Australian Government
Australian Institute of Criminology

Research in Practice

No. 41 March 2016

Fraud within the Commonwealth: A census of the most costly incidents, 2010–11 to 2012–13

Penny Jorna & Russell G Smith

Fraud against the Commonwealth is defined as 'dishonestly obtaining a benefit or causing a loss, by deception or other means'. This definition is set out in the current Commonwealth Resource Management Guide (no. 201) *Preventing, detecting and dealing with fraud*, issued by the Australian Government Minister for Justice (2014). This form of fraud may be committed by individuals who do not work for government bodies, such as those who dishonestly claim benefits or some other financial advantage (external fraud), or by those employed by entities including staff and contractors (internal fraud). Fraud may also involve collaboration between internal and external parties.

Button & Brooks (2009) suggest that the development of an anti-fraud culture is largely targeted at combatting internal fraud. The Association of Certified Fraud Examiners (ACFE) has defined internal fraud as:

> ...the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organisations' resources or assets (ACFE 2014: 6).

This paper aims to provide a better understanding of the nature of internal fraud against the Commonwealth, and the personal background details of those alleged to have committed the deception. It reports on the results of an annual census of Commonwealth entities which collected information on the single 'most costly' incident of internal fraud that they experienced in 2010–11 to 2012–13. During these years, 137 Commonwealth entities reported 7,809 incidents of internal fraud. Of these, 125 chose one incident each year that they considered their most costly internal fraud. Information was provided on how and why fraud was committed, estimated financial losses involved, the personal circumstances of the principal alleged perpetrators, and how the incidents were dealt with in terms of investigation, prosecution and judicial outcomes. Most incidents involved non-corporate Commonwealth entities (formerly governed under the *Financial Management and Accountability Act 1997* (Cth) see Table 1). Entities with more than 1,000 staff contributed more incidents for this study than smaller bodies.

Table 1 Size and governance of reporting entities, 2010–11 to 2012–13 (n)

Governance and size of entity	2010–11	2011–12	2012–13
Corporate entity	12	14	15
Non-corporate entity	30	24	30
0–500 staff	13	7	9
501–1,000 staff	6	7	9
1,000+ staff	22	24	27

Note: These data relate only to those entities that provided information on the most costly incidents of internal fraud experienced

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

 ISSN 1836-9111

The results provide a concise summary of the most serious cases of occupational fraud detected by Commonwealth entities in recent years. They will be used to develop fraud prevention and risk management within entities and to deter those who may be at risk of committing fraud, or re-offending (see Armstrong 2012).

Internal fraud, although just one aspect of fraud against the Commonwealth, can be particularly damaging to the organisations involved. For example, fraud incidents may damage its reputation or result in adverse media attention for the government as a whole. Internal fraud within Commonwealth entities may deplete government resources that could be used for important programs, lead to loss of employment for other staff, or damage the working environment in the organisations involved (Peltier-Rivest & Lanoue 2001).

Methodology

All Commonwealth entities are required by the Commonwealth Fraud Control Policy to complete a confidential, online questionnaire each September regarding their experience of fraud during the preceding financial year and their current fraud control arrangements. More than 80 percent of entities usually participate, reporting details of their fraud control arrangements, and instances of suspected fraud that they had detected or been informed of during the relevant 12 months. Respondents are also asked to choose one incident involving internal fraud from all those experienced in which an investigation or review had been concluded during the relevant financial year. This is irrespective of whether the fraud had been committed or the investigation or review had been started during or prior to that year. The incident must have resulted in the largest financial loss being suffered by the reporting entity among all the internal fraud investigations that were finalised during that year. If an incident involved more than one person, respondents were asked for information relating only to the principal suspect. Participants were left to determine their own definition of principal suspect. A comparable study by the Association of Certified Fraud Examiners (ACFE) and Peltier-Rivest (2007: 28), defines principal suspect as: 'the person who works for the victim organisation and is the primary culprit'.

Sample

Of the 137 entities experiencing internal fraud during the three years examined, 125 (91.2%) completed all or part of the questions dealing with their most costly incident each year (Table 2). A number of respondents were unable to provide all of the demographic information sought such as 'highest level of education', 'sex of offender' and 'length of period of employment with agency'. Other information was more readily available.

Table 2 Responding entities

Year	No. of entities that experienced internal fraud	No. and % of entities that responded to questions on the most costly incident	
	N	N	%
2010–11	48	42	87.5
2011–12	44	38	86.4
2012–13	45	45	100.0
All	137	125	91.2

Source: Commonwealth fraud monitoring datasets 2010–11, 2011–12 and 2012–13 [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 information provided in response to the questionnaire. On occasions, suspects may not have told entities why they committed the offence and if the suspect was simply dismissed from the organisation, details of the outcome of the case may not be known.

Gill & Goldstraw-White (2012) note that often offenders themselves could not explain why they committed an offence. So it may be difficult for entity representatives to know

what motivated the offence. The risk is that respondents may not be aware of the correct information and instead provide their best guess as to what transpired.

It is apparent from the results below that a number of respondents were unable or unwilling to answer some questions. Often the relevant information had not been collected during investigations, or could not be retrieved.

