



Australian Government

Australian Institute of Criminology

AIC reports

Statistical Report

03

Fraud against the Commonwealth:

Report to Government 2014-15

Penny Jorna
Russell G Smith

© Australian Institute of Criminology 2018

ISSN (Online) 2206-7930

Apart from any fair dealing for the purpose of private study, research, criticism or review, as permitted under the *Copyright Act 1968* (Cth), no part of this publication may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Inquiries should be addressed to the publisher.

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: aic.gov.au

Please note: Minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

Disclaimer: This research report does not necessarily reflect the policy position of the Australian Government.

General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at aic.gov.au

Foreword

Risk of fraud affects every Commonwealth entity in all areas of business, including the provision of benefits and grants, the collection of taxation, procurement, and leave and travel entitlements for public servants. In the wider Australian community, fraud was estimated to cost Australia around \$6.5b in 2011 (Smith et al. 2014), making it the most expensive crime type in Australia. In addition to economic harm, fraud entails many indirect costs, including damage to morale within organisations and emotional stress for victims of fraud.

Fraud in the public sector involves ‘dishonestly obtaining a benefit, or causing a loss, by deception or other means’ (AGD 2014: 4.1) and can be perpetrated by public servants, who may abuse their privileges for personal gain, or by other members of the public or corporations who may seek to unlawfully obtain benefits or payments from government entities. Between 2010–11 and 2012–13, fraud against the Commonwealth was estimated to cost Commonwealth entities over \$500m, with only a small percentage (less than 5%) able to be recovered by entities (Jorna & Smith 2015). In the challenging economic times facing Australia, reducing the impact of fraud should be high on the policy agenda.

Each year, a census is conducted of Commonwealth entities to document their experience of fraud during the preceding year and to examine the fraud control measures that they employ. This report presents information gathered for the 2014–15 financial year and compares this with the census results for the two immediately preceding financial years. The report identifies the level of fraud risk affecting the Commonwealth each year and how entities approach their task of preventing and responding to acts of dishonesty that have been detected.

Fraud is a constantly evolving crime type. In order for research about fraud to be useful and up-to-date, data collected must be reliable and use consistent approaches to measurement. The 2016 questionnaire was modified substantially in light of the Public Governance, Performance and Accountability Act 2013 (Cth; PGPA Act) and the release of the report of the Independent Review of Whole-of-Government Internal Regulation (Belcher Red Tape Review 2015), as well as feedback from respondents and consultations with stakeholders, including the Attorney-General’s Department (AGD). This report will be the final one that includes information about alleged or suspected fraud ‘incidents’. Future questionnaires will ask questions about fraud ‘investigations’, which will enable data to be reported in a more complete and uniform way than previously. These changes will result in greater consistency between entity responses and will allow for more accurate trend data to be reported.

Contents

B	Foreword	
C	Contents	
D	Tables	
E	Figures	
H	Acknowledgements	
1	Executive summary	
1	Summary of findings	
8	How the information was gathered	
10	Introduction	
13	The Fraud Rule	
13	What the Report covers	
14	Trends in suspected fraud	
14	Experience of fraud	
16	Extent of fraud	
19	Internal fraud trends	
21	How fraud was committed	
22	Internal fraud	
28	External fraud	
33	The value of fraud	
33	What respondents were asked to report	
34	Value of fraud by type	
34	Value by focus category	
36	Recovered funds	
40	Dealing with fraud	
40	How fraud was detected	
42	How fraud was investigated	
46	Referrals for criminal action	
48	Australian Federal Police investigations	
50	Fraud prosecutions by the CDDP	
53	Sentencing dispositions	
54	Fraud compliance, control and prevention	
55	Compliance with fraud control framework	
61	Fraud control staff	
62	Staffing	
63	Training	
65	Conclusions	
65	Principal trends 2012-15	
65	Changing risks	
67	Fraud costs	
68	The Belcher Review and entity feedback	
71	References	
73	Methodology	
75	Glossary	
79	Appendix: Details of how fraud was committed and fraud targets	
79	Internal fraud focus	
80	External fraud focus	
82	Internal fraud method	
84	External fraud method	

Tables

- 14 Table 1 Number and percentage of entities experiencing fraud, 2012–13 to 2014–15 (N&%)
- 17 Table 2 Incidents involving internal and external fraud, collusion and unclassified incidents (N)
- 18 Table 3 Entities that experienced fraud by entity size and year (N)
- 18 Table 4 Number of entities by fraud section, experience of fraud and year (N)
- 19 Table 5 Internal fraud summary results (N)
- 20 Table 6 External fraud summary results (N)
- 27 Table 7 Internal fraud committed by misuse of ICT sub-categories, number of alleged incidents, 2012–13 to 2014–15 (N)
- 30 Table 8 Entitlement fraud subcategories and alleged incidents, 2012–13 to 2014–15 (N) (External fraud)
- 34 Table 9 Dollar value of suspected fraud incidents by type of fraud, 2012–13 to 2014–14 (S)
- 36 Table 10 External fraud focus categories by dollar value and percentage of entities affected, 2012–13 to 2014–15 (\$&%)
- 36 Table 11 Amounts recovered by entities for both internal and external fraud, 2012–13 to 2014–15 (number of entities involved in recoveries in parentheses) (\$)
- 38 Table 12 External fraud focus categories by dollar value and amounts recovered, 2012–13 to 2014–15 (\$)
- 39 Table 13 Monies recovered in 2012–13 to 2014–15 by method of recovery and incident focus category (\$&N)
- 39 Table 14 Monies recovered using criminal action by focus category by year recovered (\$)
- 41 Table 15 Methods of detecting internal fraud incidents, 2012–13 to 2014–15 (N)
- 41 Table 16 Methods of detecting external fraud incidents, 2012–13 to 2014–15 (N)
- 42 Table 17 Detection of fraud by presence of a fraud control section in entities (N)
- 46 Table 18 External investigations of alleged external fraud, by investigating organisation, 2012–13 to 2014–15 (N&%)
- 46 Table 19 Internal fraud incidents referred for criminal action by fraud focus category, 2012–13 to 2014–15 (N)
- 47 Table 20 External fraud incidents referred for criminal action by focus category, 2012–13 to 2014–15 (N)
- 47 Table 21 Internal fraud incidents referred for criminal action by method category, 2012–13 to 2014–15 (N)
- 48 Table 22 External fraud incidents referred for criminal action, by method category, 2012–13 to 2014–15 (N)
- 52 Table 23 Prosecutions of fraud by jurisdiction, 2012–13 to 2014–15 (N)
- 55 Table 24 Entities invited to participate in the census and responding entities (N&%)
- 56 Table 25 Non-corporate Head of entity certification of adequate fraud measures (N&%)
- 56 Table 26 Corporate Head of entity certification of adequate fraud measures (N&%)
- 58 Table 27 Non-corporate entity (previously FMA Act) year of risk assessment (N&%)
- 59 Table 28 Corporate entity (previously CAC Act) year of risk assessment (N&%)
- 60 Table 29 Non-corporate entity (previously FMA Act) year of fraud control plan (N)

- | | |
|--|--|
| <p>61 Table 30 Corporate entity (previously CAC Act) year of fraud control plan (N)</p> <p>61 Table 31 Entities and fraud control sections (N&%)</p> <p>62 Table 32 Total number of fraud control staff and entities with fraud control sections, 2012–13 to 2014–15 (N&%)</p> <p>63 Table 33 Fraud control staff and their qualifications, 2012–13 to 2014–15 (N)</p> <p>73 Table 34 Participating entities (N&%)</p> <p>79 Table 35 Internal fraud focus of fraud, 2012–13 to 2014–15 (N)</p> <p>81 Table 36 External fraud focus of fraud, 2012–13 to 2014–15 (N)</p> <p>82 Table 37 Internal fraud methods of commission 2012–13 to 2014–15 (N)</p> <p>84 Table 38 External fraud methods of commission 2012–13 to 2014–15 (N)</p> | <p>24 Figure 8 Internal fraud focus categories and number of alleged incidents, 2012–13 to 2014–15 (N)</p> <p>25 Figure 9 Internal fraud involving financial benefits subcategories and alleged incidents 2012–13 to 2014–15 (N)</p> <p>26 Figure 10 Percentage of entities affected by fraud, by internal fraud method category, 2012–13 to 2014–15 (%)</p> <p>27 Figure 11 Number of alleged internal fraud incidents by fraud method, 2012–13 to 2014–15 (N)</p> <p>28 Figure 12 External fraud focus categories and entities affected, 2012–13 to 2014–15 (%)</p> <p>29 Figure 13 External fraud focus categories and alleged incidents, 2012–13 to 2014–15 (N)</p> <p>31 Figure 14 External fraud method categories and entities affected, 2012–13 to 2014–15 (%)</p> |
|--|--|

Figures

- | | |
|--|--|
| <p>12 Figure 1 Number of recorded offenders whose principal offence was fraud, 2010–11 to 2014–15, Australian Bureau of Statistics</p> <p>15 Figure 2 Percentage of entities experiencing internal and external fraud over five years, 2010–11 to 2014–15 (%)</p> <p>16 Figure 3 Entities experiencing fraud by type, 2012–13 to 2014–15 (%)</p> <p>17 Figure 4 Entities experiencing fraud by size, 2012–13 to 2014–15 (%)</p> <p>19 Figure 5 Internal fraud incidents and suspects, 2012–13 to 2014–15 (N)</p> <p>21 Figure 6 External fraud incidents and suspects, 2012–13 to 2014–15 (N)</p> <p>23 Figure 7 Internal fraud focus categories and entities affected, 2012–13 to 2014–15 (%)</p> | <p>31 Figure 15 External fraud method categories and alleged incidents, 2012–13 to 2014–15 (N)</p> <p>35 Figure 16 Internal fraud focus categories by dollar value and percentage of type of fraud incidents, 2012–13 to 2014–15 (\$&%)</p> <p>37 Figure 17 Internal fraud focus categories by dollar value and amounts lost and recovered (\$)</p> <p>43 Figure 18 Alleged internal fraud incidents (including collusion and unclassified frauds) and total number of investigations conducted, by year (N)</p> <p>44 Figure 19 Alleged internal fraud by external investigating organisation, 2012–13 to 2014–15 (N)</p> |
|--|--|

- 45 Figure 20 Alleged external fraud incidents and total number of investigations conducted, by year (N)
- 49 Figure 21 Referrals accepted and declined by the AFP 2012–13 to 2014–15 (N)
- 51 Figure 22 Fraud matters prosecuted by the CDPP, 2012–13 to 2014–15 (N)
- 53 Figure 23 Highest sentencing disposition 2012–13 to 2014–15 (%)
- 57 Figure 24 Year entities conducted most recent risk assessment (N)
- 60 Figure 25 Year entities developed most recent fraud control plan (N)
- 64 Figure 26 Top four suggested ways of improving fraud control training (percentage of respondents who answered the question)
- 65 Figure 27 Respondents' views as to what had made a difference to the prevention of fraud (percentage of respondents who answered the question)

Acknowledgements

This report would not have been possible without the provision of information and support from the fraud control staff within each of the responding Commonwealth entities. Officers within the Protective Security and Fraud Control Policy Section of the Commonwealth Attorney-General's Department also provided guidance and assistance in connection with the annual census and the preparation of this report.

Executive summary

Key findings

During the three years examined, 2012–13 to 2014–15, more than one-third of Commonwealth entities reported experiencing fraud. The proportion of entities experiencing fraud increased from 40 percent of responding entities in 2012–13 to 42 percent of entities in the 2014–15 financial year. As with previous reports, the majority of incidents were alleged to have involved people external to the entities.

Over the three years, 417,480 incidents of suspected or proved fraud were reported by Commonwealth entities.

During the same period, entities reported monetary losses totalling approximately \$1.208b, comprising \$207m in 2012–13, \$673m in 2013–14 and decreasing to \$329m in 2014–15. Entities recovered \$50.4m during the reference period, although this may have included monies recovered from fraud losses sustained in earlier years.

Experience of fraud

Between 2012–13 and 2014–15, the percentage of entities experiencing internal fraud increased, (from 28% to 31%). The percentage of entities experiencing external fraud also increased, but to a lesser extent, from 30 percent to 32 percent.

Each year, entities with more than 1,000 staff experienced more fraud than smaller entities with 500 or fewer staff.

Extent of fraud

In each year, the number of internal fraud incidents reported declined, with a 12 percent total reduction from 1,685 incidents of internal fraud in 2012–13 to 1,485 incidents in 2014–15. This decline was generalised across all entities that experienced internal fraud, rather than a few entities experiencing reductions in large numbers.

As with earlier reports, substantially larger numbers of external fraud incidents were reported than internal fraud incidents. In 2014–15 there were 154,221 incidents of suspected external fraud detected, compared with 1,485 incidents of suspected internal fraud. There were some

fluctuations in the numbers of external fraud incidents detected over the three years. In 2012–13 there were 133,969 incidents detected, and in 2013–14 the number of incidents reported reduced to 123,876; however, in 2014–15 the number of reported external fraud incidents increased substantially, to 154,221, representing a 24 percent increase between 2013–14 and 2014–15.

In addition to questions asked about suspected incidents of internal or external fraud, respondents answered questions about their experience of fraud involving collusion between staff and individuals outside the public sector. The number of incidents involving collusion fluctuated over the three years, ranging from 17 in 2012–13, down to four in 2013–14 and increasing substantially in 2014–15 to 107. The percentage of entities experiencing collusion over the three-year period remained steady at 2–3 percent.

The number of incidents of fraud that could not be classified (as either internal, external or collusion) also varied over the three-year period, from one incident in 2012–13, to 428 in 2013–14 and decreasing to 30 in 2014–15.

In addition to incidents of fraud experienced, the census also asked about the number of individuals suspected of committing fraud. Over the three-year period the number of suspects identified was lower than the number of incidents reported. In 2014–15 there was a reduction of 26 percent in the number of suspects identified for internal fraud incidents and a 91 percent reduction in the number of suspects identified with external fraud incidents. The reasons for this decline may include entities not always being able to identify suspected individuals, particularly when investigations have just commenced, or changes in fraud reporting processes within some large entities that resulted in fraud allegations being handled differently.

How fraud was committed

Respondents were asked to indicate two main aspects of how the fraud incidents they detected had been committed: their focus (that is, the target of the alleged fraudulent activity, or the benefit to be derived from the illegal conduct) and the method of carrying out the alleged fraud (such as misuse of technology, information, identity etc).

Internal fraud

The largest number of entities reported suspected internal fraud incidents involving financial benefits, such as obtaining cash without permission, or misuse of government credit cards, with around 20 percent of entities reporting this type of internal fraud each year. Although more entities experienced an incident of fraud targeting financial benefits, in terms of the numbers of incidents experienced, the most prevalent type involved misuse of information. Over the three years there was a steady increase in the number of incidents categorised as misuse of information, from 721 incidents in 2012–13 to 811 incidents in 2014–15.

In relation to the methods by which internal fraud incidents had allegedly been committed, the

method affecting the highest percentage of entities was misuse of documents and/or information. However, between 2013–14 and 2014–15 there was a slight increase in the number of entities experiencing fraud committed through the misuse of information and communications technologies (ICT) and corruption (increasing from 11% of entities in 2013–14 to 12% of entities in 2014–15 inclusive). The number of internal fraud incidents overwhelmingly involved the misuse of ICT. In 2014–15 there was an increase in the number of incidents of internal fraud committed via misuse of identity and misuse of documents/information.

External fraud

Fraud involving financial benefits was the most frequently reported type of external fraud over the three years, with the proportion of entities experiencing such fraud increasing from 21 percent in 2012–13 and 2013–14 to 25 percent in 2014–15.

The greatest number of external fraud incidents related to government entitlements. This category of external fraud continued to increase, from 90,773 incidents in 2012–13, to 110,698 incidents in 2013–14 and to 125,047 in 2014–15. Fraud of this nature most often involved three subtypes: revenue fraud, visa/citizenship fraud and social security fraud.

Misuse of documents was the most commonly reported method of committing external fraud. The number of entities experiencing external fraud involving corruption declined from 17 percent of entities in 2012–13 to 10 percent of entities in 2014–15. While the largest percentage of entities experienced external fraud involving misuse of documents, the number of incidents experienced within that category declined from 62,382 incidents in 2012–13 to just 2,908 incidents in 2014–15, while at the same time the number of incidents involving misuse of identity rose from 16,967 incidents in 2012–13 to 98,573 incidents in 2014–15. These changes were largely due to one large entity changing the way in which it classified misuse of documents and misuse of identity, and to an increased government focus on identity crime and misuse (AGD 2012).

Cost of fraud

The total reported cost of fraud each year is likely to be an underestimate of actual losses incurred. There are a number of reasons for this difference:

- The research findings are limited to entities that participated in the census and were able to detect (and then quantify losses from) fraud incidents.
- Fraud investigations are becoming longer, which may mean details will not be known for several years to come.
- Some types of fraud cannot be quantified in dollar terms, such as loss of information or accessing ICT systems. While these may cause substantial reputational damage to entities, there is generally a low dollar value (in terms of entity losses) associated with such frauds, although other non-financial impacts can be substantial.

- In addition, there are many associated costs involved with fraud incidents and investigations which are not quantified in the present research, such as time and cost of investigation, monetary value associated with replacing employees, and other indirect costs that may arise with a fraud investigation. Therefore, the present report was only able to provide an estimate of the cost of fraud to the Commonwealth based on data provided by entities from the questionnaires.

Over the three-year period, between 20 and 34 percent of entities were unable to quantify the value of the losses experienced.

The present study asked respondents to indicate the total amount thought to have been lost from fraud incidents, prior to the recovery of any funds and excluding the costs of detection, investigation or prosecution. The responses indicated estimated losses at the time of reporting, as opposed to final losses determined once investigations or criminal action was concluded. Separate questions asked about amounts recovered by entities.

For the three years included in the report, entities reported fraud losses totalling approximately \$1.208b, increasing from \$207m in 2012–13 to \$673m in 2013–14 and reducing to \$329m in 2014–15. The large amount in 2013–14 was due to one entity attempting to quantify the cost of fraud incidents for the first time in 2013–14, while the reduction in 2014–15 was due to the same entity changing the way its losses were quantified.

External fraud caused the vast majority of fraud losses, with external fraud totalling \$1.2b over the three years (99% of all losses incurred). The total reported amount lost due to internal fraud incidents totalled \$11.3m.

Over the three years, internal fraud losses increased by 23 percent between 2012–13 and 2014–15. Losses due to external fraud incidents fluctuated over the three years.

Entities were also asked to indicate how much had been recovered using various means. Their responses related to amounts recovered during the financial year in question and did not necessarily reflect amounts lost due to fraud incidents in the same financial year that recoveries were made. Over the three years, \$1.8m of internal fraud losses and \$48.6m of external fraud losses were recovered, totalling \$50.4m. This equates to approximately four percent of the total losses reported over the three financial years. However, because the recovery process may in some cases take years to finalise, monies recovered within any given financial year may not necessarily align with monies lost in that financial year. As such, it is difficult to determine how much money is ultimately recovered by entities that relate to frauds included in any specific year.

The majority of funds were recovered through the use of criminal proceedings, although administrative remedies and other means were also common ways of recovering lost monies.

How fraud was detected

Between 2012–13 and 2014–15 fraud was most often detected through internal controls, such as auditing or internal investigation of both internal and external fraud incidents. The next most common method used for detecting fraud incidents was by staff. Detection of external

fraud incidents differed from internal fraud, with 'other' methods being the second most commonly reported method of detection; however, a large number of those related to community notifications, which might be considered external whistleblowers.

Only three incidents of internal fraud were detected via the media over the three years. In contrast, the number of external fraud incidents detected via the media increased, from five incidents in 2012–13 to 31 incidents in 2014–15.

Entities with a dedicated fraud control section were more likely to detect fraud incidents than entities without a dedicated fraud control section. This may be because entities with a dedicated fraud control section are likely to be larger entities with more fraud risks, and because an entity with a dedicated fraud section may actively look for incidents involving fraud and potential misconduct.

Investigations within entities

The Commonwealth Fraud Control Framework (AGD 2014) requires entities themselves to investigate routine or minor instances of fraud, and to discipline responsible parties. The findings presented in this report indicate that entities do indeed conduct the vast majority of initial investigations or reviews of fraud allegations. For example, over the three-year period, between 83 and 93 percent of internal fraud incidents were investigated internally by the entity, using an investigation, review or administrative review. As noted above, only a small number of entities without a dedicated fraud control section reported detecting fraud incidents; in 2014–15 over half of those entities still conducted a review/assessment or investigation of the alleged fraud incident.

As with internal fraud investigations, the vast majority of external fraud incidents were primarily investigated by entities themselves, accounting for between 65 and 97 percent of alleged external fraud over the three-year period.

Between 2012–13 and 2014–15, the number of fraud control staff engaged in fraud prevention and investigation duties steadily decreased, from 843 people employed in a fraud prevention capacity in 2012–13 to 804 people in 2014–15.

Police investigations

Over the three years, just over five percent (5.4%) of detected internal fraud incidents were referred to police, prosecution or other organisations for investigation or prosecution (259 incidents referred in total), with just under four percent (3.8%) of external fraud incidents referred to other organisations for investigation or prosecution (15,626 incidents).

Information about the number of referrals received and accepted by the Australian Federal Police (AFP) was also gathered. The AFP accepted 203 of the 239 fraud referrals made to it over the three years. In 2014–15 there was a decrease in the number of matters referred to the AFP and the subsequent matters accepted by the AFP. As of 30 June 2015 the AFP was investigating 160 fraud-related matters with an estimated loss value of \$1.8b.

Prosecution of fraud

Over the three years, 4,214 defendants in fraud-type cases were referred to the Office of the Commonwealth Director of Public Prosecutions (CDPP). Of these, the CDPP prosecuted 3,699 defendants, the majority involving direct referrals from entities rather than referrals via law enforcement agencies.

Between 2013–14 and 2014–15, there was an increase of 17 percent in the number of defendants referred to the CDPP for prosecution. In total, however, the number of defendants prosecuted declined, from 1,271 in 2013–14 to 1,033 in 2014–15.

The total amount initially charged in fraud-type prosecutions decreased from \$41m in 2013–14 to \$25m in 2014–15. The number of convictions declined during the census period, by 22 percent between 2012–13 (1,062 defendants convicted) and 2014–15 (833 convictions).

In 2014–15 there was a change in the most frequently imposed sentence for proved fraud offences. In previous years (2012–13 and 2013–14) the most frequently imposed sentence was a recognisance order; however, a fully suspended term of imprisonment was the most frequently imposed sanction in the current year, followed by recognisance orders. The use of custodial sentences again increased over the three-year period, from 12.5 percent of cases in 2012–13 to 17.3 percent of cases in 2014–15. The sentence imposed depended greatly upon the nature and seriousness of the offence(s) and the various factors relating to each individual defendant, although the increase in harsher sentencing may indicate a change in courts' views regarding fraud offences.

Fraud compliance and prevention

Most non-corporate entities (over 92% each year) met the Commonwealth Fraud Control Framework (AGD 2014) requirement to provide the Australian Institute of Criminology (AIC) with data on fraud incidents and compliance with the terms of the framework.

Over the three years, there was a slight increase in the percentage of entities with a dedicated fraud control section to deal with the prevention, investigation and control of fraud risk—from 74 percent of entities in 2012–13 to 77 percent in 2014–15. The number of staff employed in fraud control activities increased overall, from 3,160 staff in 2012–13 to 3,588 staff in 2014–15. However, the number of fraud control staff with a specific fraud qualification reduced, from 45 percent of all staff in a fraud control section in 2012–13 to 33 percent in 2014–15.

The Commonwealth Fraud Control Framework (AGD 2014) requires a fraud risk assessment to be conducted by entities regularly or when there has been a substantial change to the activities or functions of the entity. Over the three years examined, the percentage of entities complying with this requirement remained high. In 2012–13, 94 percent of entities had completed a fraud risk assessment within the previous two years; in 2013–14, 95 percent of entities had done so; in 2014–15, the percentage reduced slightly to 92 percent.

A high proportion of respondent entities in 2014–15 had completed a fraud control plan within the previous two financial years (91%, N=140). This was similar to the 92 percent (N=152)

which had done so in 2013–14, although it was a decline from the 94 percent (N=153) which had done so in 2012–13.

Fraud awareness training (43% of respondents), compliance with the Commonwealth Fraud Control Framework (39% of respondents) and strong internal controls (21% of respondents) were some of the most frequently cited suggestions for what had made a difference to an entity's fraud prevention in 2014–15.

Fraud risks for the Commonwealth

In the Commonwealth, fraud may be perpetrated by employees or contractors of an entity (internal fraud) as well as by members of the public who have dealings with the government (external fraud), such as when they are obtaining benefits or paying taxes. Fraud risk factors are diverse when dealing with the Commonwealth, as fraud may arise through third-party contractors, procurement processes, provision of government-funded grants, or even overseas cyber attacks.

The principal risks of internal fraud arise from inadequate or outdated internal controls, poor recruitment practices, and insider threats (where staff are compromised or groomed by external parties). External fraud risks arise in connection with the provision of new benefits, failing to build appropriate prevention measures into program and policy design, inadequate procurement practices, new government-funded programs where fraud risks have not been adequately assessed, and Machinery of Government (MoG) changes resulting in new and changing functions for entities.

Between 2012–13 and 2014–15, the number of incidents of external fraud involving the misuse of identity rose by over 450 percent. Identity crime and misuse of documents and information are ongoing areas of risk for Commonwealth entities. Potentially, with more government services moving online, establishing one's identity and the use of identity documents will remain a concern for entities, with effort required to reduce fraud involving these activities.

Belcher review and changes to the questionnaire

The Belcher Red Tape Review was undertaken in 2015, and the report recommended several changes in relation to fraud reporting and the AIC's annual census (Belcher 2015). These included suggestions for reducing the burden associated with completion of the online questionnaire, and combining the Attorney-General Department's (AGD's) annual fraud control compliance report to government with the AIC fraud report to government.

Consultations were undertaken with entities to determine how best to improve and streamline the questionnaire. As a result, the key changes to the 2016 questionnaire will include:

- changing the unit of measurement in the new questionnaire to fraud 'investigations' undertaken each year rather than fraud 'incidents';
- moving the questions about fraud control, in the previously identifiable section collected for the AGD, to the start of the 2016 questionnaire;

- including additional conditional response questions in the online questionnaire, to enable those for whom a section is not applicable to proceed quickly to other sections without having to provide responses;
- adding a new section that examines the most costly external fraud investigations in addition to the previous questions about the most costly internal fraud investigations;
- enabling respondents to respond to both internal and external fraud questions in the one set of questions, to reduce the overall burden of the questions; and
- changing the categories of fraud ‘focus’ and ‘methods of committing fraud’ to ensure the categories are mutually exclusive and as exhaustive as possible.

