception intended to result in financial or personal gain.***

5.1 Scheme credit, debit and charge cards

- Fraud statistics for the scheme credit, debit and charge card fraud statistics are provided to APCA each quarter by the international card schemes operating in Australia. The schemes included in the collection (Visa, MasterCard, Amex, Diners and JCB) cover nearly all credit card activity in Australia plus an increasing proportion of debit cards.

- Fraud statistics relating to scheme credit, debit and charge cards include three types of fraudulent transactions:

  - fraudulent transactions on cards which have been issued in Australia and where the fraud occurred in Australia;

  - fraudulent transactions on cards which have been issued in Australia and where the fraud occurred overseas; and

  - fraudulent transactions on cards which were issued overseas and where the fraud occurred in Australia.

- Financial institutions issuing scheme credit or scheme debit cards are required to provide ongoing and up-to-date transaction data to the card scheme. The card scheme collects all this transaction data directly from individual member institutions including data on instances of fraud.

- The way in which the card schemes' fraud categories are aggregated by APCA has been developed with the help and agreement of these card schemes.

5.2 Proprietary Debit Cards

- The term "Proprietary Debit Cards' is used to distinguish between the original bank-issued debit cards and scheme debit cards (from Visa and MasterCard). Proprietary debit card data covers eftpos and most ATM transactions in Australia (it excludes cash advances made on credit cards and international withdrawals).

- Proprietary debit card fraud statistics are provided to APCA each quarter by its members who issue these cards. These include retail banks, building societies and credit unions (via their industry bodies). It is estimated that these institutions make up nearly all proprietary debit card activity in Australia.
- Proprietary debit card fraud includes all fraud arising from transactions on the financial institutions' Australian domestic network. The data does not include fraud arising from transactions carried over the card schemes' network.
- "Combo" (or combination cards) are cards which enable cardholders to access their financial institutions via:
  - an international scheme (Visa, MasterCard) when the "credit" option is chosen at a POS device; and
  - the domestic eftpos network when the "cheque" or "savings" option is chosen at the POS device.

The fraud on these cards is reported as "scheme credit or debit card" fraud to the card schemes if the "credit" option was chosen and as "proprietary debit card" fraud to APCA if the "cheque" or "savings" options were chosen.

5.3 Cheques

- Cheque fraud statistics are provided to APCA each month by members of the Australian Paper Clearing System (APCS). This information covers all cheque collection and payment activity by financial institutions in Australia. Cheques include customer cheques, financial institution cheques and AUD drafts.

- Cheque fraud data includes:

    1. cheques which were issued in Australia and the fraud occurred in Australia; and

    2. cheques which were issued in Australia and deposited overseas (i.e. the fraud occurred overseas). These cheques will eventually return to the drawee financial institution in Australia which will report the fraud to APCA.

- Fraud data relating to foreign currency cheques issued by overseas financial institutions which are deposited in Australia is not collected by APCA as the overseas financial institutions (the drawee financial institutions) are not members of APCS.
- In some circumstances the collecting institution may allow access to funds prior to the cheque clearing process (usually 3 days). The collecting institution will take on exposure to fraud as well as any actual loss if the cheque is subject to fraud. In this event, the issuing and collecting institution may report an exposure to fraud while the collecting institution only will report any loss.

6. Data Reporting and Timing

6.1 Data Reporting

The following section outlines how data is reported and how timing issues impact on output from the collections.

Card Fraud Data Reporting

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

Cheque Fraud Data Reporting

- Financial institutions report three set of figures:

    1. the actual amount of fraud losses written off during that month as recorded on the financial institution's ledgers. Actual losses can relate to exposure during

an earlier period. This explains why, in some reporting periods, actual losses may exceed exposure;

2. their exposure to loss - (a) where actual loss has occurred, plus (b) where fraud has been detected and stopped prior to payment (i.e. no loss has taken place); and
3. recoveries relating to cheque fraud. These figures show the total amount recovered within that reporting period and may include recoveries against amounts written off (usually associated with a repayment plan and/or associated with compensation/court orders etc) and/or recoveries against monies that have been paid into the collecting financial institution's account, traced and frozen and later recovered. The recovery amount can relate to actual losses from an earlier reporting period.