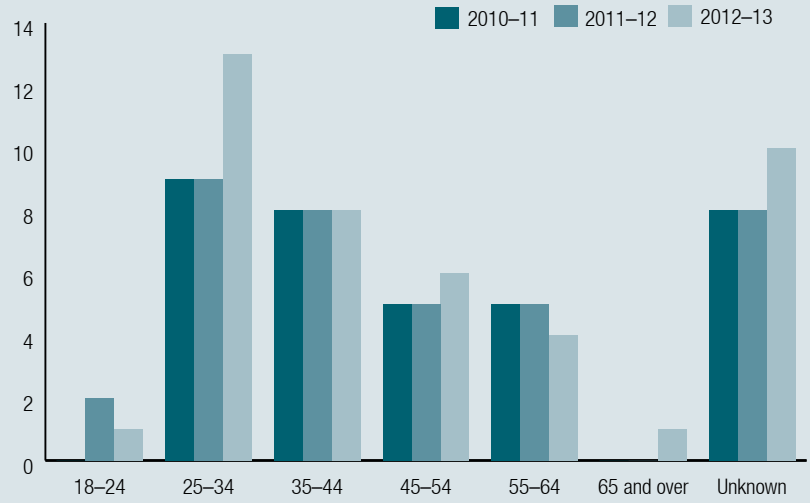
Information on the outcomes of proceedings was also often unavailable as some had not been finalised, or those reporting had not been notified of the results of trials and appeals.

Nonetheless, the study provides a useful indication of how, why and by whom fraud within the Commonwealth takes place. It should be useful to those in fraud control and risk management who are working to address the problem.

Profiling occupational fraud

One of the principal research questions of the study focuses on the characteristics of those alleged to have committed fraud within Commonwealth entities. Questions were asked about the demographic backgrounds of suspects, their employment histories and security clearance levels. This information can be used to help distinguish groups of offenders sharing common characteristics from groups of non-offenders (Miethe, McCorkle & Listwan 2006). Such information can also be used to develop risk profiles of those most likely to commit fraud and as well as risk-reduction strategies (Bales & Fox 2009). Ramamoorti (2008) stresses the importance of organisations understanding who commits fraud, and the causes and motivations. This can be used to manage fraud risks more effectively and to develop effective prevention strategies.

Figure 1 Number of suspects by age category, by year



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

Fraud profiling is not a complete solution to the problem of occupational dishonesty. As Smith (2015: np) argues:

> The evidence available from fraud profiling can be used to identify those at highest risk of offending who can then be provided with additional support and advice to help them to act honestly in the workplace. As with other areas of crime control, intervening at the earliest opportunity has considerable benefit in terms of reducing losses and harms and enabling otherwise productive employees to continue to pursue risk-free patterns of work.

Results

The results of the 124 most-costly incidents reported by respondents for the three years are divided into three categories:

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

Caution is needed in interpreting some of the results, as response rates for some variables were low where information was not collected or unavailable. The total sample of 124 incidents was also relatively small, although in keeping with prior research. At the end of each section, some brief comparisons are made with the results of prior fraud survey research.

Characteristics of suspects

Age

In 24 percent (n=43) of cases, the age of the suspect was unknown. Where it was known (n=33), few were over the age of 65 and relatively few aged between 18 and 24 years. No suspects were aged 17 years and under as might be expected for a sample of this kind. As shown in Figure 1, the age group with the highest number of suspects was 25–34 years.

This is somewhat younger than KPMG's (2013a) typical fraudster age of between 36 and 55 years. However, KPMG's study of 596 fraud investigations conducted between 2011 and 2013 in Australia and New Zealand included both internal as well as external fraud in both public and private sectors.

One of the few industry surveys that looked solely at internal fraud incidents among more than 1,400 occupational fraudsters from over 100 countries conducted by ACFE (2014) found that 52 percent of fraudsters were aged between 31 and 45 years. Those who were older tended to cause larger losses.

Gender

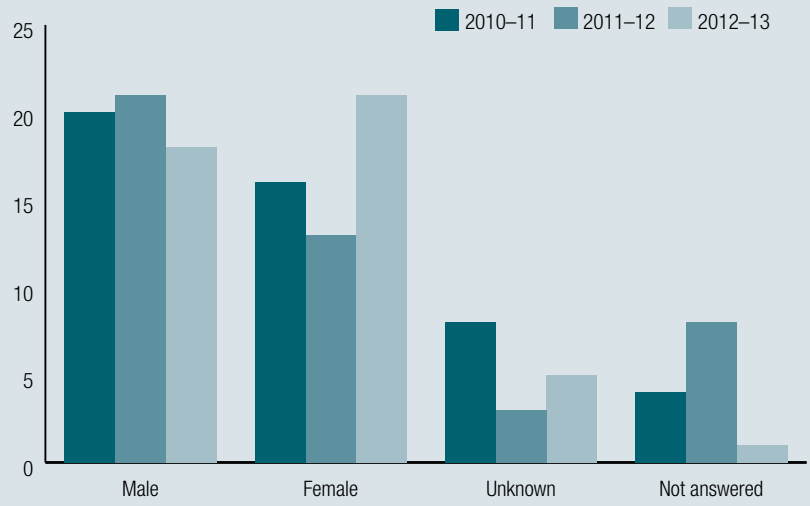
A large number of entities were unable to identify the gender of suspects, or chose not to respond to that question (see Figure 2).

Generally, there were slightly more male than female suspects, except in 2012–13, with 21 (46.6%) entities identifying a female suspect compared with 18 (40%) identifying a male suspect.

