Australian Government
Australian Institute of Criminology

Statistical bulletin 02

ISSN 2206-7302

March 2017

Abstract | From financial years 2010–11 to 2014–14, Commonwealth entities experienced 9,467 incidents of internal fraud, with losses of over $12.7m. This study analysed information about the most costly incidents each entity experienced each year and those who perpetrated these.

The majority of the 166 frauds related to employee entitlements or financial benefits, and most were committed through the misuse of documents or technology.

The findings provide an insight into the fraud risks facing the Commonwealth and how these might best be addressed.

Fraud within the Commonwealth: A census of the most costly incidents 2013-14

Russell G Smith & Penny Jorna

Fraud within Commonwealth government entities covers a range of criminal conduct that entails 'dishonestly obtaining a benefit, or causing a loss, by deception or other means' (AGD 2011: 7). Dishonesty is the key behavioural attribute that distinguishes fraudulent conduct from innocent conduct. Although fraud is a wide-ranging category of crime, and the personal backgrounds and socio-demographic characteristics of offenders can differ considerably, both incidents and offenders display enduring features that act as red flags.

This study focuses on internal fraud committed by Commonwealth officials, as opposed to fraud against the Commonwealth by external parties. While internal fraud is just one of a number of Commonwealth fraud risks, it can be especially damaging to the entities it affects. For example, internal fraud may damage the reputation of the entities involved, or lead to adverse media attention across the whole of government. It may also deplete government resources that could otherwise be used for

important programs, lead to loss of employment for other staff or damage the working environment of the public sector as a whole (Peltier-Rivest & Lanoue 2012).

This report presents some of the findings of the annual census of Commonwealth entities undertaken pursuant to the *Commonwealth Fraud Control Guidelines 2011* (AGD 2011). In the financial years 2010–11 to 2013–14 a total of 9,467 detected incidents of internal fraud, worth over $12.7m, were reported by 181 Commonwealth entities. Although the number of suspected incidents of internal fraud was halved over this period, the annual cost increased by over 20 percent.

The following discussion analyses in detail how the most costly incidents were commissioned, detected and dealt with by the affected entities and the courts. The findings will help Commonwealth entities understand the fraud risks they face and the characteristics of those alleged to have committed the most costly incidents of fraud against their employers. The information may also help entities develop strategies for minimising fraud by identifying gaps in their internal controls and improving other fraud-minimisation activities. Ramamoorti (2008) stresses the importance of organisations understanding who commits fraud, and its causes and motivations, so they can better manage the risks of fraud they face. This paper is intended to assist Commonwealth entities to make fraud harder to commit and a less lucrative activity for Commonwealth employees to contemplate.

Methodology

Every year, all Commonwealth entities are asked to complete a confidential online questionnaire about their experience of fraud incidents in the previous financial year, by September of the next. On average, over 80 percent of entities participate, reporting details of their fraud-control arrangements and instances of suspected internal and external fraud they detected or were informed of during the preceding financial year. Respondents are also asked to nominate that incident of internal fraud which resulted in the largest financial loss or other impact suffered by the entity of all incidents for which an investigation or review was concluded during that financial year (regardless of whether the fraud was committed or the investigation commenced during or prior to that year). Each of these nominated cases was considered as a single incident, despite incidents potentially involving more than one criminal offence or criminal count, or more than a single accused party. If an incident involved more than one accused person, respondents were asked to report only that information related to the principal suspect. Most incidents involved non-corporate Commonwealth entities (formerly governed under the *Financial Management and Accountability Act 1997* [FMA Act, Cth]; see Table 1).

Table 1: Size and governance framework of reporting entities, 2010–11 to 2013–14 (number of entities)

Governance framework and size of entity	2010–11	2011–12	2012–13	2013–14
Corporate entity (CAC Act)	13	14	15	15
Non-corporate entity (FMA)	30	24	30	29
0–500 staff	13	7	9	11
501–1,000 staff	6	7	9	7
1,000+ staff	24	24	27	26

Note: These data relate only to those entities that provided information on the most costly incident of internal fraud experienced
Source: Commonwealth fraud monitoring datasets 2010–11, 2011–12, 2012–13 and 2013–14 [AIC computer file]

Sample

Of the 181 entities that reported an incident of internal fraud during the four years in question, 166 (165 included in analysis; 91.2%), completed all or some of the questions dealing with the most costly incident (Table 2). A number of respondents were unable to provide all the requested demographic and other information, such as the perpetrator's highest level of education, their motivation and the length of their employment with the agency. Other information was more readily available.

Table 2: Responding entities

Year	Entities that experienced internal fraud (number)	Entities that responded to questions on the most costly incident of internal fraud (number and %)	
	N	N	%
2010–11	48	42	87.5
2011–12	44	38	86.4
2012–13	45	45	100.0
2013–14	44	40*	90.9
Total	181	165	91.2

Note: Due to Machinery of Government changes, one entity was split into two entities, with both reporting the same incident as the most costly incident of internal fraud. Only one of these reported incidents was included in the analysis, meaning that although 41 entities reported, only 40 cases were included for analysis in 2013-14

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

Limitations

Self-reported research of this kind has a number of limitations, one of the most important of which relates to the veracity and accuracy of responses to the questionnaire. The census was generally limited to detected fraud incidents; undetected or unreported fraud was excluded, as were incidents that were detected but written off due to their low value or because there were insufficient resources to investigate. This could affect the generalisability of the results to wider populations (Padgett 2015). On occasion, suspects may not have told an entity why they committed the offence and, if the suspect was simply dismissed from the organisation, details of the case's outcome may not be known. The collection of data relied upon respondents to the census—the entities' delegates—knowing the full details of the alleged fraud and subsequent investigation. In some cases that may not have been the case—for example, where no suspect was identified.

As the results presented below show, a number of respondents were unable or unwilling to answer some questions. Often the relevant information had not been collected during the investigation or could not be retrieved for the purpose of answering the questions, possibly because the person completing the census was not involved in investigating the incident. Information on the outcome of an investigation was also unavailable where proceedings had not been finalised, or reporting entities had not yet been notified of the result of any trials and appeals. Nonetheless the study provides a comprehensive indication of how and why fraud within the Commonwealth takes place and by whom it is committed. As such, it should be of use to those working in fraud control and risk management charged with addressing the problem.

Profiling occupational fraud

Prior research on fraud types and fraud offenders has found that fraud offences often share common characteristics, as do fraud offenders (Padgett 2015; Smith 2015). For example, KPMG (2013) created a profile of the typical fraudster (not necessarily one who perpetrated internal fraud) across both the public and private sectors, using the details of 596 fraud investigations conducted between 2011 and 2013. This typical fraudster was a person aged 36 to 55 who had been employed by their organisation for more than six years and had committed fraud against their own employer. Fraudsters generally held senior management positions and collaborated with another perpetrator. KPMG (2013) noted that, while there was no single unchanging profile of a person who commits fraud, it was good for organisations to be aware of patterns and trends in fraud when developing prevention and response measures.

Although PricewaterhouseCoopers (PwC) was cautious about the use of such profiles it did note, in its report on its Global Economic Crime Survey 2011, that organisations need to improve internal controls and be more aware of fraudster profiles. PwC's 2014 Global Economic Crime Survey found 39 percent of the perpetrators of the fraud incidents included in the survey were aged between 31 and 40; 29 percent had been employed by the victim organisation for between three and five years and 24 percent for between six and 10 years (PwC 2014). The similarities between the findings of both surveys support the view that some employees may be at higher risk of offending than others and, accordingly, require greater support (Smith 2015). It must, however, be stressed that it is difficult to comprehend all the factors and variables that would need to be understood and measured before the actions of employees in any given situation could be predicted (Padgett 2015). The best fraud survey research can do is identify similar traits or common behavioural characteristics of offenders that could be used by an organisation to identify vulnerabilities to fraud in the workplace.