The purpose of these changes is to increase the internal consistency of how entities report fraud to allow for greater comparisons between census years.

How the information was gathered

Each year Commonwealth entities were invited to participate in an annual census about their experience of fraud incidents, how they managed fraud risks and the entities’ compliance with the former Commonwealth Fraud Control Guidelines (AGD 2011) and the new Commonwealth Fraud Control Framework (AGD 2014) that came into effect on 1 July 2014. The period examined in this report covers the earlier guidelines and the new framework and the differences they may involve. The framework (AGD 2014) consists of:

- section 10 of the Public Governance, Performance and Accountability Rule 2014 (Fraud Rule);
- Commonwealth Fraud Control Policy (Fraud Policy); and
- Resource Management Guide No. 201: Preventing, detecting and dealing with fraud (Fraud Guidance).

Although the three-year period examined is covered by both the guidelines and the framework, for the purposes of this report reference will be made to the 2014 framework now applicable throughout the Commonwealth.

Under the 2014 framework (AGD 2014), fraud against the Commonwealth was defined as ‘dishonestly obtaining a benefit, or causing a loss, by deception or other means’ (AGD 2014: 4.1). Entities were asked to provide information about all suspected and proved incidents of internal and external fraud against the Commonwealth. Further details relating to the data collection procedures are provided in the Methodology section at the end of this report.

Information was provided by 163 entities in 2012–13 (with 162 responses included for analysis), 166 entities in 2013–14 and 154 entities in 2014–15 (for 2013–14 and 2014–15, all responses were included for analysis). Each year, this represents over 80 percent of those invited to participate.

The data collection periods for all three years covered a period of considerable change for the Australian Public Service, as the government implemented a number of MoG changes. A MoG change consists of a variety of organisational or functional changes affecting the

Commonwealth (Department of Finance 2015). These changes were relevant to the collection of fraud information because of the alteration in the number of responding entities as well as changes in their functions during the financial years in question. In some instances MoG changes may have led to investigations being terminated by one entity and taken over by another, which may occasionally have led to inaccuracies in reporting.

Respondents were asked to provide information by completing a secure, online questionnaire that recorded results anonymously (without naming individual entities or individual suspects). The aim was to canvass the experience of fraud across the Australian government as a whole, rather than by identifying what each individual entity had experienced.

Further information on the investigation and prosecution of fraud incidents within the Commonwealth was also provided by the AFP and the CDPP for matters handled within each year (regardless of when they were committed).

Introduction

Fraud is a category of crime that can affect any organisation, regardless of its size or type (Peltier-Rivest & Lanoue 2015). In the Commonwealth, areas particularly at risk of fraud include those relating to the provision of benefits and grants, collection of revenue, procurement, and provision of leave and travel entitlements to public servants. In addition to reducing government revenue and wasting resources, fraud reduces the funds available for delivering public goods and services, undermines public confidence in the government, and damages the reputation of, and morale within, government entities.

The Commonwealth Fraud Control Framework defines fraud against the Commonwealth as ‘dishonestly obtaining a benefit, or causing a loss, by deception or other means’ (AGD 2014: 4.1). It is necessary to prove dishonesty when establishing criminal liability; conduct that is accidental or involves inadvertent error or mere carelessness does not meet acceptable standards of proof. A person must knowingly engage in conduct that is dishonest in order for fraud to be present, such as by not applying for leave when taking time off work (a form of internal fraud) or not providing accurate information on a form when seeking government benefits (a form of external fraud). Benefits are not limited to a financial gain and may be direct or indirect. A benefit does not need to be directly related to the person committing fraud, as the benefit could be for a third party—for example, providing information about an upcoming tender to a friend in order to help their business.

Commonwealth entities are attractive targets for persons wishing to commit fraud, as they have extensive resources, including equipment, property, money and information, to name a few. Fraud may be committed by those external to an entity or those employed within an entity. The perpetrator may not always be located in Australia, especially in relation to fraud relating to online transactions. Entities need to know where their fraud risks lie, the types of fraud likely to be perpetrated against them, how long fraudulent conduct lasts and the financial losses incurred. Providing information of this nature is one of the principal aims of the present research, so that Commonwealth entities will be well placed to understand fraud risk and respond effectively.

Comparable research has been conducted overseas. For example, the Report to the Nations by the Association of Certified Fraud Examiners (ACFE) for 2016 examined 2,410 fraud cases from around the world and found the cases considered involved \$6.3b of fraud losses. The report also found asset misappropriation to be the most common form of occupational fraud, occurring in more than 53 percent of cases analysed (ACFE 2016).

The United Kingdom (UK) National Audit Office (2016) also recently reviewed internal and external fraud experienced by government departments (excluding tax and welfare fraud, where the risks and losses were already well known). The review involved interviewing

representatives from the Cabinet Office fraud, error and debt team, and fraud representatives from five government departments, in addition to departmental self-assessments about fraud from select departments. The review found that government departments experienced 52 instances of internal fraud in the 2014–15 financial year, totalling £1.6m. The principal internal fraud risks identified by departments were:

- travel and subsistence claims;
- staff reporting of abuse; and
- change of supplier details (by employees) for payment (UK NAO 2016).

Departments in the UK reported 47 instances of external fraud (excluding tax and welfare), totalling £30.5m in 2014–15. The differences between the number of frauds reported in the UK and in Australia relate primarily to the fact that the UK data exclude cases of suspected revenue and welfare fraud, which account for high numbers in the Australian data. The areas of perceived fraud risk identified by departments for external fraud included:

- the processes and payments people apply for, such as identity documents, student support payments and benefit payments;
- inappropriate grant payments; and
- external contracts/subcontracts (UK NAO 2016: 14).

Australian Commonwealth entities face many of the same fraud risks as those identified by UK government departments (Jorna & Smith 2015). While some fraud risks are well known, fraud is becoming more complex and diverse, and some changes pertaining to economic crime may not be as well known or as easily recognised by entities (PwC 2016; UK NAO 2016). The changing nature of fraud means it may become harder to detect and investigate, and even harder to prove, resulting in the need to update or change current fraud risk policies to keep pace with technology and changing patterns of risk.

It is unlikely that fraud will ever be eliminated; it is also unlikely that the true extent of fraud will ever be known. Nonetheless, attempts must be made both to prevent fraud to the best of an organisation's ability and to ensure there are suitable mechanisms in place to detect and quantify the full extent of the problem (Gee & Button 2015). In Australia, fraud is one area of crime that is not decreasing, unlike other types of property crime (Figure 1; ABS 2016).

Figure 1: Number of recorded offenders whose principal offence was fraud, 2010–11 to 2014–15, Australian Bureau of Statistics



Source: Australian Bureau of Statistics 2016, Recorded crime - offenders 2014–15

Global industry surveys have also shown that the number of organisations experiencing fraud around the world has either increased or remained constant. Kroll's (2015) report on global fraud found that 75 percent of organisations participating in the survey had experienced a fraud incident in 2015–16, an increase of 14 percent from three years earlier. A global fraud survey by PricewaterhouseCoopers (PwC 2016) found 36 percent of respondent organisations had experienced a fraud incident in 2015, which was very similar to the 37 percent of responding organisations that experienced fraud in 2014 but an increase on the number of organisations affected in 2011 (34%).

While recorded incidents of fraud are increasing, it should be noted that discovering fraud is not necessarily a bad thing: it does not necessarily mean an organisation has poor fraud controls in place but could indicate a greater ability to detect and quantify fraud that has occurred. For example, ACFE (2016) found that, the longer a fraud went undetected, the higher the losses incurred by the organisation. Conversely, an organisation reporting an absence of fraud does not necessarily mean that fraud has not occurred—simply that it has not been uncovered (UK NAO 2016).

The present research provides a better indication of the extent of fraud occurring in the public sector than simply relying on officially recorded crime statistics, as the entities who respond to the AIC's census are well placed to understand the nature and scope of fraud that has occurred within their own organisations and can report on fraud dealt with by means other than a criminal investigation. Clearly, some fraud will never be detected, or will not be detected for many years; apart from these cases, the results of the present census give a good indication of the extent of the problem as it affects Commonwealth entities.

The fraud framework

On 1 July 2014 the Commonwealth Fraud Control Framework replaced the Commonwealth Fraud Control Guidelines (AGD 2011). The framework (2014) was developed in line with the change in Commonwealth resource management under the Public Governance, Performance and Accountability Act 2013 (Cth; PGPA Act), which moved from a compliance approach to a principles-based framework.

The framework 2014 consists of:

- section 10 of the Public Governance, Performance and Accountability Rule 2014 (Fraud Rule);
- Commonwealth Fraud Control Policy (Fraud Policy); and
- Resource Management Guide No. 201: Preventing, detecting and dealing with fraud (Fraud Guidance).

These provisions seek to protect public resources, including information and property, and the integrity and good reputation of entities and the Commonwealth. Although the framework 2014 came into effect on 1 July 2014, in the data collection period for this report, the references used throughout the report are consistent with the 2014 framework.

What the report covers

The annual census covers all incidents of suspected fraud, incidents under investigation, and completed investigations, whether the fraud was proved or not, and whether the incident was dealt with by a criminal, civil or administrative remedy. This report presents the results of the analysis of this information for the years 2012–13 to 2014–15. Details of the methodology used to gather the information, response rates and how the data were analysed are set out at the end of this report.

The results are presented in six distinct sections covering:

- key trends in fraud incidents experienced by entities over the three-year period;
- types of fraud incidents, descriptions of fraud targets and fraud modus operandi;
- the cost of fraud to entities, focusing on the amount initially lost due to fraud and amounts recovered;
- the manner of detection and investigation of fraud incidents;
- prevention, fraud control measures and compliance with the Fraud Rule experience within Commonwealth entities; and
- changes to the 2015–16 data collection processes.

Trends in suspected fraud

This section presents data from the three years examined on reporting entities' experience of fraud, including whether suspects were located within or external to an entity, the size of the entity, the number of incidents detected, and information about the suspects involved. Internal fraud was defined as any incident of fraud or suspected fraud allegedly committed by an employee or contractor of an entity, while external fraud was defined as any incident of fraud or suspected fraud allegedly committed by a person other than an employee or contractor of the entity. Where an employee or contractor was alleged to have committed fraud in collaboration with an external party, this was categorised as collusion—for counting purposes, this was included within internal fraud rather than external fraud. The three years covered in this report are 2012–13, 2013–14 and 2014–15, extending from 1 July 2012 to 30 June 2015. During the three-year period examined, there were substantial changes to some entities (eg MoG changes), some of which are reflected in the data presented.

Experience of fraud

Respondents were asked to indicate whether or not their entity had identified or were informed of alleged incidents of internal or external fraud. Over the three financial years 2012–13 to 2014–15, the percentage of entities that did not experience any fraud in the previous financial year declined, from 61 percent in 2012–13 to 58 percent in 2014–15. Compared with 2013–14, in 2014–15 there were higher percentages experienced in all fraud types (Table 1).

Table 1: Number and percentage of entities experiencing fraud, 2012–13 to 2014–15 (N&%)

Year	Respon- dents	No fraud experienced			Fraud experienced		Solely internal fraud experienced		Solely external fraud experienced		Collusion experienced		Entities experiencing both types of fraud	
		N	N	%	N	%	N	%	N	%	N	%	N	%
2012-13		162	98	61	64	40	45	28	48	30	5	3	29	18
2013-14		166	107	64	59	36	44	27	46	28	4	2	31	19
2014-15		154	89	58	65	42	47	31	49	32	5	3	31	20

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

In 2014–15, 16 entities experienced only internal fraud and 18 entities experienced only external fraud. Even though not all entities experienced fraud, all entities need to be aware of the risks they face with both internal and external fraud. Many factors influence an entity's fraud detection. These may involve strong detection mechanisms and fraud control policies which enable them to uncover fraudulent activity. However, an organisation not detecting fraud risks does not mean the entity does not have a fraud risk.

Figure 2 presents data on the difference between the percentage of entities experiencing internal fraud and external fraud incidents over the last five years. More entities experienced internal fraud in 2010–11 compared with those that experienced external fraud. In 2011–12 the difference between the percentage of entities experiencing external and internal fraud decreased, and from 2013–14 there was only a one percent difference between the percentage of entities experiencing external and internal fraud.

Figure 2: Percentage of entities experiencing internal and external fraud over five years, 2010–11 to 2014–15 (%)



Source: Commonwealth fraud census 2010–11, 2011–12, 2012–13, 2013–14 and 2014–15 [AIC computer file]

Figure 3 presents data on the changes over the years in the percentage of entities experiencing the different fraud types (internal, external, both or collusion). On the whole, a higher percentage of entities experienced at least one fraud incident in 2014–15 than in the other two years included in the report. In addition to more fraud being experienced by entities, in 2014–15 a higher percentage of entities had incidents of both internal fraud and external fraud compared with the previous years (with internal fraud rising from 28% in 2012–13 to 31% in 2014–15, and external fraud rising from 29% in 2012–13 to 32% in 2014–15). In addition, during the three years, the percentage of entities that experienced incidents of both internal and external fraud rose from 18 percent in 2012–13 to 20 percent in 2014–15. The number of

entities not experiencing fraud declined, from 64 percent in 2013–14 to 58 percent in 2014–15 (see Table 1), whereas the percentage of entities experiencing any fraud increased between 2013–14 and 2014–15 (from 36% in 2013–14 to 42% in 2014–15).

Figure 3: Entities experiencing fraud by type, 2012–13 to 2014–15 (%)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Extent of fraud

Respondents were also asked to indicate the total numbers of incidents of internal fraud, external fraud, collusion and frauds that they could not classify as involving either internal or external fraud. These questions were the only ones which distinguished between internal fraud and collusion. The remaining questions required respondents to include incidents involving collusion within the category of internal fraud.

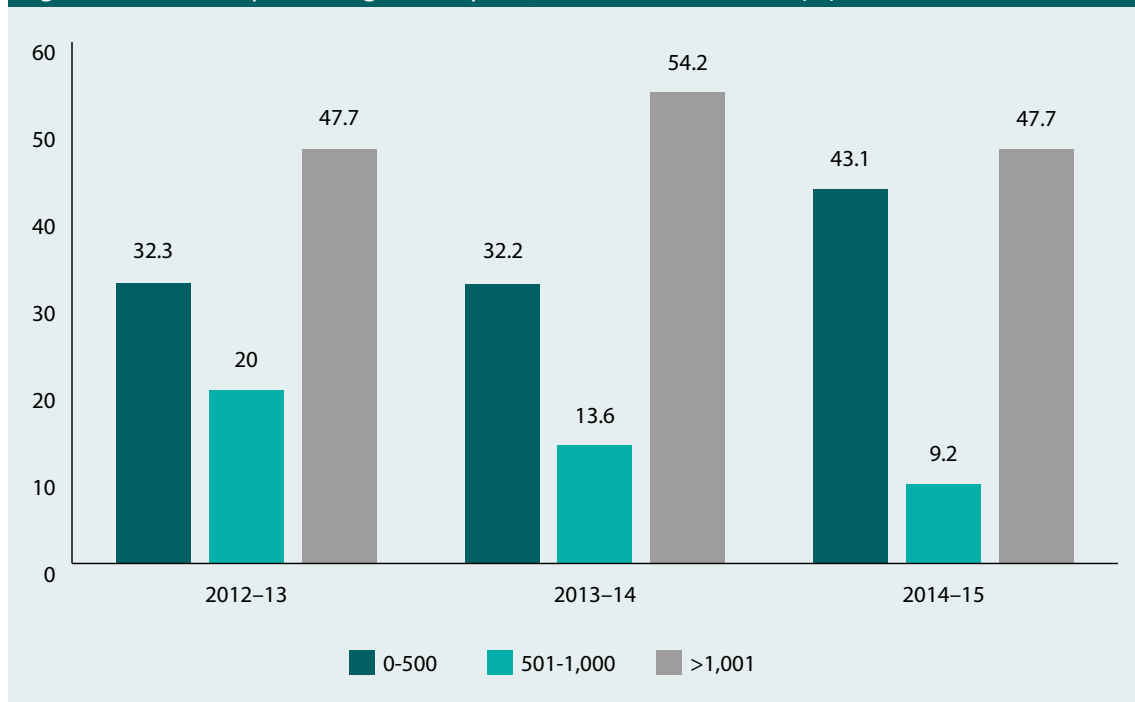
The number of alleged incidents of solely internal fraud experienced by entities declined over the three years, from 1,685 incidents in 2012–13 to 1,485 in 2014–15 (Table 2). The number of alleged incidents of solely external fraud experienced by entities during the three years fluctuated slightly (as indicated in Table 2), from 133,969 incidents in 2012–13 to 154,221 in 2014–15, with a decline in 2013–14. The number of incidents of collusion experienced by entities in 2014–15 increased to 107 from only four in the previous financial year.

Table 2: Incidents involving internal and external fraud, collusion and unclassified incidents (N)					
Year	Solely internal fraud	Solely external fraud	Collusion	Unclassified	Total
2012–13	1,685	133,969	17	1	135,672
2013–14	1,658	123,876	4	428	125,965
2014–15	1,485	154,221	107	30	155,843

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Figure 4 presents information on entities' experience of fraud in terms of the number of staff employed. Over the three years, entities with more than 1,000 staff consistently experienced more fraud than smaller entities (see Figure 4 and Table 3); however, in 2014–15 there was an increase in the percentage of entities with 500 or fewer employees experiencing fraud. Mid-sized entities employing between 501 and 1,000 staff experienced the least fraud incidents of all three size groups over the three years.

Figure 4: Entities experiencing fraud by size, 2012–13 to 2014–15 (%)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Although mid-sized entities (501–1,000 employees) experienced less fraud than other entities (see Table 3), they comprised only a small percentage of all Commonwealth entities. Small-sized entities (those with 500 or fewer employees) contributed to approximately 65 percent of all Commonwealth entities participating in the annual census. However, a relatively small proportion of small-sized entities experienced an incident of fraud compared with entities of other sizes. By contrast, entities with more than 1,000 employees experienced fraud at higher rates than entities of other sizes.

Table 3: Number of entities that experienced fraud by entity size and year (N)									
Staff (N)	2012–13 (N=162)			2013–14 (N=166)			2014–15 (N=154)		
	N	%	Total (N)	N	%	Total (N)	N	%	Total (N)
0–500	21	20.0	105	19	16.5	115	28	25.9	108
501–1,000	13	54.2	24	8	50.0	16	6	46.2	13
≥1,001	31	93.9	33	32	91.4	35	31	93.9	33
Total	65		162	59		166	65		154

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Larger Commonwealth entities are more likely than smaller ones to have dedicated fraud control personnel. This is in part due to the higher fraud risk that larger entities face and also the availability of resources to allocate staff to specific fraud control activities. An analysis was undertaken of entity size, the presence of dedicated fraud control staff, and experience of fraud during the three years, with results presented in Table 4.

Table 4: Number of entities by fraud section, experience of fraud and year (N)						
Fraud experience	0–500 staff (N)		501–1000 staff (N)		≥1001 (N)	
	No fraud section	Fraud section	No fraud section	Fraud section	No fraud section	Fraud section
2012–13 No fraud experienced	32	52	2	9	1	2
2012–13 Fraud experienced	2	19	3	10	2	28
2013–14 No fraud experienced	37	59	1	7	1	2
2013–14 Fraud experienced	3	16	2	6	0	32
2014–15 No fraud experienced	29	51	2	5	0	2
2014–15 Fraud experienced	3	25	0	6	2	29

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Entities were divided into two groups: those that had at least one person who worked in a fraud control capacity, and those that did not have any employees working in fraud control. Entities with more than 1,000 employees were more likely to have at least one person spending a portion of their time dedicated to fraud control. Entities with 500 or fewer employees were the least likely to have anyone who worked at least part-time in fraud control. Each year there were small numbers of entities where fraud was experienced but the entity did not have at least one employee who had a dedicated fraud control role. Even some of the large entities that had no dedicated fraud control staff experienced fraud. These findings could indicate a need for specific fraud control staff to be appointed.

Internal fraud trends

While the number of entities experiencing internal fraud incidents remained relatively constant over the three years, the number of incidents reported declined by 12 percent (see Table 5). Both the mean and median number of incidents per entity decreased between 2012–13 and 2014–15, although reductions were relatively small.

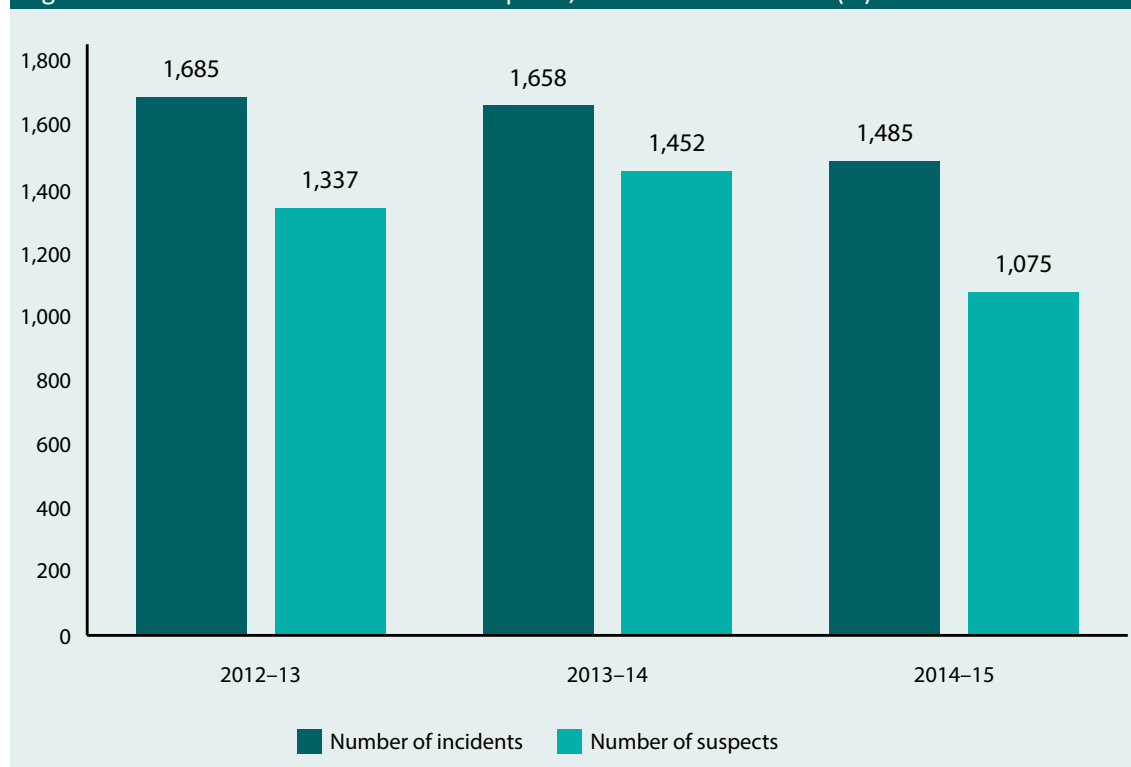
Table 5: Internal fraud summary results (N)

Year	Entities (N)	Total incidents (N)	Mean incidents (N)	Median incidents (N)	Range for incidents (N)
2012–13	45	1,685	37	5	1–633
2013–14	44	1,658	39	3	1–557
2014–15	47	1,485	32	2	1–600

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Figure 5 shows the number of internal fraud suspects identified by entities, compared with the number of internal fraud incidents reported by entities each year for the three-year period. The rates of suspects identified per number of incidents of internal fraud remained fairly constant over the three years. For example, in 2012–13 there were 1.3 internal fraud incidents per suspect identified, in 2013–14 there were 1.1 (very close to a suspect identified for every incident) and in 2014–15 there were 1.4.

Figure 5: Internal fraud incidents and suspects, 2012–13 to 2014–15 (N)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

External fraud trends

External fraud has always posed a greater risk for Commonwealth entities because of the extensive payments made by large entities (Jorna & Smith 2015), and in 2014–15 this continued to be the case. The higher levels of external fraud compared with internal fraud incidents experienced by Commonwealth entities' differs from other non-government organisations (KPMG 2014). In 2014–15 the number of entities reporting external fraud increased to 49 entities (32% of all participating entities, N=154), from 46 entities in 2013–14. In addition to an increase in the number of entities experiencing external fraud between 2012–13 and 2014–15, the number of external fraud incidents increased by 23 percent, from 125,541 incidents in 2013–14 to 154,221 incidents in 2014–15. From Table 6 it is apparent that the mean number of incidents experienced by entities decreased by almost 60 percent, from 7,768 in 2013–14 to 3,147 in 2014–15. Although more entities reported an external fraud incident in 2014–15, on the whole those entities experienced fewer incidents of external fraud. It is noteworthy that in 2014–15 one entity accounted for 60 percent of incidents reported by all entities.

