Australian Government
Australian Institute of Criminology

Statistical Bulletin 04

ISSN 2206-7302

March 2018

Abstract | During financial years 2012-13 to 2014-15, Commonwealth entities detected or were informed of 4,828 incidents of internal fraud alleged against public servants or contractors, with losses totalling $11.3m. Each entity that experienced internal fraud was asked to select the one most costly incident each year and to provide information on the nature of the incident, the type of person who was alleged to have perpetrated it and how the matter was dealt with. The majority of the 126 incidents examined related to abuse of employee entitlements or financial benefits, with most committed through the misuse of information or documents, or other technology-enabled means. The findings show where risks of serious fraud against the Commonwealth lie and provide insight into how fraud prevention resources could most effectively be targeted.

Fraud within the Commonwealth: A census of the most costly internal fraud incidents 2014-15

Penny Jorna & Russell G Smith

Fraud within Commonwealth government entities, perpetrated by Commonwealth officials, harms the public sector in a variety of ways. It depletes government resources, causes reputational damage to the government, attracts negative media attention and lowers the morale and productivity of staff within the workplace. Fraud within the Commonwealth covers a range of criminal conduct that entails 'dishonestly obtaining a benefit, or causing a loss, by deception or other means' (AGD 2014: C7). Dishonesty is the key mental element of the offence that distinguishes fraudulent from innocent conduct.

Although fraud is a wide-ranging category of crime, and the personal backgrounds and sociodemographic characteristics of offenders can differ considerably, both incidents and offenders display enduring features that act as red flags or indicators of dishonesty taking place.

Internal fraud can be just as diverse as fraud perpetrated by external actors. It may involve identity crime, when staff claim to be people they are not or to hold qualifications they do not, or it may involve theft of cash or information belonging to government, or it may entail bribery and corruption (Cifas 2015).

Every organisation, public or private, is vulnerable to fraud, but this does not necessarily mean that it is possible to predict who will commit internal fraud. Prior research has found similarities among the demographic factors of those who commit internal fraud as well as similarities in how they commit fraud (Smith 2015). In its latest global survey, the Association of Certified Fraud Examiners (ACFE) reported that most organisational fraud was committed by perpetrators at the employee or manager level, with most perpetrators being men (69% in 2016 and 67% in 2014), and that just under 40 percent of perpetrators were between the ages of 31 and 45 years. ACFE (2016) also found that 42 percent had been employed by the victim organisation for between one and five years. Similarly, PricewaterhouseCoopers (PwC) 2014 Global Economic Crime Survey found 39 percent of the perpetrators were aged between 31 and 40; 29 percent had been employed by the victim organisation for between three and five years; and 24 percent employed between six and 10 years (PwC 2014).

The similarities between the findings of these surveys support the view that some employees are more likely to offend than others and, accordingly, require greater support and encouragement not to act dishonestly (Smith 2015). Padgett (2015) highlighted the benefits of understanding the characteristics of internal fraud perpetrators and how they commit fraud. The main reason for understanding who is committing fraud in an organisation, and how they are committing that fraud, is to reduce the risk it will occur again (Padgett 2015; PwC 2011).

This study focuses on internal fraud committed by Commonwealth officials, as opposed to fraud committed by members of the public, external to the Commonwealth. This paper is a companion to the *Fraud against the Commonwealth: Report to Government 2015* (Jorna & Smith 2017), which contains details about all forms of fraud and the financial losses incurred as a result. The purpose of this paper is to gain a better understanding of how internal fraud affects entities and the damage internal fraud may cause. Its findings confirm those of industry surveys that have found an increase in the number of organisations reporting internal fraud incidents in recent years. For instance, Kroll (2016) reported in its latest global survey that of those companies experiencing fraud, where the perpetrator was known, 81 percent were victims of at least one fraud committed by an insider—an increase from the 72 percent reported in the previous survey for 2013–14. Cifas (2015), a not-for-profit company that works to protect organisations and individuals from financial crime, also found an increase of 18 percent in internal fraud incidents detected between 2013 and 2014 in the United Kingdom (UK).

This paper presents findings from the annual census of Commonwealth entities undertaken pursuant to the Commonwealth Fraud Control Framework (AGD 2014). In the financial years 2012–13 to 2014–15 a total of 4,828 detected incidents of internal fraud, worth $11.3m, were reported by 136 Commonwealth entities. Although the number of suspected incidents of internal fraud declined over this period, the annual cost increased by over 23 percent. Table 1 presents data on the total number of internal fraud incidents recorded by entities over the three-year period and the number of the most costly incidents analysed in this report for each year. The dollar values for internal fraud each year included in the report are also presented, as are the total dollar values lost for all internal fraud incidents in the three years.

Table 1: Number of internal fraud incidents and dollars lost, 2012–13 to 2014–15 (N)

Year	No. of incidents of all internal fraud	Dollars lost to all internal fraud	No. of incidents of internal fraud, total of most costly section	% of most costly incidents out of all internal fraud incidents	Dollars lost to internal fraud, total of most costly section	Dollars lost to internal fraud, total of most costly section % of dollars lost in most costly incidents out of total internal fraud dollars lost
2012–13	1,685	$3,426,546	45	2.7	$1,328,617	38.8
2013–14	1,658	$3,607,740	40*	2.4	$1,001,181	27.8
2014–15	1,485	$4,225,288	41*	2.8	$5,185,026**	NA

Notes: * Due to a Machinery of Government change, 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. While 43 entities completed the section in 2014–15, only 41 were included for analysis, due to two entities reporting duplicate incidents and another entity completing the section even though fraud was not found.

** In 2014–15 four entities did not quantify total dollars lost to internal fraud. However, they were able to quantify dollars lost for the finalised internal fraud investigations included in the 'most costly incident of internal fraud' section; therefore, the total dollars lost were higher than the total dollars lost due to internal fraud. This was due to the large dollar amounts not quantified in the general internal fraud questions.

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

Methodology

In September each year, all Commonwealth entities are asked to complete a confidential online questionnaire about their experience of fraud during the previous financial year. 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. Respondents are also asked to nominate one incident of internal fraud which resulted in the largest financial loss or other impact suffered by the entity in respect of which an investigation or review had been concluded during that financial year (regardless of when the fraud was committed or the investigation commenced). Each of these nominated cases was considered as a single incident, despite them 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 information related only 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 2).

Table 2: Size and governance framework of entities reporting internal fraud, 2012–13 to 2014–15 (N&%)

Size of entity	2012–13				2013–14				2014–15			
	Corporate entity		Non-corporate entity		Corporate entity		Non-corporate entity		Corporate entity		Non-corporate entity	
	N	%	N	%	N	%	N	%	N	%	N	%
0–500 staff	4	25	4	14	5	33	6	21	8	50	9	29
501–1,000 staff	3	19	7	24	3	20	4	14	0	0	4	13
1,000+ staff	9	56	18	66	7	47	19	65	8	50	18	58
Total	16	100	29	100	15	100	29	100	16	100	31	100

Note: These data relate only to those entities that reported an incident of internal fraud in any of the three years examined, 2012–13 to 2014–15. In 2012–13 all 45 entities that reported an internal fraud incident completed the most costly incident of internal fraud section; in 2013–14 only 41 out of 44 entities completed the section and in 2014–15 only 43 out of 47 entities completed the section.

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

Sample

Of the 136 entities that reported an incident of internal fraud during the three years in question, 126 (93%) completed all or some of the questions dealing with the most costly incident (Table 3). 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 3: Number of responding entities, 2012–13 to 2014–15 (N&%)

Year	Entities that experienced internal fraud (number and % of total entities with internal fraud)		Entities that responded to questions on the most costly incident of internal fraud (number and % of entities with internal fraud)	
	N	%	N	%
2012–13	45	33.0	45	100.0
2013–14	44	32.0	40*	90.9
2014–15	47	35.0	41*	87.2
Total	136	100.0	126	92.6

Note: Due to a Machinery of Government change, 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. While 43 entities completed the section in 2014–15, only 41 were included for analysis. In 2014–15 one entity completed some sections of the most costly incident of internal fraud questions; however, this entity's answers said that an investigation determined the matter was not fraud, and was therefore removed from analysis, as was one case reported by two entities to avoid double counting.

Source: Commonwealth fraud monitoring datasets 2012–13, 2013–14 and 2014–15 [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 provided. 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 occasions, suspects may not have explained why they committed the offence and, if the suspect had simply been dismissed from the organisation, details of the case's outcome may not have been recorded. 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 assist in informing those working in fraud control and risk management who are charged with understanding and addressing the problem.

Results

The information provided with regard to the 126 most costly incidents reported by respondents for the three years fell into four categories:

- the cost of internal fraud;
- the nature of offending;
- the discovery, investigation and outcomes of incidents; and
- the demographic and other characteristics of suspects.

The results should be interpreted with some caution, as response rates for some variables were low, owing to information being either not collected or unavailable. The total sample of 129 incidents (126 of which were analysed) was also relatively small, although in keeping with prior research. As examples of the most costly frauds detected, they are, however, worthy of scrutiny and analysis.

The cost of internal fraud

Respondents were asked to indicate the extent of the financial loss 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 caused to the entity, had the incident of fraud been successful and completed?
- What was the total financial loss or other impact actually suffered by the entity as a result of the fraud incident?

Table 4 presents information on the minimum and maximum financial losses for the most costly incidents of internal fraud experienced by entities for each financial year. More entities reported experiencing a financial loss due to a fraud incident in 2014–15 than in previous years. In 2014–15 the loss amounts reported by entities were also higher. One entity, for example, reported a maximum loss of $2m, with a median loss across all 19 entities of $6,070.

Table 4: Most costly internal fraud incident losses by entities 2012–13 to 2014–15 (N&$)

Year	Entities experiencing a loss (N)	Entities experiencing internal fraud (N)	Minimum to maximum amount lost	Mean amount lost	Median amount lost	Total
2012–13	23	45	$1,000–$597,997	$57,766	$11,904	$1,328,617
2013–14	19	44	$79–370,000	$52,694	$5,000	$1,001,181*
2014–15	24	47	$47–2,000,000	$225,436	$6,070	$5,185,026*

* In 2013–14 one amount for one entity was excluded, as two entities reported a duplicated incident. In 2014–15 one amount for one entity was excluded, as two entities reported a duplicated incident.