Prior fraud research has found that males rather than females usually commit fraud (Smith & PwC 2003; BDO Stoy Hayward 2008; KPMG 2011; ACFE 2014). One possible reason for relatively more female suspects in the Australian Public Service (APS) is that more females than males are employed within the service. During 2010–11, 57.4 percent of ongoing APS employees were females. That declined in 2011–12 to 57.3 percent and, as at June 2013, it had risen to 57.5 percent (APSC 2011, APSC 2013).

Supporting the APS findings, the Australian Bureau of Statistics (ABS) labour force statistics for the 12 months to 30 June 2013 indicate that the number of females employed full-time had increased, whereas the number of males employed full-time had decreased (ABS 2013).

Figure 2 Number of suspects by gender by year



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

A study by Goldstraw, Smith and Sakurai (2005), examines a sample of 208 serious fraud cases heard in the Australian and New Zealand higher courts. It was found that 21 percent (n=43) of offenders were females, with most frauds committed by males. Nearly 70 percent (n=29) of the females who had offended were accused of committing fraud while employed. The findings of this study might explain some of the differences found in the current report when compared with industry surveys.

The ACFE (2014) survey found that gender was associated with the amount of money lost. It found that males who committed fraud had losses attributed to them that were 123 percent higher in value than frauds committed by females. The findings from the present research were mixed regarding gender and losses. In 2010–11 and 2011–12 the results were more consistent with the ACFE (2014) findings, with the most costly frauds all being perpetrated by males. However, in 2012–13 the suspect in the most costly incident was a female.

Residence

As was to be expected with the high concentration of Commonwealth entities located in the Australian Capital Territory (ACT) suspects were most likely to live in the ACT. In 2010–11, 16 (38.1%) suspects lived in the ACT, while in 2011–12 this decreased to 11 (28.9%). In that year, more suspects lived in New South Wales (39.5%, N=15). In 2012–13, 35.6 percent (N=16) of all suspects lived in the ACT.

Education

Little information was provided by respondents on the highest educational level attained by suspects. For example, in 2012–13, 30 respondents indicated that the highest educational level the suspect obtained was unknown. Although little information was provided by respondents regarding this variable, the findings showed that when an educational level of a suspect was known, the most common level completed was at tertiary level. However, as ACFE (2014) research noted, education is a secondary factor in predicting fraud as other factors, such as employment level and occupation may be better indicators of fraud risk.

Employment

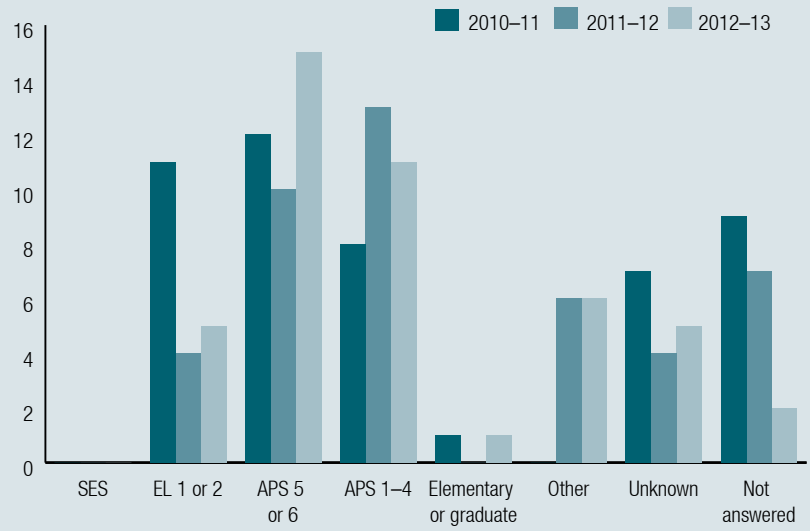
Most suspects were employed full time (76.2% in 2010–11, 68.4% in 2011–12 and 66.7% in 2012–13).

Respondents were asked to indicate the occupation of the suspect at the time the fraud was detected. From Figure 3 it is apparent that there were no suspects employed as executive

management at the senior executive level (SES). These findings are somewhat different from research into occupational fraud carried out in the past (KPMG 2013a; ACFE 2014), although Kroll (2014) did find that 42 percent of internal fraud incidents involved a junior employee. The absence of SES-level suspects in the present study could be due to such individuals not being identified as fraud suspects, or not being suspected of the specific most costly incidents reported in this study. Further research may be required to understand this finding more fully.

Respondents reported that in 2012–13 the highest number of suspects were at APS Levels 5 and 6 (n=15, 40% of respondents who provided this information). For the 2011–12 census period, the highest number of suspects were employed at APS 1–4 levels (n=13, 39%). This is consistent with ACFEs (2014) research that found that 42 percent of internal fraud perpetrators were employed at the employee level, 36 percent at the managerial level and 19 percent were owners or part of the executive.