Results

The information provided on the 165 most costly incidents reported by respondents for the four years was divided into three categories:

- demographic and other characteristics of suspects;
- characteristics of alleged offences, including estimated financial losses; and
- information on investigations and outcomes.

The results should be interpreted with some caution, as response rates for some variables where information was either not collected or unavailable were low. The total sample of 166 incidents (165 of which were analysed) was also relatively small, although in keeping with prior research.

Some brief comparisons with the results of prior fraud survey research are made at the end of each section below.

Characteristics of suspects

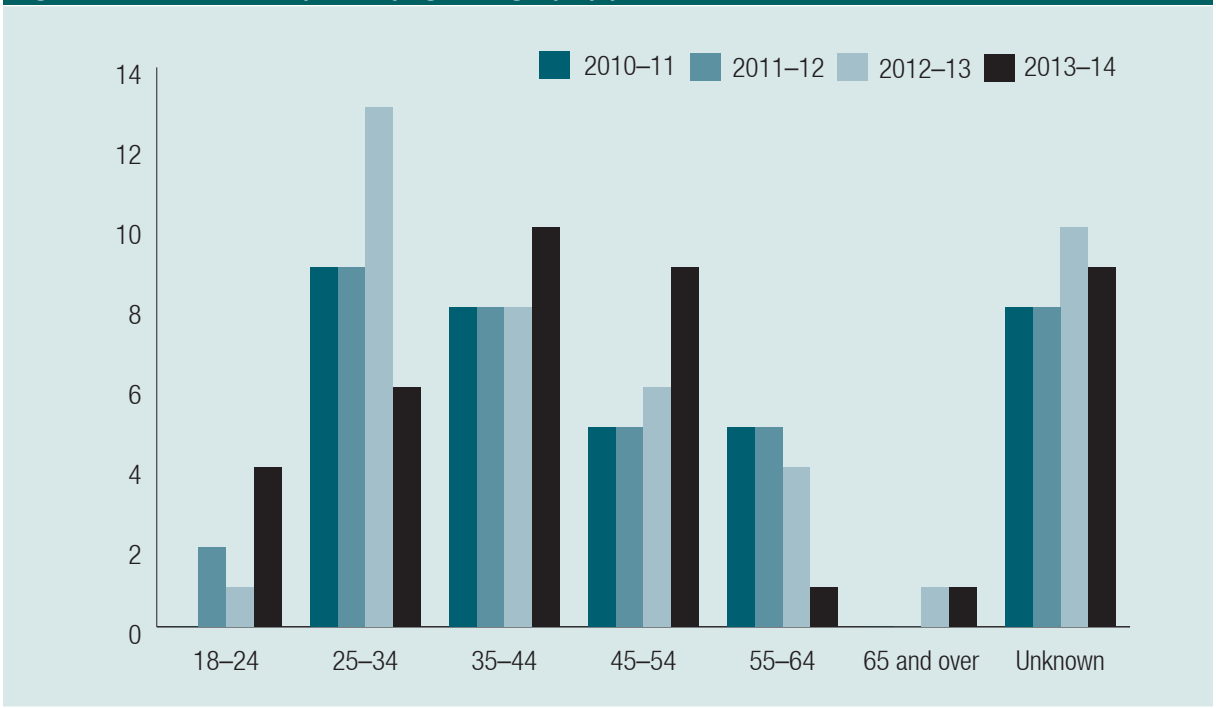
Each year, respondents were asked to answer a number of questions about the demographic characteristics of the suspected perpetrator(s) of the most costly incident of internal fraud. A range of standard demographic information such as age, gender and educational status was sought; there

were also specific questions about the suspects' employment, such as their employment level at the time the fraud was detected and what, if any, motive they gave for committing the fraud. These details can be used to distinguish groups of offenders who share common characteristics from groups of non-offenders (Miethe, McCorkle & Listwan 2006). They may also be useful in identifying issues with internal governance practices such as recruitment and security vetting.

Age

Respondents were asked to indicate the suspect's age at the time the fraud was detected. Information on age was provided in 77 percent of cases (n=120; Figure 1).

Figure 1: Number of suspects by age category by year, 2010–11 to 2013–14



Note: In 2010–11 five entities did not respond to this question (and four skipped most of the section); in 2011–12 seven entities did not respond; in 2012–13 two entities did not respond; in 2013–14 three entities did not respond and one entity's responses were excluded from the analysis due to duplication

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

There were substantial differences in the age category data reported. In 2010–11, 2011–12 and 2012–13, suspects were most frequently aged 25 to 34, with the next most common age group 35 to 44 years. However, in 2013–14, suspects were most frequently reported to be aged 35 to 44 (10 suspects), followed by 45 to 54 (9 suspects). The 2013–14 Commonwealth census findings were more in line with industry surveys like the PwC 2014 survey, which found 39 percent of internal fraud perpetrators were aged 31 to 40, and the 2013 KPMG survey, which found 70 percent of those who committed internal fraud were aged between 36 and 55.

The Association of Certified Fraud Examiners' (ACFE) 2014 survey, one of the few industry surveys that looked at internal fraud incidents committed by more than 1,400 occupational fraudsters from over 100 countries, found the highest percentage of fraudsters (52%) were between the ages of 31 and 45; those who were older tended to commit frauds resulting in larger losses.

Gender

Many entities were unable to report the gender of suspects or chose not to respond to that question (see Figure 2); it is possible that at the time of reporting some entities may not have identified a suspect for the most costly incident of fraud.

Figure 2: Number of suspects by gender by year, 2010–11 to 2013–14

Note: In 2011–12 seven entities did not respond to the question; in 2012–13 one entity did not respond; in 2013–14 three entities did not respond and one entity's responses were excluded from the analysis due to duplication. All 44 entities that participated in 2010–11 provided a response to this question

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

Generally, suspects were more likely to be men than women, except in 2012–13 when 21 (46.6%) suspects were women, compared with 18 (40%) men. The differences between genders narrowed in 2013–14, with 45 percent of suspects being male and 40 percent female. This trend of an increase in female suspects goes against some prior research which found fraud is usually committed by men rather than women (Smith & PwC 2003; ACFE 2014; Warfield 2012; PwC 2015). In contrast to the industry surveys, however, Cifas (2014) found the proportion of female fraud suspects increased from 38 percent in 2012 to 47 percent in 2013. Cifas (2014) noted that it was unknown whether the increase was due to a genuine increase in female offending or, rather, to an increased number of women in the workforce, with more women therefore in a position to commit fraud.

Residence

As expected, given the concentration of Commonwealth entities in the Australian Capital Territory (ACT), suspects were most likely to live in the ACT at the time the fraud was detected. In 2010–11, 16 (38.1%) suspects resided in the ACT; while in 2011–12 this decreased to 11 (28.9%), with suspects most likely to reside in New South Wales (39.5%; n=15). In both 2012–3 and 2013–14, most suspects lived in the ACT (36.4% and 35.0%, respectively).