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

While the financial losses associated with internal fraud incidents are substantial, there are other indirect costs associated with fraud incidents. Respondents referred to the time and costs incurred by entities to investigate the fraud, advertise and replace staff who had been dismissed, and the need to replace equipment stolen or used to commit the crime. Research undertaken by the University of Portsmouth found that even in the case of relatively low-level frauds, with losses less than £25,000, the cost of investigation, disciplinary costs, staff replacement costs and other miscellaneous costs increased the initial fraud loss by over 200 percent (Cifas 2015). Other impacts that may have been experienced by entities included damage to the integrity of the entity, impacts on implementing policies and programs, and other impacts in areas of business in which the suspect worked.

Prior survey research found offenders in managerial positions were responsible for the highest financial losses arising from fraud incidents (ACFE 2016; KPMG 2013). The present census, however, found employees at the Australian Public Service (APS) 5–6 level were alleged to have committed more costly frauds than staff at other levels (see Table 5 and Figure 12, below).

Table 5: Most costly internal fraud incident losses by employment level, 2012–13 to 2014–15 (N)

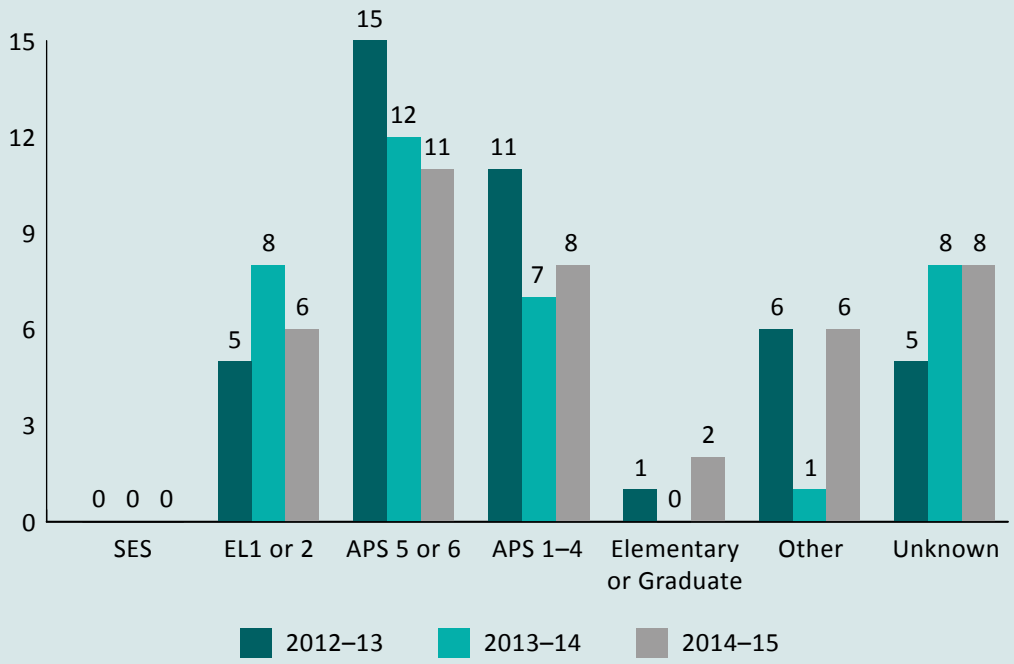
Amount lost	SES	EL1–2	APS 5–6	APS 1–4	Graduate	Unknown	Other
			(N)				
Unknown	0	6	5	3	0	4	5
$0–1,000	0	8	16	11	1	6	3
$1,001–10,000	0	3	8	2	2	11	1
$10,001–50,000	0	3	5	3	0	0	4
$50,001–100,000	0	0	2	3	0	0	2
$100,001–300,000	0	0	0	3	0	0	0
$300,001–600,000	0	1	0	0	0	1	2
$600,001 and over	0	0	2	1	0	0	0

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

Of the three Commonwealth officials alleged to have caused losses over $600,000, two were employed at the APS 5–6 level. The third, who was alleged to have defrauded $2m in 2014–15, was employed at the APS 1–4 level; in that particular incident $1.5m was recovered by the entity. Of the four other suspects who were allegedly responsible for losses of between $300,001 and $600,000, one was employed at the EL 1–2 level, one as a contractor by the entity and one in a non-APS position; the final suspect's employment level was listed as unknown. No suspects were employed at Senior Executive Service (SES) level. This is somewhat surprising given prior research which suggests that senior management is frequently involved in fraud offending. For example, in the ACFE (2016) survey, 19 percent of identified perpetrators were either the owner of the organisation or employed as an executive, and the median amounts lost as a result of fraud perpetrated by people in those positions was over seven times higher than those classified as employees. KPMG (2013) also found a higher number of people at the executive level were committing fraud than found in the present research, finding that 29 percent of frauds were committed by executive directors. On the basis of other industry research, it appears to be unlikely that no SES-level Commonwealth employees were involved in fraud in recent years (ACFE 2016; KPMG 2013; Kroll 2016). This result requires further research to understand the reasons behind the absence of SES staff being involved in these most costly incidents of internal fraud.

Respondents reported that the majority of suspects were employed at APS 5–6 levels, followed by those employed at the APS 1–4 level (Figure 1). In the 2014–15 census, respondents classified high numbers of suspects as having an employment level characterised as 'other'. Examples of other occupational levels included contractors, non-APS employees and licensees.

Figure 1: Number of suspects by employment level, 2012–13 to 2014–15 (N)



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

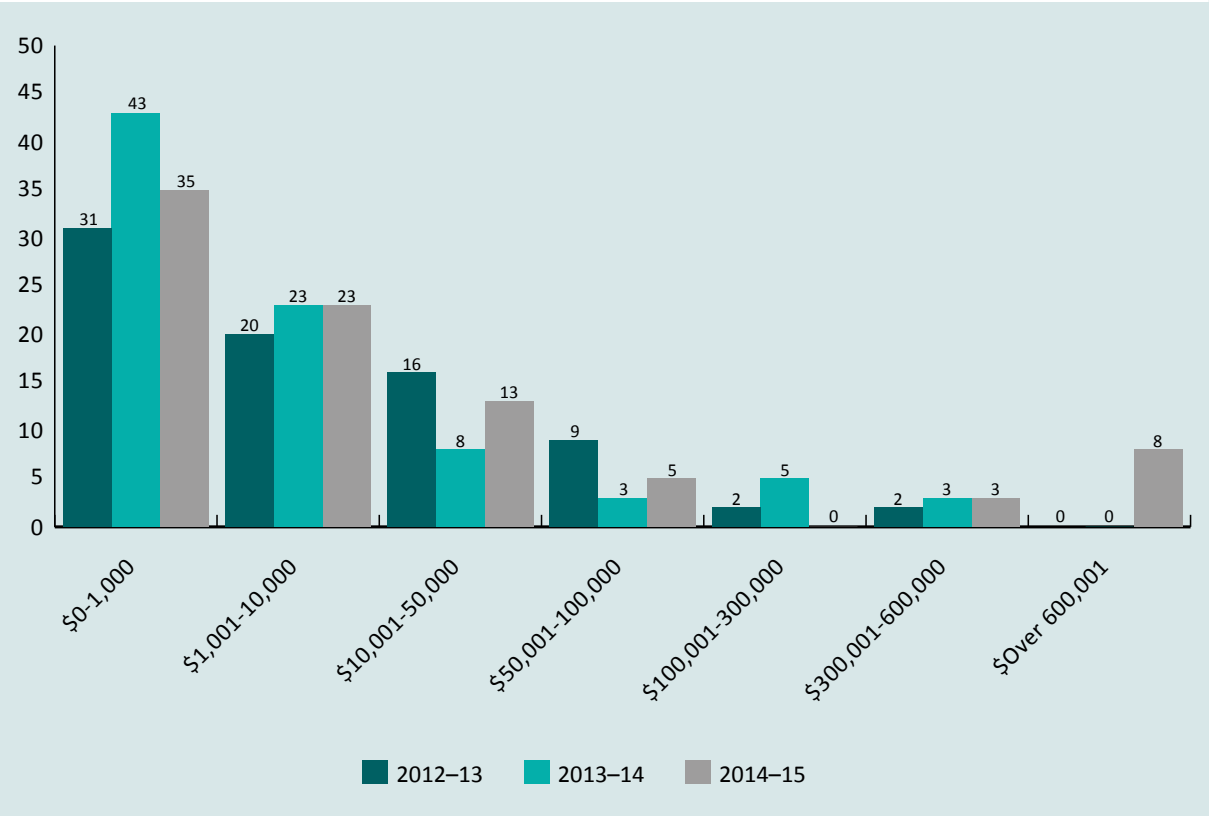
Box 1: Example of unauthorised government credit card usage

The suspect was a full-time employee at the time the fraud was detected, with a Top Secret security clearance. She had been employed by the entity for 24 months and was in the age category 35–44 years. She resided in New South Wales and was educated to tertiary postgraduate level, being employed at APS 5–6 level. The fraud involved the withdrawal of funds from a government credit card account without authorisation. The incident was detected through external audit/investigation, and the entity then investigated the incident internally. The amount lost was $15,000 with no funds recovered. The fraud took place over one month and the suspect acted alone. At the time the census was completed legal proceedings were incomplete.

Source: Commonwealth fraud monitoring dataset 2012–13 [AIC computer file]

Figure 2 shows the percentage of incidents that fell into specified loss categories. It is apparent that the majority of fraud incidents had losses of $1,000 or less for all three years. In 2014–15 eight percent of fraud incidents incurred losses of over $600,000. These findings differ slightly from other internal fraud studies. For example, ACFE (2016) found around 50 percent of cases involved losses of less than $200,000, whereas the current study found that approximately 90 percent of fraud incidents involved losses of $100,000 or less. ACFE (2016) found 20 percent of cases experienced losses of $1m or more, while the present study found only two fraud incidents with this level of loss, both of which were reported in 2014–15.

Figure 2: Percentage of cases by financial loss category, 2012–13 to 2014–15 (%)



Note: Cases where the loss amount listed was not specified were not included in the analyses. As a result, percentages do not total 100.
Source: Commonwealth fraud monitoring datasets 2012–13, 2013–14 and 2014–15 [AIC computer file]

Losses suffered by the Commonwealth are occasionally recovered from offenders through various forms of court and administrative action. Details of recoveries are presented in Table 7, below. Usually only a relatively small proportion of funds defrauded are able to be recovered from offenders.