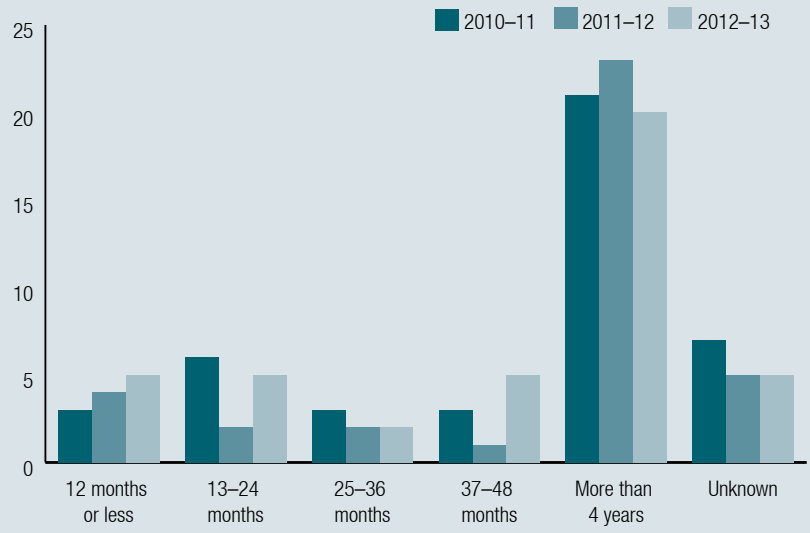
Figure 3 Number of suspects by employment category by year



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

Respondents were also asked to indicate how long the suspect had been employed/contracted by the entity in any capacity and at any time in the past. As shown in Figure 4, most suspects had been employed by the entity for more than four years. This would indicate that suspects had sufficient time to discover security weaknesses in management or other opportunities that could be used to perpetrate fraud. In 2012–13, nine respondents indicated that suspects had been employed by the entity for longer than six years. These are included in the category 'more than four years' in Figure 4. This finding is consistent with prior research that has found that employees who committed fraud had been employed for six years or longer (KPMG 2013b; Warfield 2013).

Figure 4 Number of suspects by length of employment with the entity by year



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

Security clearances

Respondents were also asked to indicate the highest security clearance held by the suspect when the most costly internal fraud incident had been detected. In the Commonwealth, the categories of clearance levels changed during the three years examined and so data reflect the principal groupings of categories of clearance. In the Commonwealth, the Australian Government Security Vetting Agency (AGSVA) issues most security clearances. As at 16 July 2013, almost 320,000 security clearances were held. Some entities 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 (personal correspondence AGSVA 15 December 2014). 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 undertaken, it is assumed that if a person has successfully undergone a clearance procedure there should be little in their past to indicate that they might commit a criminal or fraudulent act. It is also important to note that security clearances may not be required for public servants who do not have reason to access classified information or resources. Such individuals may pose lower fraud risks, as often access to sensitive classified information is needed to commit some kinds of financial crime.

Table 3 Security clearances held by suspects when most costly internal fraud incidents were detected

Security clearance level grouping		2011 N	2012 N	2013 N
Positive vetting/top secret (PV)	Held[a]	8,991	9,859	10,122
	Suspects[b]	4	4	2
Negative vetting level 2/top secret (NV)	Held[a]	28,032	29,927	29,881
	Suspects[b]	0	0	2
Negative vetting level 1/ secret/highly protected	Held[a]	86,447	109,125	113,959
	Suspects[b]	4	0	6
Baseline/protected/entry/ restricted/confidential	Held[a]	157,599	175,994	165,816
	Suspects[b]	14	3	9
Other checks (non-AGSVA)		0	6	9
None		13	15	11
Not applicable		1	2	0
Unknown		12	8	8
Not answered		4	7	0

a AGSVA security clearance data extracted on 23 March 2011, 25 July 2012, and 16 July 2013
Source: Australian Government Security Vetting Agency (AGSVA) data

b Suspects identified in 2010–11, 2011–12 and 2012–13
Source: Commonwealth fraud monitoring datasets 2010–11, 2011–12 and 2012–13 [AIC computer file]

An individual's clearance level may be relevant to fraud risk in a number of ways. On the one hand, a person employed at a higher level (with a higher level of clearance) may have access to material that could facilitate fraud and thus be more likely to offend. On the other hand, a person employed at a lower level (without a clearance) may have fraud risk factors present in their background that might make them susceptible to offending.

Over the three-year period, 10 suspects held the highest security clearance (either top secret or positive vetting in 2012–13) when the fraud was detected. Of these, six were from law enforcement or national security bodies, where the highest-level security clearances are most often required of staff. A total of 46 suspects held some level of security clearance when the alleged fraud was detected, with a further 15 suspects who had undertaken either security clearances within entities or some other form of police background check (see Table 3). A large number of respondents failed to answer this question, or did not know the answer (28%, N=39). This could have been due to the person completing the questionnaire not having all the relevant details about the suspect, or the suspect not being identified following the investigation.

Prior fraud survey research has not examined government security vetting procedures, although some studies have considered the prior criminal history of offenders. For example, Warfield (2013) found in his review of 120 cases of fraud in Australia, involving 123 employees, that only five had a prior criminal history of deception-related offences. Similarly, the study of serious fraud by Smith & PricewaterhouseCoopers (2003: 40–41) found that 56 percent of offenders had no prior criminal history, while 17 percent had prior fraud offences, and a further 10 percent had both fraud and non-fraud offences. These findings demonstrate that a clean criminal record is not a guarantee against fraud.

Primary motivation

To gain an insight into why fraud occurred, respondents were asked to indicate the primary motivation or other reason for committing the suspected fraud incident (see Figure 5). Ten categories were provided, including a further miscellaneous category. The information provided was unable to be independently verified, but was the respondent's assessment of the primary motivation, based on current available information. A large percentage of respondents simply did not know why the suspect committed the fraud.