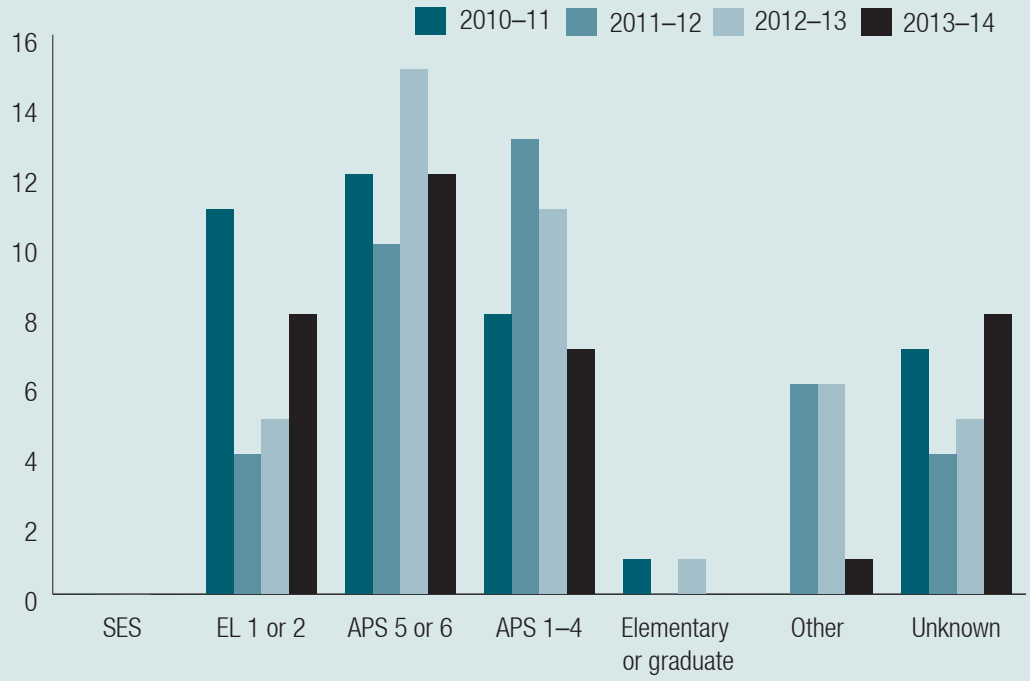
Education

Respondents provided little information on the highest educational level completed by suspects. In 2012–13, 30 respondents indicated the highest educational level completed by suspects was unknown, while in 2013–14, 22 respondents could not specify the highest educational level the suspect had completed. Where respondents knew the suspect's highest educational qualification, tertiary qualifications were most common. In 2013–14, nine suspects (22.5%) had a bachelor's degree or equivalent.

Employment

More than two thirds of suspects each year were employed full time (76.2% in 2010–11, 68.4% in 2011–12, 66.7% in 2012–13 and 67.5% in 2013–14).

Figure 3: Number of suspects by employment level by year, 2010–11 to 2013–14



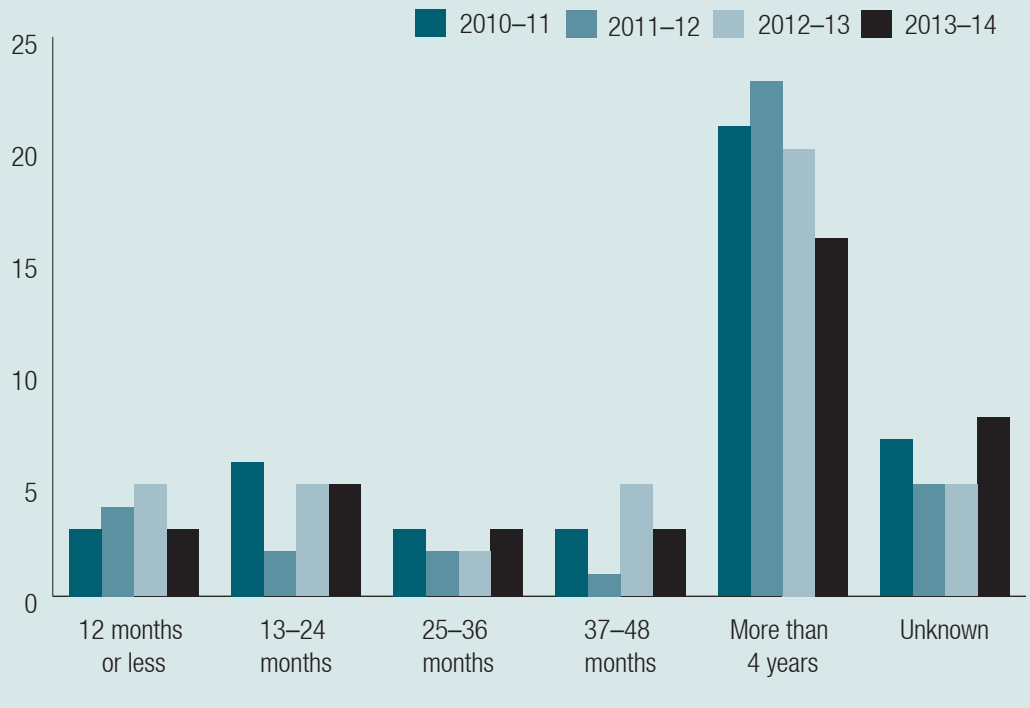
Note: In 2010–11 three entities failed to respond to the question; in 2011–12 seven entities did not respond; in 2012–13 two entities did not respond; and in 2013–14 three entities did not respond and one entity's responses were excluded from the analysis due to duplication

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

Respondents were also asked to indicate the occupational level of the suspect at the time the fraud was detected. As shown in Figure 3, no suspects were employed at Senior Executive Service (SES) level. Respondents reported the majority of suspects were employed at Australian Public Service (APS) levels 5 and 6. In the 2011–12 census, suspects were mainly employed at APS 1 to 4 levels. This is consistent with ACFE's (2014) research, which found 42 percent of internal fraud perpetrators were employees, 36 percent were managers and 19 percent were members of the executive. In contrast, KPMG (2013) found a high percentage of fraud (29%) was committed by executive directors. These differences are largely explicable by the different survey samples involved. For example, the ACFE survey asked organisations about their experiences of fraud against the organisation by employees, whereas the KPMG research asked organisations (in Australia and New Zealand only) to report on the largest fraud perpetrated against their organisation.

Respondents were asked to specify how long the suspect had been employed by or contracted to the entity in any capacity and at any time in the past. As Figure 4 shows, the majority of suspects had been employed by the entity for more than four years. This would indicate that suspects had sufficient time in which to acquire information on any security weaknesses in management, or other opportunities, that could be exploited to perpetrate fraud. This finding is consistent with prior research that found employees who committed fraud had been employed by their organisations for six years or longer (Cifas 2014; Warfield 2012). In 2013–14, there was an increase in the number of entities who could not say how long the employee had been with them.

Figure 4: Number of suspects by length of employment with the entity by year, 2010–11 to 2013–14



Note: In 2010–11 six entities did not respond to this question; in 2011–12 eight entities did not respond; in 2012–13 two entities did not respond; and in 2013–14 three entities did not respond and one entity's responses were excluded from the analysis due to duplication

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

Security clearances

Respondents were asked to indicate the level of security clearance held by the suspect when the most costly internal fraud incident was detected (see Table 3). The majority of security clearances for Commonwealth employees are issued by the Australian Government Security Vetting Agency (AGSVA). At 16 July 2013, just under 320,000 AGSVA-issued security clearances were held by Commonwealth employees; some entities, however, conduct their own security checks or are authorised to conduct security clearances and so the number of individuals who have undergone rigorous scrutiny may be greater than formal clearance statistics alone would indicate (personal correspondence, AGSVA 15 December 2014). Commonwealth security clearance categories and levels changed during the four years examined in this study; Table 3 therefore presents only the principal categories.

Security clearances, while not undertaken specifically as a fraud prevention measure, do assess a person's background, character and values. Depending on the level of clearance held, it should be possible to assume there would be little in the past of a person who has successfully obtained a clearance that would indicate they are likely to commit a criminal or fraudulent act. Nonetheless, each year a small number of Commonwealth employees who hold clearances do commit fraud offences.