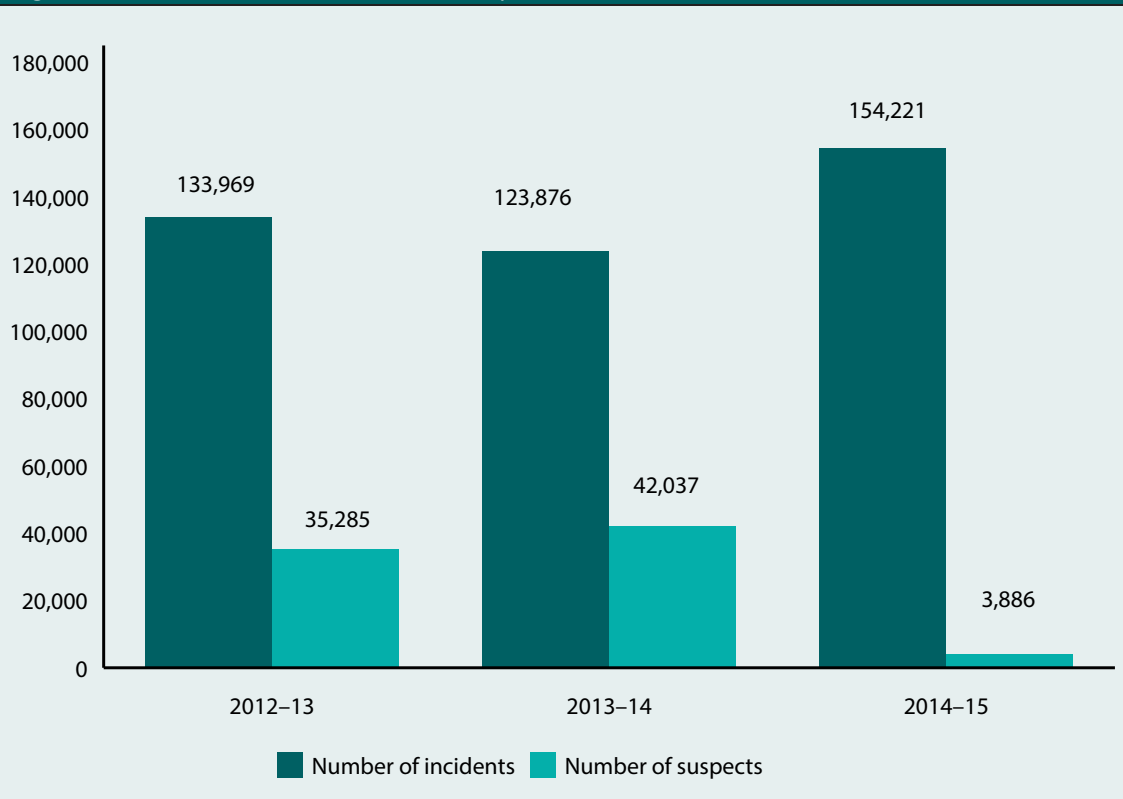
Table 6: External fraud summary results (N)

Year	Number of entities	Total incidents	Mean incidents	Median incidents	Range for incidents
2012–13	48	133,969	2,791	9	1–97,216
2013–14	46	125,541	7,768	8	1–78,461
2014–15	49	154,221	3,147	5	1–92,778

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

The increase in the number of reported external fraud incidents was not matched by an increase in the number of suspects (Figure 6). In 2014–15 only 3,886 suspects were identified for the 154,221 incidents reported, corresponding with one suspect being identified for every 39.3 incidents. This compares with one suspect being identified for every 2.9 external fraud incidents in 2013–14. This decline may be because some respondents were not in a position to identify specific suspects, such as where fraud had only recently been detected and investigations commenced.

Figure 6: External fraud incidents and suspects, 2012–13 to 2014–15 (N)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

How fraud was committed

The definition of fraud against the Commonwealth is extremely broad and can include anything from theft of Commonwealth property to accessing information without proper authority. This diversity makes it challenging to develop meaningful and policy-relevant classifications of how fraud was committed. The census asked respondents to indicate two main aspects of how the fraud incidents they detected had been committed—their focus, or the target of the alleged fraudulent activity and/or the benefit to be derived from the suspected illegal conduct, and the method used to carry out the alleged activity (such as misuse of technology, information, identity etc).

Five categories of focus were examined:

- equipment such as computers or consumable stock;
- entitlements such as travel and expense claims;
- information such as misuse of intellectual property;
- financial benefits such as misuse of petty cash or credit cards in the case of internal fraud, or dishonest claims for welfare and other benefits in the case of external fraud; and
- an 'other' category, for any incidents that did not fall into one of the four specified categories.

Because fraud incidents could entail more than one type of focus, respondents were at liberty to provide multiple focuses for each incident if appropriate; therefore, the total number of responses exceeds the number of separate incidents.

Respondents were also asked to choose from among four methods by which the incidents were committed:

- misuse of ICT;
- misuse of identity;
- misuse of documents or information; and
- acts of corruption (such as paying or accepting bribes or kickbacks).

In addition, an 'other' option could be selected where the method of fraud was not specified. As was the case with the focus questions, respondents were able to provide multiple responses in relation to each fraud incident.

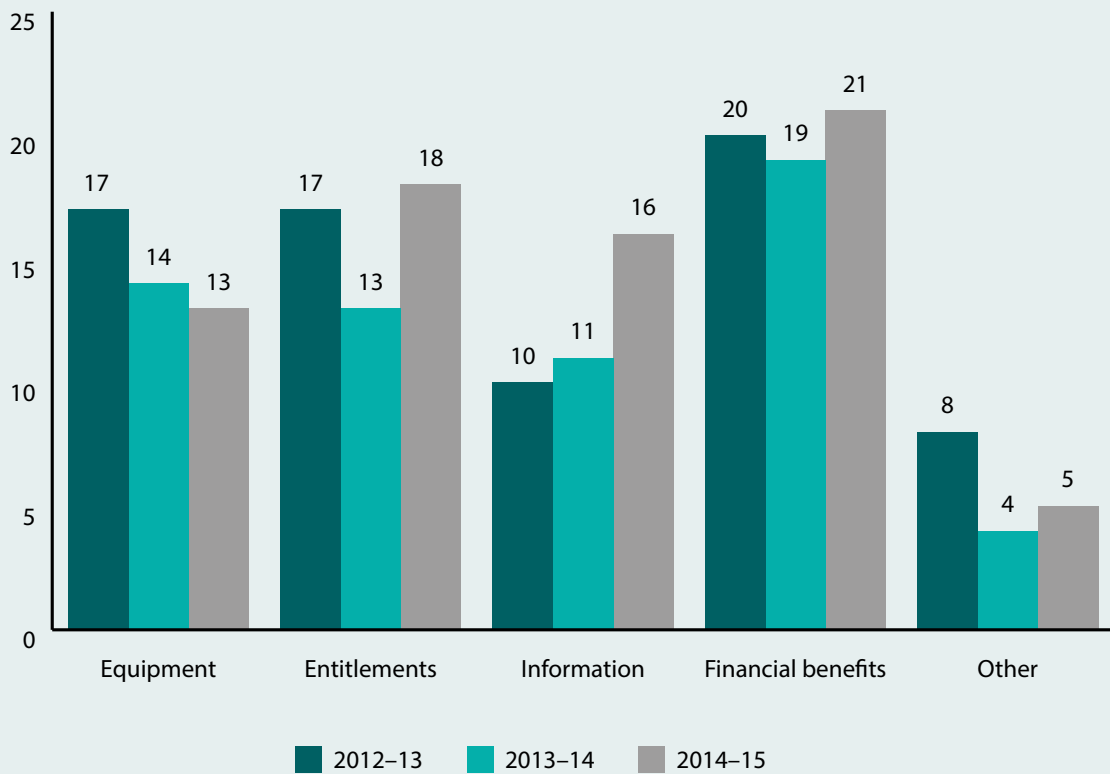
Aggregate data on both focus of fraud and methods in terms of the number of entities and number of incidents are provided in the appendix to this report. For discussion purposes, selected results are presented in the following section.

Internal fraud

Focus

The most prevalent focus of internal fraud was financial benefits (such as obtaining cash without permission or misuse of government credit cards), as has been the case for the past three years, with approximately 20 percent of entities reporting this type of fraud each year (Figure 7). However, in contrast with previous years, in 2014–15 equipment (such as theft of computers or Commonwealth property) was no longer the second most cited focus of fraud. In 2014–15, 18 percent of respondents reported their entities experienced an internal fraud where the focus was on entitlements (such as abuse of travel or leave allowances), an increase from the 13 percent of reporting incidents with that focus in 2013–14. There was an increase in the number of entities that had experienced an incident of fraud focused on information, from 11 percent in 2013–14 to 16 percent in 2014–15. Unauthorised access of information and misuse of information held by entities remains a serious concern for Commonwealth entities.

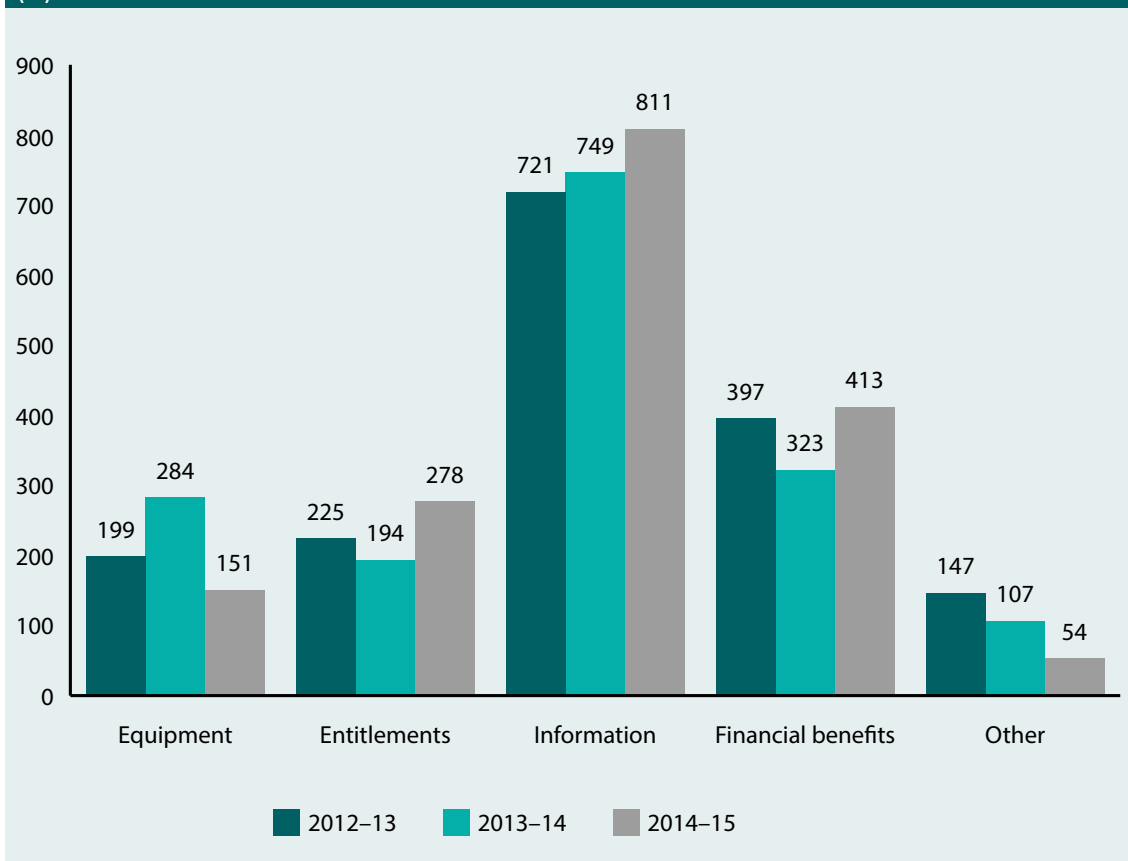
Figure 7: Internal fraud focus categories and entities affected, 2012–13 to 2014–15 (%)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

In terms of incidents for each focus type, there was an increase in the number of incidents involving entitlements, information and financial benefits between 2013–14 and 2014–15. Fraud focused on both equipment and other types decreased between 2013–14 and 2014–15. While there is little to indicate a trend in the type of focus being targeted by internal fraudsters, in the past three years the number of incidents involving accessing and/or misusing information increased, from 721 incidents in 2012–13 to 749 incidents in 2013–14, again increasing to 811 incidents in 2014–15 (Figure 8). Information was the most frequently cited internal fraud type for all three years.

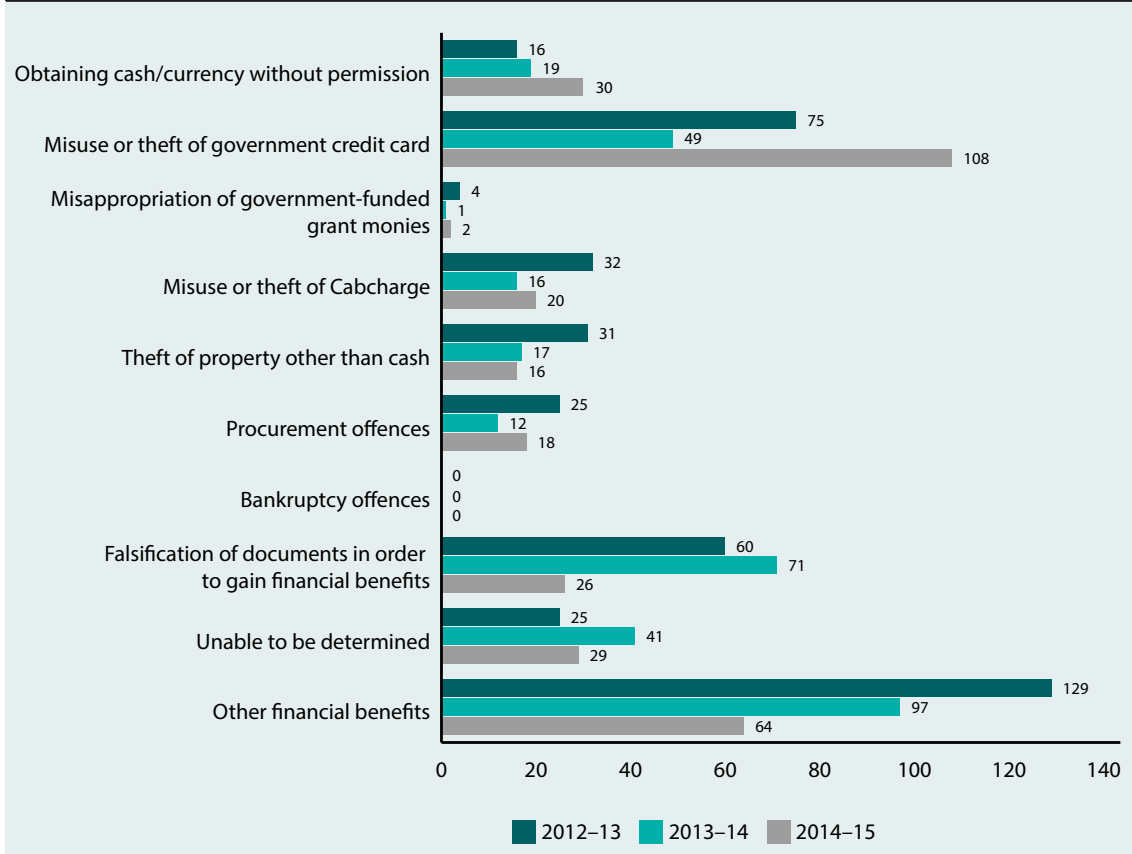
Figure 8: Internal fraud focus categories and number of alleged incidents, 2012–13 to 2014–15 (N)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Few patterns were discernible after reviewing the incidents of financial benefit fraud reported by respondents. In 2014–15 more incidents of misuse or theft of government credit cards were reported (108 incidents), representing an increase of 120 percent on the 49 incidents of that type in 2013–14. As in previous years, none of the responding entities experienced incidents of bankruptcy offences (Figure 9).

Figure 9: Internal fraud involving financial benefits subcategories and alleged incidents, 2012–13 to 2014–15 (N)

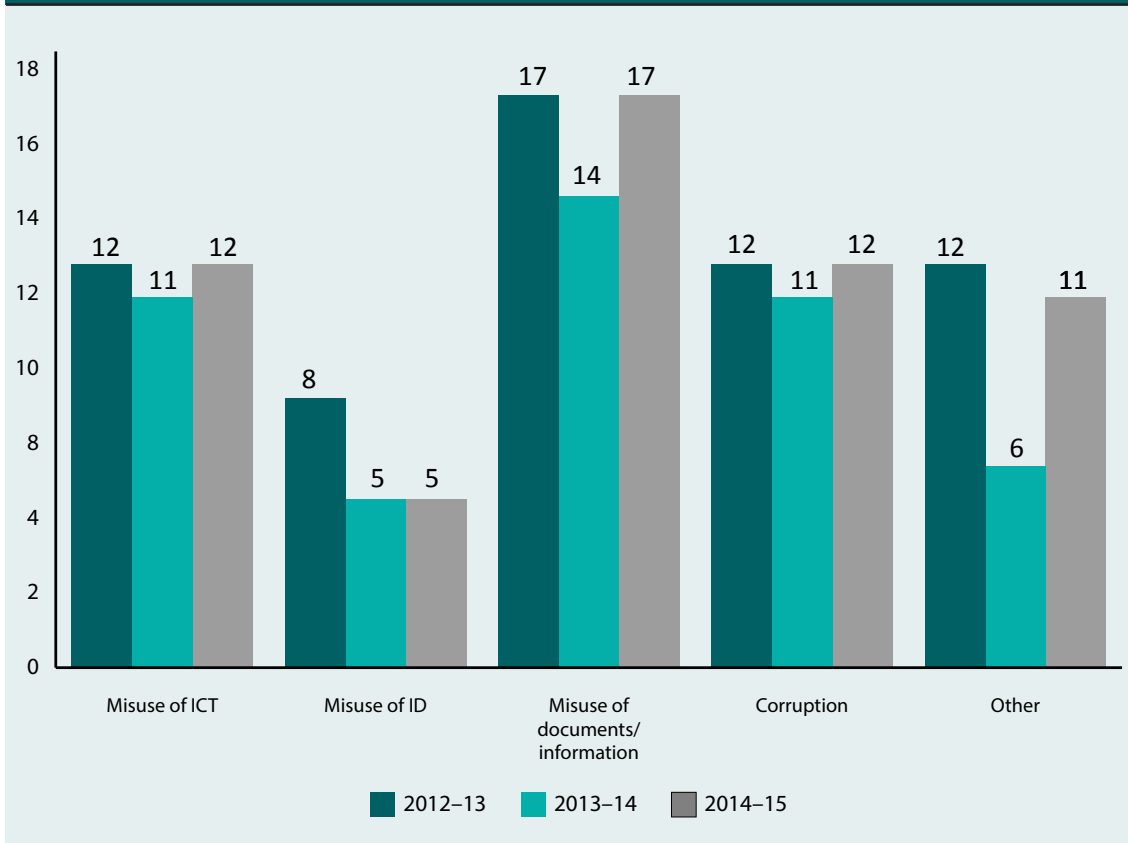


Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Method

In 2014–15 the method most commonly cited by respondents (not including the ‘other’ methods category) was misuse of documents. This method was also the most frequently reported method in 2012–13 and 2013–14 (Figure 10). Misuse of documents included various subcategories for the use of information and/or documents. In 2014–15, the most commonly reported categories were creating and/or using a false or altered entity document, creating and/or using a false or altered document (not belonging to the entity), and failing to provide documents when required to do so.

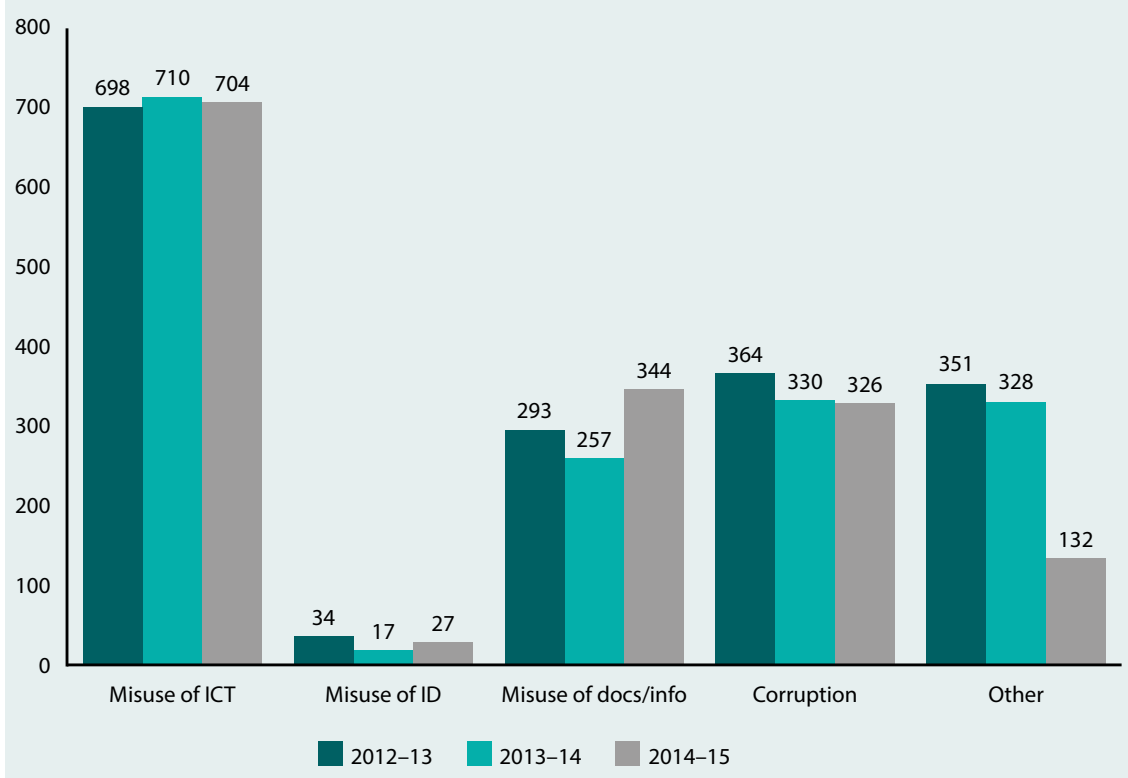
Figure 10: Percentage of entities affected by fraud, by internal fraud method category, 2012–13 to 2014–15 (%)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Although misuse of documents/information was the method that affected more entities, the category where the most incidents were recorded was misuse of ICT (Figure 11). While fewer entities reported experiencing a fraud incident involving that particular method, the entities that did experience fraud involving misuse of ICT experienced incidents in greater numbers than other method types. The numbers of incidents experienced each year by entities for that particular internal fraud method remained fairly constant. In 2014–15, there was an increase in the number of incidents involving misuse of documents/information, and a decrease in the number of incidents involving other methods.

Figure 11: Number of alleged internal fraud incidents by fraud method, 2012–13 to 2014–15 (N)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Table 7 presents the subcategories of the misuse of ICT category. Over the past three years, the method subcategory ‘accessing information or programs via a computer without authorisation’ was the most common method used to commit internal fraud. The numbers of incidents recorded for that subcategory fluctuated slightly over the three years, although in 2014–15 the number of incidents increased by five percent, to 617 incidents.

Table 7: Internal fraud committed by misuse of ICT subcategories, number of alleged incidents, 2012–13 to 2014–15 (N)

Misuse of ICT	2012–13	2013–14	2014–15
Accessing information or programs via a computer without authorisation	612	588	617
Copying or altering data or programs without authorisation	26	18	10
Misuse of email	25	82	48
Manipulation of a computerised accounting system	24	3	5

Insertion of malicious code	2	0	0
Interference with computer networks	0	0	0
Unable to be determined	3	1	7
Other misuse of IT	6	18	17

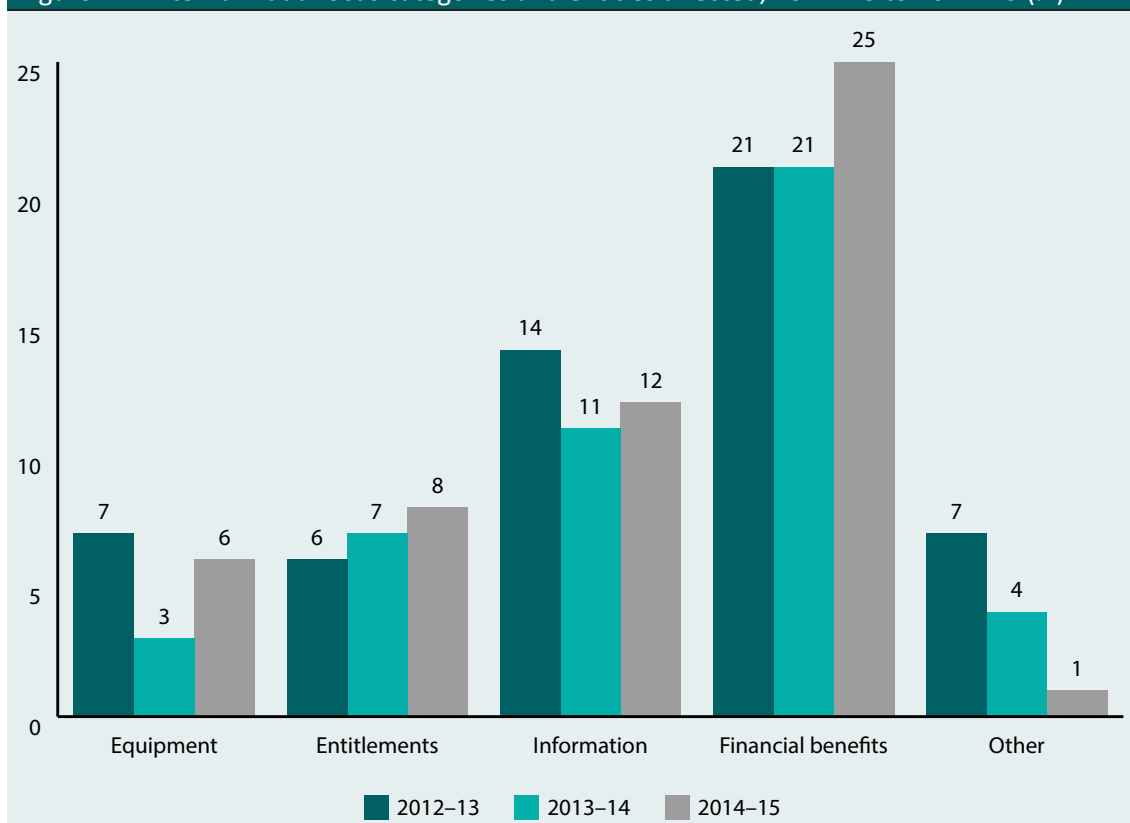
Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

External fraud

Focus

Fraud involving financial benefits was the most frequently reported target of external fraud for the 2014–15 financial year. This was consistent with earlier years (Lindley, Jorna & Smith 2012), although the percentage of entities affected by that fraud type rose in 2014–15 to 25 percent (Figure 12). As in previous years, the next most common target of external fraud was information, affecting 12 percent of reporting entities in 2014–15. Respondents reported a slight increase in the number of entities where fraud targeted entitlements; however, the percentage of entities affected remains low, increasing from six percent in 2012–13 to eight percent in 2014–15.