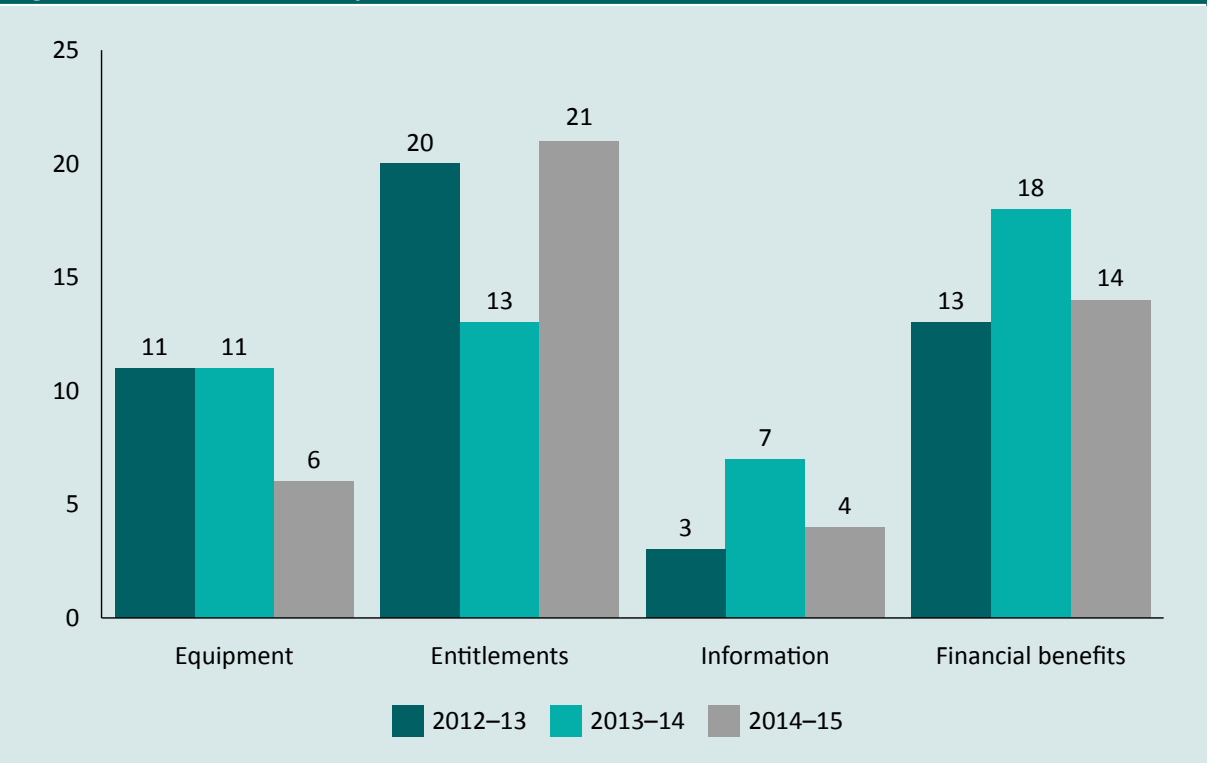
The nature of offending

Respondents were asked a number of questions about how the frauds were committed, including what the target or focus of the incident was and how the fraud was committed.

Focus of offending

The most frequently reported targets of dishonesty 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 three years, information was the least commonly reported focus of fraud (Figure 3). This finding may in part be because it can be difficult for entities to quantify the financial value of information loss and, as such, these incidents may not be reported as the most costly internal fraud. Future questionnaires are designed to address this issue by stating that 'most costly' includes the incident that resulted in the greatest financial loss or impact to the entity.

Figure 3: Focus of most costly internal fraud incidents, 2012–13 to 2014–15 (N)



Note: Respondents were asked to select all that apply; therefore, totals may exceed responding entities totals

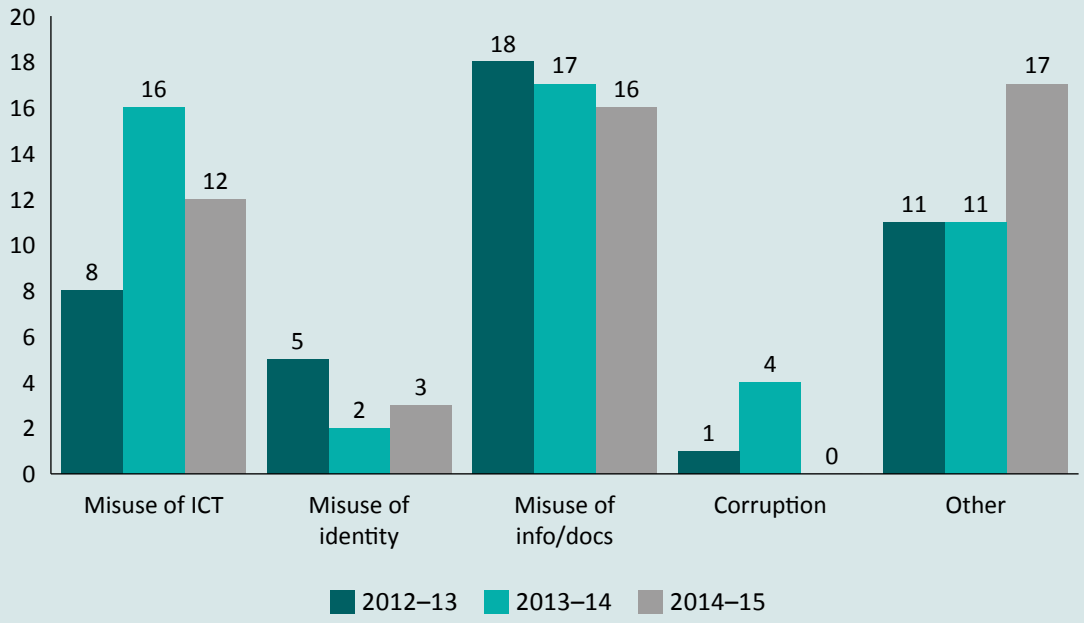
Source: Commonwealth fraud monitoring datasets 2012–13, 2013–14 and 2014–15 [AIC computer file]

In 2014–15 the most frequently cited focus of the incidents examined was entitlements, reported by 21 entities (45% of entities which experienced an internal fraud incident). The second most cited focus for 2014–15 was fraud aimed at financial benefits, reported by 14 entities (30% of entities). These findings are similar to those from industry surveys of internal fraud. For example, ACFE (2016) found 83 percent of cases in its global study involved asset misappropriation, the subcategories of which included theft of cash, skimming and other financially directed frauds. In 2014–15 there was a reduction in the number of entities experiencing fraud focused on equipment, from 11 entities in both 2012–13 and 2013–14 to just six in the most recent year.

Method of offending

Respondents were also asked how the fraud was committed. The most commonly reported means of committing fraud involved the misuse of documents. Frequent methods 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 was also a common form of misuse of documents (see Figure 4). In 2014–15 a large number of entities (N=17) reported 'other' types of committing fraud. Examples included abuse of power, falsifying flex-sheets, misuse of Australian government credit cards and lack of financial reporting and cash payments.

Figure 4: Method of committing most costly internal fraud incident, 2012–13 to 2014–15 (N)



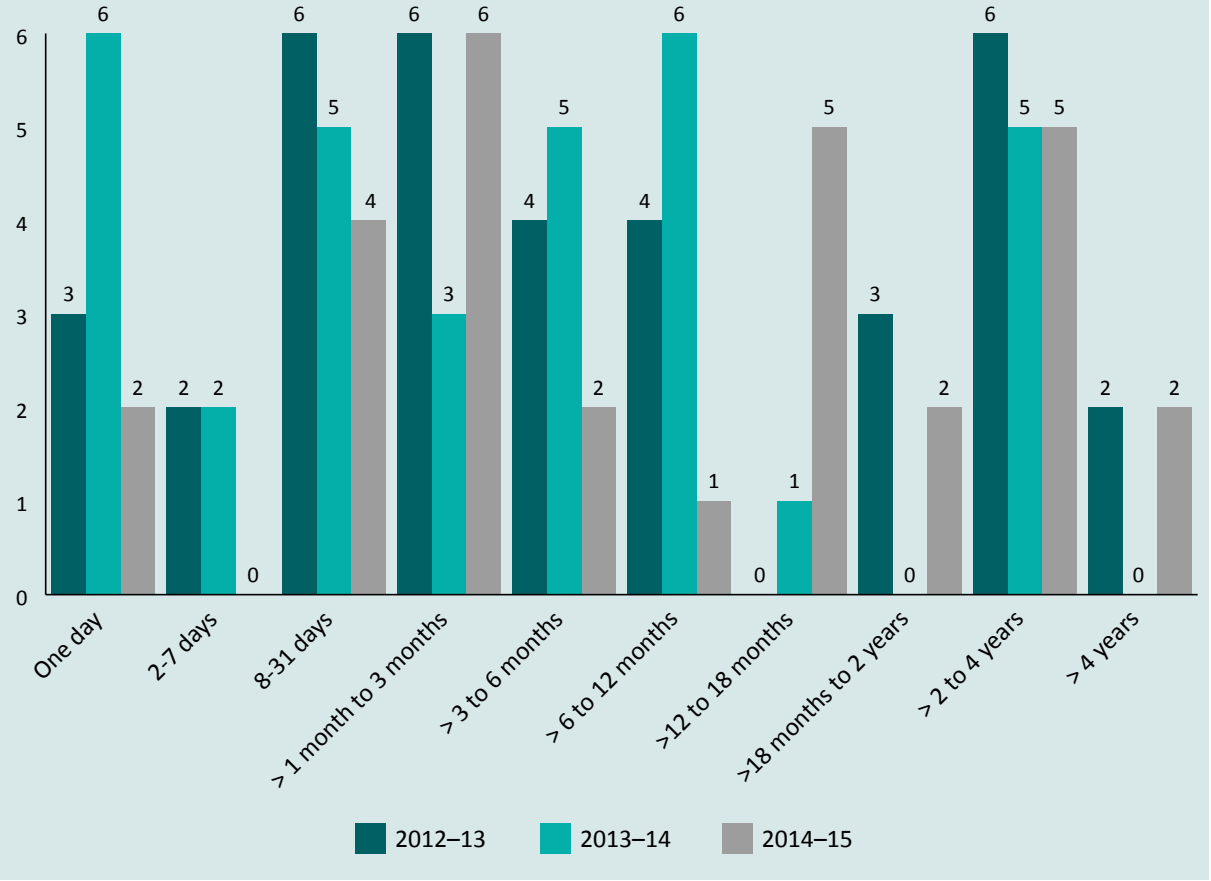
Source: Commonwealth fraud monitoring datasets 2012–13, 2013–14 and 2014–15 [AIC computer file]

Investigations and outcomes

Duration of the fraud

The longer a Commonwealth official is engaged in fraudulent conduct, the greater the ramifications for the entity. Fraud is damaging to office morale; staff may need to be replaced, which can be costly and disruptive; and there are fewer resources to continue the everyday running of the organisation. Thirty-six (N=45) percent of fraud incidents lasted less than three months, and nine percent of incidents lasted just one day. Fraud occurring over a longer duration may also indicate weaknesses in an entity's fraud prevention or detection mechanisms. Four fraud incidents continued for longer than four years (in 2012–13 and 2014–15, Figure 5). The duration of the largest number of frauds during the three years was between two and four years.