6.2 Timing

Fraudulent transactions may have occurred days or weeks prior to the customer discovering that a fraud incident has occurred.

Scheme credit, debit and charge card fraud data for a given period is intended to include data on all fraud transacted in that period. To achieve this, a 3 month period after the end of the reporting period is required for fraud to be discovered and all relevant fraud details gathered.

Cheque and proprietary debit card fraud statistics include fraudulent transactions discovered within the reporting period, but which may have been transacted some time before.

7. Data Processing

Each individual return is checked for consistency, missing values etc. Respondents are contacted to verify and/or correct their returns when issues arise. Once all data is received and checked, the data is aggregated to produce final totals. At this stage, the data series are checked for consistency.

8. Data Items and Definitions

This section defines the fraud categories in which data is released.

8.1 Definitions – scheme credit, debit and charge card fraud statistics

The fraud categories and definitions which are used for scheme credit, debit and charge card fraud statistics are:

- *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).

8.2 Definitions – proprietary debit card fraud statistics

Data is collected separately for events where the PIN is present and PIN not present. PIN not present arises from the use of a PIN based card transaction at a merchant whose network connection is down and hence the PIN cannot be verified.

The fraud categories and definitions which are used for proprietary debit card fraud statistics are:

- *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.

8.3 Definitions - cheque fraud statistics

Most cheque fraud is detected and reported by the drawee financial institution. The categories used by the drawee institution to report cheque fraud are listed below under On-us Fraud. Less often fraud is detected and reported by the collecting financial institution – where the cheque is deposited. The categories used by the collecting financial institution to report cheque fraud are listed below under Deposit Fraud.

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.

9. Release of Statistics

All statistics will be presented in annualized terms only. That is, data will be aggregated on the basis of 12 month periods. Using annualized data ensures that the lead and lag effect caused by timing differences in discovering, reporting and/or resolving fraud events is minimized.

Release of annualized data is also consistent with the release of this type of data for similar international statistics.

A rolling annualized 12 months of statistics for each collection will be released every six months. There are two separate sets of statistics:

1. card fraud data, made up of:
    a. scheme credit, debit and charge cards fraud data, and

b. proprietary debit cards fraud data; and

2. cheque fraud data.

These statistics can be found on the APCA website on the statistics page at www.apca.com.au

10. Recovery of Losses and Revisions

After a fraud incident occurs, losses may be recovered by authorities or by the financial institution. Treatment of recoveries for the purposes of APCA fraud statistics is as follows:

- Card fraud statistics will not be revised for any recoveries. Once the event is determined to be a fraud event, it will be recorded as a fraud transaction for purposes of the total number of fraud transactions for that period. Similarly, the value of a fraud transaction will be recorded against the total value of fraud transactions for that period.
- For cheque fraud APCA asks financial institutions to report recoveries. This is released as a separate aggregate in the Cheque Fraud data.

Revisions are sometimes made to APCA fraud statistics when more information becomes available. The data is marked appropriately when revisions are made.

11. Confidentiality

APCA does not release any individual financial institution's statistics, either on its web site or to its members.

12. Other APCA Statistics and Information

A broad range of statistics on the Australian Payments Clearing Systems is available on the APCA website, www.apca.com.au, including:

- Cheque Payment Transactions (Monthly volume and value)
- Cheque Payment Transactions (Daily volume and value)
- Number of Direct Debit and Credit Users
- Direct Entry Transactions (Daily volume and value)
- Direct Entry Transactions (Monthly volume and value)
- Number of ATMs and EFTPOS terminals
- Cards Transactions (ATM / Debit cards / Credit cards) - (Monthly volume)
- Cards Transactions (ATM / Debit cards / Credit cards) - (Monthly value)
- Number of Customer Payment Accounts and Cards
- High Value Clearing System (HVCS) Transactions - (Daily value)
- High Value Clearing System (HVCS) Transactions - (Monthly value)

APCA also keeps the community informed of payments clearing developments through the quarterly publication Payments Monitor and its annual reports, available on APCA's website.

13. Further Information

For further information about these statistics or for other information please contact, in the first instance, APCA Communications on (02) 9216 4888 or email: info@apca.com.au.