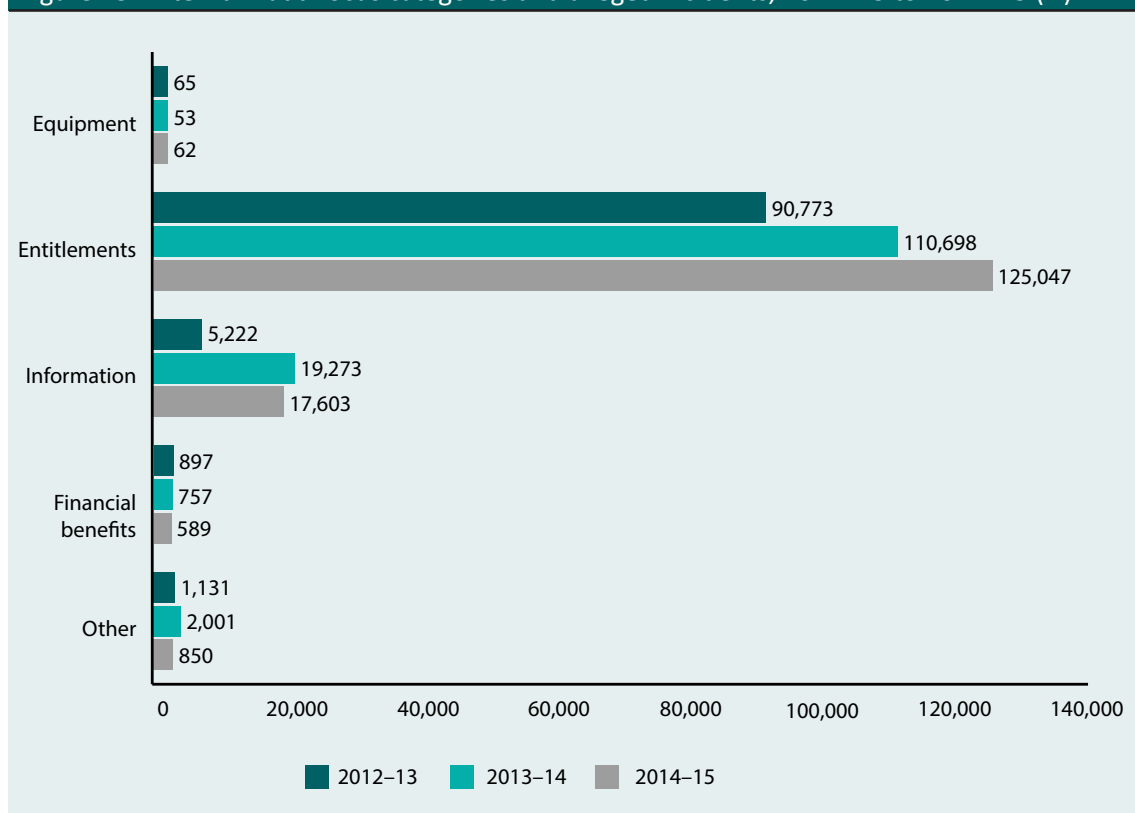
Figure 12: External fraud focus categories and entities affected, 2012–13 to 2014–15 (%)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

In terms of reported incidents of external fraud, however, the vast majority involved fraud relating to government entitlements. The numbers of incidents reported fluctuated substantially, with a large increase from 90,773 incidents in 2012–13 to 110,698 incidents in 2013–14, further increasing to 125,047 incidents in 2014–15 (Figure 13). Although more entities experienced fraud focused on financial benefits, the actual numbers of incidents were low, whereas, although fewer entities experienced external fraud focusing on entitlements, those entities that did experience that type of fraud did so more frequently. This finding is not unexpected, as those categories include some of the larger entities providing services to the public.

Figure 13: External fraud focus categories and alleged incidents, 2012–13 to 2014–15 (N)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Entitlement fraud most often involved three main types: revenue fraud, visa and citizenship fraud, and social security fraud arising from the three large service provider entities (Table 8). It is apparent from these data that the manner in which these large entities classified and counted fraud incidents changed considerably over time, thus affecting the total numbers recorded each year, rather than reflecting actual changes in the incidence of social security, health, welfare and revenue fraud. In particular, in 2014–15 one large entity reclassified ‘revenue fraud’ as ‘other entitlements’.

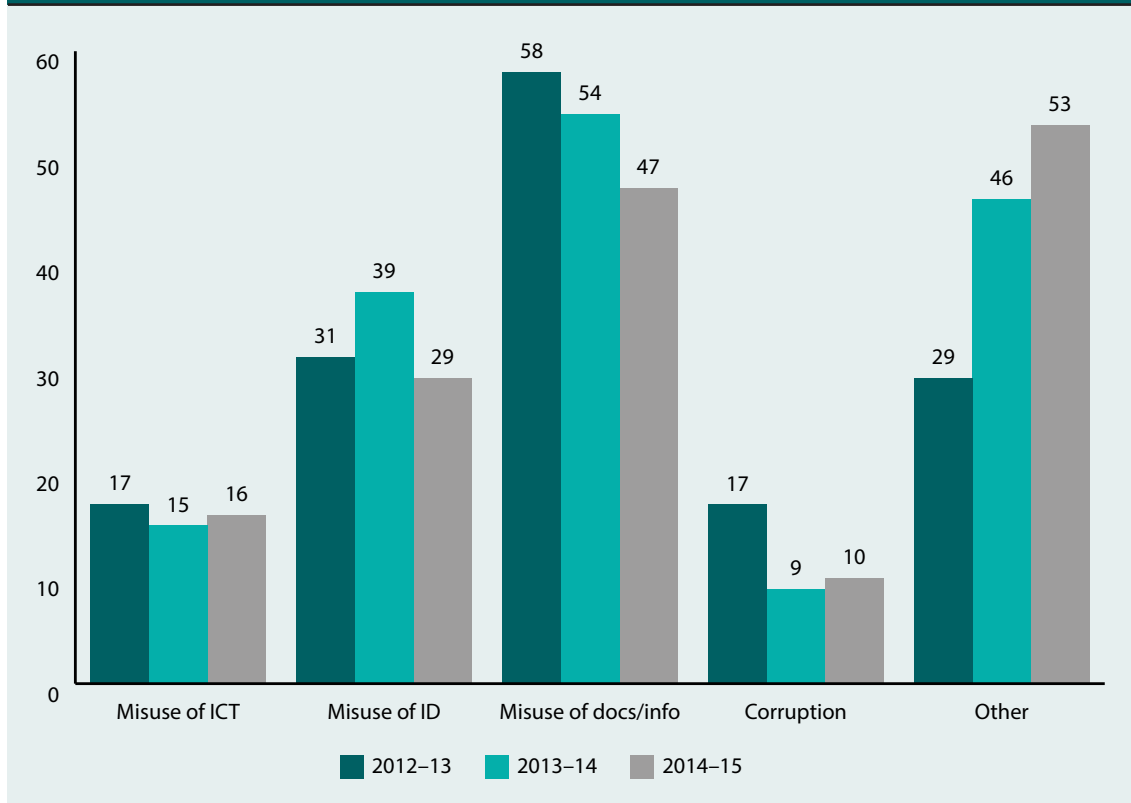
Table 8: Entitlement fraud subcategories and alleged incidents, 2012–13 to 2014–15 (external fraud) (N)			
Entitlements categories—External fraud	2012–13	2013–14	2014–15
Misusing or claiming benefits without entitlement relating to housing	0	0	1
Misusing or claiming benefits without entitlement relating to social security	3,254	2,641	2,351
Misusing or claiming benefits without entitlement relating to health benefits	390	327	1,187
Misusing or claiming benefits without entitlement relating to visas/citizenship	28,142	27,206	28,166
Misusing evading or claiming benefits without entitlement relating to child support	232	305	65
Revenue fraud	58,364	79,495	1
Customs and excise fraud (evading excise)	299	0	456
Unable to be determined	13	486	0
Other entitlements	79	239	92,820

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Method

Figure 14 presents data on the percentages of entities experiencing external fraud in terms of the methods employed. The data presented for 2014–15 differed from previous years, with the highest percentage of entities in 2014–15 reporting external fraud allegedly committed through ‘other’ means (53%). In earlier years the method category cited by more entities was misuse of documents and information; in 2014–15 this was the second most frequently cited method of committing external fraud, with 47 percent of entities that experienced an external fraud incident citing that method. Some of the examples supplied by respondents that could not be attributed to the other categories provided included ‘false statements’ (just under 9,000 incidents), ‘not specified in data system’ (1,200 incidents), ‘counterfeit money used’, ‘theft’, and ‘cannot be categorised’.

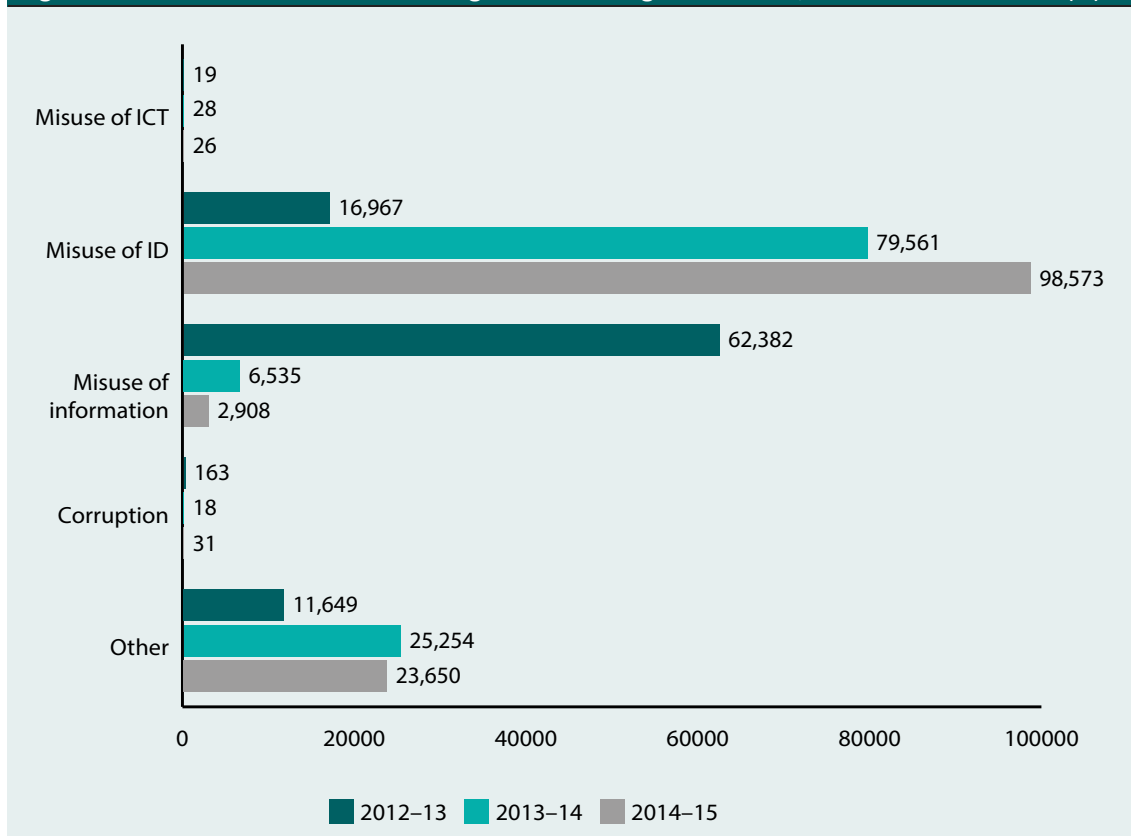
Figure 14: External fraud method categories and entities affected, 2012–13 to 2014–15 (%)



Note: Multiple methods may have been selected; percentages will not total 100

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Figure 15: External fraud method categories and alleged incidents, 2012–13 to 2014–15 (N)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

While more entities may have categorised methods of committing fraud as 'other', overwhelmingly more incidents involved misuse of identity (Figure 15). In 2014–15, external fraud involving misuse of identity increased, from 79,561 incidents in 2013–14 to 98,573 in 2014–15 (a 24% increase). This may be due to the increased focus on identity misuse by the Commonwealth under the National Identity Security Strategy (AGD 2012) and the need for entities to improve their data holdings relating to identity crime and misuse (see also AGD 2015). By way of contrast, the number of incidents of fraud involving misuse of information and/or documents declined, from 62,382 incidents in 2012–13 to just 2,908 incidents in 2014–15. However, this somewhat substantial change was due to one large entity changing the way it recorded a large number of incidents. In 2012–13 the incidents had been recorded as 'other misuse of information/documents'; however, in 2013–14 and 2014–15 the incidents were recorded as 'other misuse of identity'. As there is some potential overlap between these two categories, this was not viewed as an anomaly but rather something to be noted should changes be made to the questionnaire in the future. This change in the way the entity recorded incidents caused the large differences between the years.

The value of fraud

Assessing the scale of loss due to fraud is an important component in developing approaches for reducing the impact of fraud on Commonwealth entities. A number of limitations and difficulties are associated with trying to quantify the value of fraud against the Commonwealth. These include:

- determining whether to attempt to quantify the cost of suspected incidents as initially detected or those that have been substantiated through investigation or court proceedings;
- determining whether to include the costs of investigation and prosecution; and
- determining how to quantify the time lost due to fraud investigations, and the costs of replacing staff dismissed due to committing fraud; and
- fraud, like other crime types, is not detected 100 percent of the time; there are always unknown or unreported incidents that will be unable to be costed (Smith et al. 2014).

A number of approaches were adopted to provide a general indication of gross costs of suspected fraud detected by Commonwealth entities. Respondents were, at the outset, asked to indicate the total number of fraud incidents that had been identified or that the entity was informed of, how many persons were alleged to have committed them and what financial losses were suffered as a result. Losses were defined as funds thought to have been lost by the entity prior to the recovery of any funds and excluding the costs of investigation or prosecution. Thus, respondents were asked to report the dollar value of suspected fraud, rather than fraud that had been substantiated following investigation or judicial proceedings.

Respondents were also asked to indicate any amounts recovered using criminal or civil proceedings or other administrative methods of recovery. This excluded money that was recovered by the Commonwealth that was not returned to the entity in question, such as fines or the proceeds of confiscation orders that remain in consolidated revenue.

The results presented below examine the value of fraud in terms of incidents that solely involved internal fraud, incidents that solely involved external fraud, incidents that involved collusion between entity employees and external parties, and fraud that could not be classified by entities in any of these ways. Further analyses examined the fraud costs in terms of the various focus categories described above. The results presented below invariably either underestimate the actual financial impact, particularly where the scope of fraud is found to be more extensive after investigation, or overestimate the loss where fraud is not proved or less extensive than originally reported.

Value of fraud by type

Table 9: Dollar value of suspected fraud incidents by type of fraud, 2012–13 to 2014–15 (\$)

Year	Internal fraud	External fraud	Collusion	Unclassified	Total
2012–13	3,426,546	203,270,364	402,764	3,031	207,102,705
2013–14	3,607,740	669,282,134	0	34,200	672,924,074
2014–15	4,225,288	324,701,760	0	32,229	328,959,277
Total three years	11,259,574	1,197,254,258	402,764	69,460	1,208,986,056

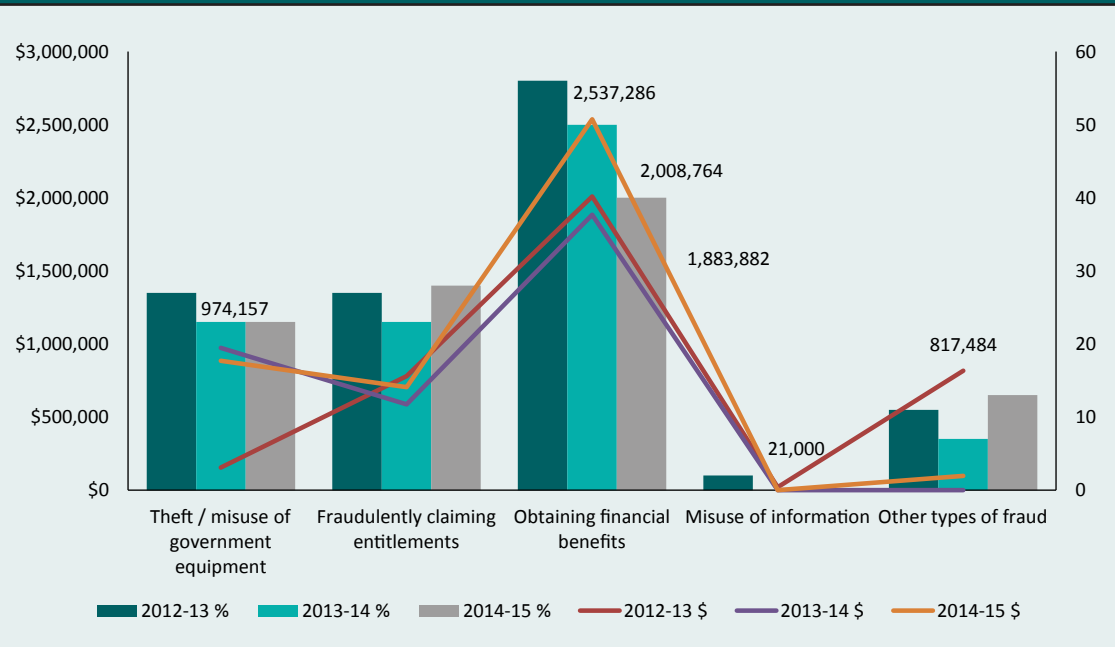
Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Not all entities were able to quantify the value of the fraud incidents they experienced. In 2012–13, 51 out of 64 (80%) were able to quantify losses, decreasing to 39 out of 59 (66%) entities in 2013–14 and increasing to 80 percent (52 out of 65) in 2014–15. There was a large increase in the total value of fraud incidents between 2012–13 (\$207m) and 2013–14 (\$673m); however, this amount decreased in 2014–15 to \$329m (Table 9). While the overall total fraud losses decreased between 2013–14 and 2014–15, the losses due to internal fraud continued to increase over the three years, from \$3.4m in 2012–13, to \$3.6m in 2013–14 and to \$4.2m in 2014–15.

Value by focus category

Figure 16 and Table 10 present data on the reported value of internal and external fraud, respectively, in terms of the percentages of entities experiencing such incidents and the focus of incidents. The dollar values largely follow the distribution of entities' experience of fraud types, with the highest values involving fraud relating to obtaining financial benefits—for both internal and external fraud. For the purposes of this analysis, incidents involving collusion were merged with the reported incidents of internal fraud.

Figure 16: Internal fraud focus categories by dollar value and percentage type of fraud incidents, 2012–13 to 2014–15 (\$&%)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Figure 16 shows that more entities experienced an incident of internal fraud and lost money due to internal fraud aimed at financial benefits. The largest dollar amount lost to that fraud type in 2014–15 was over \$2.5m. In 2013–14 and 2014–15 entities did not report losing any money due to internal fraud focused on misuse of information, for which it is difficult to quantify in terms of dollars.

There were large differences between the years examined with respect to the costs of external frauds focusing on financial benefits. This is at odds with the numbers of incidents reported by entities (see Figure 11 above), which showed that, although fewer entities experienced fraud focusing on entitlements, the number of incidents was substantially higher for that fraud type than any other. Potentially, these differences are due to the way in which entities interpret a financial benefit as opposed to an entitlement. In various parts of the questionnaire, specific categories were provided to assist respondents in determining how incidents should be classified. In the section of the questionnaire that asks about losses incurred, no subcategories are provided. Therefore, the difference between a loss due to fraud focused on entitlements or financial benefits is based on the interpretation of the respondent, as ultimately both frauds involve a financial gain.

Table 10: External fraud focus categories by dollar value and percentage of entities affected, 2012–13 to 2014–15 (\$&%)						
Focus category	2012–13		2013–14		2014–15	
	% of entities	Amount lost	% of entities	Amount lost	% of entities	Amount lost
Theft/misuse of government equipment	19	47,645	7	159,592	16	38,884
Entitlements	8	41,224,059	9	56,149,054	12	51,246,981
Financial benefits	54	161,143,720	57	569,697,462	53	265,362,759
Misuse of information	8	731,027	2	88,500	2	933,941
Other fraud	4	124,742	9	426,200	12	4,885,549

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Table 10 presents data on dollars lost by entities for the different fraud categories. In 2013–14 the least amount lost by entities pertained to fraud focused on misuse of information; however, in 2012–13 and 2014–15 the least amount lost by entities with respect to fraud focused on information. Overwhelmingly, external fraud involving financial benefits resulted in the highest loss values for all three years included in the report. Between 2013–14 and 2014–15, the amount lost due to financial benefit fraud more than halved. Corresponding to that decrease, fewer entities experienced an external fraud involving financial benefits in 2014–15.

Recovered funds

Respondents were asked to indicate the whole dollar amount that had been recovered in each financial year using various methods. This excluded money that was recovered by the Commonwealth that had not been returned to the entity in question, such as fines or the proceeds of confiscation orders that remained in consolidated revenue. The amounts recovered did not necessarily relate to the value of the fraud detected in the same year, as recovery of funds could have related to incidents committed or detected in previous financial years. Accordingly, it was not possible to indicate the net actual losses suffered each year, as often recovery action took many years to finalise. In addition, losses were estimates only and did not include money spent replacing staff or hardening targets.

Table 11: Amounts recovered by entities for both internal and external fraud, 2012–13 to 2014–15 (number of entities involved in recoveries in parentheses) (\$)			
Year	Internal fraud (\$)	External fraud (\$)	Total amount recovered (\$)
2012–13	794,027 (19 entities)	9,142,614 (18 entities)	9,936,641
2013–14	572,182 (15 entities)	19,480,142 (16 entities)	19,980,324
2014–15	457,230 (12 entities)	20,008,829 (25 entities)	20,466,059
Total	1,823,439	48,559,585	50,383,024

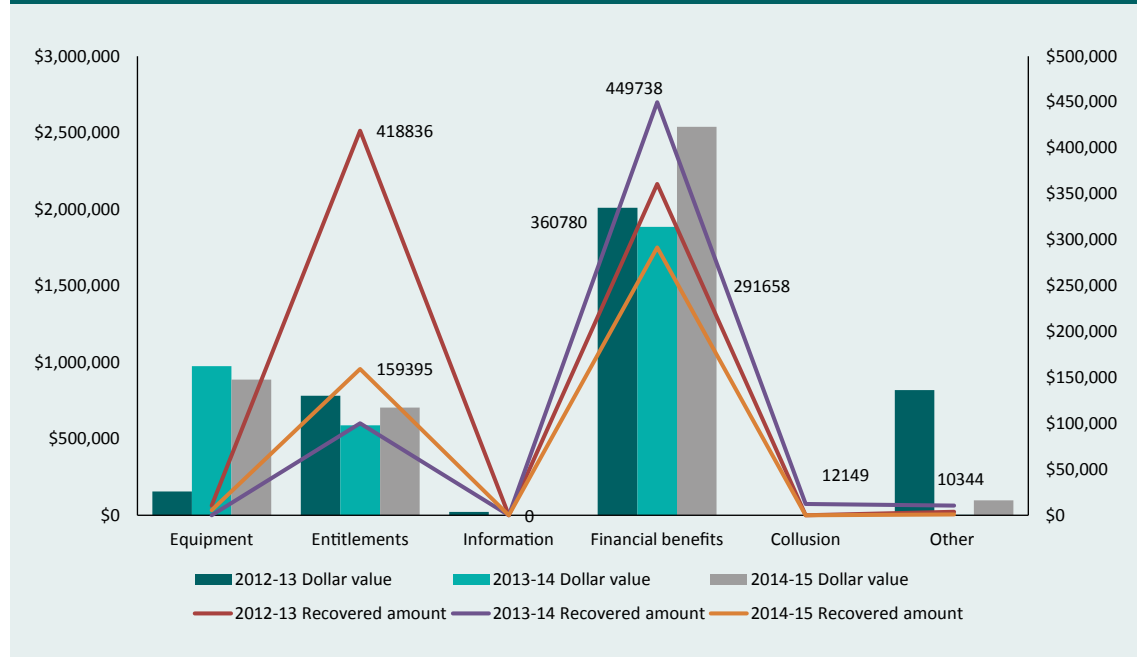
Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

For the three years, \$1.8m was recovered in respect of internal fraud, and \$48.6m in respect of external fraud, totalling just over \$50.3m (Table 11). Although these sums recovered do not necessarily relate to reported losses over the same years, it is clear that sums recovered represent a small proportion of losses suffered by entities. For example, over the three years, reported losses totalled in excess of \$1.2b.

Amounts recovered by focus category

Figure 17 shows the reported dollar value of losses due to internal fraud by focus category and the amounts recovered each year. Financial benefit fraud was responsible for the highest internal fraud losses and the largest recovery amounts, followed by entitlement fraud. Between 2012–13 and 2013–14, there was a decline in the amount recovered involving allegations of fraud focused on equipment and entitlements. In 2013–14 no monies were recovered with respect to fraud incidents relating to equipment. For all three years, no monies were recovered with respect to fraud losses involving information. In 2013–14 an amount was recovered from fraud losses involving collusion, although the figure did not correspond to loss of monies from fraud involving collusion in that year. However, the recovery may have related to fraud detected in earlier years.

Figure 17: Internal fraud focus categories by dollar value and amounts lost and recovered (\$)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Table 12 shows the reported cost of fraud in each of the three years and the amounts recovered each year by external fraud focus category. Fraud incidents involving financial benefits and entitlements were responsible for the highest external fraud losses and the largest amounts recovered, as was the case with internal fraud incidents. As these fraud types had the largest losses, it would be expected that they would also have larger recovery values. Over the three years, there was a substantial increase in monies recovered relating to financial benefits. In 2012–13 entities recovered \$4.1m of funds with respect to financial benefits, in 2013–14 the amount recovered was \$14.9m and in 2014–15 the amount recovered was \$20.1m.

Table 12: External fraud focus categories by dollar value and amounts recovered, 2012–13 to 2014–15 (\$)

Fraud focus	2012–13		2013–14		2014–15	
	Dollar value of fraud	Amount recovered	Dollar value of fraud	Amount recovered	Dollar value of fraud	Amount recovered
Equipment	47,645	15,075	159,592	8,123	38,884	18,241
Entitlements	41,224,059	4,663,245	56,149,054	4,445,767	51,246,981	2,738,155
Information	731,027	10,377	88,500	44,370	933,941	154,796
Financial benefits	161,143,720	4,097,807	569,697,462	14,907,123	265,362,759	20,150,143
Unclassified fraud	124,742	356,110*	426,200	2,759	4,885,549	2,554

Note: '*' Recoveries could relate to earlier years and therefore do not relate directly to the dollar value of fraud losses for that year.

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Amounts recovered by method of recovery

Commonwealth entities recover fraud losses in a variety of ways, including through orders made during criminal proceedings, civil legal recovery, administrative means and other ways. Respondents were asked to indicate amounts recovered during each financial year (irrespective of when the fraud actually occurred or was detected) for each fraud focus category. Over the three years of census data, respondents provided information about the method of recovery for 6,724 incidents (Table 13). The most prevalent means of recovering funds varied depending on the fraud focus category. For example, criminal proceedings was the most prevalent type of recovery for frauds that focused on financial benefits, with over \$37m recovered by that method; however, for frauds focused on entitlements more money was recovered through the use of administrative remedies (\$11.3m).