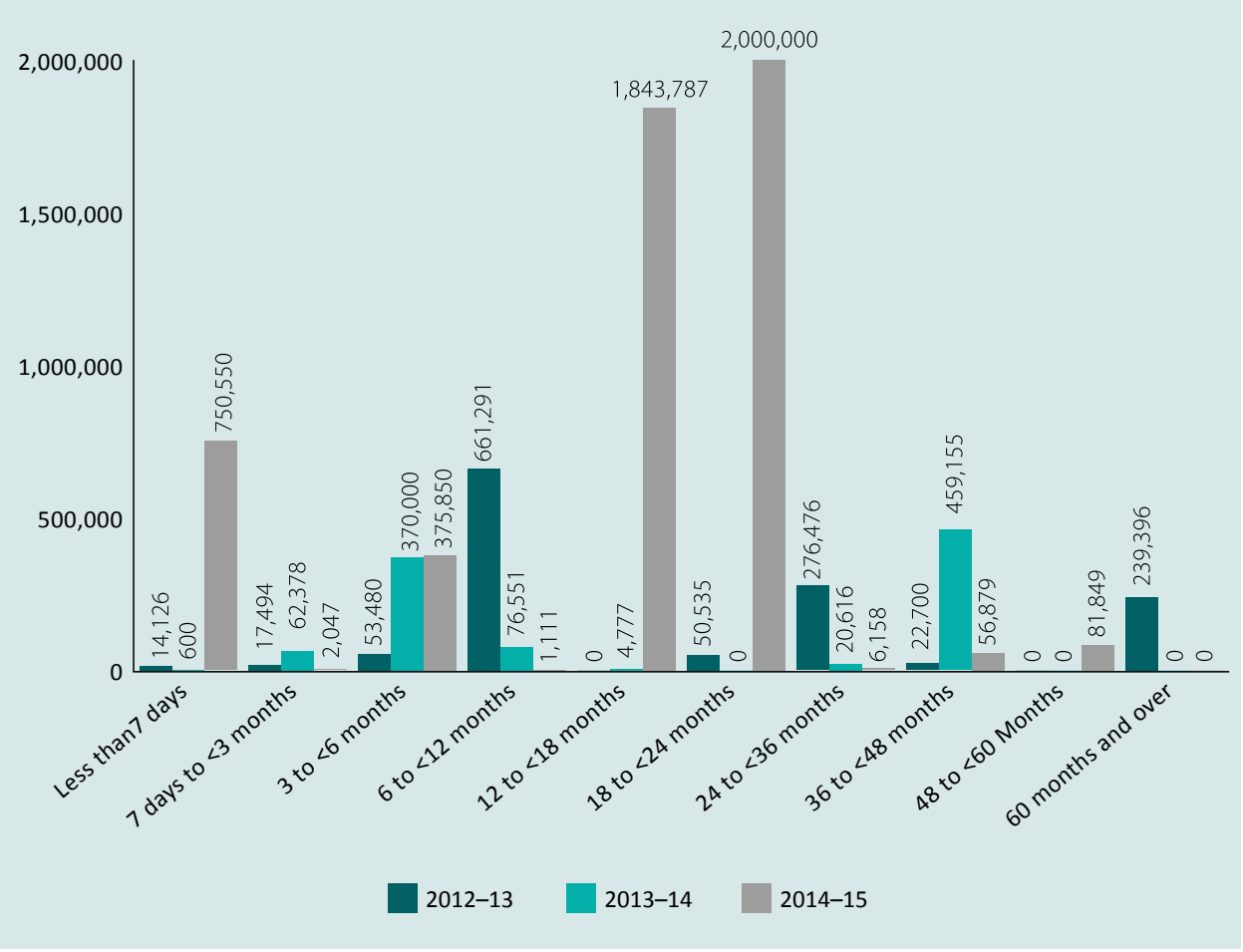
Figure 5: Duration of fraud incidents, 2012–13 to 2014–15 (N)



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

ACFE (2016) found the longer the duration of a fraud incident, the higher the loss sustained. The present study, however, found the relationship between duration of fraud incidents and the value of the fraud not to be linear (Figure 6). For example, in 2014–15 there was one incident that lasted only one day, but the value of that fraud was $750,000. The losses due to fraud incidents in 2014–15 were greater than the two previous years, with two fraud cases involving losses of over $1m.

Figure 6: Duration of internal fraud incidents until detection by fraud losses, 2012–13 to 2014–15 ($)

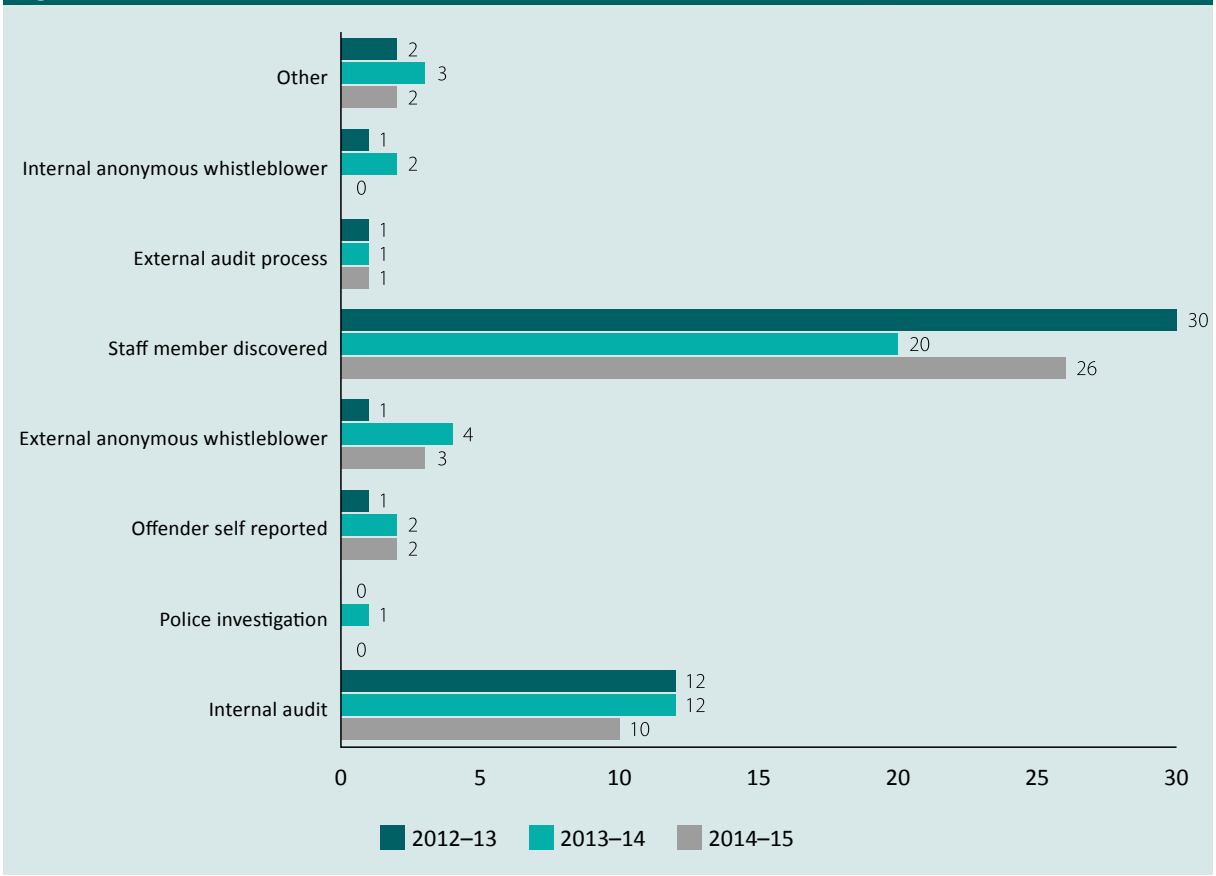


Source: Commonwealth fraud monitoring datasets 2012–13, 2013–14 and 2014–15 [AIC computer file]

Discovery of the fraud

Respondents were asked how the alleged fraud was detected. Each year, most frauds were detected through internal controls—that is, internal audits or discovery by colleagues (see Figure 7). Infrequently, fraud was detected externally, including through tip-offs, whistleblower action and detection by external agencies.

Figure 7: Manner of detection of fraud incidents, 2012–13 to 2014–15 (N)



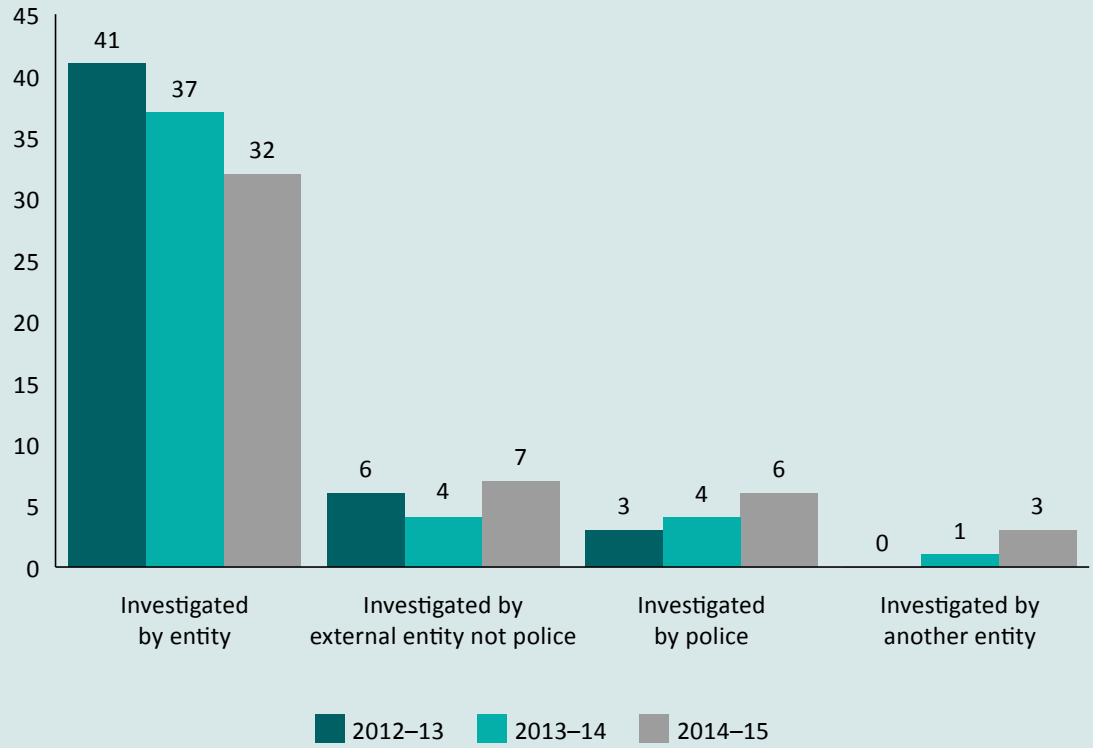
Source: Commonwealth fraud monitoring datasets 2012–13, 2013–14 and 2014–15 [AIC computer file]