Table 3 shows that each year approximately 10,000 individuals held the highest possible clearance of Positive Vetting (formerly Top Secret). Between 2010–11 and 2013–14 the number of fraud suspects holding this clearance decreased from four to just two. This is still of concern, however, as these individuals have undergone the most thorough vetting yet are nevertheless alleged to have acted fraudulently. Very large numbers of Commonwealth employees held lower clearances, and an extremely small proportion of these were alleged to have acted fraudulently (0.005% or less in 2013–14). Between 11 and 15 fraud suspects detected during the four years examined had not undergone any security clearance vetting.

Table 3: Security clearances held by suspects at the time most costly internal fraud was detected, by year 2010–11 to 2013–14 (N)				
Security clearance held	2010–11	2011–12	2012–13	2013–14
	N	N	N	N
Positive Vetting /Top Secret (PV)				
Held[a]	8,991	9,859	10,122	9,773
Suspects[b]	4	4	2	2
Negative Vetting level 2/Top Secret (NV)				
Held[a]	28,032	29,927	29,881	31,534
Suspects[b]	0	0	2	1
Negative Vetting Level 1/Secret/Highly Protected				
Held[a]	86,447	109,125	113,959	125,534
Suspects[b]	4	0	4	4
Baseline/Protected/Entry/Restricted/Confidential				
Held[a]	157,599	175,994	165,816	182,102
Suspects[b]	9	3	9	10
Other checks (non-AGSVA)	1	6	9	1
None	13	15	11	11
Not applicable	1	2	0	1
Unknown	12	8	8	10

Note: In 2010–11 four entities did not respond to the question; in 2011–12 seven entities did not respond; in 2012–13 all entities responded; and in 2013–14 three entities did not complete any of the 'most costly incident' questions and one entity's responses were excluded from the analysis due to duplication

a: AGSVA security clearance data extracted on 25/07/2012, 16/07/2013 and 01/07/2014

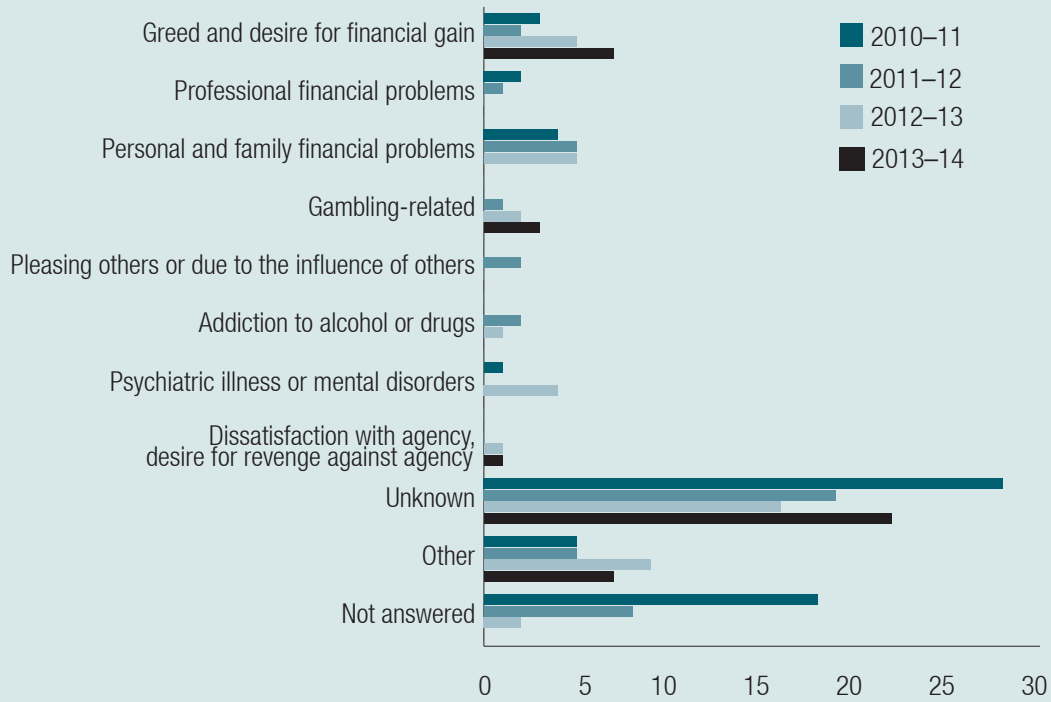
b: Number of suspects identified in 2010–11, 2011–12, 2012–13 and 2013–14

Source: Commonwealth fraud monitoring datasets 2010–11, 2011–12, 2012–13 and 2013–14 [AIC computer file]; AGSVA data

Primary motivation

To gain an insight into why fraud occurs, respondents were asked to indicate the primary motivation for the suspected fraud (see Figure 5). A large percentage of respondents were unable to provide details of the suspect's motivation, and those that were provided could not be independently verified. Responses were based on the information available to respondents at the time of the census.

Figure 5: Primary motivation for the commission of the fraud by year, 2010–11 to 2013–14 (N)



Note: In 2010–11, four entities failed to provide a response to the question; in 2011–12 seven entities did not respond; in 2012–13 two entities did not respond; and in 2013–14 three entities did not respond and one entity's responses were excluded from the analysis due to duplication

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

Of the responses provided, the most frequently cited motive was 'greed and desire for financial gain', which was closely followed by 'personal and family financial problems'. These principal motivations largely correspond with those identified by prior international fraud survey research, where financial strain has been found to be the main motivation for fraud offending (Smith & PwC 2003; ACFE 2014).

Other reasons given for the commission of the suspected fraud incident included the desire 'to avoid staffing cuts'; an 'ambition to have material to protect position'; 'malicious…to cause trouble or mischief' (from the 2010–11 census); reasons that reflected potential stressors in suspects' lives, such as a 'medical condition' and 'personal issues' (both from the 2011–12 census); because they were 'involved in a sexual relationship with another employee' (2013–14 census); or as 'payback for [an] unrelated alleged incident' (2012–13 census).

An example of a suspected internal fraud incident reported in the 2013–14 census is presented in Box 1.

Box 1: Example of internal fraud from the 2013–14 census

The suspect was a full-time female employee who had been employed by the entity for over four years. At the time the fraud was detected the suspect was aged between 25 and 34, held a baseline security clearance and resided in Queensland. The suspect held a bachelor's degree and was employed by the entity at APS level 5–6. The focus of the fraud was information, specifically obtaining or using information without authorisation. The suspect was found to have misused ICT to commit the fraud—that is, accessed information via a computer without authorisation, copied and/or altered data or programs without authorisation and misused email. She did not act alone, colluding with another person to commit the fraud. The fraud was detected through an internal audit; it was investigated by the entity and referred to the AFP.

The fraud continued for a month before it was detected. Had it continued any longer, it would have cost the entity $50,000; however, no money was actually lost as the fraud was discovered before losses were incurred. The suspect was motivated by dissatisfaction with the entity and a desire for revenge. Criminal sanctions were imposed and she was sentenced to six months imprisonment and a fine of $1,000.

Source: Commonwealth fraud monitoring dataset 2013–14

There were indications that some incidents were not the suspects' fault. For example, in three reported instances of fraud, the reasons suspects gave for their actions lacked the element of dishonesty necessary to establish that fraud had been committed. One respondent stated the fraud had occurred due to a 'misunderstanding of entitlements' and another claimed 'accidental usage' to explain suspected fraud relating to the misuse of a government credit card. In 2012–13, one respondent stated the fraud was 'accidental'. In 2013–14, one respondent reported an unintentional fraud that occurred because of 'inaccurate record-keeping'.