Table 13: Monies recovered in 2012–13 to 2014–15 by method of recovery and incident focus category (\$&N)

Fraud focus		Criminal	Civil	Administrative remedy	Other	Total
Equipment	Dollars	0	0	47,301	10,210	57,511
	Incidents	0	0	77	10	87
Entitlements	Dollars	705,693	2,000	11,266,536	551,120	12,525,349
	Incidents	40	1	2,535	43	2,619
Information	Dollars	104,223	0	50,464	54,856	209,543
	Incidents	25	0	41	71	137
Financial benefits	Dollars	37,798,273	2,468	3,017,715	383,256	41,201,712
	Incidents	3,189	1	468	214	3,872
Other	Dollars	3,800	0	356,446	5,693	365,939
	Incidents	2	0	5	5	9
Total		38,611,989	4,468	14,738,462	1,005,135	54,360,054 (6,724 incidents)

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Over the three years of census data, the recovery of funds in conjunction with criminal proceedings remained the method by which the largest funds were recovered by entities. In 2014–15 the amount recovered by that method increased in terms of frauds focused on financial benefits, information and entitlements. No money was recovered via that method for fraud losses involving equipment or other fraud focuses during the 2013–14 and 2014–15 financial years (Table 14).

Table 14: Monies recovered using criminal action by focus category by year recovered (\$)

Fraud focus	2012–13	2013–14	2014–15	Total
Equipment	0	0	0	0
Entitlements	10,825	214,847	480,021	705,693
Information	10,377	44,370	49,477	104,224
Financial benefits	3,642,672	14,242,847	19,912,691	37,798,210
Other	3,800	0	0	3,800

Source: Commonwealth Fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Dealing with fraud

Fraud against the Commonwealth may be detected in a variety of ways. It may be discovered through regular fraud risk management activities or uncovered inadvertently when a staff member leaves their employment or takes leave, allowing accounting inconsistencies to become apparent. Other staff or external parties may also report their suspicion of fraud—sometimes anonymously, or through hotlines available in the workplace or externally. Some of the largest Commonwealth entities also engage in sophisticated data mining and analytics in which accounting and other anomalies are identified and analysed for signs of fraud.

This study explores how fraud was detected within entities and how fraud involving members of the public was identified, with the aim of understanding how entities became aware of suspected incidents of fraud, how these were investigated, and the extent to which they were referred to police and prosecution agencies. Data came from the annual census undertaken by the AIC, and from separate reports provided to the AIC by the AFP and CDPP which included information on fraud-related investigations and prosecutions undertaken each year.

How fraud was detected

Respondents were asked to indicate the primary method by which incidents of internal and external fraud were detected. Nine categories were provided, along with options for other methods of detection to be reported and if it was unknown or not recorded how the fraud was discovered. The results for each year are shown in Table 15 (internal fraud) and Table 16 (external fraud).

Table 15: Methods of detecting internal fraud incidents, 2012–13 to 2014–15 (N)						
Method of detection	2012–13		2013–14		2014–15	
	N	%	N	%	N	%
Credit card issuer	2	0.1	1	0.1	4	0.2
Media	2	0.1	1	0.1	0	0
External audit	27	1.6	11	0.7	3	0.2
Offender self-reported	27	1.6	8	0.5	6	0.3
Not recorded/unknown	3	0.2	7	0.4	49	2.8
Notification by police	36	2.1	8	0.5	26	1.5
External whistleblower	144	8.5	117	7.5	113	6.5
Internal anonymous whistleblower	70	4.1	76	4.9	59	3.4
Staff member	507	29.8	536	34.3	535	30.9
Internal controls	862	50.6	798	51.0	890	51.4
Other	23	1.4	1	0.1	46	6.3

Note: In the 2014–15 census multiple entities provided multiple responses; therefore, the number of ways incidents were detected exceeds the number of incidents reported. Internal incidents detected in 2014–15 was 1,485, not the total number in Table 15.

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Generally, internal controls were responsible for the highest number of detections of internal fraud each year (Table 15). The other main avenue of discovery of internal fraud was through the actions of staff members employed by the entities. There were no incidents of internal fraud detected by the media in 2014–15. In 2014–15 the number of internal fraud detected by other methods increased to 46 incidents (from 23 incidents detected by that method in 2012–13, and from just one in 2013–14). Examples of other method of detection in 2014–15 included Public Interest Disclosure statements and external anonymous complainants.

Overwhelmingly, internal controls and audits were the most common methods of detecting external fraud. Detection by staff and other methods was also frequent (Table 16).

Table 16: Methods of detecting external fraud incidents, 2012–13 to 2014–15 (N)						
Method of detection	2012–13		2013–14		2014–15	
	N	%	N	%	N	%
Credit card issuer	17	<0.1	np	np	51	<0.1
Media	5	<0.1	4	<0.1	31	<0.1
External audit	7	<0.1	15	<0.1	288	0.2
Offender self-reported	2	<0.1	1	<0.1	1	<0.1
Notification by police	60	0.1	1,508	1.2	1,613	1.0
External whistleblower	1,729	1.9	25,630	20.2	476	0.3
Internal anonymous whistleblower	27	<0.1	3	<0.1	2	<0.1
Staff member	2,019	2.2	6,551	5.2	3,501	2.3
Internal controls/audits	34,544	38.3	89,449	70.6	110,894	72.0
Not recorded/unknown	36	<0.1	1,848	1.5	82	0.1
Other	51,803	57.4	1,676	1.3	37,060	24.1

Note: 'np' indicates that the category was not provided that year

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Examples of detection methods included in the other methods category included 35,322 incidents that were categorised only as community (reported by a single entity). These may have been tip-offs or other methods included in the external whistleblower category, as were other incidents listed as compliance-related tip-offs. The inclusion of those methods in the other category may indicate that some respondents felt the term ‘whistleblower’ did not adequately describe a tip-off, or perhaps respondents did not understand the scope of all the categories provided. If the tip-off methods (if they were all related to tip-offs) were included in the external whistleblower category then that category would be the second most frequently used method for detecting external fraud incidents in 2014–15.

In contrast to the way internal fraud incidents were detected, there was an increase in the number of external fraud incidents detected via the media in 2014–15, although this was largely due to one entity that reported 29 of the 31 incidents.

Fraud was also detected through the work of staff in dedicated fraud control sections who undertook fraud risk analysis and investigated anomalies in accounting and other procedures. Such sections are more likely to be present in the largest entities that experience more incidents of suspected fraud. Table 17 shows that, over the three years, entities with a dedicated fraud control section were more likely to detect fraud incidents than those without a dedicated fraud control section.

Table 17: Detection of fraud by presence of a fraud control section in entities (N)

Presence of a fraud control section	Internal fraud incident experienced			External fraud incident experienced			Any fraud incident experienced		
	2012–13	2013–14	2014–15	2012–13	2013–14	2014–15	2012–13	2013–14	2014–15
Yes	39	40	42	46	43	48	57	54	60
No	6	4	5	2	3	1	7	5	5

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

The findings were fairly consistent over the three years reviewed. Each year a small number of entities did not have a fraud control section where fraud was detected; however, the majority of entities that detected fraud had a dedicated fraud control section. Employees play a substantial role in detecting and preventing fraud. When employers dedicate some of their full-time equivalent (FTE) staff to fraud control, they ensure the entity has trained individuals who are able to identify warning signs of fraud and know how to deal with investigations and entity responses (ANAO 2011).

How fraud was investigated

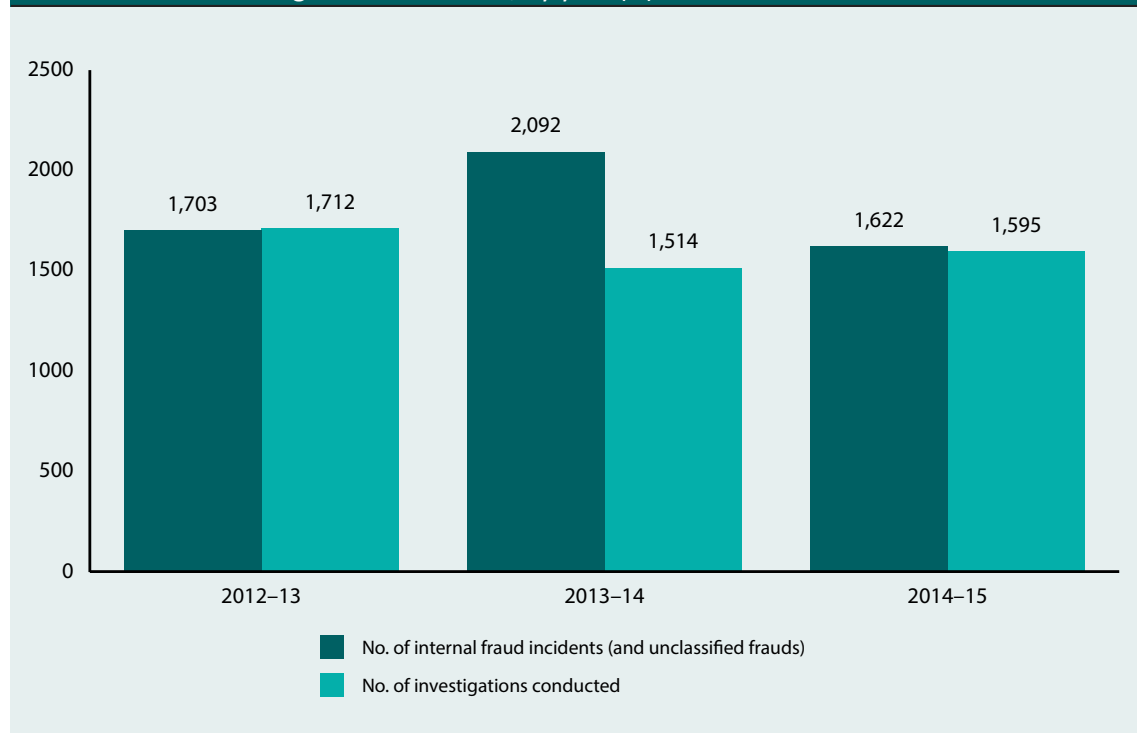
Under the Commonwealth Fraud Control Framework 2014, an entity is responsible for investigating instances of fraud or suspected fraud against it, including investigating disciplinary matters, unless the matter is referred to and accepted by the AFP or another law enforcement agency (AGD 2014: B2). The purpose of a fraud investigation is to gather evidence about a specific allegation or fraud incident (ANAO 2011). The investigation should also consider any

suitable action to be taken with respect to the matter. If the AFP declines to accept the referral, entities must conduct an investigation internally in accordance with Commonwealth guidelines. Investigators and investigations must also meet the requirements set out in the Australian Government Investigations Standards (AGIS; AGD & AFP, 2003, 2011).

Who conducted investigations

The findings presented in this report indicate that entities do indeed conduct the vast majority of initial investigations or reviews of fraud allegations. For example, in 2014–15, 83 percent of incidents were investigated internally, either by an investigation, review or administrative investigation. Similarly high percentages of suspected internal fraud allegations were investigated or reviewed internally in 2012–13 (93%) and in 2013–14 (88%). Figure 18 presents information pertaining to internal fraud, collusion and unclassified frauds and the number of investigations conducted by entities. Entities were asked to initially provide details about any internal investigation or review of an incident that they had conducted, and then provide details about investigations conducted by organisations external to the entity. In some cases, more than one investigation may have been conducted.

Figure 18: Alleged internal fraud incidents (including collusion and unclassified fraud) and total number of investigations conducted, by year (N)

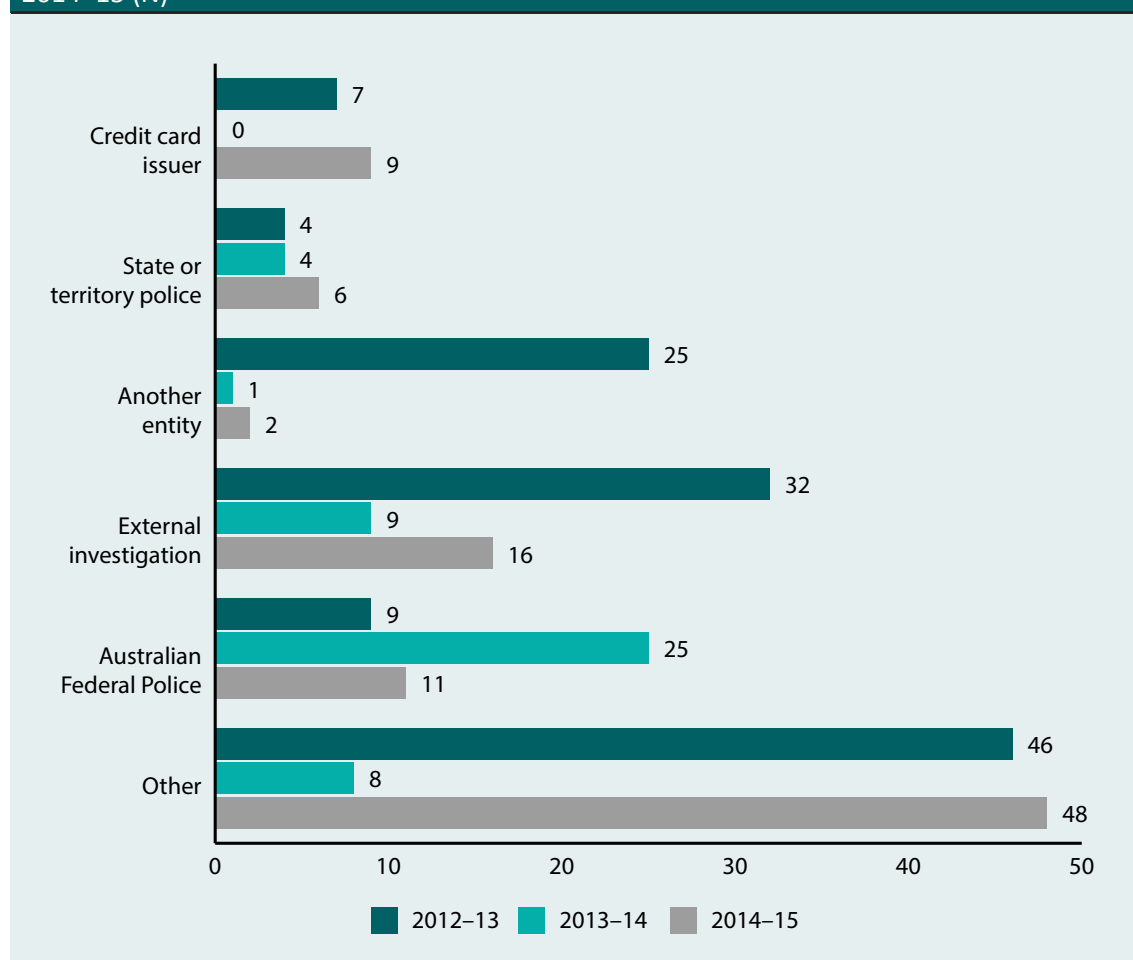


Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Respondents were also asked to indicate the number of incidents of alleged internal fraud that were investigated or reviewed externally, once an internal investigation or review had been completed. Figure 19 shows the numbers of incidents investigated primarily by various external organisations.

As presented in Table 4 above, in 2014–15 five entities where suspected fraud incidents were detected did not have dedicated fraud sections (the majority of incidents related to internal fraud; however, one entity also experienced one incident of external fraud). Three of those entities conducted internal reviews or investigations of the alleged incidents, and another used an external investigator to review the alleged fraud incident. No details were supplied for the other fraud incident, or how the external fraud incident was investigated.

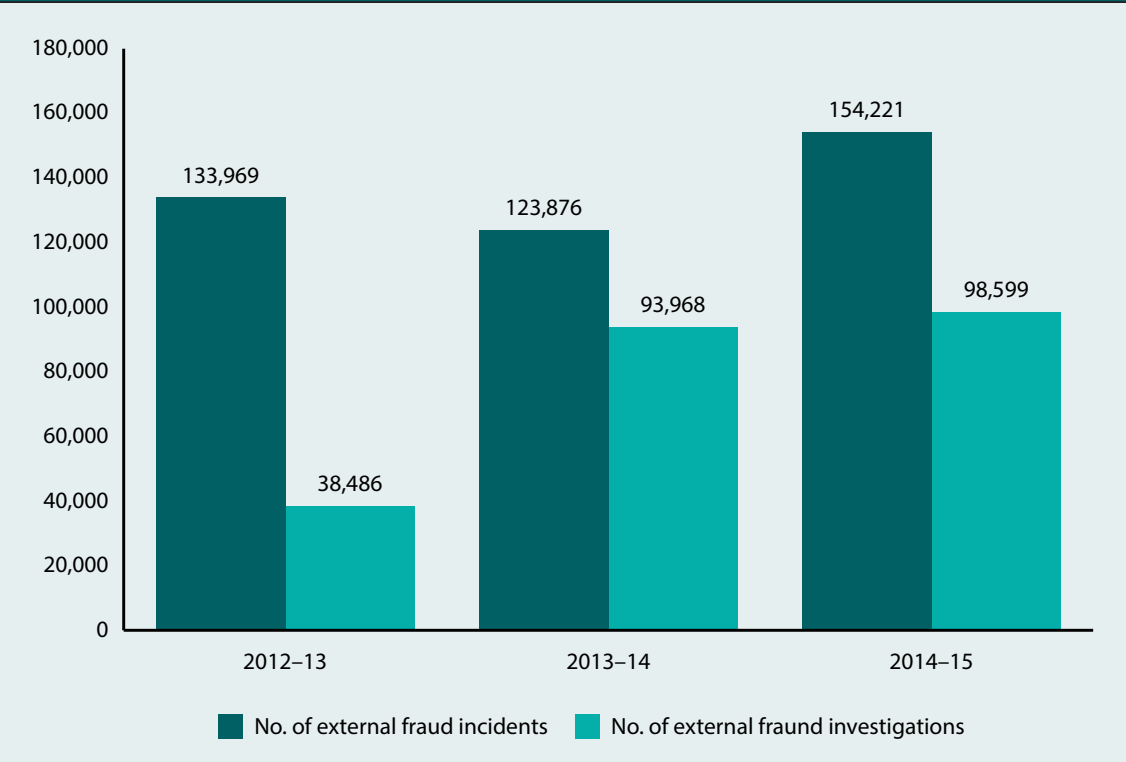
Figure 19: Alleged internal fraud incidents by external investigating organisation, 2012–13 to 2014–15 (N)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

As with internal fraud, the vast majority of external fraud incidents were investigated primarily by entities themselves, accounting for over 97 percent of alleged external fraud in 2012–13, 68 percent of alleged external fraud incidents in 2013–14, and 65 percent of alleged incidents in 2014–15. In 2014–15 more than 98,000 incidents of external fraud were investigated by entities themselves with no further external investigation.

Figure 20: Alleged external fraud incidents and total number of investigations conducted, by year (N)



Source: Commonwealth fraud census 2012-13, 2013-14 and 2014-15 [AIC computer file]

Figure 20 shows the number of external fraud incidents reported by entities and the number of investigations conducted. Investigations could be conducted either internally by the entity or externally; alternatively, the entity could have conducted an investigation and then referred the matter to law enforcement or external organisations to pursue. Respondents were not asked questions about the number of ongoing investigations, how many investigations were finalised, or how many did not meet an individual entity's threshold for initiating investigations. These questions will be addressed in future questionnaires structured to look at the investigations conducted in more depth.

Table 18 shows the number of external fraud incidents investigated primarily by various external organisations following internal review by the entities themselves.

In 2014-15 there was an increase in the number of external fraud incidents conducted by credit card issuers, most probably due to an increase in the number of card skimming incidents or card-not-present fraud affecting Commonwealth entities. The number of investigations conducted by other government entities also increased in 2014-15. The number of investigations conducted by the AFP rose from 211 in 2012-13 to 7,760 in 2013-14, then declined greatly to just 47 incidents in 2014-15. This large increase in 2013-14 was due to one entity being responsible for 99 percent of the 7,760 incidents referred to the AFP. Those incidents related to potential fraud involving the entities' legislation; they do not appear in the AFP figures of referrals accepted and declined later in this report, as they would have been under legislation other than the Criminal Code, thus excluding them from the reports made by the AFP each year.

Table 18: External investigations of alleged external fraud, by investigating organisation, 2012–13 to 2014–15 (N&%)

Investigating organisation	2012–13		2013–14		2014–15	
	N	%	N	%	N	%
Credit card issuer	22	5.6	47	0.5	111	26.8
State or territory police	119	30.4	40	0.5	72	17.4
External investigator	4	1.0	3	<0.1	np	np
Another government entity	27	6.9	28	0.3	182	44.0
Australian Federal Police	211	54.0	7,760	89.4	47	11.4
Other	8	2.0	805	9.3	2	0.5
Total external investigations	391		8,683		414	

Note: 'np' indicates the category was not provided that year

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Referrals for criminal action

Respondents were asked to indicate how many and what types of incidents were referred directly to various specified organisations for criminal investigation or prosecution, including the AFP, state or territory police, the CDPP and other organisations in Australia or overseas. These incidents had not been dealt with by entities themselves and, accordingly, represented more serious matters.

Table 19: Internal fraud incidents referred for criminal proceedings by fraud focus category, 2012–13 to 2014–15 (N)

Focus of fraud	Australian Federal Police (AFP)			State or territory police			Commonwealth Director of Public Prosecutions			Other, inside or outside of Australia		
	2012–13	2013–14	2014–15	2012–13	2013–14	2014–15	2012–13	2013–14	2014–15	2012–13	2013–14	2014–15
Equipment	3	2	3	0	0	1	2	1	1	0	3	6
Entitlements	28	0	4	0	0	0	3	7	5	0	12	13
Information	3	2	10	0	0	0	2	0	1	7	0	10
Financial benefits	7	2	11	0	2	4	13	10	7	4	11	25
Other	1	2	2	2	1	0	4	1	0	13	2	7

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Table 19 shows the number of internal fraud incidents referred by entities for criminal action for each fraud focus category, including the 'other' option. Very few incidents were referred for either criminal investigation or prosecution by entities each year. The largest number of incidents, relating to entitlement fraud, was referred to the AFP in 2012–13. The 2013–14 financial year had particularly low levels of referrals, most relating to financial benefits. In 2014–15 financial benefit fraud was again the focus of incidents resulting in the most referrals and, as with 2013–14, the largest number of referrals was made to other organisations.

In the case of external fraud, Table 20 shows that, consistently over the three years, most referrals to the CDPP for criminal prosecution related to allegations of entitlement fraud. In 2013–14 and 2014–15 referrals to other organisations related largely to financial benefit fraud. In 2013–14 a large number of incidents of external fraud focused on information referred to the AFP for investigation. Ninety-nine percent of those were attributed to one entity and a single Australia-wide event. It should be noted that at the time of that census the entity advised that those incidents involved suspected fraud that had not yet been substantiated.

Table 20: External fraud incidents referred for criminal action by focus category, 2012–13 to 2014–15 (N)												
Focus of fraud	Australian Federal Police (AFP)			State or territory police			Commonwealth Director of Public Prosecutions			Other, inside or outside of Australia		
	2012–13	2013–14	2014–15	2012–13	2013–14	2014–15	2012–13	2013–14	2014–15	2012–13	2013–14	2014–15
Equipment	1	0	1	17	11	9	0	0	0	6	22	23
Entitlements	1	0	0	0	12	0	1,217	1,109	1,376	1	5	9
Information	5	7,751	37	1	0	10	200	42	41	4	8	0
Financial benefits	9	16	5	92	21	52	248	272	159	24	1,758	1,632
Other	0	3	3	0	0	1	36	19	4	20	22	2

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Respondents were asked to provide details of the methods by which fraud had been committed for each type of referral. Over the three years reviewed, few internal fraud referrals involving misuse of information technology (IT) or misuse of identity were made (Table 21). In 2014–15, 12 incidents were referred to the AFP for fraud involving the misuse of information or documents, and eight incidents involving corruption. For all three years, larger numbers of incidents relating both to misuse of information/documents and to corruption were made.

Table 21: Internal fraud incidents referred for criminal action by method category, 2012–13 to 2014–15 (N)												
Method of fraud	Australian Federal Police (AFP)			State or territory police			Commonwealth Director of Public Prosecutions			Other, inside or outside of Australia		
	2012–13	2013–14	2014–15	2012–13	2013–14	2014–15	2012–13	2013–14	2014–15	2012–13	2013–14	2014–15
Misuse of IT	1	2	4	0	0	0	2	0	0	4	2	2
Misuse of identity	2	0	0	1	0	0	1	0	0	0	0	0
Misuse of information/docs	4	2	12	0	0	3	11	7	9	0	16	22
Corruption	2	3	8	0	0	0	2	1	0	19	0	21
Other	1	2	5	2	1	3	8	6	3	1	10	15

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Table 22 presents data on external fraud referrals by method of commission of the alleged fraud incident. These questions proved difficult for entities, who were asked to select a primary method for how the fraud incident occurred. As can be seen, for all three years, large numbers of external fraud incidents were referred to the CDPP for ‘other’ methods. As with referrals in Table 21, in 2013–14 a large number of incidents of external fraud focused on information referred to the AFP for investigation. Ninety-nine percent of those were attributed to one entity and a single Australia-wide event. As mentioned previously, at the time of the data collection period those allegations were unsubstantiated.

Table 22: External fraud incidents referred for criminal action, by method category, 2012–13 to 2014–15 (N)

Method of fraud	Australian Federal Police (AFP)			State or territory police			Commonwealth Director of Public Prosecutions			Other, inside or outside of Australia		
	2012 -13	2013 -14	2014 -15	2012 -13	2013 -14	2014 -15	2012 -13	2013 -14	2014 -15	2012 -13	2013 -14	2014 -15
Misuse of IT	0	1	0	1	2	0	0	11	1	4	0	1
Misuse of identity	5	3	2	7	3	24	178	56	35	15	3	6
Misuse of information/docs	4	7,752	35	19	0	12	27	66	18	2	15	26
Corruption	0	1	1	0	0	0	0	1	0	4	2	3
Other	2	1	4	16	14	35	1,254	1,100	1,471	21	1,734	1,628

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

AFP investigations

In addition to the information provided by respondents in the annual census, both the AFP and CDPP provided data to the AIC concerning the investigation and prosecution of fraud against the Commonwealth. The data were received in aggregate form and could not be attributed to any individual incidents reported by specific entities. Nor could the type of fraud investigated or prosecuted be categorised as internal or external fraud. Data collection practices within the AFP and CDPP also differed in various respects, as described below.