Entities' use of internal audits to detect fraud remained constant over the three-year period, with 12 entities using that method in 2012–13 and 2013–14, decreasing slightly to 10 in 2014–15. Rarely are entities notified of internal fraud incidents by the police. During the three years, only one respondent reported an internal fraud as having been detected through police contact, in 2013–14. The role of colleagues and employees in detecting fraud is important as invariably they work with perpetrators and are the first to observe anomalies in payments and systems. The findings from this study showed that the most common means of detection of the internal frauds examined was by workplace colleagues. In its global survey, Kroll (2016) found that 41 percent of cases were detected through internal whistleblowers, followed by external audits (31%) and then internal audits (25%). By way of contrast, Cifas (2014) found that only 11 percent of internal frauds were detected and/or reported by staff. It was noted in that report that the low rate of fraud detection by staff members 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).

Investigations

Respondents reported that a large number of investigations into the most costly internal fraud incidents each year were conducted internally within entities. Respondents were asked to indicate all methods by which incidents were dealt with and by whom (Figure 8).

Figure 8: Who conducted investigations, 2012–13 to 2014–15 (N)



Note: Respondents reported all ways matters were investigated; therefore, investigation numbers exceed incidents included in the report

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

In 2014–15, six respondents indicated their entity had conducted an initial review or investigation which was then investigated by another entity, such as the police or an external investigator. Another three entities indicated that a formal investigation was not undertaken, with one entity reporting the matter was resolved when the suspect self-reported and funds were recovered.

Outcomes

Respondents were also 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). The findings are presented in Table 6.

Table 6: Outcome of internal investigation by incident number, 2012–13 to 2014–15 (N)			
Outcome	2012–13	2013–14	2014–15
Suspect admitted allegation in full	3	3	11
Suspect admitted allegation in part only	2	0	2
Matter referred for civil action	0	0	2
Suspect dismissed from employment	8	4	5
Suspect reprimanded	4	4	4
Suspect resigned or left employment	8	7	8
Matter referred to law enforcement agency	1	3	5
Matter referred to prosecution agency	3	4	3

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

Respondents were able to choose all outcomes applicable. In 2014–15 there was one investigation in which no further action was taken after the suspect repaid the money in full, and another matter that was treated as a code of conduct matter. One further investigation was ongoing (despite the fact that the questions asked only about finalised investigations).

Respondents were asked about the outcome of any legal proceedings. In 2014–15 no legal proceedings were undertaken in relation to 27 incidents (involving the primary suspect only). Details were provided by respondents for four criminal sanctions imposed after prosecution. One suspect was convicted and sentenced to seven years' imprisonment, with a non-parole period of 30 months, and ordered to pay $266,000 to the Commonwealth. In another, the suspect was found guilty in a District Court and sentenced to four years' imprisonment, with a non-parole period of 10 months. Suspended sentences and good behaviour bonds were imposed in the other two cases. These sentences are comparable with those found in prior research into serious fraud cases (Smith & PricewaterhouseCoopers 2003).

The present census also found a number of individuals who had been dismissed from their employment each year following investigations. The number of suspects dismissed from employment has been declining over the three years examined in this report (8 Commonwealth officials dismissed in 2012–13, 4 in 2013–14 and 5 in 2014–15). Of the eight suspects dismissed from employment in 2012–13, there was one case in which monies lost due to the fraud incident were recovered in full at the time of the census, and no legal proceedings were undertaken in any of the other cases. In one other case of dismissal, no money had been recovered at the time of the census.

In 2013–14 four suspects were dismissed with no legal proceedings undertaken at the time of the census; in two of those cases no money was lost, in another case no monies had been recovered and in the other case recovery was made in full. In 2014–15 two of the cases in which Commonwealth officials were dismissed resulted in full and partial recovery of lost monies, in one case there was no recovery of lost monies and in the final two cases no monies were lost by the victim entity. In its review of internal organisational fraud in the UK, Cifas (2014) found a higher percentage of employees (63%) had been dismissed from their employment for fraud than the current study.

Recoveries

Following detection of Commonwealth fraud, entities have a responsibility to attempt to recover any outstanding losses from those responsible. Respondents were asked to indicate how much money or other property was recovered from suspects in the year of reporting. An 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 in each year. Over the three years examined, the proportion of losses recovered from suspects fluctuated considerably (see Table 7), ranging from just 3.4 percent in 2013–14 to 57.4 percent in 2012–13. It must also be noted that recoveries are unlikely to occur in the same financial year as the finalisation of an investigation, and some of the amounts recovered may include court ordered compensation that may take years to eventuate.

Table 7: Entities' financial losses and monies recovered from most costly incident, 2012–13 to 2014–15 (N&$)

Year	Number of entities that quantified a loss amount	Amount lost ($)	Number of entities that recovered monies (in full or part)	Amount recovered ($)
2012–13	34	1,328,617	14	762,361
2013–14	20	1,001,181	8	34,244
2014–15	19	5,185,026	10	1,623,339

Note: In 2012–13, 14 entities suffered $0 losses; in 2013–14, 13 entities suffered $0 losses; in 2014–15, 12 entities suffered $0 losses. 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. In 2014–15, 19 entities quantified a loss (excluding one entity that reported a duplicated incident). In 2014–15, 10 entities recovered funds from the suspect.

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

The highest losses occurred in 2014–15, when two entities experienced financial losses of over $1m. While a large proportion of the losses were recovered in 2014–15 a greater proportion of funds, more funds were recovered in 2012–13. The amount of money recovered each year fluctuates for a variety of reasons. For example, the recovery process may take considerable time even after a court order has been obtained. There have also been instances in which suspects who have fraudulently obtained Commonwealth funds have simply spent the monies on expensive cars or lavish lifestyles, thereby denying any possibility of recovery.

Box 2: Example of a most costly internal fraud involving unauthorised access to data

The suspect was a non-ongoing APS employee who had been employed by the entity for between 13 and 24 months. He did not hold a security clearance, nor did the entity have details about his educational attainments. The suspect was located in Victoria and was employed at the APS 1–4 level. The suspect targeted information held by the entity, specifically obtaining or using information without authorisation. The fraud involved the misuse of information and communications technology (ICT), by accessing a computer without authorisation and copying data without authorisation. The fraud was first detected in January 2013 and came to the attention of the entity via an external whistleblower. The entity estimated that, if the fraud had continued, losses would have been around $7.5m, although the entity's actual total financial loss was $2m, with $1.5m recovered. The fraud continued for 18 months and the suspect collaborated with six other people. The motive cited by the respondent was greed. The investigation was finalised in December 2014 (almost two years after detection). The suspect admitted the allegations in full and resigned his employment with the entity. Criminal sanctions were imposed after legal proceedings, and the suspect was convicted and sentenced to 20 months' imprisonment (suspended) with a $3,000 surety and a three-year good behaviour bond.

Source: Commonwealth fraud monitoring dataset 2014–15

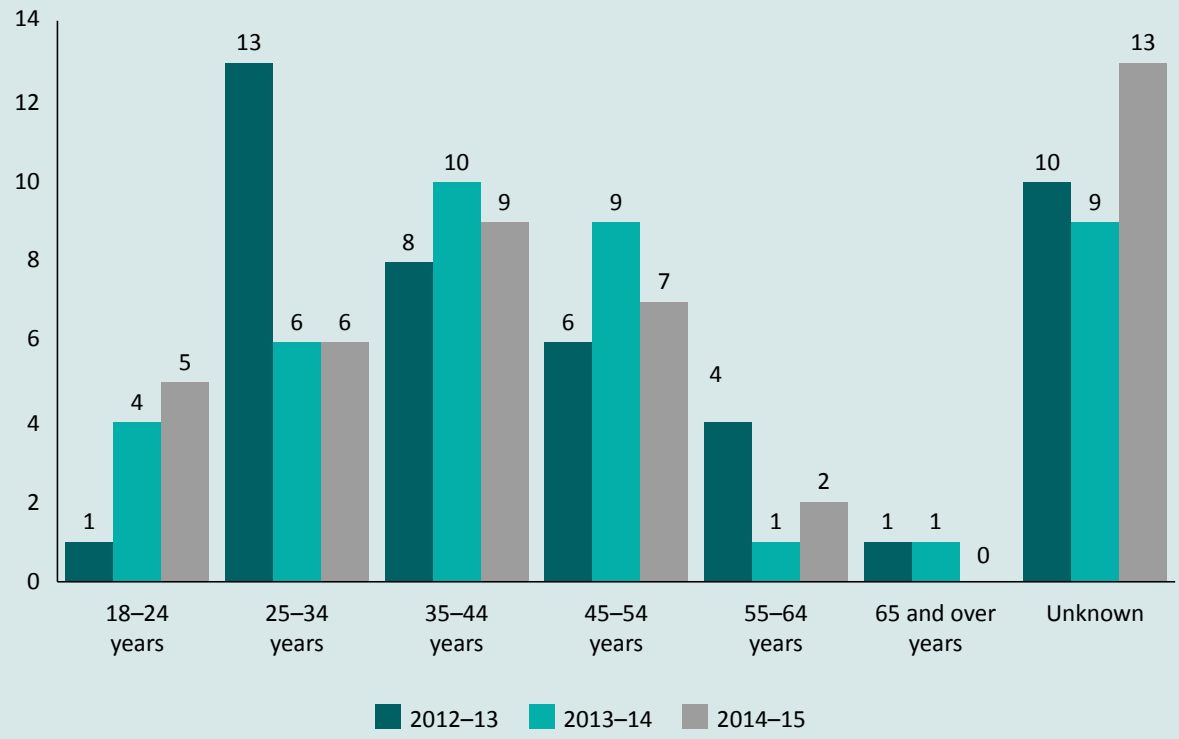
Characteristics of suspects

Respondents were asked to provide information concerning a wide range of demographic and other details about suspects and their employment. In a number of instances, only partial information was collected and able to be reported.