In their UK research, Gill & Goldstraw-White (2012) noted offenders often cannot explain why they committed an offence. Accordingly, it may be difficult for those who respond on behalf of an entity to know what precisely motivated the fraudulent conduct. The risk here is that respondents may not know what motivated the fraud and therefore provide instead their best guess as to what transpired. Access to accurate information about what motivates fraud would, importantly, help Commonwealth entities to understand why fraud occurs and how best to guard against it in the future (Padgett 2015).

Offence details

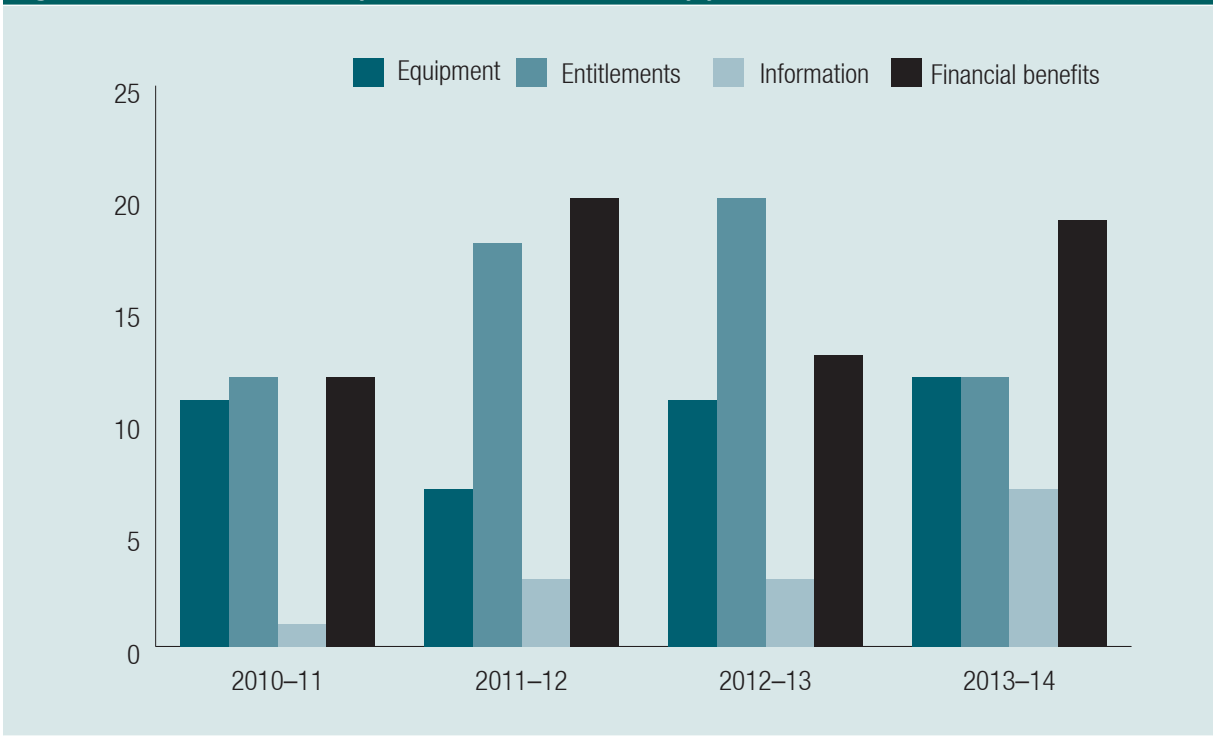
Respondents were asked a number of questions about how suspected frauds were committed, including what the target or focus of the incident was, how the fraud was committed, how long the fraudulent behaviour continued and what financial loss or other impact it caused.

Focus of offending

The most frequently reported targets or focuses of alleged fraud incidents were either financial benefits (such as the theft of cash or currency) or entitlements (such as payroll monies, travel expenses or leave entitlements). Over the four years analysed, information was the least commonly reported focus of fraud (Figure 6), although incidents of fraud focused on information increased from three in 2012–13 to seven in 2013–14. It should be noted that fraud involving access to information may not have a direct financial impact on an entity and, accordingly, may not be have been considered to be a most costly internal fraud incident.

Misuse of information remains an important fraud risk for both the Commonwealth and the private sector. For example, Kroll (2014) found the percentage of organisations that believed they were vulnerable to information theft rose from just seven percent in 2012 to 21 percent in the 2013 survey. Verizon's (2015) *Data breach investigations report* and the Commonwealth Attorney-General's Department *Identity crime and misuse report* (AGD 2015) give an indication of the scale of the problem of misuse of personal information.

Figure 6: Focus of most costly internal fraud incidents by year, 2010–11 to 2013–14 (N)



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

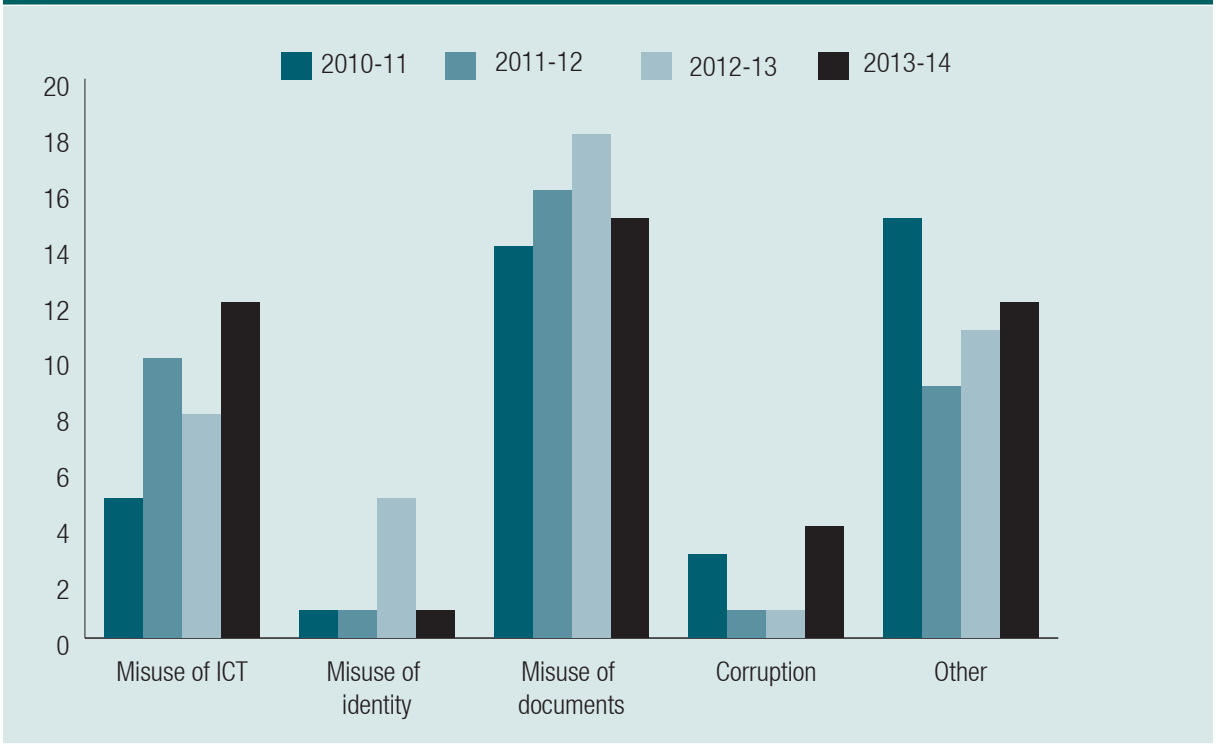
The greatest number of most costly internal fraud incidents each year were focused either on financial benefits or entitlements. This accords with prior fraud research. For example, the ACFE (2014) survey found the most frequent aim of fraud was 'asset misappropriation' involving the theft of monies (and associated financial expenses), equipment or other inventory; it is therefore apparent the primary focus of organisational fraud is similar across both the public and private sectors. Kroll's (2014) survey also found the number of organisations facing internal financial fraud rose from 12 percent in their 2012 survey to 16 percent in the 2013 survey.