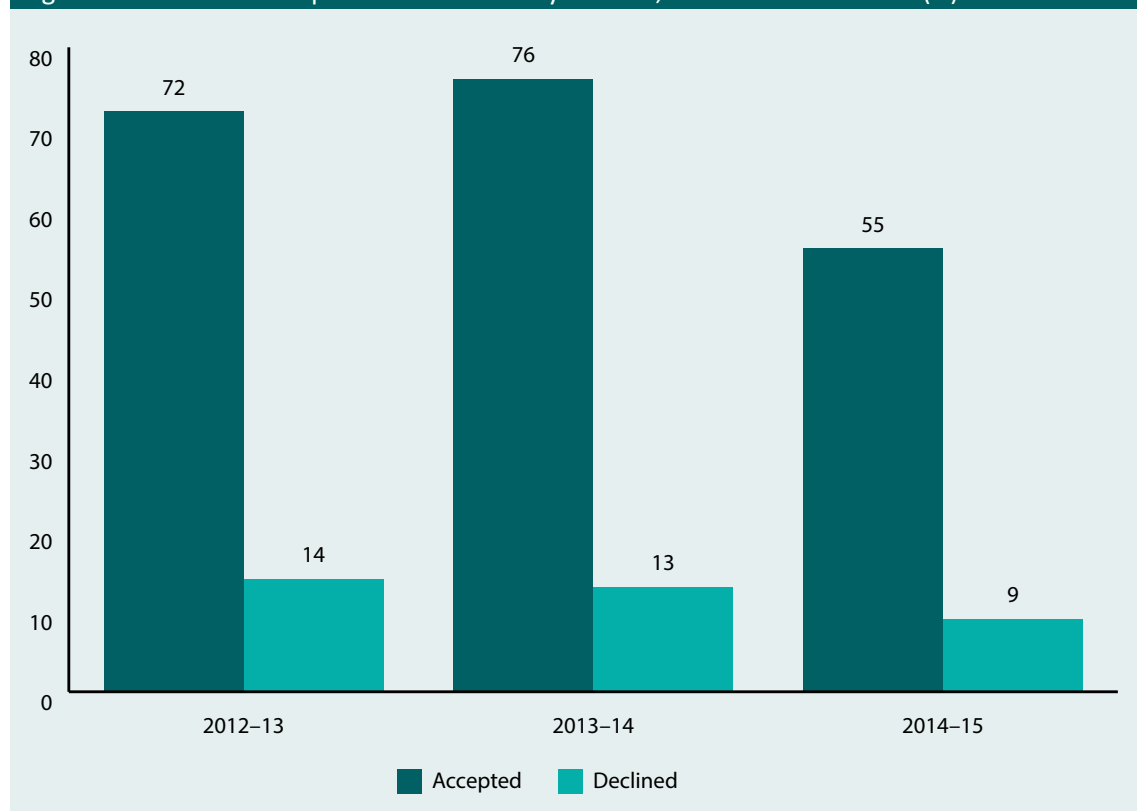
Paragraph 18 of the Commonwealth Fraud Control Framework 2014 required the AFP to provide the AIC with the following information relating to fraud-related matters against the Commonwealth:

- the number of matters referred to, accepted by and declined by the AFP during the previous financial year;
- the types of offences involved;
- the estimated financial loss of matters investigated;
- the fulfilment of AFP service standards relating to case handling; and
- the results of the investigation quality assurance review process, with an analysis of best practice and deficiencies (AGD 2014).

The framework (AGD 2014) provided the following list of matters that are considered to be of sufficient seriousness and complexity to warrant referral to the AFP:

- significant or potentially significant monetary or property loss to the Commonwealth;
- damage to the security, standing or integrity of the Commonwealth or an entity;
- harm to the economy, national security, resources, assets, environment or wellbeing of Australia;
- a serious breach of trust by a Commonwealth employee or contractor of an entity;
- the use of sophisticated techniques or technology to avoid detection, that require specialised skills and technology for the matter to be successfully investigated;
- the elements of a criminal conspiracy;
- bribery, corruption or attempted bribery or corruption of a Commonwealth employee or contractor to an entity;
- known or suspected criminal activity against more than one entity;
- activities which could affect wider aspects of Commonwealth law enforcement (eg illegal immigration, money laundering); and
- politically sensitive matters.

Figure 21: Referrals accepted and declined by the AFP, 2012–13 to 2014–15 (N)



Source: AFP internal data provided to AIC in 2013, 2014 and 2015

During the three years in question, the number of referrals generally declined, from 86 in 2012–13 to 64 in 2014–15, with a slight increase in 2013–14 to 89. Over the three years, the number of matters declined by the AFP reduced, from 14 referrals declined in 2012–13 to nine in 2014–15 (Figure 21). The AFP estimated that the financial loss attributable to the 72 accepted matters in 2012–13 was \$102,426,346 and the estimated loss for the 76 accepted matters in 2013–14 was \$304,403,145. In 2014–15 just 55 matters were accepted by the AFP, with an estimated loss amount of \$471,134,682. In dollar value, this represented a substantial increase over the three years, especially as the number of accepted fraud matters decreased by 28 percent from those accepted in 2013–14 to those accepted in 2014–15. However, it should also be noted there was a decrease in the number of cases referred to the AFP in 2014–15. At 30 June 2015, the AFP had 160 fraud-related matters still on hand (some of those fraud-related matters reflected ongoing cases from long-running investigations that commenced in previous years) with an estimated dollar value of \$1,802,084,653.

Fraud prosecutions by the CDPP

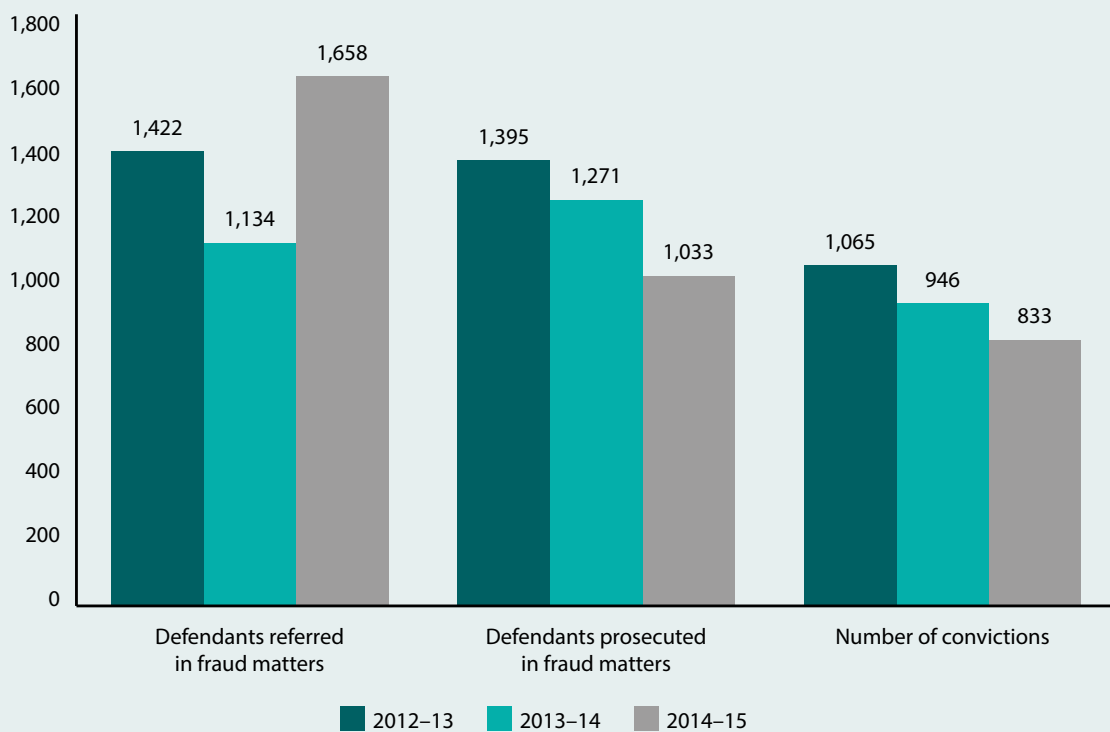
Statistics on Commonwealth fraud cases referred to the CDPP for prosecution, and the outcomes of those cases, are provided to the AIC each year pursuant to the Commonwealth Fraud Control Framework (AGD 2014), paragraph 19 of the Fraud Policy and reporting requirements.

For each financial year, individual state and territory statistics were provided on:

- the number of fraud-type matters referred to the CDPP;
- the number of defendants and charges prosecuted;
- the amount initially charged in each fraud-type prosecution;
- the outcomes of prosecutions, including:
 - the number of convictions;
 - the number of acquittals;
 - the number of other outcomes; and
 - amounts ordered by courts by way of reparation orders under the Crimes Act 1914 and pecuniary penalty orders under the Proceeds of Crime Act 1987.
- the number of charges by offence;
- the number of charges by referring entity; and
- the number of proved offences by highest sentencing disposition.

Again, these statistics cannot be related to the incidents reported by entities in response to the annual census, as reporting periods and counting rules differ.

Figure 22: Fraud matters prosecuted by the CDPP, 2012–13 to 2014–15 (N)



Source: CDPP internal data provided to AIC in 2013, 2014 and 2015

Figure 22 presents data on the numbers of defendants referred and prosecuted, and the numbers of fraud convictions obtained each year. Prior to 2014–15, there had been a general decline in these numbers, which may be due to declining referrals from entities. The CDPP assesses each brief of evidence referred to it in accordance with the *Prosecution Policy of the Commonwealth*. The CDPP makes a decision to prosecute where there is a reasonable prospect of conviction and prosecution is in the public interest. However, as can be seen for 2014–15, the number of defendants referred to the CDPP rose by over 45 percent, although the number of defendants prosecuted and the number of convictions for fraud matters continued to decline. The High Court’s decision in *DPP v Keating* (2013) 297 ALR 394 had an impact on the number of prosecutions during the period of the draft report. The decision led to the CDPP discontinuing or deciding not to prosecute in many social security fraud matters. It must be noted that although more fraud matters were referred to the CDPP than prosecuted, this does not mean that the referrals were declined by the CDPP. It takes time for a brief of evidence to be assessed and for a prosecution to progress through the court system. A referral to the CDPP therefore usually only results in a finalised prosecution in later financial years.

Table 23 shows corresponding statistics on referrals, defendants, convictions, acquittals and charges in fraud-type prosecutions handled over the three years for each state and territory. There were some differences in trends in individual jurisdictions, with referrals increasing in all jurisdictions except New South Wales and the Northern Territory. In terms of charges prosecuted and convictions obtained, there were declines in all jurisdictions except Queensland and Western Australia.

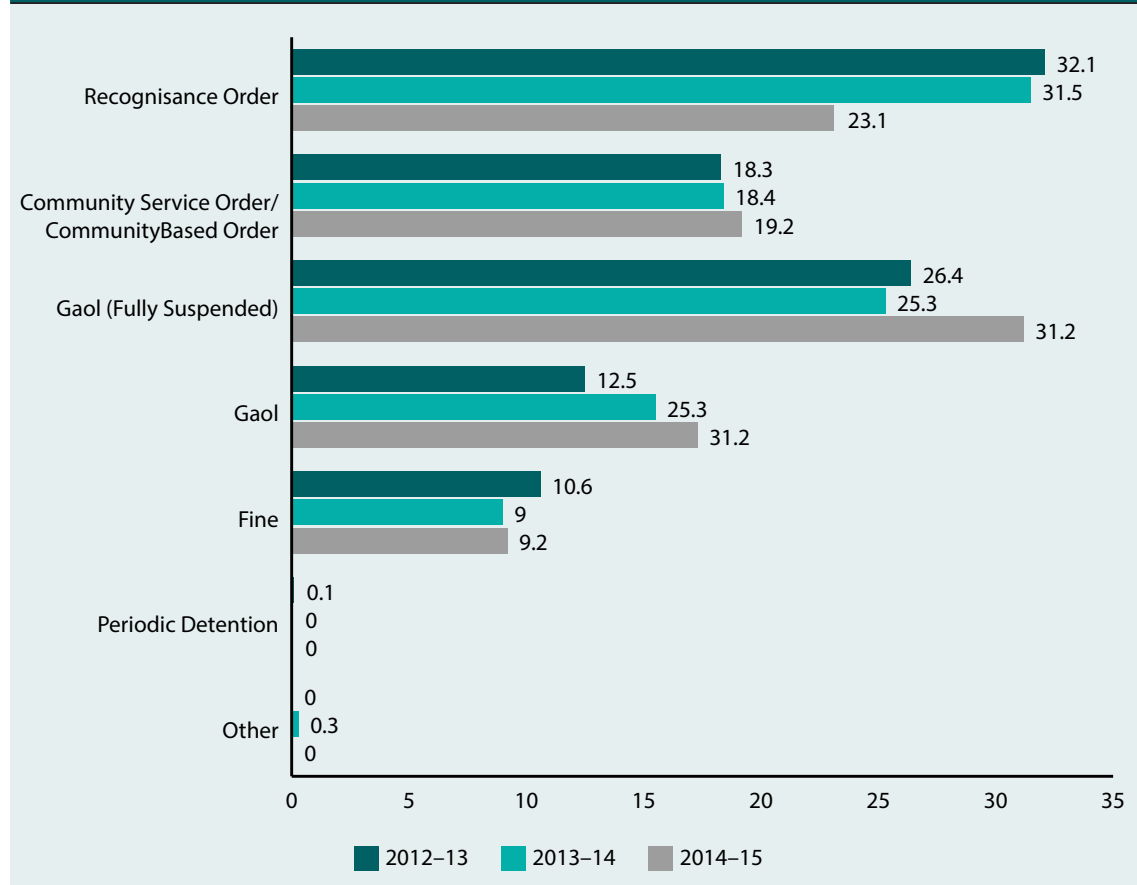
Table 23: Prosecutions of fraud by jurisdiction, 2012–13 to 2014–15 (N)					
Year	Referrals	Defendants prosecuted	Convictions	Acquittals	Charges prosecuted
New South Wales					
2012–13	501	443	342	4	2,165
2013–14	235	299	233	7	1,395
2014–15	397	126	95	3	736
Victoria					
2012–13	311	323	245	1	692
2013–14	236	373	261	1	855
2014–15	355	266	216	0	524
Queensland					
2012–13	321	296	241	2	671
2013–14	378	340	276	0	1,018
2014–15	444	375	308	1	1,009
South Australia					
2012–13	76	120	103	0	644
2013–14	76	81	51	0	467
2014–15	178	83	74	0	494
Western Australia					
2012–13	111	111	66	1	313
2013–14	114	73	58	1	271
2014–15	161	105	81	0	349
Tasmania					
2012–13	48	59	42	0	527
2013–14	46	72	49	4	731
2014–15	52	48	39	0	261
Northern Territory					
2012–13	22	19	9	0	106
2013–14	19	19	8	0	84
2014–15	17	16	8	0	33
Australian Capital Territory					
2012–13	32	24	14	0	115
2013–14	30	17	10	0	141
2014–15	54	14	12	0	34
Totals					
Total 2012–13	1,422	1,395	1,062	8	5,233
Total 2013–14	1,134	1,271	946	13	4,962
Total 2014–15	1,658	1,033	833	4	3,440

Source: CDPP internal data provided to AIC in 2013, 2014 and 2015

Sentencing dispositions

Each year the CDPP also provides statistics on the highest sentencing disposition given for fraud-related offences that were proved (Figure 23). Again, these data relate to the years in which defendants were sentenced, rather than the years in which the CDPP received referrals from entities.

Figure 23: Highest sentencing disposition, 2012–13 to 2014–15 (%)



Source: CDPP internal data provided to AIC in 2013, 2014 and 2015

Over the three-year period there was an increase in the use of imprisonment (either fully suspended or jail sentence) as the highest sentence imposed on defendants convicted of fraud matters. This move to more severe sentencing may reflect the changes in the types of fraud matters before the courts, and the value of fraud matters, necessitating harsher penalties to deter further offending. Periodic detention and other forms of sentences were not imposed at all in the 2014–15 financial year.

Fraud compliance, control and prevention

The Commonwealth Fraud Control Framework 2014 (AGD 2014) established a range of fraud control principles and guidance within which entities can determine their own specific practices, plans and procedures appropriate to their risk environment to manage the prevention and detection of fraudulent activities. The framework also deals with policies and procedures governing investigations and, where appropriate, prosecution of offenders. Fraud control is based on a thorough assessment of fraud risks particular to the operating environments of entities and of the programs they administer, as well as development and implementation of processes and systems to prevent fraud from occurring. This includes training of all employees and relevant contractors in fraud awareness, and specialised training of employees involved in fraud control activities. The framework was developed to reflect the change from a compliance-based approach to a principles-based framework established under the PGPA Act. On 30 August 2016 the Minister for Justice issued a revised Fraud Policy which reflected the recommendations of the Belcher review. The data in this report are based on the Fraud Policy issued in 2014.

Under paragraph 20 of the Fraud Policy 2014 (AGD 2014), the AGD was tasked with providing an annual compliance report to the government, through the Minister for Justice, on whole-of-government compliance with the Fraud Rule. Following a recommendation from the Belcher Red Tape Review (Belcher 2015), information on compliance with the framework was merged into this report.

In 2012–13 and 2013–14, 194 entities were invited each year to participate in the census. In 2012–13, 162 entities participated, resulting in an 84 percent participation rate. The rate among non-corporate entities (that are bound by the framework and previous Commonwealth Fraud Control Guidelines 2011) was even higher, at 93 percent (for non-corporate entities previously governed by the Financial Management and Accountability Act 1997) participating in the census in 2012–13. In 2013–14 the participation rate was 86 percent of all entities participating, and 95 percent for non-corporate entities (Table 24).

Table 24: Entities invited to participate in the census and responding entities (N&%)						
Responding entities	Year					
	2012–13		2013–14		2014–15	
	N	%	N	%	N	%
Non-corporate entities invited to participate	108	55.7	109	56.2	96	53.6
Non-corporate entities participating	100	51.5	104	53.6	91	50.8
Corporate entities invited to participate	86	44.3	85	43.8	83	46.4
Corporate entities participating	62	32.0	62	32.0	63	35.2
Total participation	162	83.5	166	85.6	154	86.0
Total Commonwealth entities	194	100	194	100	179	100

Source: Department of Finance PGPA Commonwealth entities and companies 30 September 2015; Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

The Fraud Rule and accompanying framework (AGD 2014) came into effect on 1 July 2014. Accordingly, 2014–15 was the first census data collection governed by the new framework. The Fraud Policy, which outlines the reporting requirements for Commonwealth entities, is considered best practice for corporate entities and is binding for non-corporate entities. Section 17 of the Fraud Policy 2014 requires all entities to:

collect information on fraud and provide it to the Australian Institute of Criminology (AIC), by 30 September each year to facilitate production of an AIC annual report on fraud against the Commonwealth and fraud control arrangements.

The Fraud Policy was specifically designed for non-corporate entities to be able to fulfil their responsibilities under the PGPA Act 2013.

In 2014–15, 76 percent of corporate entities and 95 percent of non-corporate entities completed the AIC census, with an overall response rate of 86 percent. With the introduction of the PGPA Act and the Fraud Policy and accompanying framework (AGD 2014), there was concern that a small number of corporate entities would not participate in the census. However, this did not occur; the number of corporate entities participating remained similar to earlier years.

Each year a small number of non-corporate entities fail to participate in the census. A range of reasons for not participating are given by the entities, such as matters of national security and having adequate fraud control arrangements in place.

Compliance with Commonwealth Fraud Control Framework

Responsibility for fraud control arrangements for each entity rests with its accountable authority—for example, its chief executive officer (CEO) or head. The accountable authority has a duty to keep the responsible minister informed of the activities of the entity, which includes fraud occurring against the entity and the entity's fraud control measures.

In the Fraud against the Commonwealth census, respondents are asked to indicate if their accountable authority had reported to either their minister or their presiding officer by certifying their entity had adequate fraud control measures for the relevant financial year. The only options available to respondents were 'yes' or 'no'. Table 25 presents findings for non-corporate entities (previously governed by the FMA Act) over the previous three years.

Table 25: Non-corporate head of entity certification of adequate fraud measures (N&%)						
Certification	2012–13		2013–14		2014–15	
	N	%	N	%	N	%
CEO certified	97	97.0	94	90.4	76	83.5
CEO has not certified	3	3.0	10	9.6	15	16.5
Total	100	100	104	100	91	100

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

In 2014–15, 84 percent of non-corporate entities' CEOs or heads were certified to have reported to their minister or presiding officer that the entity employed adequate fraud control throughout the financial year. This percentage was lower than in the previous two years—90 percent of CEOs/heads had reported in 2013–14, and 97 percent had reported in 2012–13.

Table 26: Corporate head of entity certification of adequate fraud measures (N&%)						
Certification	2012–13		2013–14		2014–15	
	N	%	N	%	N	%
CEO certified	48	77.4	27	43.5	36	57.1
CEO has not certified	13	21.0	35	56.5	27	42.9
Question not answered	1	1.6	0	0	0	0
Total	62	100	62	100	63	100

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Table 26 presents the findings of corporate entities' CEOs/heads reporting adequate fraud control arrangements within the financial year (corporate entities were previously governed by the Commonwealth Authorities and Companies Act 1997). Of the 63 corporate entities that responded in 2014–15, 36 (57%) CEOs/heads reported having adequate fraud control arrangements in place. This was an increase from the number of corporate (or Commonwealth Authorities and Companies Act 1997) entities that reported CEO/head certification in 2013–14 (27 entities, 44%). This represented a decline in both 2013–14 and 2014–15 from 2012–13, when the percentage was 77%.

No reasons were given by respondents as to why their CEOs/heads had not certified adequacy of fraud control arrangements. However, MoG changes that occurred during 2013–14, and the move to the PGPA Act scheme may have resulted in a delay in fraud control arrangements being signed off.

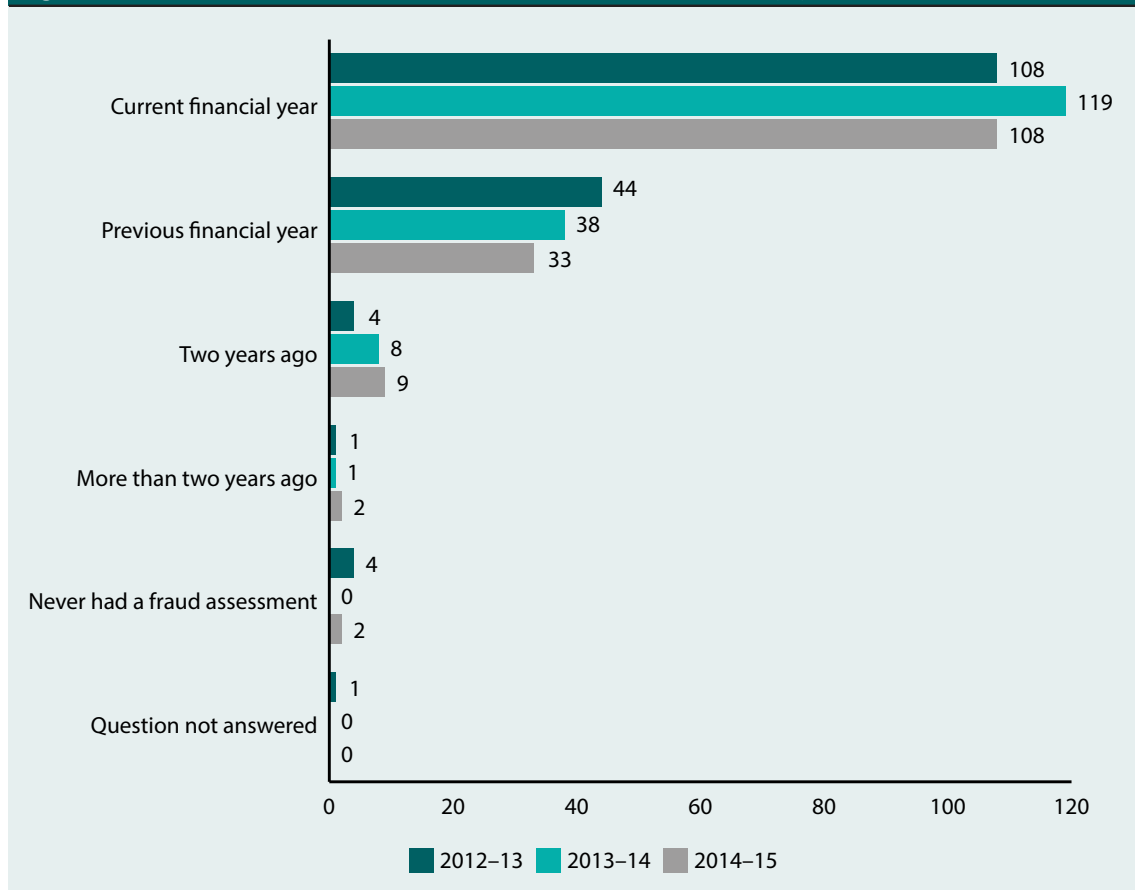
Fraud control arrangements

Two essential elements of maintaining adequate fraud control arrangements include the preparation of a fraud control plan and the conduct of regular fraud risk assessments. It should be noted that this report does not comment on the adequacy of entities' risk assessments or fraud control plans, only whether they have occurred. The framework (AGD 2014) requires that a fraud risk assessment must be conducted regularly and when there is a substantial change in the structure, functions or activities of the entity. It is recommended that, at a minimum, fraud risk assessments are conducted biennially (AGD 2014). However, depending on an entity's risk environment, it may be appropriate to conduct risk assessments more often. Risk assessments are an important tool in fraud control as they assist entities to identify and address fraud risks.

Fraud risk assessments

Over the three years examined, the number of respondents who reported their entity had completed a fraud risk assessment within the previous two financial years remained high (Figure 24). In 2014–15, 91 percent of respondents reported their entity had completed a fraud risk assessment in the previous two years.

Figure 24: Year entities conducted most recent risk assessment (N)



Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

The 2014–15 census asked respondents an additional question about whether their entity had undergone a MoG change or any other substantial changes in structure, function or programs, or undergone a transfer of functions to another entity in the financial year. This question was asked because fraud risk assessments need to be updated or substantially changed with any change of organisational function. In 2014–15, 32 entities advised they had either been involved in a MoG change, had their budget substantially reduced or had part of their functions transferred to another entity or took over additional functions or programs. Of those 32 entities, 28 conducted risk assessments in the 2014–15 period (some of the changes to entities did not occur in the 2014–15 financial year, with some occurring in the previous financial year and others in the 2015–16 period, and eight respondents did not provide a date for the changes to their entity), another three entities conducted their fraud risk assessments in 2013–14, and in one entity substantial restructuring had occurred and the entity had never conducted a fraud risk assessment.

When looking specifically at non-corporate entities, a high number of entities that had conducted risk assessments within the previous two years (Table 27). Of the 91 non-corporate entities participating in the 2014–15 census, 85 entities (93%) had completed a fraud risk assessment in the previous two financial years. Only one had conducted a risk assessment more than two years previously. In 2014–15, all non-corporate entities had completed a fraud risk assessment at some time.