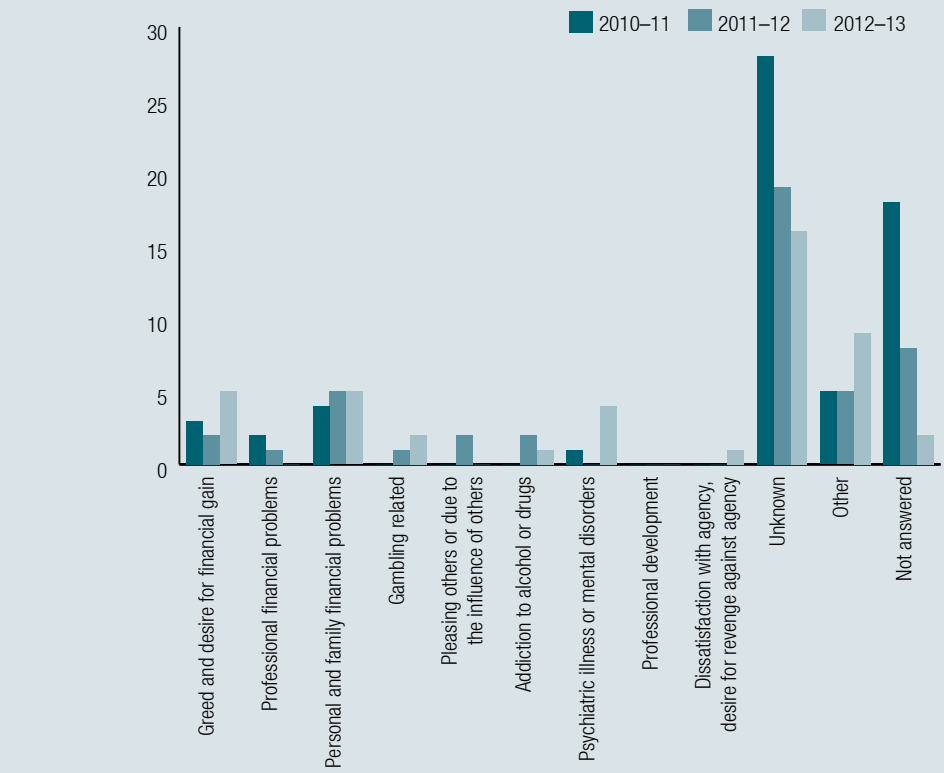
The most frequently cited motive was 'personal and family financial problems' which was closely followed by 'greed and desire for financial gain'. These principal motivations largely

follow those of prior survey research that has identified financial strain and cupidity as the main motivations for fraud (Smith & PwC 2003; KPMG 2013a; ACFE 2014).

Other motivations or reasons given included the 'belief that it was common practice', 'to avoid staffing cuts', or 'ambition to have material to protect position'. Other reasons reflected the perception of the suspect's personality as 'malicious and to cause trouble or mischief' (2010–11 census) or 'payback for unrelated alleged incident' (2012–13 census).

Respondents also included some reasons that may indicate that the incident was not the suspect's fault. For example three reasons were given that lacked the dishonesty needed for a fraud offence. One respondent stated that the reason the fraud occurred was a 'misunderstanding of entitlements' and another reported 'accidental usage' to explain suspected fraud relating to misuse of a government credit card. In 2012–13, one respondent indicated that the motive was 'accidental'. In 2011–12, another respondent indicated that the suspect had a 'medical condition' and that was the reason the fraud was committed.

Figure 5 Primary motivation for committing the incident, by year



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

An illustrative example of one suspected fraud incident reported in 2010–11 is described in Box 1, below.

Box 1 Example from 2010–11

The suspect had been employed with the Commonwealth for more than four years, and, at the time of the incident he was aged between 55 and 64 years and residing in New South Wales. The focus of the fraud was 'financial benefits' and the specific target of the fraud was 'theft of cash/currency (including theft of petty cash)'. The method allegedly used to commit the fraud was 'manipulation of a computerised accounting system' (within the category of 'misuse of information and communications technologies'). The total financial loss to the entity was $129,960 and no money was recovered at the time of the census. The duration of the alleged fraud was believed to be 45 months. The suspect acted alone and admitted the allegation in full.

Source: Commonwealth fraud dataset 2010–11.

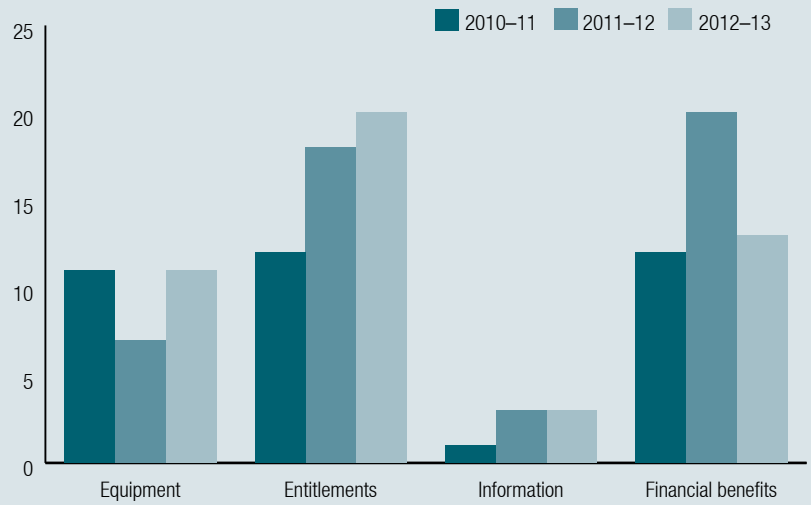
Offence details

The questionnaires asked respondents to indicate the 'target' of the fraud (the focus of the alleged illegality), how the fraud occurred (the method) and the financial loss sustained by the entity.