Method of offending

Respondents were also asked how the fraud occurred. The most commonly reported method of committing fraud involved the misuse of documents. Methods included in this category included 'creating a false agency document' and 'using a counterfeit or altered document'. The failure to submit a leave application or falsifying a leave application were common responses in the 'other misuse of documents' category (see Figure 7).

The number of fraud incidents involving the misuse of ICT rose from five incidents in 2010–11 to 12 incidents in 2013–14.

Figure 7: Method of committing most costly internal fraud incident by year, 2010–11 to 2013–14 (N)



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

Comparisons of the current findings with those of other research show some differences in the types of frauds perpetrated and the methods used. In a review of employee fraud in Australia that examined 89 frauds resulting in losses of more than $1m, Warfield (2012) found the perpetrator had transferred money from the organisation to a personal bank account in 43 cases. The present census, however, found the most usual method involved the misuse of documents, such as 'creating a false agency document' (reported in five cases in 2011–12 and another five cases in 2012–13), 'falsifying time sheets' (reported in three cases in 2013–14), and 'other…misuse of documents' (reported in 11 cases in 2013–14).

Warfield (2012) examined cases from a variety of industries; only 10 of these incidents occurred in government agencies. Banking was the industry most represented in the report; it could be considered a high-risk environment by comparison with the majority of Commonwealth entities. Unlike the present research, the cases reviewed by Warfield (2012) involved many perpetrators employed in finance. In addition, Warfield's (2012) sample was limited to high-value frauds in excess of $1m, while the present study involved individual losses of approximately half this amount (see below).

Table 4 presents information on the suspect's employment level and means of committing the fraud. The results show no means was used more frequently by individuals at any specific level than any other. Regardless of level, those who committed internal fraud did so primarily through the misuse of documents or information; this was the most common method of committing fraud.

Table 4: Method of committing fraud by employment level, 2010–11 to 2013–14 (N; combined years)

Employment level	Misuse of ICT	Misuse of identity	Misuse of documents/ information	Corruption	Other methods of committing fraud
EL1 & 2	5	2	12	0	9
APS 5 & 6	8	1	23	2	14
APS1–4	14	4	16	1	10
Graduate	1	0	1	0	1
Other	5	1	9	0	3
Unknown	2	1	0	2	11

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

Respondents were also asked if the most costly internal fraud had been committed in concert with other employees. The responses indicate very few internal frauds were committed in collaboration with others. In 2011–12, only three of the most costly internal frauds involved collaboration while, in 2012–13, the number increased to six and, in 2013–14, there were seven internal frauds involving collusion. These results differ from those reported in KPMG's (2013) fraud survey, which found 70 percent of the frauds examined were committed collaboratively. It is possible Commonwealth entities may have difficulty detecting fraud involving collusion, while fraud committed by an individual might be easier to detect; this may account for the observed difference. Further research is required to better understand these differences. Collaborative frauds also tended to occur over long periods, with one fraud reported in 2013–14 continuing for 36 months prior to detection. KPMG's (2013) survey findings support this, indicating that 74 percent of collaborative frauds continued for between one and five years and had a greater financial impact on organisations than those involving sole perpetrators.

Financial loss

Respondents were asked to indicate the extent of the financial loss and costs arising from the most costly incident of internal fraud each year. They were asked:

- What would have been the total financial loss or other impact to the agency, had the incident of fraud been successful and completed?
- What was the total financial loss or other impact actually suffered by the agency as a result of the fraud incident?

Table 5 presents information on the governance arrangements and size of the victim entity for the five most costly frauds reported each financial year.

All of the top five highest-loss cases involved entities with 1,001 or more staff, except for a single *Commonwealth Authorities and Companies Act 1997* (CAC Act) entity with less than 500 staff, which experienced a $36,000 fraud in 2011–12. The greatest loss in these five cases ranged from a minimum of $27,450 to a maximum of $597,997.

There are many reasons why entities that employ more people also report more fraud than others. For example, larger entities:

- may have dedicated fraud control teams and therefore be better equipped to detect fraud than smaller entities;
- may provide services to the public involving greater revenue that could make them more attractive targets than smaller entities; and
- might have more complex administrative and management arrangements, potentially providing additional opportunities for dishonest actions.

Working in a large organisation might also allow greater opportunity to conceal fraud once it has been committed.

Table 5: The five highest-value frauds over four years, by entity size and governance framework

Year, entity size and governance framework	Highest fraud loss	Second highest fraud loss	Third highest fraud loss	Fourth highest fraud loss	Fifth highest fraud loss
2010–11					
FMA	$524,789	$211,826	-	$37,399	$30,000
CAC	-	-	$129,960	-	-
No. of entity employees	1,001+	1,001+	1,001+	1,001+	1,001+
2011–12					
FMA	$330,000	$224,000	-	$40,960	-
CAC	-	-	$129,960	-	$36,000
No. of entity employees	1,001+	1,001+	1,001+	1,001+	0-500
2012–13					
FMA	-	$239,396	$91,107	-	$80,085
CAC	$597,997	-	-	$90,000	-
No. of entity employees	1,001+	1,001+	1,001+	1,001+	1,001+
2013–14					
FMA	$370,000	$231,155	-	$27,450	-
CAC	-	-	$228,000	-	$45,000
No. of entity employees	1,001+	1,001+	1,001+	1,001+	1,001+

Note: Entity staffing levels are subject to fluctuation; these are shown as reported at time of census
Source: Commonwealth fraud monitoring datasets 2010–11, 2011–12, 2012–13 and 2013–14 [AIC computer file]

Prior survey research has found offenders in managerial positions were responsible for the highest financial losses arising from fraud incidents (KPMG 2013; ACFE 2014). The present census, however, found employees at the APS 1–4 level were alleged to have committed more frauds valued between $100,001 and $300,000 than staff at other levels (see Table 6). Of the three employees alleged to have caused losses over $300,000, one was an Executive Level (EL) 1–2, another was an APS 5–6 and the third, who was alleged to have defrauded $370,000 in 2013–14, was employed in a non-APS position; no funds were recovered in that case. Four other suspects employed at the APS 1–4 level were allegedly responsible for losses of between $100,001 and $300,000.