Table 27: Non-corporate entity (previously FMA Act) year of risk assessment (N&%)						
Certification	2012–13		2013–14		2014–15	
	N	%	N	%	N	%
Current financial year	67	67.0	76	73.1	67	73.6
Previous financial year	28	28.0	27	26.0	18	19.8
Two years ago	0	0	0	0	5	5.5
More than two years ago	3	3.0	1	1.0	1	1.1
Never had a fraud assessment	2	2.0	0	0	0	0
Question not answered	0	0	0	0	0	0
Total	100	100	104	100	91	100

Note: Percentages may not total 100 due to rounding

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

In 2014–15 two corporate entities, at the time of the census, had never conducted a fraud risk assessment (Table 28), and one had conducted a risk assessment more than two years previously. While the Fraud Policy and Fraud Guidance (including the framework) are considered better practice for corporate entities, the Fraud Rule is binding for all Commonwealth entities. The Fraud Rule states that entities ‘must take all reasonable measures to prevent, detect and deal with fraud’, and one such method is regularly conducting fraud risk assessments. Therefore, in 2014–15, three entities are not compliant with the Commonwealth Fraud Rule. Further analysis of those entities which had never conducted a fraud risk assessment showed that neither entity experienced an incident of fraud in 2014–15.

Table 28: Corporate entity (previously CAC Act) year of risk assessment (N&%)						
Certification	2012–13		2013–14		2014–15	
	N	%	N	%	N	%
Current financial year	41	66.1	43	69.4	41	65.1
Previous financial year	16	25.8	12	19.4	15	23.8
Two years ago	2	3.2	7	11.3	4	6.3
More than two years ago	0		0	0	1	1.6
Never had a fraud assessment	2	3.2	0	0	2	3.2
Question not answered	1	1.6	0	0	0	0
Total	62	100	62	100	63	100

Note: Percentages may not total 100 due to rounding

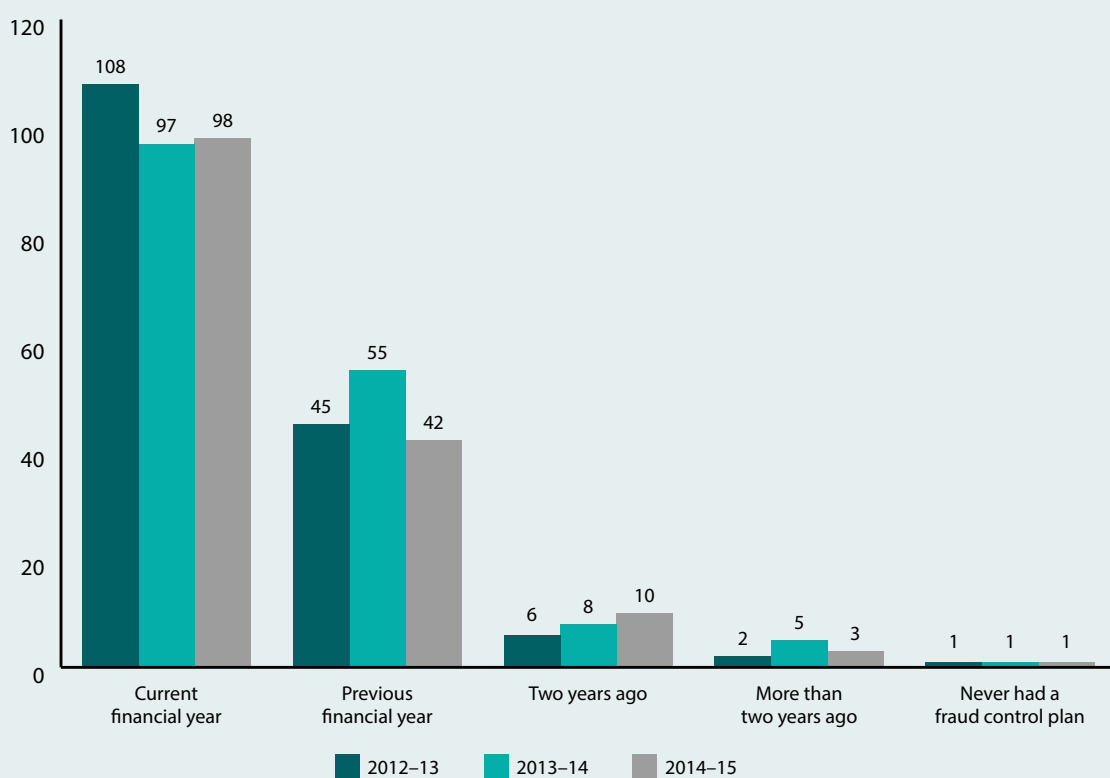
Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Fraud control plans

In addition to fraud risk assessments, another component of maintaining adequate fraud control is for entities to develop fraud control plans after a risk assessment has been conducted. Fraud control plans identify how fraud risks will be mitigated and how fraud prevention, detection, investigation, reporting and response will be handled. A fraud control plan is a document that explains an entity's approach to controlling fraud at a strategic, operational and tactical level and should document how the entity will prevent, detect, investigate and report fraud (AGD 2014).

Respondents were asked to indicate when their most recent fraud control plan was developed. The census noted that fraud control plans need not necessarily be standalone documents but may be included within more general risk management plans. In 2014–15, 91 percent (N=140) of respondent entities had completed a fraud control plan within the previous two financial years. This was similar to the 92 percent (N=152) in 2013–14, although it was a decline from the 94 percent (N=153) of entities which had completed fraud control plans in the previous financial years in 2012–13 (Figure 25).

Figure 25: Year entities developed most recent fraud control plan (N)



Source: Commonwealth fraud census 2012-13, 2013-14 and 2014-15 [AIC computer file]

Table 29 presents data on the number of non-corporate entities and the year their latest fraud control plan was conducted. No non-corporate entities had never had a fraud control plan over the three-year period (AGD 2014). However, in 2013-14 three entities had not conducted a fraud control plan within the previous two years, and in 2014-15 one non-corporate entity had conducted a fraud control plan more than two years ago. While the framework (AGD 2014) does not specify a time frame for conducting fraud control plans, it does stipulate that whenever a risk assessment is conducted a fraud control plan should follow. As it is recommended that risk assessments be conducted at least every two years unless required more frequently, it would be expected that entities (2014) should also have completed fraud control plans within the preceding two years.

Table 29: Non-corporate entity (previously FMA Act) year of fraud control plan (N)

Certification	2012-13		2013-14		2014-15	
	N	%	N	%	N	%
Current financial year	66	66	60	57.7	57	62.6
Previous financial year	31	31	39	37.5	25	27.5
Two years ago	3	3	2	1.9	8	8.8
More than two years ago	0	0	3	2.9	1	1.1
Never had a fraud control plan	0	0	0	0	0	0
Total	100	100	104	100	91	100

Source: Commonwealth fraud census 2012-13, 2013-14 and 2014-15 [AIC computer file]

Persistently, for the last two financial years, one respondent representing a corporate entity failed to complete the question about fraud control plans, raising the possibility that a fraud control plan has not been made for that entity (Table 30). For the past three years, each year, one entity reported that a fraud control plan has never been conducted. In 2014–15, a review of responses indicated that the entity in question had no fraud incidents for the year. However, this does not necessarily mean fraud did not occur in the past financial year—simply that fraud had not been detected.

Table 30: Corporate entity (previously CAC Act) year of fraud control plan (N)						
Certification	2012–13		2013–14		2014–15	
	N	%	N	%	N	%
Current financial year	42	67.7	37	59.7	41	65.1
Previous financial year	14	22.6	16	25.8	17	27.0
Two years ago	3	4.8	6	9.7	2	3.2
More than two years ago	2	3.2	1	1.6	1	1.6
Never had a fraud assessment	1	1.6	1	1.6	1	1.6
Question not answered	0	0	1	1.6	1	1.6
Total	62	100	62	100	63	100

Note: Percentages may not total 100 due to rounding

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Fraud control staff

Fraud control is based on a thorough assessment of fraud risks particular to the operating environments of entities and of the programs they administer, as well as development and implementation of processes and systems to prevent fraud from occurring. This includes training of all employees and relevant contractors in fraud awareness and specialised training of employees involved in fraud control activities. An important element of fraud control generally is to have appropriately trained staff dedicated to fraud risk management and prevention working within entities.

Table 31: Entities and fraud control sections (N&%)												
Fraud sections	2012–13				2013–14				2014–15			
	No fraud section		Fraud section		No fraud section		Fraud section		No fraud section		Fraud section	
	N	%	N	%	N	%	N	%	N	%	N	%
Non-corporate entity	23	23.0	77	77.0	24	23.1	80	76.9	18	19.8	73	80.2
Corporate entity	19	30.6	43	69.4	20	32.3	42	67.7	18	28.6	45	71.4
Total	42	25.9	120	74.1	44	26.5	122	73.5	36	23.4	118	76.6

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Table 31 presents the number of non-corporate and corporate entities where a fraud control section operates—that is, areas that have at least one person who spends a portion of their FTE on fraud control. Over the three years, the numbers of entities with a dedicated fraud control section increased (74% in 2012–13, 74% in 2013–14 and 77% in 2014–15).

Staffing

An important element of fraud control generally is to have appropriately trained staff dedicated to fraud risk management and prevention working within entities. Over the three years, there was a 14 percent increase in the number of staff employed within fraud sections of entities, from 3,160 to 3,588 staff (Table 32). As a percentage of entities, this represented an increase from 74 percent of entities with a fraud control section in 2012–13 to 77 percent of entities with a fraud control section in 2014–15. However, even though the number of people employed in a fraud control function increased between 2012–13 and 2014–15, the number of those staff with a relevant fraud qualification decreased, from 1,419 people in 2012–13 to 1,192 people in 2014–15. Overall, the percentage of fraud section staff with a fraud qualification decreased, from 45 percent in 2012–13 to 33 percent in 2014–15.

The Commonwealth Fraud Control Framework (AGD 2014) requires entities to ensure that officials primarily engaged in fraud control activities possess or attain relevant qualifications or training to enable them to effectively carry out their duties within 12 months of being engaged in fraud control activities. The decline of staff with qualifications over the three-year period is of concern to the Commonwealth, as without those specific qualifications fraud control staff may not be able to recognise all fraud risks or the early warning signs of when fraud is occurring and may struggle to conduct an investigation that will meet the approval of the AFP or the standard required for the CDPP (ANAO 2011).

Table 32: Total number of fraud control staff and entities with fraud control sections, 2012–13 to 2014–15 (N&%)

Category	2012–13	2013–14	2014–15
Staff in fraud section (N)	3,160	3,343	3,588
Percentage of entities with a fraud control section (%)	74	73	77
Staff with a qualification (N)	1,419	1,341	1,192
Percentage of fraud section staff with a qualification (%)	45	40	33

Note: Some staff may have been engaged in more than one type of function, resulting in totals being in excess of actual staff numbers

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15

For this report, if entities had recorded they had a person working in some fraud-related area but could not categorise their functions further, the entity was taken to have staff dedicated to fraud control. It was thought that this would better reflect fraud control functions across entities of all sizes. For example, in the 2014–15 census one entity included a staff member who had a 0.05 FTE in a fraud control capacity.

Entity fraud control staff with specific roles

In order to assess the resources allocated to fraud control within the Commonwealth, respondents were asked to specify the numbers of staff dedicated to various fraud control functions. Information was gathered on the numbers of staff working in fraud prevention, investigation and other fraud control tasks and whether or not they possessed formal qualifications, such as certificates or diplomas related to fraud investigation.

Table 33: Fraud control staff and their qualifications, 2012–13 to 2014–15 (N)									
Category	Fraud prevention			Fraud investigation			Other functions		
	2012 –13	2013 –14	2014 –15	2012 –13	2013 –14	2014 –15	2012 –13	2013 –14	2014 –15
Staff in fraud section (N)	843	850	804	2,089	2,090	2,056	228	403	416
Staff with a qualification (N)	125	110	60	1,133	1,037	652	161	194	189
Fraud section with a qualification (%)	15	13	7	54	50	32	71	48	45

Note: Some staff may have been engaged in more than one type of function, resulting in totals being in excess of actual staff numbers

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15

The Commonwealth Fraud Framework 2014 (AGD 2014) stipulates that officials and contractors who are primarily engaged in detecting or investigating fraud should be appropriately skilled and experienced. Appropriately skilled staff are necessary to ensure the integrity of the investigation process and evidence collected, and fairness for the person being investigated.

Between 2012–13 and 2014–15, the number of fraud control staff engaged in fraud prevention and investigation duties steadily decreased, from 843 people employed in a prevention capacity in 2012–13 to 804 people employed in fraud prevention in 2014–15. In the same period, there was an 82 percent increase in the number of staff employed in other fraud functions. By way of contrast, however, the percentage of staff with formal qualifications working in all areas of fraud control declined (Table 33).

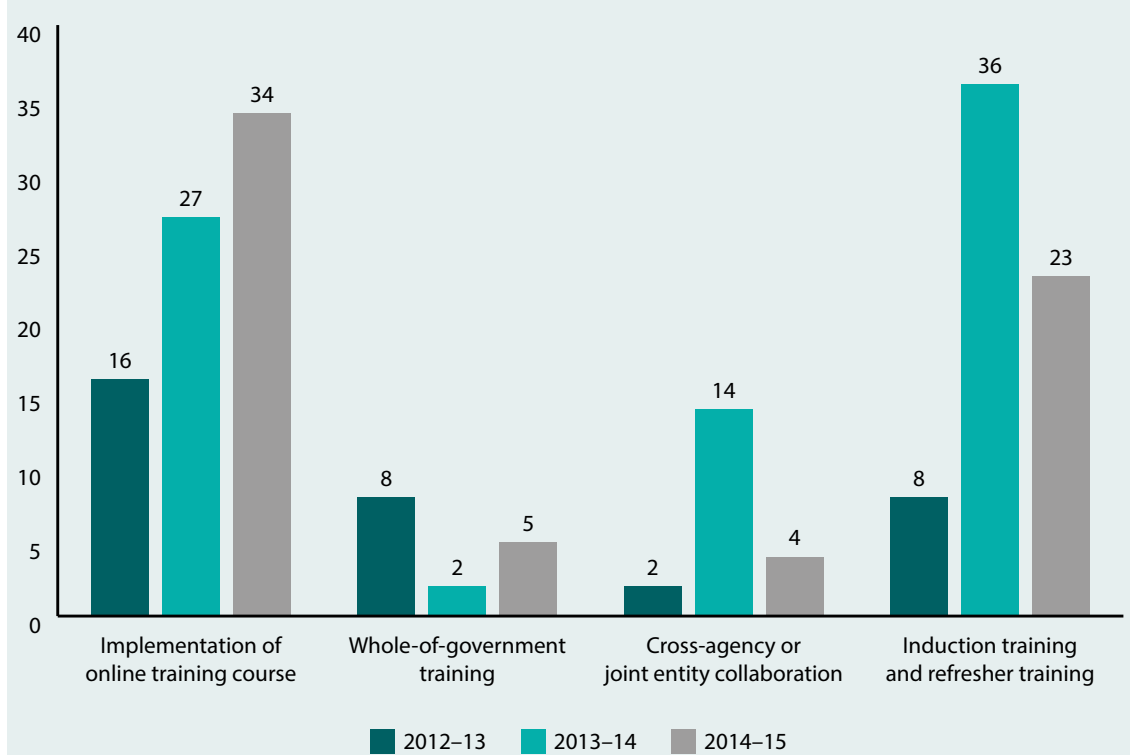
Training

The Commonwealth Fraud Control Framework (AGD 2014) stated that fraud awareness training should be included in all staff induction programs and that all entities should document their procedures and instructions to assist employees in dealing with fraud. Respondents were asked each year what changes they would suggest for improving the training of staff around fraud control within their entity. A range of responses were received, with more than 70 responses from entities received each year. Responses were analysed to determine common themes or similar needs that respondents believed would assist with fraud control.

For all three years there were certain similarities in the views of entities in relation to what would help staff understand fraud and improve fraud control training. The top four responses for the three years are presented in Figure 26. In 2013–14, 27 percent of responses suggested online training courses, which increased to 34 percent in 2014–15. Recently the AGD, with the assistance of other government entities, developed a whole-of-government fraud awareness e-learning training package. The package is designed for Commonwealth entities (corporate

and non-corporate) and can be requested by contacting the AGD's Security and Integrity Reform Branch. It was uncertain, from the majority of responses received in 2014–15, if entities wanted to implement an online training package or had recently implemented the AGD's training package. However, over the three years, online fraud training was of increasing interest.

Figure 26: Top four suggested ways of improving fraud control training (percentage of respondents who answered the question)



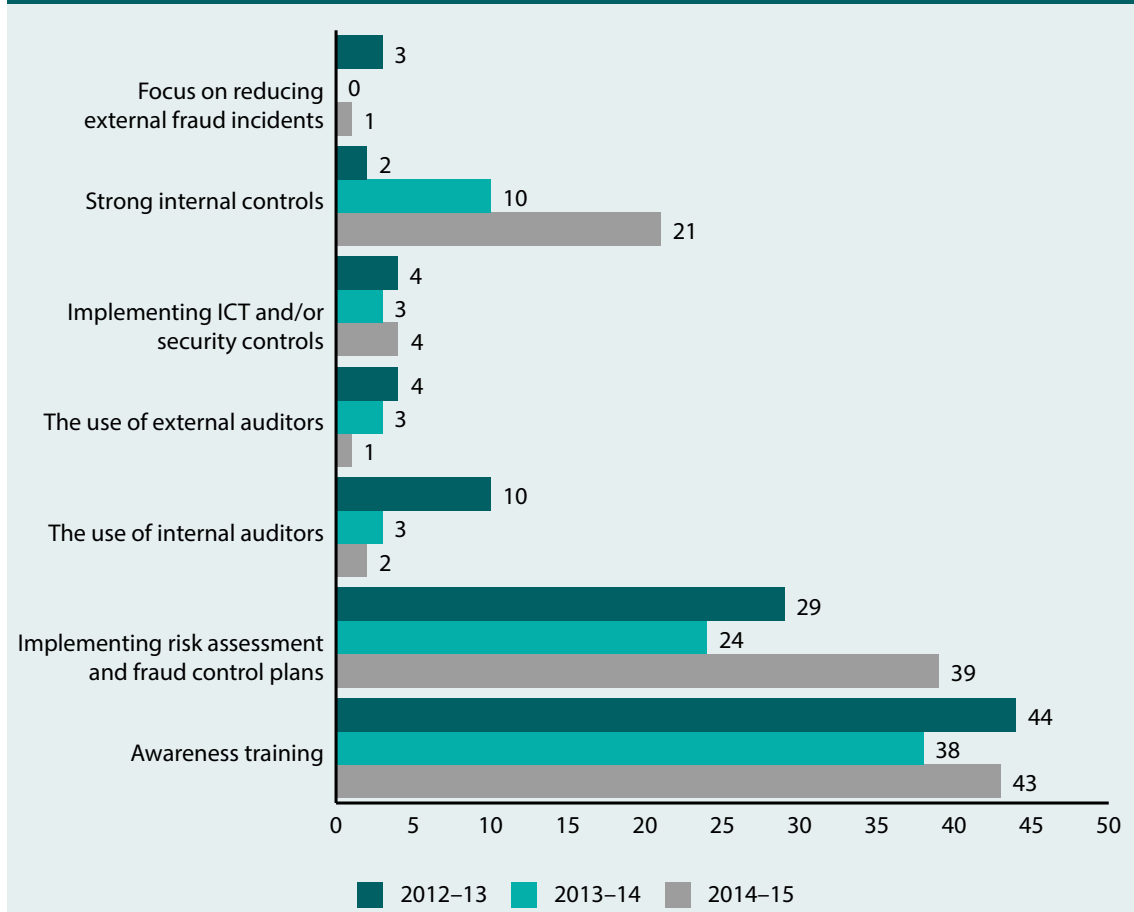
Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Respondents also expressed the need for ongoing training, with a number of entities noting the use of yearly refresher training to remind all employees about their fraud control obligations. In 2013–14, 36 percent of respondents believed a combination of induction training for new staff and ongoing refresher training for all staff would assist with fraud control. In 2014–15 this had decreased to 23 percent but was the second most frequently cited response.

In addition, respondents were asked to provide their opinions as to what had made a difference to the prevention of fraud during the previous year. The most frequent response in each year related to the use of fraud awareness training, followed by the presence of fraud control plans and the implementation of fraud risk assessments (see Figure 27). These findings were largely uniform over the three years of data collection, and some respondents mentioned multiple suggestions for what had helped their entity's fraud prevention and control over the preceding year. In 2014–15 there was an increase in the number of respondents who credited their fraud prevention successes to the effort put into strengthening the entity's internal controls. There were some additional differences apparent in 2014–15, with 17 percent (N=18, of 104 respondents who provided comments) of respondents indicating they implemented

fraud review processes which differed to, or were carried out in conjunction with, fraud risk assessments and fraud control plans. Thirty respondents (29%) also discussed the role of culture within the organisation and how engagement with employees assisted with fraud prevention.

Figure 27: Respondents' views as to what had made a difference to the prevention of fraud (percentage of respondents who answered the question)



Source: Commonwealth fraud census 2012-13, 2013-14 and 2014-15 [AIC computer file]

Conclusions

Principal trends 2012–15

Fraud against the Commonwealth may involve public servants or consultants working for Commonwealth entities engaging in acts of dishonesty (internal fraud) or members of the public seeking to derive welfare, taxation or other Commonwealth benefits improperly (external fraud). In 2014–15, a higher number of entities (42%) experienced incidents of fraud than in previous years. As has been found in past reports, fraud incidents involving persons external to the entity—that is, members of the public, cybercriminals or organisations contracted to Commonwealth entities—are more of a concern for entities than are internal staff. Of the 155,843 incidents of fraud reported by entities in 2014–15, 99 percent entailed external fraud. Although external fraud incidents were more costly and experienced by greater numbers of entities in 2014–15, a persistent concern to the reputation of entities and staff morale is internal fraud. In 2014–15, the number of entities experiencing internal fraud increased, although the overall number of incidents of internal fraud declined.

Changing risks

In relation to internal fraud, the principal fraud risks related to manipulation of internal controls, compromise of employee entitlements and avoidance of risk management procedures. In relation to external fraud, risks arose in connection with the provision of new government-funded programs, changes to management practices within entities and the services they deliver, procurement practices, and the tax and welfare benefits available to the public.

With regard to internal fraud, more entities experienced a fraud incident focused on financial benefits, such as misuse of government credit cards or theft of cash, and procurement offences. However, more incidents involved access to and/or misuse of information held by their entities without authorisation. This particular fraud type continues to be an ongoing problem. Entities may hold and be responsible for the security of a variety of different sources of information, ranging from information that concerns national security to financial information, and health and immigration data, to name a few. The security of that information is essential to the safety of Australian citizens and the integrity of Commonwealth entities.

In the case of external fraud, a much larger number of entities experienced fraud focused on financial benefits. However, when looking at the number of incidents experienced for each fraud type, many more incidents involved fraud relating to entitlements, rather than financial

benefits. This finding has been consistent over the years the census has been conducted, and the number of incidents involved with that particular fraud type have increased over the three-year period. Between 2013–14 and 2014–15, although the number of entities experiencing external fraud focused on information remained stable, the number of incidents declined, from 19,273 in 2013–14 to 17,603 in 2014–15.

In relation to the methods by which internal fraud incidents had allegedly been committed, over the three years the method affecting the highest percentage of entities involved misuse of documents and/or information. In 2014–15 there were increases in the numbers of entities experiencing fraud committed via the misuse of ICT, corruption and other means. Only misuse of identity remained stable. In terms of the numbers of incidents per category of method for internal fraud incidents, misuse of ICT consistently resulted in the highest number of internal frauds reported over the three years. In 2014–15 the number of incidents of internal fraud committed via misuse of identity and misuse of documents/information increased. The Australian Public Service is strongly encouraged to use ICT systems to increase productivity, improve service delivery and government operations, and be more available to the public (Department of Finance 2012). However, ICT systems in the Commonwealth hold a wealth of data and information; misuse by employees or external parties can damage entities and cause potential harm to the public.

Misuse of identity is a fraud risk that arises in connection with the provision of most government services (Smith 2014). Government service delivery agencies and revenue authorities, in particular, maintain extensive confidential databases of personal information that, if compromised and made public, provide abundant information for use in financial crime, perpetrated both by and against members of the public (AGD 2015). Between 2012–13 and 2014–15, the number of incidents of external fraud involving the misuse of identity rose by over 450 percent. This increase was in part due to increased awareness of identity crime and improved data collection procedures used to record this crime type, although the majority of the increase was attributable to one large entity and a change in the way fraud was recorded.

Fraud costs

It has always been difficult and complex to estimate the amounts entities lose from fraud. There are many barriers to the effective quantification of the cost of fraud, such as problems in estimating the costs of incidents that have not yet been fully investigated; difficulties of quantifying fraud that does not have a direct financial impact, such as loss of information or misuse of intellectual property; and the inevitable inability to quantify undetected fraud incidents. These difficulties have led to very different amounts being reported by entities over time.

Despite these difficulties, estimated losses due to internal fraud have continued to increase, even with the decline in the number of incidents of internal fraud. The costs associated with internal fraud incidents increased from \$3.4m in 2012–13 to over \$4.2m in 2014–15. The progress entities have made in decreasing incident numbers of internal fraud is commendable; however, the percentage of entities experiencing internal fraud has increased, and the fact that the dollar value of losses has increased is a concerning trend.

Over the three years included in this report, the value associated with external fraud losses fluctuated substantially. In contrast to internal fraud, even though there was an increase in the number of external fraud incidents, the costs incurred by entities declined, from \$669m in 2013–14 to just over \$324m in 2014–15.

Overall, the total amount lost to fraud in 2012–13 was \$207m, \$673m in 2013–14 and \$329m in 2014–15, a decrease from the previous financial year. This decrease in the value of fraud incidents is not reflected in the reported value of fraud incidents accepted for investigation by the AFP each year. For example, in 2013–14 the estimated loss for the 76 accepted matters was \$304,403,145. In 2014–15 just 55 matters were accepted, with an estimated loss amount of \$471,134,682. Therefore, although entities are showing an increase in fraud incidents and a decline in the costs associated with those matters, the AFP has reported a decrease in the number of fraud referrals accepted, and those matters accepted had a substantially higher value than in the previous financial year.

The results presented highlight the need for individual entities to remain vigilant to the unique risks they face, and to work consistently to update fraud prevention strategies and control plans so they are tailored to meet current and emerging risks. The results of the three years of censuses provide important data on the areas of fraud risk that Commonwealth entities face and how they can prevent and respond to such risks.