Age

There were substantial differences in the age category data reported. Over the three years, respondents were unable to provide age information in 32 cases. Of the remaining cases, in 2012–13 suspects were most frequently aged 25–34, with the next most common age group being 35–44 (Figure 9). In both 2013–14 and 2014–15, the largest age category for suspects was 35–44 years, followed by 45–54 years.

Figure 9: Number of suspects by age category by year, 2012–13 to 2014–15 (N)



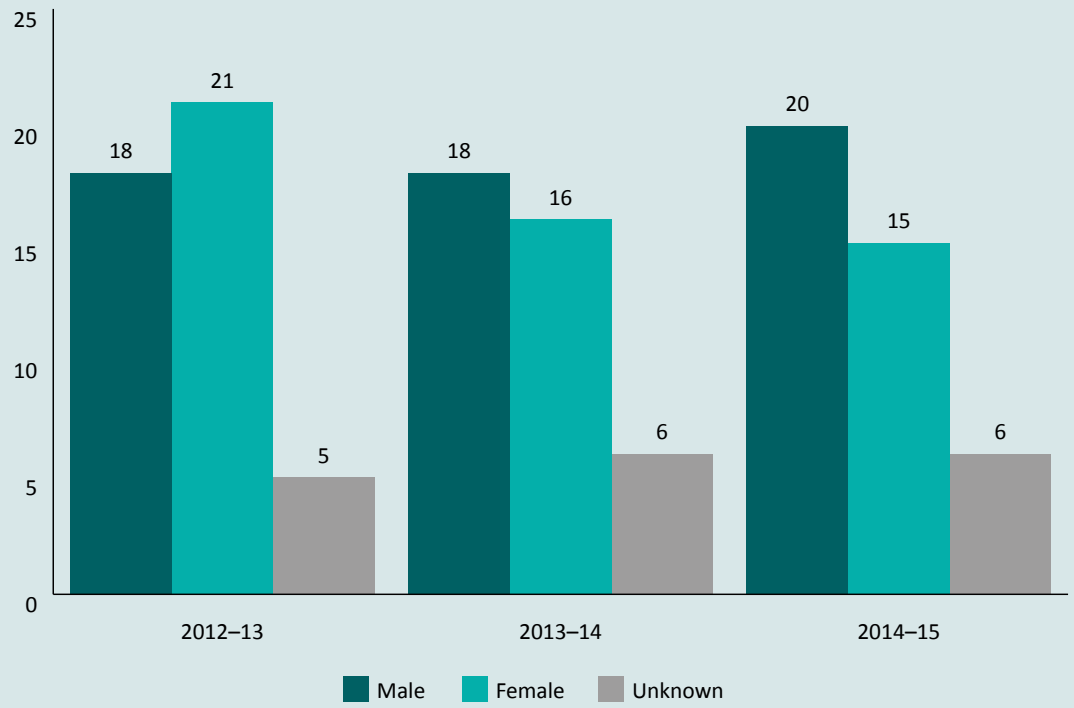
Source: Commonwealth fraud monitoring datasets 2012–13, 2013–14 and 2014–15 [AIC computer file]

In the 2013–14 and 2014–15 cases in which the suspect's age was known, Commonwealth census findings were more in line with industry surveys such as that by PricewaterhouseCoopers in 2014, which found 39 percent of internal fraud perpetrators were aged 31–40, and the 2013 KPMG survey, which found 70 percent of those who committed internal fraud were aged 36–55.

Gender

Many entities were unable to report the gender of suspects, or chose not to respond to that question (see Figure 10). It is possible that, at the time of reporting, some entities may not have identified a suspect for the most costly incident of fraud; although, once again, it was expected that this information should have been available to respondents, as a completed most costly investigation should have been chosen for analysis.

Figure 10: Number of suspects by gender by year, 2012–13 to 2014–15 (N)



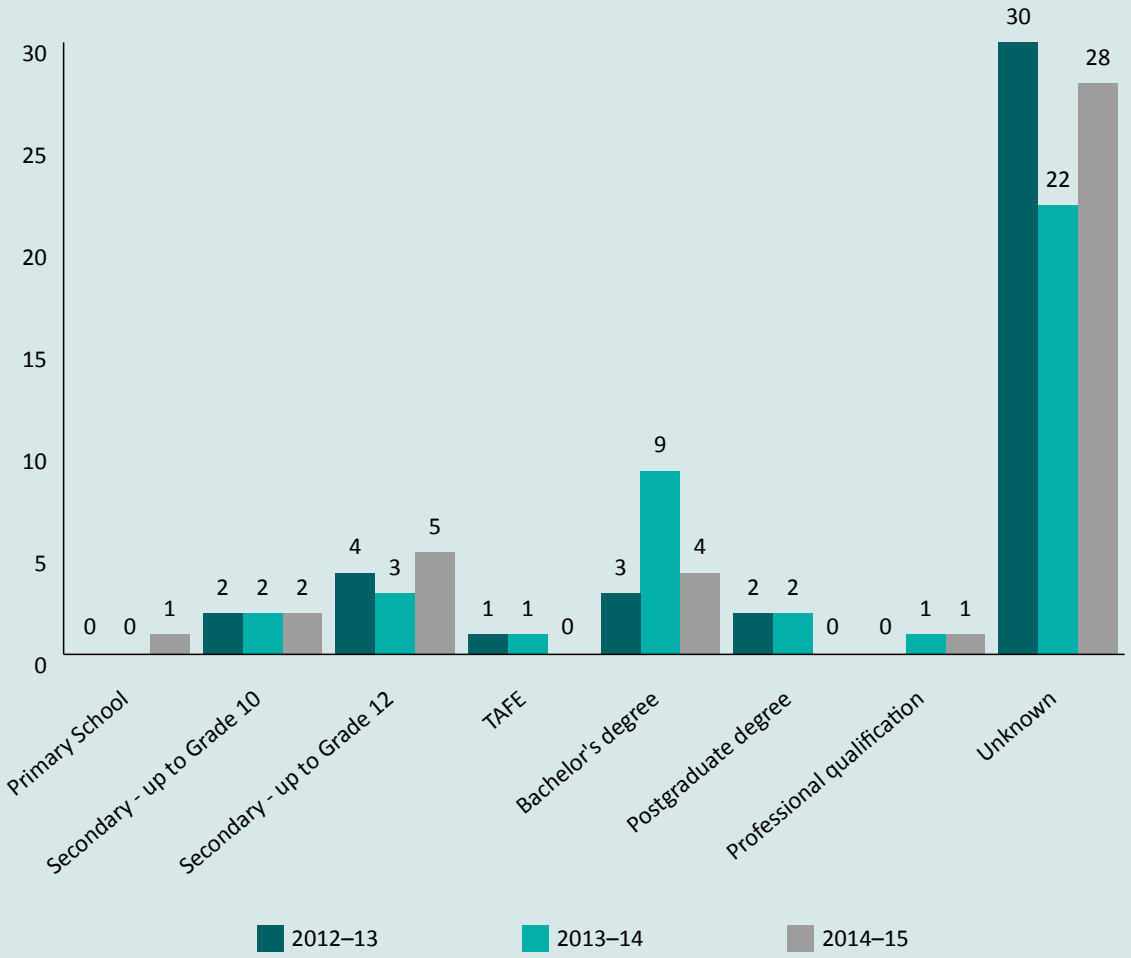
Source: Commonwealth fraud monitoring datasets 2012–13, 2013–14 and 2014–15 [AIC computer file]

In 2012–13, more women (21) than men (18) were suspects in incidents of fraud; however, in 2014–15, 49 percent of suspects were identified as men, whereas 37 percent of suspects were women. In the Commonwealth public sector in 2014–15, 58.4 percent of employees were women (APSC 2015: 17). This finding is more in line with prior research, such as ACFE's (2016) global survey of occupational fraud, which found 69 percent of identified perpetrators were men compared with just 31 percent of women.

Educational level

Respondents were asked to indicate the highest level of education that suspects had completed. As most Commonwealth entities require proof of educational levels attained, it was surprising that consistently over the three years between 55 and 68 percent of respondents listed the suspect's highest level of education as unknown (Figure 11). In 2013–14, nine suspects' highest level of education was a Bachelor's degree. Cifas (2015), using information provided by the UK's Higher Education Degree Datacheck, found 2,700 job applicants in the UK since 2009 had provided false information to prospective employers about their educational background. This remains an area of internal fraud risk that requires ongoing vigilance in terms of fraud control. Box 3 provides an example from the 2014–15 census where an internal fraud suspect had falsified their educational history in order to gain employment in the APS.

Figure 11: Number of suspects by highest level of education attained, 2012–13 to 2014–15 (N)



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

Box 3: Example of internal fraud citing misuse of information/documents from the 2014–15 census