Focus of offending

A fraud incident may have had multiple foci with respondents being able to select more than one focus if appropriate. The most frequently-reported foci of alleged fraud incidents were either financial benefits (such as theft of cash or currency) or obtaining entitlements (such as payroll monies, travel expenses or leave entitlements). Fraud that targeted information was the least commonly reported focus during the three years (Figure 6).

Figure 6 Focus of most costly internal fraud incidents, by year



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

In 2010–11 the most frequently reported foci of frauds were equipment (such as theft of Commonwealth property), entitlements and financial benefits. In 2011–12, fraud focussing on equipment decreased while fraud focussing on financial benefits increased, affecting most entities in that financial year. In 2012–13, fraud focussing on entitlements affected most entities, while fraud focussing on information increased from being reported by just one entity in 2010–11, to three organisations in both 2011–12 and 2012–13.

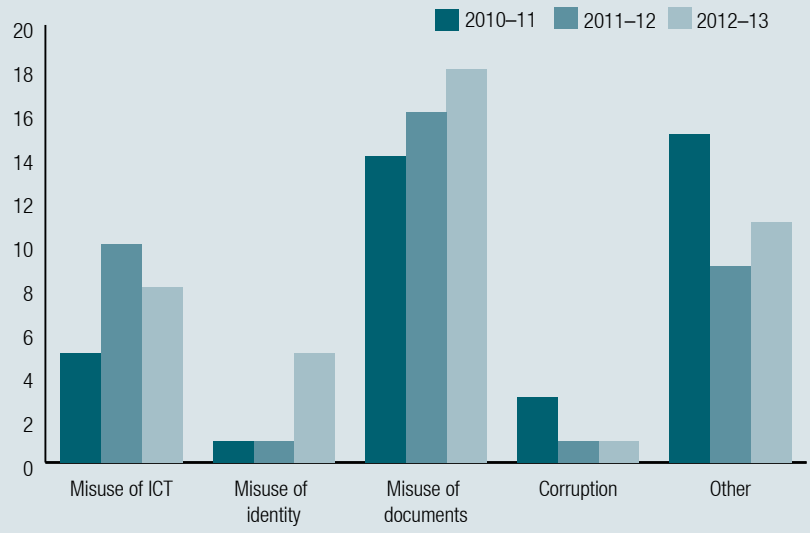
These findings are comparable with those of prior studies. For example, the ACFE (2014) survey found that the most frequent focus of fraud was 'asset misappropriation' which involved theft of monies (and associated financial expenses), equipment or other inventory. The primary focus of organisational fraud appears to be similar in the public and private sectors.

Method of offending

Respondents were asked to explain how the fraud occurred, that is what methods did the suspect use to commit the fraud.

The most commonly reported method of committing fraud was found to involve the misuse of documents. Methods included 'creating a false agency document' or 'using a counterfeit or altered document'. Failure to submit a leave application or falsifying a leave application were common responses (see Figure 7).

Figure 7 Method of committing most costly internal fraud incident, by year



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

Financial loss

Respondents were asked to estimate 'the total financial loss or other impact caused to the agency, had the incident of fraud been successful and completed' and 'what was the total financial loss or other impact actually suffered by the agency as a result of the fraud incident?'

Over the three years, the total financial loss was estimated to be almost $3.2m with the largest losses of $1,328,617 falling in the 2012–13 financial year.

While advanced-level employees (APS 5 and 6) were alleged to have committed more incidents of internal fraud, it was expected on the basis of prior research (KPMG 2013a; ACFE 2014) that those in management would account for the highest amounts lost. It was, however, found that employees at the APS 5 and 6 levels, were alleged to have committed frauds of higher value than other level staff (see Table 4). Of the two employees who were alleged to have defrauded more than $300,000, one was employed at the Executive Level (EL1 or 2) and the other at APS Level 5 or 6. However, there were two suspects employed at the APS 1–4 levels who were allegedly responsible for losses of between $100,001 and $300,000. These findings may simply reflect the proportion of Commonwealth employees at different levels of seniority. For example, the State of the service report for 2012–13 found that APS employees at the APS 5–6 levels comprised more than 35 percent of the entire public service (APSC 2013).

The highest amount involved in any of the cases examined was $597,997 in 2012–13. In that case the suspect was female and all funds were recovered in full. In 2010–11 the highest loss allegedly suffered due to internal fraud, was $524,789, and in that case the entity was able to recover $13,327 from the male suspect, although no details were given as to whether that was through criminal prosecution or other means. In 2011–12 the largest alleged loss was $330,000 by a male suspect who was employed at the APS 5–6 level. In 2012–13 one entity experienced a loss of $239,395 by a female suspect with no funds being able to be recovered.