The Belcher review and entity feedback

Since its inception, the fraud against the Commonwealth census has increased in length and complexity. Regular feedback has been sought from entities as to ways in which the data collection can be streamlined and improved. Most recently, in March 2015 the Secretaries Board, established by the Australian Public Service Act 1999 (Cth), commissioned former senior public servant Barbara Belcher, in response to a perceived burgeoning of regulation within the Commonwealth, to conduct an Independent Review of Whole-of-Government Internal Regulation. The review's objectives were to:

- identify regulations that could be ceased or modified;
- assess the need for, and impact of, regulations against a set of common principles;
- recommend minimum levels of regulation required for entities to meet the needs of government and the public; and
- assess the culture of departments and selected entities with regard to the creation and removal of self-imposed requirements, identify characteristics and examples of good culture and practice, and make recommendations for structural and cultural improvements which would be adopted by entities.

The review was presented to the Secretaries Board in October 2015 and included 134 recommendations for reducing red tape and regulatory burden experienced by entities. All recommendations were accepted in conjunction with the Department of Finance's Public Management Reform Agenda. Recommendation 19 specifically referred to the AIC's annual fraud census and the AGD's Commonwealth Fraud Control Policy. The Belcher review identified

a number of ways in which the collection of fraud control information from Commonwealth entities could be streamlined and duplication of collection activities reduced.

While the review was being conducted, the AIC undertook extensive consultation with major Commonwealth entities to discuss ways in which the collection of information could be improved so as to reduce the burden on respondents. Feedback from earlier discussions with entities had highlighted some concerns around ‘fraud allegations’ as the unit of measurement, the interpretation of what an ‘incident’ was, and the overlapping of some categories between the focus of the fraud and method. For example, the focus category ‘financial benefits’ included a subcategory of ‘obtaining cash/currency without permission’, which could also constitute a type of method of committing fraud. Other concerns centred on the ability of respondents to print outputs of results from the online system.

In 2015, two further meetings were held, with all entities who had participated in the 2014 census invited to attend. Based on the feedback obtained, a revised draft questionnaire was distributed to key stakeholders for testing. After further amendments and approval from the AGD, a new questionnaire was distributed to all entities to ensure their data collection processes would align with the changes implemented. Discussions were also held with the online survey’s software developer to deal with printing and other formatting questions.

The key changes to the questionnaire were:

- a change in the unit of measurement away from allegations relating to fraud ‘incidents’ to fraud ‘investigations’ undertaken each year;
- a reorganisation of the questionnaire to have questions about fraud control at the start of the 2016 questionnaire;
- an increase in conditional response questions that enable those for whom a section is not applicable to proceed quickly to remaining sections without having to provide responses that are irrelevant;
- adding a new section that examines entities’ most costly external fraud investigation in addition to the previous questions about entities’ most costly internal fraud investigation;
- enabling respondents to respond both to internal and external aspects of questions in the one location; and
- changing the categories of fraud ‘focus’ and ‘methods’ of committing fraud to ensure the categories are mutually exclusive and as exhaustive as possible.

In addition, reporting will be consolidated, with census results and compliance information gathered in one report.

The changes made to the 2015–16 questionnaire should provide greater consistency in reporting both within and among entities. Having consistent data collection practices will allow for greater trend analysis and the identification of emerging fraud risks. Such information can be obtained only with the cooperation and resources of all Commonwealth entities. The AIC is confident that the revised data collection practices that will operate from the 2015–16 year will enable respondents to complete their reporting in a more efficient and concise way but still provide in-depth evidence that can inform future fraud control activities.

Conclusion

Fraud control within the Commonwealth is vital to minimise waste of government resources and to ensure that adequate funds are available for schools, health, social welfare and other services. Commonwealth entities have consistently demonstrated a willingness to ensure their employees are aware of fraud risks and have implemented policies to limit the damage fraud poses, such as through the use of risk assessments, regular reviews and awareness training for employees. However, constant vigilance is required to identify areas of future fraud risk. The information collected from entities in the AIC's annual census provides an important benchmark to enable entities to be aware of new and developing fraud risks across government and to develop responses accordingly.

The current results show that the trend for the provision of online services by government continues to create fraud risks for the Commonwealth. Over the three years, there was an increase in the percentage of entities experiencing incidents of both internal and external fraud that involved the misuse of ICT. With more services and functions being made available online, and the amount of personal and government information being stored online increasing exponentially, it is essential for entities to ensure that data are stored securely and that effective systems are in place to minimise risks of unauthorised access and misuse that lie at the heart of public sector fraud.

References

Attorney-General's Department (AGD) 2015. Identity crime and misuse in Australia, 2013-14. Canberra: AGD. <http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Identity-Crime-and-Misuse-in-Australia-2013-14.DOCX>

Attorney-General's Department (AGD) 2014. Commonwealth Fraud Control Framework. Canberra: AGD. <http://www.ag.gov.au/CrimeAndCorruption/FraudControl/Pages/default.aspx>

Attorney-General's Department (AGD) 2012. National Identity Security Strategy 2012. Canberra: AGD <http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/National%20Identity%20Security%20Strategy%202012.PDF>

Attorney-General's Department (AGD) & Australian Federal Police (AFP) 2011. Australian Government Investigation Standards. Canberra: AGD/AFP. <http://www.ag.gov.au//RightsAndProtections/FOI/Pages/FreedomOfInformationDisclosureLog/australiangovernmentInvestigationStandards2011andAustralianGovernmentInvestigationsStandards2003.aspx>

Attorney-General's Department (AGD) & Australian Federal Police (AFP) 2003. Australian Government Investigation Standards Package. Canberra: AGD/AFP. <https://www.ag.gov.au/RightsAndProtections/FOI/Documents/2003%20Australian%20Government%20Investigation%20Standards%20Package.pdf>

Association of Certified Fraud Examiners (ACFE) 2016. Report to the nations on occupational fraud and abuse, 2016 global fraud survey. Austin, USA: ACFE. <http://www.acfe.com/rttn2016.aspx>

Australian Bureau of Statistics (ABS) 2016. Recorded crime - offenders. ABS cat. no. 4519.0. Canberra: ABS. <http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4519.0Main+Features12014-15?OpenDocument>

Australian National Audit Office (ANAO) 2011. Fraud control in Australian Government entities: Better practice guide. Canberra: ANAO

Belcher B 2015. The independent review of whole-of-government internal regulation (Belcher Red Tape Review). Canberra: Department of Finance. <http://www.finance.gov.au/publications/reducingredtape/>

Department of Finance 2015. Machinery of Government changes. Canberra: Department of Finance. <http://www.finance.gov.au/resource-management/governance/>

- Department of Finance 2012. Australian Public Service ICT Strategy 2012–2015. Canberra: Department of Finance. http://www.finance.gov.au/policy-guides-procurement/ict_strategy_2012_2015/
- Gee J & Button M 2015. The financial cost of fraud: What the latest data from around the world shows. University of Portsmouth: Centre for Counter Fraud Studies
- Jorna P & Smith RG 2015. Fraud against the Commonwealth: Report to Government 2010–11 to 2012–13. Canberra: Australian Institute of Criminology <http://www.aic.gov.au/publications/current%20series/mr/21-40/mr24.html>
- Kroll 2015. Global fraud report: Vulnerabilities on the rise 2015–16. New York: Kroll. <http://www.kroll.com/global-fraud-report>
- Lindley J, Jorna P & Smith RG 2012. Fraud against the Commonwealth 2009–10 annual report to government. Monitoring report no. 18. Canberra: AIC. <http://aic.gov.au/publications/current%20series/mr/1-20/18.html>
- PricewaterhouseCoopers 2016. Adjusting the lens on economic crime: Preparation brings opportunity back into focus. PwC's 2016 Global Economic Crime Survey 2016. Sydney: PricewaterhouseCoopers. <http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html>
- PricewaterhouseCoopers 2014. Economic crime: A threat to business globally. PwC's 2014 Global Economic Crime Survey. Sydney: PricewaterhouseCoopers. <http://www.pwc.com/gx/en/economic-crime-survey/downloads.jhtml>
- Resource Management Guide 2014. Preventing, detecting and dealing with fraud. Resource management guide no. 201. Canberra: Minister for Justice
- Smith RG, Jorna P, Sweeney J & Fuller G 2014. Counting the costs of crime in Australia: A 2011 estimate. Research and public policy series no. 129. Canberra: Australian Institute of Criminology. <http://aic.gov.au/publications/current%20series/rpp/121-140/rpp129.html>
- United Kingdom National Audit Office 2016. Fraud landscape review. London: National Audit Office. <https://www.nao.org.uk/report/fraud-landscape-review/>

Methodology

Each year Commonwealth entities are asked to complete an online questionnaire that asks about their experience of fraud incidents and how they managed and responded to risks of fraud taking place.

Under the Commonwealth Fraud Control Guidelines 2011, fraud against the Commonwealth was defined as ‘dishonestly obtaining a benefit, or causing a loss, by deception or other means’ (AGD 2011: 7). For present purposes, entities were asked to respond to questions concerning all suspected incidents of fraud against the Commonwealth alleged against those employed by government entities, including staff and contractors (internal fraud), and also alleged against those who do not work for the government but who may be seeking to claim government benefits or to obtain some other financial advantage dishonestly (external fraud).

Information was provided by 163 entities in 2012–13, 166 entities in 2013–14 and 154 entities in 2014–15 (Table 34). Each year, over 80 percent of those invited to participate responded to the census. A small number failed to complete the questionnaire, resulting in a slightly smaller number being subject to analysis in 2012–13, as opposed to corporate entities, previously governed by the CAC Act. At 1 July 2014 the FMA Act and the CAC Act ceased to operate and the PGPA Act commenced. Future reports will no longer categorise entities in terms of their governance under the FMA and CAC acts; rather, they will be grouped according to their non-corporate or corporate governance status.

	2012–13		2013–14		2014–15	
	N	%	N	%	N	%
Invited to participate	195	100	194	100	189	100
Responded	163	83.6	166	83.6	154	81.5
Included in analysis	162	83.1	166	83.6	154	81.5
Total FMA/non-corporate entities in Commonwealth	108	55.4	109	56.2	102	54.0
Total CAC Act/corporate entities in Commonwealth	87	44.6	85	43.8	87	46.0
FMA Act entities who responded	100	61.7	104	61.7	91	59.1
CAC Act entities who responded	62	38.3	62	38.3	63	40.9

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Changes in the number of entities invited to participate over the four years were due to MoG changes, that alter the number of entities present in the Australian Public Service each year by mergers or cessation of operations. Due to some MoG changes that occurred part-way through a financial year, there is the potential that some fraud investigations may have been double-counted, although such changes would only affect a small number of entities and fraud incidents.

Respondents were asked to provide information by completing a secure, online questionnaire that recorded results anonymously (without naming individual entities or people), as the aim was to canvass the experience of fraud across the government as a whole, rather than by identifying what each individual entity had experienced. Further information on the investigation and prosecution of fraud incidents within the Commonwealth was also provided by the AFP and the CDPP for matters handled within each year (regardless of when they were committed).

Glossary

Allegation of fraud

An accusation made by a person or identified by an entity that an offence has or may have been committed. This does not require substantive proof of the offence or identification of suspects; however, allegations should only be included where there exists sufficient evidence to warrant an investigation by your entity.

Collusion

Any incident of suspected fraud allegedly committed by an employee or contractor of the entity in collaboration or association with a person external to the entity.

Commonwealth entity

Formerly known as Commonwealth agencies, Commonwealth entities are departments of state, parliamentary departments, listed entities or bodies of corporate established by a law of the Commonwealth. This terminology is employed in the Commonwealth Fraud Control Framework 2014 and is used in this report despite the Commonwealth Fraud questionnaires referring to 'agencies', the term applicable under the former Guidelines 2011.

Corruption

For the purposes of Commonwealth Anti-Corruption and fraud control policies, corruption can be defined as 'the dishonest or biased exercise of a Commonwealth public official's duty'. Entities may identify corrupt conduct engaged in by a public official (internal corruption), or conduct alleged against persons external to an entity in which they have sought to corrupt, or have actually corrupted, a Commonwealth public official (external corruption). An incident of corruption may involve either internal or external participants or both.

Duration of fraud

The amount of time the offender was committing fraud against the Commonwealth, from the time the commission of fraud commenced to the time the commission of fraud ceased, whether by choice or by detection.

Entitlements

A benefit or privilege that is assigned to an individual through an agreement.

Equipment

Any equipment or property belonging to a government entity.

External fraud

Any incident of suspected fraud allegedly committed against an entity by a person other than an employee (employee includes contracted employees) of the entity.

Finalisation

Finalisation refers to the completion of the investigation, or referral to another entity, or the suspect leaving the employment of the entity.

Financial benefit

Gaining an advantage either financial or monetary through fraud, including offences relating to misuse of government finances or tools to gain an advantage, hiding income or assets and receiving or obtaining financial advantage.

Focus

The focus or target of the alleged fraud incident, that is, the benefit to be obtained.

Fraud

For the purposes of the Fraud Control Guidelines 2011, fraud against the Commonwealth was defined as 'dishonestly obtaining a benefit, or causing a loss, by deception or other means'. The definition of fraud includes suspected fraud, incidents under investigation and completed incidents, whether the fraud was proved or not and whether the incident was dealt with by a criminal, civil or administrative remedy.

Fraud control

Any means undertaken by the entity to control fraud, including prevention and detection.

Incident

An incident refers to all counts alleged during one fraud investigation and may comprise a number of counts of offences that are actually prosecuted. An incident may take place on a single date or over a period of time and may involve one or more accused persons.

Information

Any information belonging to or stored by the entity including intellectual property, personal information either of employees or members of the public that is held by the entity.

Internal fraud

Any incident of suspected fraud allegedly committed by an employee or contractor.

Investigation

Investigation includes both internal investigations in accordance with the Australian Government Investigations Standards (AGIS) as well as investigations undertaken by external law enforcement or other investigatory bodies or organisations.

Method

The methods used to carry out the alleged fraud incidents. Each incident can involve several methods and the same method can be used for different incidents.

Misuse of documents

Creation, use or theft of documents belonging to an entity, presentation of false documents or documentation to an entity. These include government documents, legal documents and personal documents.

Misuse of identity

Any unauthorised use of another person's personal information that may be used to identify that person when dealing with the Commonwealth. Personal information may include a person's name, address, date of birth, Passport information, Medicare information, Biometric information (e.g. fingerprint), Computer username and password, Tax File Number (TFN), telephone number and other pieces of information.

Misuse of Information and Communications Technologies (ICT)

Any unauthorised use of computers, computer-related equipment or software to commit an alleged incident of fraud.

Losses

The total amount, in whole dollars, thought to have been lost to the entity from fraud incidents, prior to the recovery of any funds and excluding the costs of detection, investigation or prosecution.

Non-compliance

Non-compliance is the failure to meet conditions and obligations under laws and regulations. It may occur through a lack of understanding or awareness of obligations or because compliance is difficult. Alternatively, non-compliance may be deliberate. If evidence cannot establish the requisite degree of intention, recklessness or negligence in adhering to obligations, the conduct may be characterised as non-compliance, as opposed to fraud.

Recoveries

Whole dollars recovered by criminal prosecution, civil remedies, administrative remedies or other means. Does not include money recovered from fines if the money did not return to the entity.

Referrals

The number of incidents that were passed on to another entity after an investigation.

Review

Internal administrative process to determine whether fraud is occurring.

Suspect

The individual believed to have carried out the fraud incident.

Timeframe – reference period

The reference period for incidents in the 2014-15 financial year was 1 July 2014 to 30 June 2015 (and corresponding periods in 2012-13 and 2013-14). The start date of an incident is the date that the entity was notified of or discovered the allegation of fraud.

Appendix: Details of fraud focus and methods

Internal fraud focus

Respondents were asked to indicate the number of alleged incidents of internal fraud that focused on each of a number of specified resources, objects of benefit or targets of the alleged activity. Four main categories were provided that related to government equipment, entitlements, information or financial benefits. As incidents could involve more than one focus of fraud, respondents were asked to include multiple responses where applicable. Information was collected on both the number of entities that experienced fraud and the number of alleged incidents detected.

Table 35: Internal fraud focus of fraud, 2012–13 to 2014–15 (N)

Category	2012–13		2013–14		2014–15	
	Entities (N)	Incidents (N)	Entities (N)	Incidents (N)	Entities (N)	Incidents (N)
Equipment						
Theft of telecommunications or computer equipment (including mobile devices)	8	35	6	18	6	19
Theft of other government equipment	11	91	4	104	4	55
Theft of consumable stock (office related)	2	5	1	6	5	7
Theft of consumable stock (other)	7	16	6	17	3	5
Misuse of government equipment	12	38	13	129	15	40
Unable to be determined	1	1	0	0	1	1
Other equipment	4	14	9	10	4	19
Entitlements						
Expenses (other than travel)	6	9	5	6	3	4
Travel claims	7	21	7	23	11	20
Payroll fraud	9	18	8	18	7	26
Leave and related entitlements	14	81	16	80	20	66
Unable to be determined	1	1	0	0	2	2
Other entitlements	10	95	4	67	9	160

Information						
Obtaining or using information without authorisation (excluding personal information)	8	41	12	36	10	186
Obtaining or using personal information without authorisation	5	599	7	604	7	528
Providing false or misleading information, or failing to provide information when required to do so	7	53	9	28	17	54
Use of entity logo or name without authorisation	3	7	2	6	5	9
Misuse of entity intellectual property	4	7	4	7	3	10
Unable to be determined	3	5	1	5	4	5
Other information	3	9	3	13	5	18
Financial benefits						
Obtaining cash/currency without permission	9	16	10	19	11	30
Misuse or theft of government credit cards, travel cards or other cash cards	14	75	16	49	15	108
Misappropriations of government-funded grant monies or benefits	3	4	1	1	1	2
Misuse or theft of Cabcharge	5	32	6	16	8	20
Theft of property other than cash	5	31	5	17	7	16
Procurement offences	10	25	5	12	10	18
Bankruptcy offences (hiding or disposing of assets)	0	0	0	0	0	0
Falsification of documents in order to gain financial benefit	10	60	10	71	12	126
Unable to be determined	6	25	6	41	4	29
Other financial benefits	8	129	7	97	7	64
Other fraud focus						
Other incidents	13	147	6	107	8	54

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

External fraud focus

Respondents were also asked to indicate the number of alleged incidents of external fraud that focused on each of a number of specified resources, objects of benefits or targets of the alleged activity. Four main categories were provided that related to government equipment, entitlements, information or financial benefits. As incidents could involve more than one focus of fraud, respondents were asked to include multiple responses where applicable. Information was collected on both the number of entities that experienced fraud and the number of alleged incidents detected.

Table 36: External fraud focus of fraud, 2012–13 to 2014–15 (N)						
Category	2012–13		2013–14		2014–15	
	Entities (N)	Incidents (N)	Entities (N)	Incidents (N)	Entities (N)	Incidents (N)
Equipment						
Theft of telecommunications or computer equipment (including mobile devices)	8	56	3	33	6	36
Theft of other government equipment	2	2	2	14	2	2
Theft of consumable stock (office related)	0	0	0	0	2	15
Theft of consumable stock (other)	1	1	0	0	0	0
Misuse of government equipment	2	4	1	4	0	0
Unable to be determined	0	0	0	0	0	0
Other equipment	2	2	2	2	1	19
Entitlements						
Misusing or claiming benefits without entitlement relating to housing	0	0	0	0	1	1
Misusing or claiming benefits without entitlement relating to social security	2	3,254	3	2,641	2	2,351
Misusing or claiming benefits without entitlement to health benefits	3	390	3	327	2	1,187
Misusing or claiming benefits without entitlement relating to visas/citizenship	1	28,142	2	27,206	2	28,166
Misusing, evading or claiming without entitlement relating to child support	1	232	1	305	1	65
Revenue fraud	1	58,364	2	79,495	1	1
Customs and excise fraud (evading excise)	1	299	0	0	1	456
Unable to be determined	2	13	2	486	0	0
Other entitlements	4	79	3	239	6	92,820
Information						
Obtaining or using information without authorisation (excluding personal information)	4	6	2	2	4	63
Obtaining or using personal information without authorisation	4	1,101	2	149	6	6,360
Providing false or misleading information, or failing to provide information when required to do so	19	4,100	15	19,102	10	547
Use of entity logo or name without authorisation	4	11	5	14	3	4
Misuse of entity intellectual property	0	0	1	2	0	0
Unable to be determined	1	4	2	3	2	10,617
Other information	0	0	1	1	4	12

Financial benefits						
Obtaining cash/currency without permission	7	99	8	38	5	126
Misuse or theft of government credit cards, travel cards or other cash cards	11	35	6	10	12	100
Misappropriations of government-funded grant monies or benefits	6	41	2	2	10	98
Misuse or theft of Cabcharge	0	0	1	42	3	5
Theft of property other than cash	2	39	1	20	3	4
Procurement offences	10	380	14	316	1	10
Fictitious claims/forgery	6	25	10	88	9	19
Unable to be determined	3	25	3	10	2	15
Other financial benefits	10	274	9	234	7	212
Other fraud focus						
Other incidents	11	1,132	6	2,001	2	850

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Internal fraud method

Respondents were asked to indicate the number of alleged incidents of internal fraud that were carried out using a number of specified methods, such as misuse of ICT, identity, information or acts of corruption. As incidents could involve more than one method of commission, respondents were asked to include multiple responses where applicable. Information was collected on both the number of entities that experienced fraud and the number of alleged incidents detected.

Table 37: Internal fraud methods of commission, 2012–13 to 2014–15 (N)						
Category	2012–13		2013–14		2014–15	
	Entities (N)	Incidents (N)	Entities (N)	Incidents (N)	Entities (N)	Incidents (N)
Misuse of information and communications technologies (ICT)						
Accessing information or programs via a computer without authorisation	7	612	12	588	7	617
Copying or altering data or programs without authorisation	5	26	7	18	4	10
Misuse of email	7	25	5	82	11	48
Manipulation of a computerised accounting system	4	24	3	3	4	5
Insertion of malicious code	1	2	0	0	0	0
Interference with computer networks	0	0	0	0	0	0
Unable to be determined	3	3	1	1	3	7
Other misuse of ICT	4	6	3	18	6	17

Misuse of identity						
Creating and/or using a false identity	6	7	4	5	4	7
Use of another employee's or contractor's ID without knowledge	2	2	4	4	5	6
Fraudulently using another person's identity with permission	1	1	2	2	1	3
Unauthorised use of another person's password, PIN, or access pass	3	6	0	0	2	4
Unauthorised use of another person's Tax File Number or Australian Business Number	2	2	1	1	1	1
Unable to be determined	0	0	0	0	1	2
Other misuse of identity	4	16	3	5	1	4
Misuse of Information						
Creating and/or using a false or altered entity document	13	69	13	86	12	50
Creating and/or using a false or altered document (not belonging to the entity)	14	51	12	45	12	129
Dishonestly concealing documents	4	5	3	3	5	11
Failing to provide documents when required to do so	6	97	3	62	6	70
Deliberately disclosing of sensitive information (in any form) for benefit	5	51	7	47	10	51
Unable to be determined	2	4	1	5	6	23
Other misuse of documents and/or information	7	16	5	10	4	10
Corruption						
Bribery of an employee	2	50	3	49	1	35
Accepting kickbacks and gratuities	6	24	3	4	4	5
Nepotism	1	1	4	4	3	6
Failure to disclose/abuse of conflict of interest	8	52	7	32	10	100
Collusion or conspiracy between internal and external parties	11	48	3	98	6	61
Abuse of power	9	169	11	92	10	45
Unable to be determined	2	4	8	34	4	26
Other corruption	6	16	5	20	6	48
Other methods						
Other method details	19	351	9	327	17	132

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

External fraud method

Respondents were asked to indicate the number of alleged incidents of external fraud that were carried out using a number of specified methods, such as misuse of ICT, identity, information or acts of corruption. As incidents could involve more than one method of commission, respondents were asked to include multiple responses where applicable. Information was collected on both the number of entities that experienced fraud and the number of alleged incidents detected.

Table 38: External fraud methods of commission, 2012–13 to 2014–15 (N)

Category	2012–13		2013–14		2014–15	
	Entities (N)	Incidents (N)	Entities (N)	Incidents (N)	Entities (N)	Incidents (N)
Misuse of information and communications technologies (ICT)						
Accessing information or programs via a computer without authorisation	1	1	1	1	3	5
Copying or altering data or programs without authorisation	1	1	0	0	1	1
Misuse of email					1	1
Manipulation of a computerised accounting system	1	8	1	1	1	2
Insertion of malicious code	1	1	0	0	0	0
Interference with computer networks	1	3	0	0	np	np
Unable to be determined	1	2	1	9	0	0
Other misuse of ICT	3	3	3	16	2	17
Misuse of identity						
Creating and/or using a false identity	8	625	11	645	6	1,203
Use of another employee's or contractor's ID without knowledge	4	23	5	10	4	4
Fraudulently using another person's identity with permission	3	8	5	76	3	24
Unauthorised use of another person's password, PIN, or access pass	3	7	1	47	1	23
Unauthorised use of another person's Tax File Number or Australian Business Number	1	16,079	3	14,476	1	11,773
Unable to be determined	4	214	4	64,662	5	81,465
Other misuse of identity	2	11	6	251	3	4,902
Misuse of Information						
Creating and/or using a false or altered entity document	9	141	13	109	13	95
Creating and/or using a false or altered document (not belonging to the entity)	15	2,574	18	2,533	11	415
Dishonestly concealing documents	2	4	3	3	2	7
Failing to provide documents when required to do so	9	1,170	3	69	9	1,779

Deliberately disclosing of sensitive information (in any form) for benefit	0	0	0	0	1	2
Unable to be determined	8	58,464	7	3,762	3	6
Other misuse of documents and/or information	2	29	4	59	5	604
Corruption						
Bribery of an employee	0	0	2	5	0	0
Paying kickbacks and gratuities	1	1	0	0	1	1
Failure to disclose/abuse of conflict of interest	3	5	2	5	3	7
Unable to be determined	3	12	1	1	3	10
Other corruption	5	145	2	7	2	13
Other methods						
Other method details	14	11,649	21	25,274	26	23,650

Note: 'np' indicates that the category was not provided that year

Source: Commonwealth fraud census 2012–13, 2013–14 and 2014–15 [AIC computer file]

Authors

Penny Jorna is a Research Analyst, and Dr Russell G Smith is Principal Criminologist at the AIC.

AIC reports

Statistical Report

Australia's national research and
knowledge centre on crime and justice

aic.gov.au