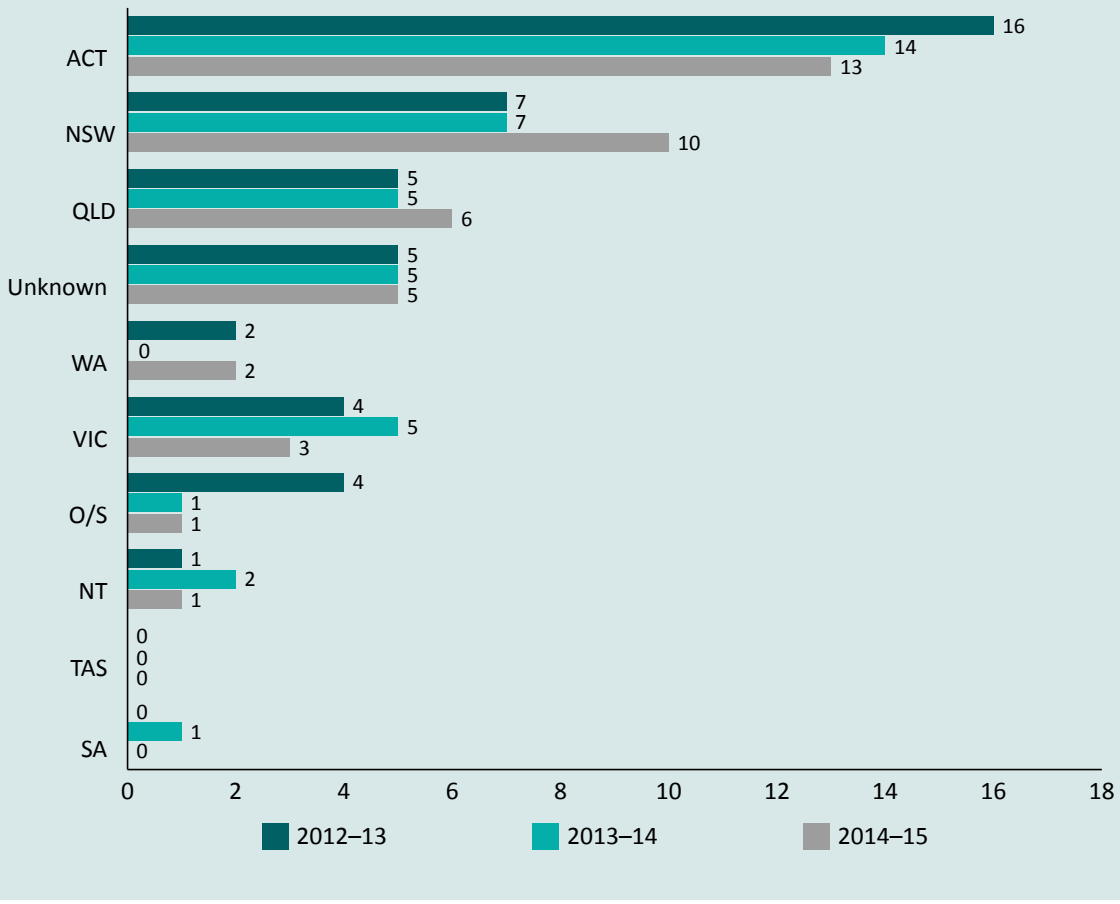
The suspect was a man who had been a full-time employee for between 37 and 48 months. At the time the fraud was detected, the suspect was aged 25–34, held a Baseline security clearance and resided in the Australian Capital Territory (ACT). The suspect was educated to grade 12 at secondary school and was employed by the entity at APS level 5–6. The fraud involved the misuse of leave and related entitlements and misuse of information, specifically the falsification of qualifications and employment details. The entity was notified of the fraudulent activity by a whistleblower who was external to the entity. An internal investigation revealed the fraud only involved the suspect, with no collaborators. No financial loss was recorded (although, arguably, the suspect may have been paid a salary to which he was not entitled). No information on motive for the fraud was provided. At the time of completing the census, the investigation had not been finalised and no outcome was available.

Source: Commonwealth fraud monitoring dataset 2014–15 [AIC computer file]

Residence

Given the concentration of Commonwealth entities in the ACT, suspects were most likely to live in the ACT at the time the fraud was detected (Figure 12). On average, over the three years just over one-third of suspects resided in the ACT (34.4%). In 2014–15, however, there was an increase in the number of suspects residing in New South Wales, from seven suspects in 2012–13 and 2013–14 to 10 suspects in 2014–15. In all three years there were no suspects residing in Tasmania.

Figure 12: Number of suspects by residence in Australian jurisdictions and overseas, 2012–13 to 2014–15 (N)



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

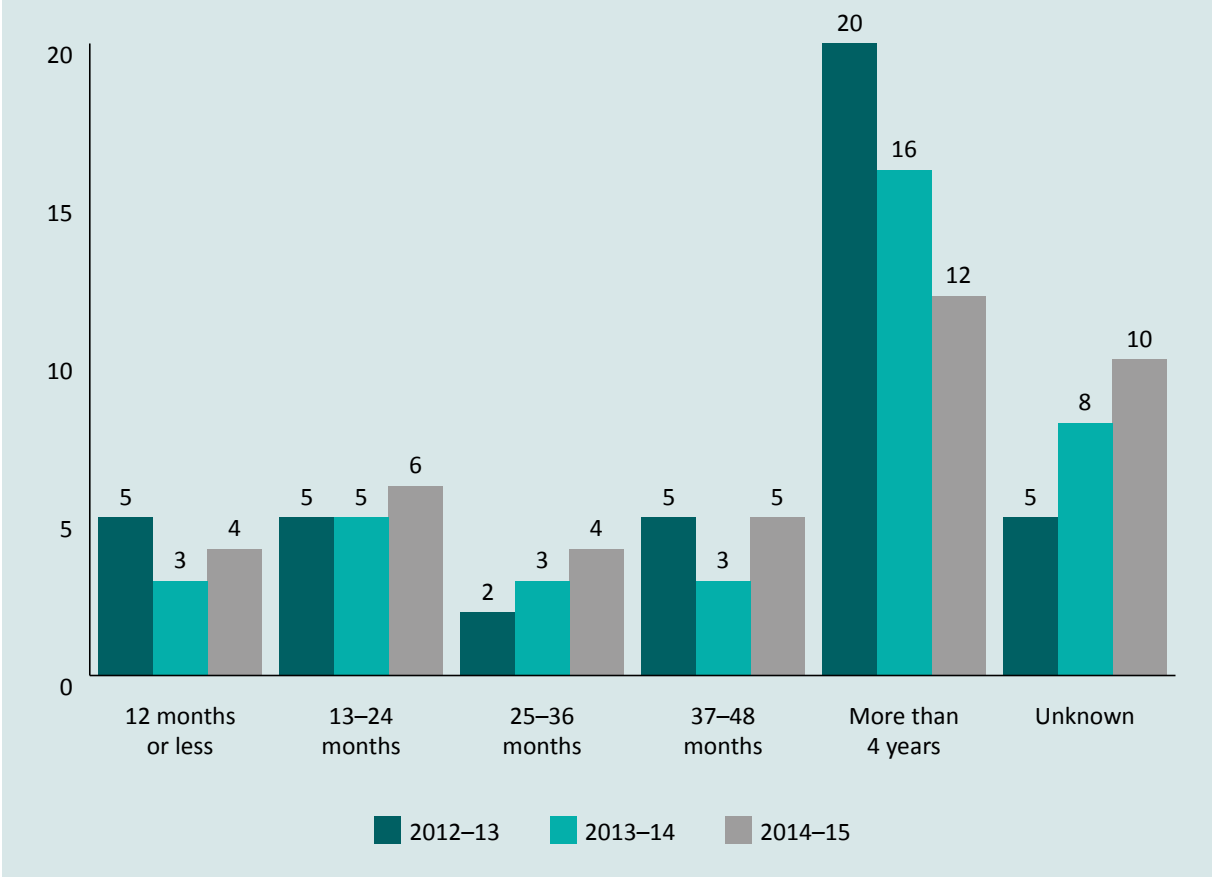
Employment

More than two-thirds of suspects each year were employed full-time (66.7% in 2012–13, 67.5% in 2013–14 and 68.3% in 2014–15). In 2014–15, nine suspects had 'other' employment relationships with entities. Examples of these included suspects who were former employees at the time the fraud was detected, or a suspect who was a secretary of a contractor employed by the entity. Other responses, such as one response that indicated that the suspect was a non-ongoing APS employee, seemed to have misinterpreted the question.

Length of employment

Respondents were also 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. Figure 13 presents data showing the majority of suspects had been employed by the entity for more than four years. This may 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. Alternatively, the fraud incident may have been purely opportunistic or due to a change in the suspects' personal circumstances. This factor is explored in more detail below. 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). Findings from the census in 2014–15 differed from previous years with regard to a decrease in the number of suspects who had been employed by the victim entity for more than four years, decreasing from 20 suspects in 2012–13 to 12 suspects in 2014–15. In 2014–15 a larger number of suspects had been employed for 37–48 months (N=5) than the three suspects who were employed for that length of time in 2013–14. As was found in 2013–14, in 2014–15 there was an increase in the number of entities who could not say how long the employee had been with them—again, this indicates that respondents might not have consulted personnel records prior to responding to the census.

Figure 13: Number of suspects by length of employment with the entity, 2012–13 to 2014–15 (N)



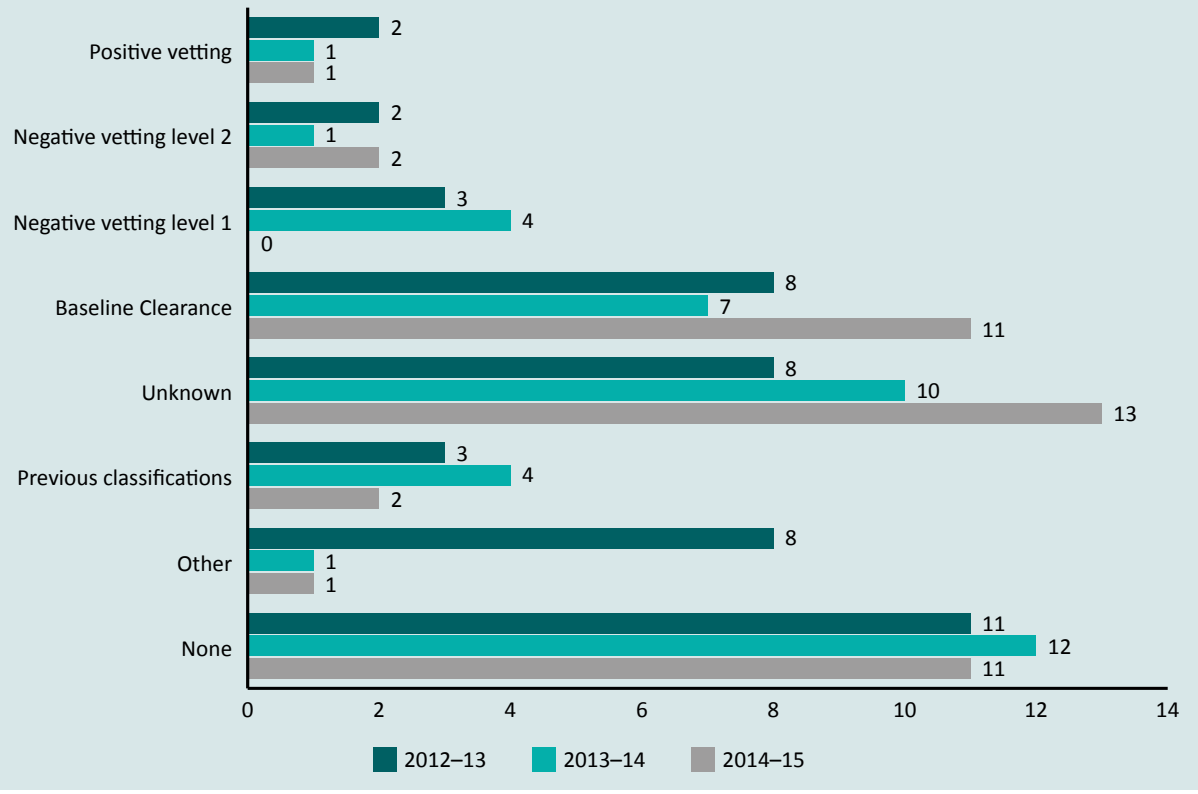
Source: Commonwealth fraud monitoring datasets 2012–13, 2013–14 and 2014–15 [AIC computer file]

Security clearances

Respondents were asked to indicate the level of security clearance held by suspects at the time the most costly internal fraud incident had been detected (see Figure 14). In the Commonwealth, the majority of security clearances are issued by the Australian Government Security Vetting Agency (AGSVA). Security clearances, while not undertaken specifically as a fraud prevention measure, do assess a person's background, character and values. However, while a security clearance assesses a Commonwealth official's previous criminal history and offending history, the latest ACFE (2016) research found only five percent of fraud offenders had a prior fraud conviction, and only eight percent had previously been let go from employment due to fraud. This finding indicates that a high percentage of fraud offenders are first-time offenders. Accordingly, security checks of background and character may have limited impact on detecting those who may commit fraud. Ultimately, each year a small number of Commonwealth employees who hold clearances do commit fraud offences.