Table 4 Loss categories for the mostly costly internal fraud incident by suspect occupational category, 2010–11 to 2012–13 combined

Amount lost	EL1 & 2	APS 5 & 6	APS 1-4	Graduate	Unknown	Other
	N	N	N	N	N	N
$0-1000	5	4	3	1	6	0
$1,001-10,000	5	10	8	1	4	0
$10,001-50,000	4	7	4	0	1	1
$50,001-100,000	0	2	1	0	0	1
$100,001-300,000	0	0	2	0	0	3
$300,001-600,000	1	1	0	0	0	0

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

Recovery

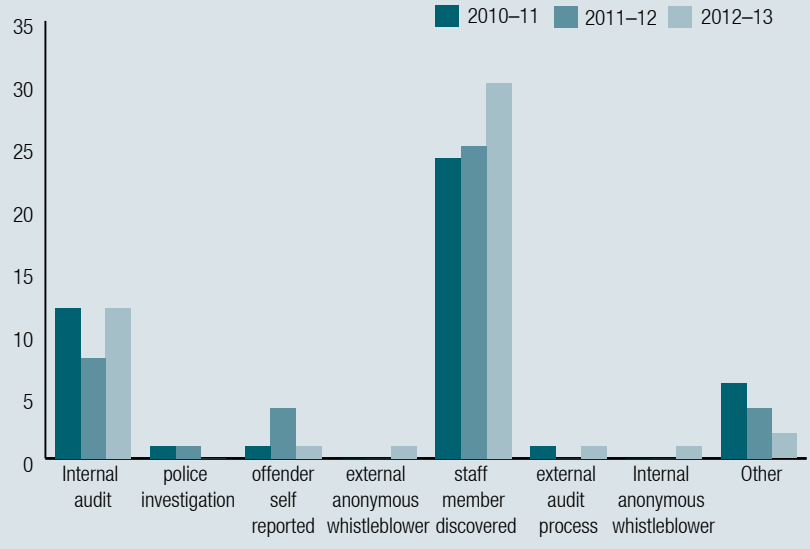
Respondents were also asked to indicate how much money or other property was recovered from suspects. Often funds are not recovered for some considerable time after the fraud has been perpetrated and detected (ACFE 2014). The present study examined funds recovered during the financial year in question, regardless of when the incident took place. It is not possible to indicate a percentage of the actual funds lost in any given year that have subsequently been recovered. In 2010–11, 17 entities were able to recover part or all of monies lost to fraud—$121,478. In the following two data collection periods the total amounts recovered rose to $366,559 in 2011–12 and $762,361 in 2012–13.

Investigations and outcomes

Discovery of the fraud

Respondents were also asked to indicate how the alleged incident was detected. It was found that internal controls such as internal audits or monitoring by colleagues were the most frequent ways in which fraud was detected (see Figure 8).

Figure 8 How most costly internal fraud incident was detected, by year



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

In 2011–12, four respondents indicated that the suspect had self-reported to the entity in question, while in each of the other years, one self-report had occurred. Self-reporting often occurs where an individual has a gambling problem or other compulsive reason for offending and realises that external help is needed to deal with the problem (Sakurai & Smith 2003). 'Other' detection methods specified by entities included 'tip-off from family member' and 'security clearance re-evaluation process'.

Investigations

Most fraud incidents were investigated internally by entities although on occasions matters were referred to police or other investigators for external examination.

In 2010–11, four respondents indicated that an external investigator, other than police, had been engaged to investigate the incident, and another five respondents indicated that police had investigated the matter. In 2011–12 one matter had been referred to the Australian Federal Police for investigation, but was rejected and then dealt with internally. External investigators, not police, investigated another three entities in 2011–12 and police investigated a further three matters. In 2012–13 external investigators, other than police investigated six incidents and police investigated another three, with 41 incidents investigated internally.

Outcomes

Respondents were asked to indicate the outcome of investigations and any associated legal proceedings. Depending on the length and complexity of the investigation some respondents supplied details of matters referred for prosecution (see Table 5).

In 2010–11 two of the most costly incidents were referred to law enforcement for further investigation and those matters were still being investigated at the time the census was completed. Two incidents in 2010–11 were also referred to a prosecution agency, one respondent advising that criminal sanctions had been imposed on the suspect, although details of the penalties imposed were not provided. In 2011–12 one incident was referred to the Australian Federal Police (AFP) for with the investigation ongoing at the time of data collection. Two incidents in 2011–12 were referred to the Commonwealth Director of Public Prosecutions (CDPP), although no further details were provided. In the 2012–13 census period three incidents were referred to the CDPP and details of sanctions imposed were provided. The sanctions ranged from a three-year good behaviour bond, 26 weeks' incarceration by periodic detention, to five years' imprisonment without parole. In six of the most costly cases, proceedings were ongoing.

Table 5 Outcome of entity investigation, by incident number

Outcome	2010–11	2011–12	2012–13
	N	N	N
Suspect admitted allegation in full	10	4	3
Suspect admitted allegation in part only	0	3	2
Referred for civil action	0	0	0
Suspect dismissed from employment	5	6	8
Suspect reprimanded	3	1	4
Suspect resigned or left employment	7	5	8
Referred to law enforcement agency	2	1	1
Referred to prosecution agency	2	2	3

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

An illustrative example of a completed investigation involving a most costly case from 2012–13 is described in Box 2.

Box 2 Example of internal fraud from the 2012–13 census

The suspect was a full-time employee who had been employed by the entity for between 49 and 72 months. The suspect did not hold a security clearance, was aged 45–54 years old and was a female. The suspect lived in Queensland and no details about the suspect's educational details were known. The suspect was employed at the APS 1–4 level. The focus of the fraud was determined to be 'financial benefits' and listed as 'other financial benefit'. The method used to commit the fraud involved 'misuse of identity' and 'creating and/or using a fictitious identity. The fraud was discovered through an internal audit/investigation. The employer investigated the alleged incident. The amount lost due to the fraud incident was $239,395.54 and the entity recovered $2,840.91. The suspect acted alone over a period of 61 months. The matter was referred to the Commonwealth Director of Public Prosecutions and a criminal sanction was imposed on the suspect of five years in prison, no parole period, 20 months and a reparation order for $236,554.63.