Table 6: Losses for the most costly internal fraud incident by employment level, 2010–11 to 2013–14 (N; combined years)

Amount lost	EL1 & 2	APS 5 & 6	APS 1–4	Graduate	Unknown	Other
			(N)			
$0–1,000	6	4	3	0	9	4
$1,001-10,000	7	13	8	1	6	1
$10,001–50,000	4	8	5	0	1	2
$50,001–100,000	0	2	2	0	0	1
$100,001–300,000	0	0	4	0	0	3
$300,001–600,000	1	1	0	0	0	1

Note: In 2011–12 one entity could not specify an occupational category; in 2012–13 two entities that provided no occupational details; and in 2013–14 two entities reported the same most costly incident of internal fraud, but only one was included for analysis. In 2010–11, all respondents provided employment details

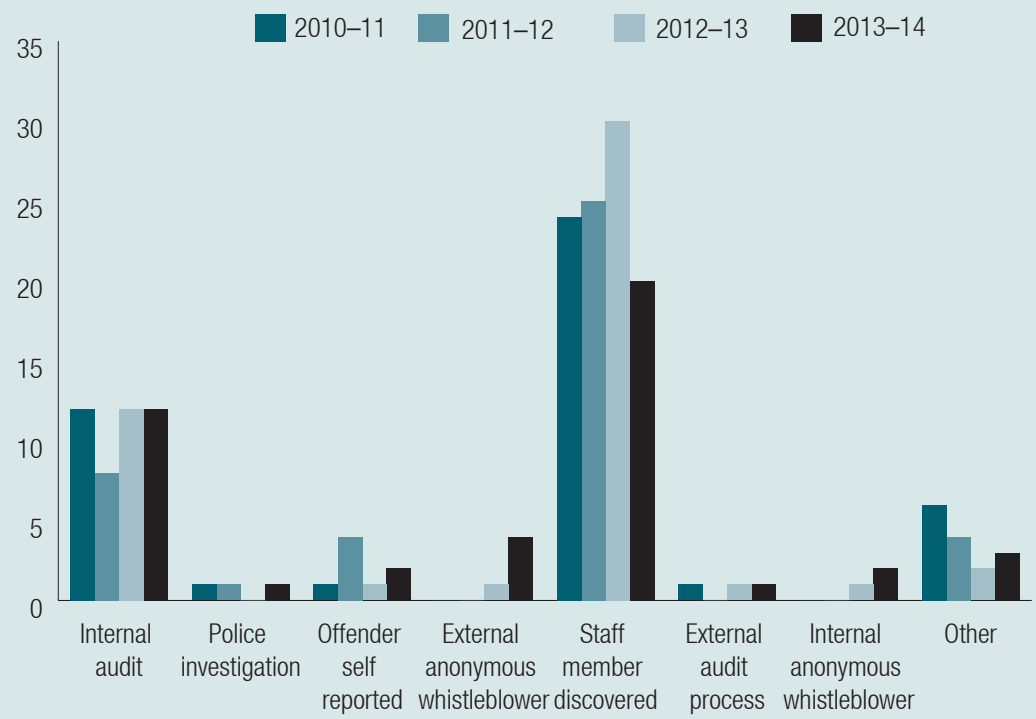
Source: Commonwealth fraud monitoring datasets 2010–11, 2011–12, 2012–13 and 2013–14 [AIC computer file]

Discovery of the fraud and outcome

Detection

Respondents were asked how the alleged fraud was detected. In all four years analysed, most frauds were detected through internal controls—that is, internal audits or discovery by colleagues (see Figure 8). Infrequently, fraud was detected externally, including through tip-offs, whistleblower action and detection by external agencies.

Figure 8: Detection of fraud incidents by year, 2010–11 to 2013–14 (N)



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

In 2011–12, four respondents indicated the suspect had self-reported to the entity in question; in 2013–14 two suspects self-reported; and in each of the other years only one self-report occurred. Self-reporting often occurs where an individual has a gambling problem or other compulsive reason for offending, and realises they need external help to deal with the problem (Sakurai & Smith 2003). Other detection methods specified by entities included that they were 'advised by another agency' and through a 'security clearance re-evaluation process'. Whistleblowing by both external and internal parties led to more detections between 2012–13 and 2013–14; just one entity detected fraud via an external whistleblower in 2012–13, rising to four entities in 2013–14. Whistleblowing has long been important in the detection of organisational fraud (KMPG 2013; PwC 2014).

In Kroll's (2014) annual global fraud survey, insider fraud was found to be on the rise, as were internally detected frauds. PricewaterhouseCoopers (2014) separated approaches to detection into three categories in its 2014 survey:

- corporate controls (including data analytics, internal audits and fraud-risk management), which accounted for 55 percent of fraud detected;
- corporate culture (such as tip-off lines and whistleblowers), which accounted for 23 percent of detected fraud; and
- means of detection that were beyond corporate control, which accounted for 21 percent of detected fraud.

In contrast to Commonwealth entities surveyed, where the majority of fraud was detected by staff members or colleagues, Cifas (2014) found only 11 percent of internal frauds were detected and/or reported by staff. Their report noted the low rate of fraud detection by staff members was something that needed to be improved—in particular, managers must create a culture in which all employees are made aware of the risk of fraud and their obligation to report any incidents that come to their attention (Cifas 2014). The results of the present research show Commonwealth officials understand the importance of their role in detecting and preventing fraud.

Investigation outcomes

Respondents reported that over 80 percent of investigations into the most costly internal fraud incidents each year were internal. In 2011–12, one respondent reported the matter was dealt with internally after the Australian Federal Police (AFP) declined to investigate.

Respondents were asked to describe the outcome of investigations and any associated legal proceedings. Depending on the length and complexity of the investigation, some respondents were able to supply details of matters referred for prosecution, while some matters were still under investigation (despite the fact that respondents were asked to nominate only an instance of fraud for which an investigation had been completed during the year in question).

Over the four years analysed the number of suspects who admitted to fraud allegations in full declined, from 10 in 2010–11 to three in 2013–14. In 2011–12, one matter was referred to the AFP for investigation; the AFP declined to investigate and the fraud was then dealt with internally. Three matters were investigated by external investigators other than police in 2011–12, and another three matters by police. In 2012–13 six matters were investigated by external investigators other than police, another three were investigated by police, and 41 incidents were investigated internally. In 2013–14, there were four cases where an internal investigation found the allegations did not amount to fraud. No matters were referred for civil action in any of the four years analysed.

Table 7 shows the outcomes of internal investigations. In 2013–14 three matters were referred to the AFP for investigation and four to the Commonwealth Director of Public Prosecutions (CDPP) for prosecution.

Table 7: Outcome of internal investigation by incident number, 2010–11 to 2013–14 (N)				
Outcome	2010–11	2011–12	2012–13	2013–14
		(N)		
Suspect admitted allegation in full	10	4	3	3
Suspect admitted allegation in part only	0	3	2	0
Matter referred for civil action	0	0	0	0
Suspect dismissed from employment	5	6	8	4
Suspect reprimanded	3	1	4	4
Suspect resigned or left employment	7	5	8	7
Matter referred to law enforcement agency	2	1	1	3
Matter referred to prosecution agency	2	2	3	4

Note: In 2010–11 two entities did not respond to the question; in both 2011–12 and 2012-13 one entity did not respond; and in 2013–14 one entity did not respond and one was excluded from the analysis due to duplication
Source: Commonwealth fraud monitoring datasets 2010–11, 2011–12, 2012–13 and 2013–14 [AIC computer file]

In 2013–14, no legal proceedings were undertaken in relation to 20 incidents. One incident in 2013–14 was resolved by the relevant manager counselling the suspect. In 2013–14 two entities prosecuted offenders. One was convicted and sentenced to six months in custody and a fine of $1,000; the other was found guilty and fined $1,500, with a reparation order made in respect of the outstanding amount defrauded.

The present census also found a number of individuals were dismissed from their employment each year following investigations. Dismissal occurred in nine percent of matters in 2013–14 and 18 percent in 2012–13. In their review of internal organisational fraud in the United Kingdom, Cifas (2014) found a higher percentage of employees (63%) had been dismissed from their employment for fraud than the current study.

Recovery

Respondents were asked to indicate how much money or other property was recovered from the suspect in the year of reporting. Any amount recovered might not represent the total amount recovered in respect of the most costly incidents, as recovery action often continues after an investigation has concluded. What can be determined is the entity's total financial loss and the amount recovered from suspects during each year. Over the four years examined, the proportion of losses recovered from suspects fluctuated considerably (see Table 8), ranging from just 3.4 percent in 2013–14 to 57.4 percent in 2012–13.