Figure 14 shows the number of internal fraud suspects who held security clearances, when this information was known. Each year there were large numbers of incidents where it was unknown whether the suspect held a security clearance. It appears that between 11 and 12 suspects each year had not undergone any security clearance vetting, presumably owing to the nature of the work they undertook. In 2014–15, for the first time, there were no suspects who held a security clearance at the Negative vetting level 1, but two suspects held Negative vetting level 2 clearances, and one suspect held the highest security clearance available, Positive vetting. For suspects who held a security clearance at the time the fraud was detected, the most common level was a Baseline clearance. Each year, there were a few suspects who held other forms of security clearances, such as specific governmental industry clearance checks. There were also suspects who held clearances under the previous classification system, such as Confidential, Protected (equivalent of current Baseline clearances) and even Top Secret (the equivalent of a Negative vetting level 2 or above; AGSVA 2017).

Figure 14: Number of suspects' security clearances held at the time most costly internal fraud was detected, 2012–13 to 2014–15 (N)

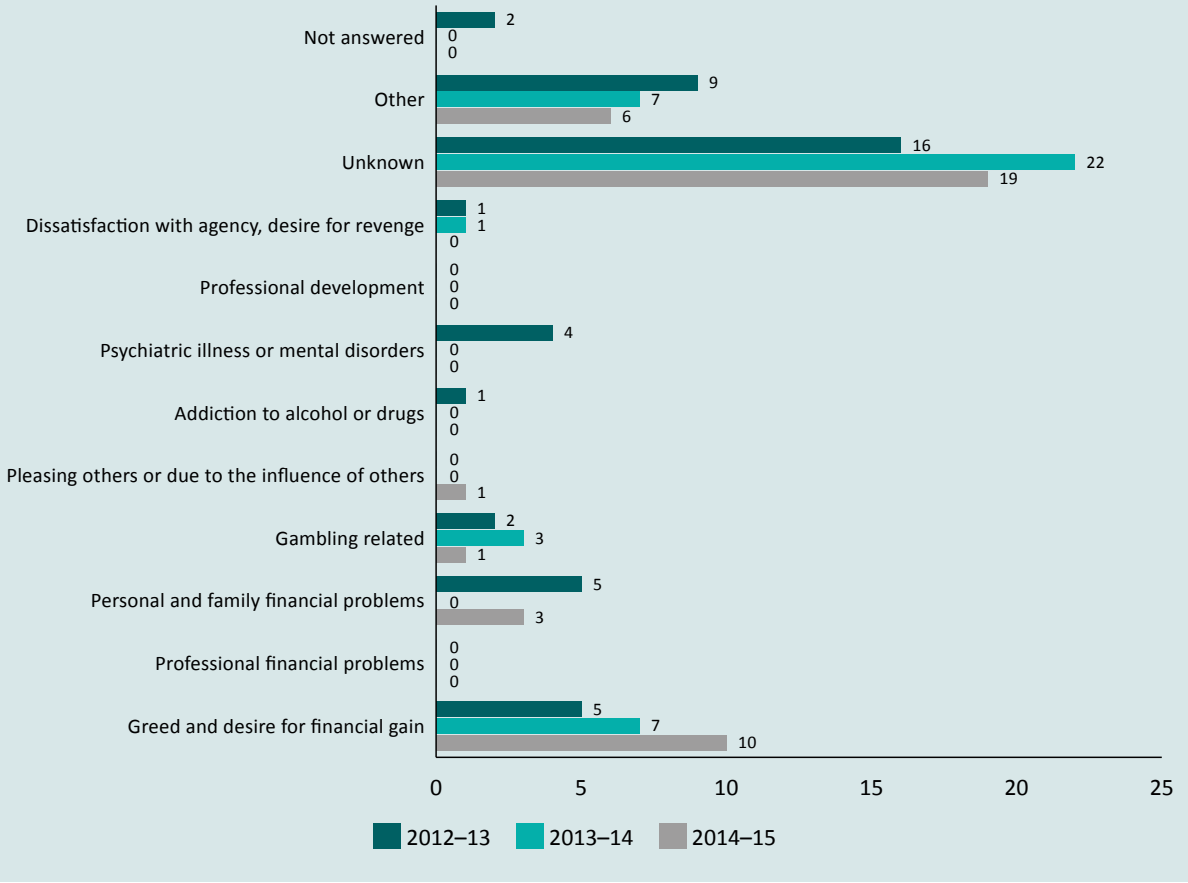


Source: Commonwealth fraud monitoring datasets 2012–13, 2013–14 and 2014–15 [AIC computer file]

Primary motivation

To gain an insight into why fraud occurs, respondents were asked to indicate the primary motivation the suspect had for committing the fraud (see Figure 15). 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. Although the information was based on completed investigations, the level of understanding as to why fraud was committed was unknown in numerous cases.

Figure 15: Primary motivation for the commission of most costly internal fraud incidents for suspects, 2012–13 to 2014–15 (N)



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

Of the responses provided, the most frequently cited motive was greed and desire for financial gain, followed by personal and family financial problems. These principal motivations largely correspond with those identified by prior international fraud survey research, where financial strain, often caused through greed, was found to be the main motivation for fraud offending (ACFE 2014; Smith & PricewaterhouseCoopers 2003). ACFE (2016) noted that motivations for committing fraud may change depending on the occupational level of the perpetrator. For example, ACFE's global survey found 38 percent of employees who committed fraud were experiencing financial difficulties at the time they committed fraud; however, that was less likely to be the case with perpetrators at higher occupational levels (such as owners or executives), who were more likely to have explanations for offending based on close associations with vendors or customers or who engaged in collusion with suppliers. In the present research, no suspects had professional financial problems as their motivation for fraud, and in 2013–14 and 2014–15 no suspects were motivated by psychiatric or mental health issues or drug additions.

Conclusions

While it may not be possible to predict who in an organisation is likely to commit fraud, some consistent trends can be identified by reviewing the most costly internal fraud incidents reported by entities each year. In all three years, the most common financial loss experienced by entities was below $1,000. This finding may indicate that fraud perpetrators are testing systems to see if planned methods of committing fraud are successful, prior to engaging in large-scale acts of dishonesty, or it may be that some entities are only detecting less sophisticated fraud, which is generally of lower value. Consistently, the two most common targets for fraudsters were either entitlements or financial benefits, although this may be influenced by what entities consider to be the most costly internal fraud incident. Over the three-year period, it was consistently found that suspects had been employed for more than four years, which implies those employees may have had more time to familiarise themselves with internal controls or had greater responsibility and were more trusted. Alternatively, there may have been a change in suspects' personal circumstances, or a previously unrealised opportunity to commit fraud may have presented itself. This finding has not changed over time, although in 2014–15 the number of respondents who indicated that such details were unknown has increased.

The large number of unknown responses supplied is of concern, as respondents were asked to select their most costly incident of internal fraud in which the investigation had been concluded. It is problematic, therefore, that respondents were unable to report information on age, gender, highest level of education, length of time with entity and security clearance, as all these details should have been identified during investigations or at least held by personnel management sections within entities. More research is also necessary to determine why no Commonwealth officials at the senior management (SES) level, or equivalent, were identified as being fraud suspects, and whether this was because they had not committed offences, their offending had not been detected, or the incidents of fraud did not fall into the most costly category. 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 (ACFE 2016).

Future questionnaires will also seek information on the behavioural red flags that might be indicative of offending. By collecting data pertaining to who committed the fraud, how it was committed and associated red flags that fraud was being committed, the government will be better placed to understand how fraud may be detected and prevented, thus minimising its financial and other impacts.

References

Association of Certified Fraud Examiners (ACFE) 2016. Report to the nations on occupational fraud and abuse: 2016 global fraud study. http://www.acfe.com/rttn.aspx

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

Australian Government Security Vetting Agency (AGSVA) 2017. About security clearances. http://www.defence.gov.au/AGSVA/FAQ/clearance-subject.asp

Australian Public Service Commission (APSC) 2015. State of the service report 2014–15. Canberra: APSC. http://www.apsc.gov.au/publications-and-media/current-publications/state-of-the-service/state-of-the-service-report-2014-15

Cifas 2015. Employee fraudscape 2015. London: Cifas. https://www.cifas.org.uk

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

Jorna P & Smith RG 2017. Fraud against the Commonwealth: Report to Government 2015, Statstical Report No 03, Canberra: Australian Institute of Criminology

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 2016. Global fraud report 2015–16: Vulnerabilities on the rise. http://www.kroll.com/global-fraud-report

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 Crime 19(1):54–64

PricewaterhouseCoopers 2016. Global Economic Crime Survey 2016. Adjusting the lens on economic crime: Preparation brings opportunity back into focus. http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html

PricewaterhouseCoopers 2014. Economic crime: A threat to business globally: PwC's 2014 Global Economic Crime Survey. http://www.pwc.com/gx/en/industries/financial-services/publications/global-economic-crime-survey-2014-financial-services.html

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

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 & PricewaterhouseCoopers 2003. Serious fraud in Australia and New Zealand. Research and Public Policy Series no. 48. Canberra: Australian Institute of Criminology/PricewaterhouseCoopers.

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

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