Source: Commonwealth fraud monitoring dataset 2012–13

Conclusions

Some consistent patterns were discernible from the data collected in the study. For example, over the three-year period, in each year most of the suspects were between 25 and 34 years, most likely employed at the APS 5–6 level, and had been employed by the entity for more than four years. The risk areas for entities remained fairly consistent with incidents focussing mostly on 'entitlements' or 'financial benefits' and with the most common method for committing fraud being via 'misuse of documents'. Detection methods for the incidents almost always involved internal auditing by entities (including colleagues discovering the incident). Generally most of the suspects were assessed as being of 'good character' with a high proportion having some level of security clearance.

Further analysis is needed of the primary motivations of suspects, as few respondents were able to supply this information. Understanding motivations and rationalisations is critically important when designing effective fraud control measures. Further research is also needed to determine the extent to which suspects' behaviour changed as a result of the incidents being detected, and whether there is any evidence of recidivism.

This study has confirmed prior research regarding a number of aspects of fraud victimisation that occur in public sector organisations, such as the high numbers of frauds detected through internal investigations and the motivations of suspects that largely confirmed prior occupational fraud research. The present study also found some areas in which serious fraud within Commonwealth agencies differed from that reported in previous studies. For example, high numbers of female suspects were involved in allegations of internal fraud, unlike in previous studies that generally show higher proportions of male offenders. In addition, the absence of senior executive level staff suspected of committing the most costly incident of internal fraud each year was different from previous organisational fraud research that found fraud at all levels of management, with the most senior managers being responsible for the highest value incidents. Future research would be required to understand these differences more fully, although the present results may simply be due to the relatively small number of incidents analysed.

References

All URLs were correct 20 April 2015.

ACFE 2014. *Report to the nations on occupational fraud and abuse: 2014 global fraud study*. Austin TX. ACFE http://www.acfe.com/rttn.aspx

ACFE & Peltier-Rivest D 2007. *Detecting occupational fraud in Canada: A study of its victims and perpetrators.* Austin TX: ACFE. http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/rttn-canadian.pdf

Armstrong J 2012. Employee fraud, in Doig A, *Fraud: The counter fraud practitioner's handbook*. Surrey, UK: Gower Publishing

Association of Certified Fraud Examiners see ACFE

Australian Bureau of Statistics (ABS) 2013. *Labour force, Australia, June 2013*. ABS cat. no. 6202.0. Canberra: ABS

Australian Government Security Vetting Agency (2014). Personal email communication

APSC 2013. *State of the service report 2012–13*. Canberra: APSC

APSC 2011. *State of the service report 2010–11.* Canberra: APSC

Australian Public Service Commission see APSC

Bales K & Fox TL 2009. Evaluating a trend analysis of fraud factors. *Journal of Finance and Accountancy* 1–85

BDO Stoy Hayward 2008. Fraud: A global challenge*. FraudTrack* 5 http://static.bdo.uk.com/imported/2010/3/BDO_FraudTrack_5.pdf

Button M & Brooks G 2009. Mind the gap: Progress towards developing anti-fraud culture strategies in UK central government bodies. *Journal of Financial Crime* 16: 229–244

Gill M & Goldstraw-White J 2012. Why commit fraud, in Doig A, *Fraud: The counter fraud practitioner's handbook*. Surrey, UK: Gower Publishing

Goldstraw J, Smith RG and Sakurai Y 2005. Gender and serious fraud in Australia and New Zealand. *Trends & Issues in Crime and Criminal Justice* no. 292. Canberra: Australian Institute of Criminology with PricewaterhouseCoopers http://www.aic.gov.au/publications/current%20series/tandi/281-300/tandi292.html

KPMG 2013a. *Survey of fraud, bribery and corruption in Australia and New Zealand 2012*. Sydney: KPMG. http://www.kpmg.com/au/en/issuesandinsights/articlespublications/fraud-survey/pages/fraud-bribery-corruption-survey-2012.aspx

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

KPMG 2011. *Who is the typical fraudster? KPMG analysis of global patterns of fraud.* Sydney: KPMG

Kroll 2014. 2013/14 Global fraud report: Who's got something to hide? New York: Kroll .http://fraud.kroll.com/report-archive/

Miethe TD, McCorkle RC & Listwan SJ 2006. *Crime profiles: The anatomy of dangerous persons, places and situations,* 3rd ed. Los Angeles: Roxbury Publishing Company

Minister for Justice 2014. Preventing, detecting and dealing with fraud, *Resource Management Guide* no. 201. Canberra: Minister for Justice

Peltier-Rivest D & Lanoue N 2011. Thieves from within: Occupational fraud in Canada. *Journal of Financial Crime* vol 19 1:54–64

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

Sakurai Y & Smith RG 2003. Gambling as a motivation for the commission of financial crime, in *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*, no. 2. http://www.ibac.vic.gov.au/news-and-publications/ibac-insights-january-2015/spotting-a-typical-fraudster

Smith RG and PricewaterhouseCoopers 2003. *Serious fraud in Australia and New Zealand*. Research and Public Policy Series no. 4. Canberra: Australian Institute of Criminology/PricewaterhouseCoopers

Warfield B 2013. Employee fraud in Australian financial institutions. Sydney: Warfield & Associates. http://www.warfield.com.au/publications.html