Table 8: Entities' financial losses and monies recovered from most costly incident, 2010–11 to 2013–14

Year	Amount lost ($)	Amount recovered ($)
2010–11	1,034,447	121,478
2011–12	830,185	346,559
2012–13	1,328,617	762,361
2013–14	1,001,181	34,244

Note: in 2010–11, 22 entities were able to quantify a loss and 17 entities recovered funds from suspects; in 2011–12, 23 entities quantified their losses and 17 entities recovered funds; in 2012–13, 23 entities quantified a loss and 14 entities recovered funds. In 2013–14, 20 entities quantified a loss (excluding one entity that reported a duplicated incident) and eight entities recovered funds from the suspect

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

The highest losses occurred in 2012–13, although the amounts recovered that year were also the highest of any of the four years (see Table 8). Between 2012–13 and 2013–14 there was a 25 percent decrease in the amount of monies lost by entities; however, during the same period the amount of money entities recovered decreased by 96 percent. This could be explained by the number of costly incidents in any given year where an offender spent the funds obtained on their lifestyle, thus making recovery impossible. Recovery action during the most recent year studied, 2013–14, may not have been completed—potentially explaining why the reported recovery rate is low. An example of one most costly internal fraud incident reported in 2010–11 is presented in Box 2.

Box 2: Example of a most costly internal fraud from the 2010–11 census

The suspect was a full-time employee at the time the incident was detected and held a baseline security clearance. He was aged between 25 and 34, lived in Victoria and had been employed by the entity for more than four years at the time the incident was detected. He had a postgraduate qualification and was employed at the APS 5–6 level. The focus of the fraud was to obtain a 'benefit by deception'. The fraud involved 'misuse of identity–other' and 'misuse of voluntary position in a non-profit organisation'.

The incident was first detected in July 2010 through an internal audit/investigation and investigated internally by the agency. The entity's total financial loss was $524,789, and $13,327 was recovered. The fraud continued for 84 months.

The individual acted alone. The motive cited by the respondent was 'greed and financial gain'. The date the investigation was finalised was not provided, but the respondent noted that the investigation was ongoing, and legal proceedings were due to commence at the time the census was completed.

Source: Commonwealth fraud monitoring dataset 2010–11

Conclusions

While there may be no such thing as a typical financial crime—that is, one that could be found in every organisation—some consistent trends can be identified by reviewing the most costly internal fraud incidents reported by entities over the four-year period. In every year, the most common focus of the frauds reported was either employee entitlements or financial benefits, suggesting these

areas should be more tightly controlled by entities. Until 2013–14, the most common means of fraud by internal perpetrators was misuse of documents; however, in 2013–14 there was an increase in the misuse of ICT, and it became the most common means of committing fraud. Over the four-year period, it was consistently found that suspects had been employed by the entity they defrauded for more than four years, which implies those employees may have had more time to familiarise themselves with internal controls or, alternatively, had greater responsibility and were more trusted.

Further analysis of suspects' primary motivations is needed, as few respondents were able to supply this information. Understanding the motivations and rationalisations of fraudsters is of critical importance in designing effective fraud-control measures. More research is also necessary to determine why no employees at the senior management (SES) level have been identified as fraudsters in census responses, and whether this is because they have not committed offences, have not been detected offending, or have committed fraud which has simply not been reported in the current research. Research suggests people employed at higher management levels do commit fraud, and that the frauds they commit cost more and have a greater impact than those committed by people employed at lower levels (KPMG 2012). In addition, further research is needed to determine how suspects indicate they may be engaging in fraudulent activity—in other words, to identify red flags in employee behaviour. By understanding the behaviours that might indicate fraud or serious misconduct, entities can act quickly to reduce its impact.

This study confirms the findings of prior research on a number of aspects of fraud within public sector organisations; it also identifies some of the ways serious fraud within Commonwealth agencies differs from that reported in previous studies. In particular, the number of women who commit costly fraud, and the number of employees with security clearances who commit fraud, requires further scrutiny. For example, high numbers of female suspects were involved in allegations of internal fraud, unlike previous studies that generally show higher proportions of male offenders. This may be due to the number of women in the Australian Public Service, but it is not known at this stage whether this is so or if there has been a genuine increase in the number of women committing internal fraud. Future research will help to identify new and emerging risks and assist in the development of new fraud-control initiatives to reduce the incidence of Australia's most costly form of crime (Smith et al. 2015).

References

URLs current at February 2016

Association of Certified Fraud Examiners 2014 (ACFE). *Report to the nations on occupational fraud and abuse: 2014 global fraud study*. http://www.acfe.com/rttn.aspx

Attorney-General's Department 2015. *Identity crime and misuse in Australia 2013–14*. http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Identity-Crime-and-Misuse-in-Australia-2013-14.DOCX

Cifas 2014. *Employee fraudscape: Depicting the UK's fraud landscape*. London: Cifas. https://www.cifas.org.uk/research_and_reports

Gill M & Goldstraw-White J 2012. Why commit fraud, in Doig A (ed), *Fraud: the counter fraud practitioner's handbook.* Surrey, UK: Gower Publishing:19–28.

KPMG 2013. *Global profiles of the fraudster: White-collar crime— present and future*. http://www.kpmg.com/global/en/issuesandinsights/articlespublications/global-profiles-of-the-fraudster/pages/default.aspx

Kroll 2014. *2013/2014 Global Fraud Report. Who's got something to hide: Searching for insider fraud*. New York: Kroll. http://fraud.kroll.com/report-archive/

Minister for Justice 2014. *Resource Management Guide No 201: Preventing, detecting and dealing with fraud*. https://www.ag.gov.au/CrimeAndCorruption/FraudControl/Pages/FraudControlFramework.aspx

Padgett S 2015. *Profiling the fraudster: Removing the mask to prevent and detect fraud*. Hoboken, NJ: John Wiley & Sons

Peltier-Rivest D & Lanoue N 2012. Thieves from within: occupational fraud in Canada. *Journal of Financial Crim*e 19(1):54–64

PricewaterhouseCoopers 2014. *Economic crime: A threat to business globally: PwC's 2014 Global Economic Crime Survey.* www.pwc.com/crimesurvey

PricewaterhouseCoopers 2011. *Global Economic Crime Survey 2011. The 6th biennial global economic crime survey*. http://www.pwc.com/us/en/forensic-services/publications/global-economic-crime-survey-2011.html

Ramamoorti S 2008. The psychology and sociology of fraud: Integrating the behavioural sciences component into fraud and forensic accounting curricula. *Issues in Accounting Education* 23(4): 521–533.

Sakurai Y & Smith RG 2003. Gambling as a motivation for the commission of financial crime. *Trends and Issues in Crime and Criminal Justice* no. 256. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/241-260/tandi256.html

Smith RG 2015. Spotting a typical fraudster. *IBAC Insights* 2. http://www.ibac.vic.gov.au/news-and-publications/ibac-insights-january-2015/spotting-a-typical-fraudster

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://www.aic.gov.au/publications/current%20series/rpp/121-140/rpp129.html

Smith RG and PricewaterhouseCoopers 2003. *Serious Fraud in Australia and New Zealand. Research and Public Policy Series* no. 48. Canberra: Australian Institute of Criminology/PricewaterhouseCoopers.

Verizon 2015. *Data Breach Investigations Report 2015*. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf

Warfield B 2012. *Million dollar employee fraud in Australia*. Sydney: Warfield & Associates http://www.warfield.com.au/publications.html

General editor, *Statistical bulletin series*: Dr Rick Brown, Deputy Director, Australian Institute of Criminology. For a complete list and the full text of the papers in the *Statistical bulletin series*, visit the AIC website at: aic.gov.au

ISSN 2206-7302

GPO Box 1936
Canberra ACT 2601, Australia
Tel: 02 6268 7166