The Auditor-General
Audit Report No.10 2010–11
Performance Audit

Centrelink Fraud Investigations

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 81154 7

Australian National
Audit Office

Canberra ACT
30 September 2010

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit in the Centrelink in accordance with the authority contained in the *Auditor-General Act 1997*. I present the report of this audit and the accompanying brochure. The report is titled *Centrelink Fraud Investigations.*

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's Homepage—http://www.anao.gov.au.

Yours sincerely

Ian McPhee
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits and financial statement audits of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Telephone: **(02) 6203 7505**
Fax: **(02) 6203 7519**
Email: **webmaster@anao.gov.au**

ANAO audit reports and information about the ANAO are available at our internet address:

http://www.anao.gov.au

Audit Team
Kay Robinson
Michael Masters
Steven Lack

Contents

Abbreviations 8
Glossary 10

Summary and Recommendations 15

Summary 17
Introduction 17
Audit objective 22
Audit scope and methodology 23
Overall conclusion 24
Key findings 27
Summary of agencies' responses 35
Recommendations 37

Audit Findings and Conclusions 39

1. Introduction 41
Background 41
Australian Government regulatory framework 45
Audit objective, scope and methodology 51
Previous audits 53
Structure of the report 54
2. Fraud Management Framework 55
Background 55
Governance framework 55
Compliance framework 59
3. Referrals Leading to Case Selection 65
Background 65
Generic referral of fraud cases 65
Automatic referral of fraud cases 66
Intelligence Assessments generated by Centrelink's intelligence capability 69
Fraud case prioritisation and categorisation policy 72
Centrelink's National Case Selection Guidelines 79
Fraud-related targets 81
4. Investigating and Responding to External Fraud 88
Background 88
Fraud investigations 88
Centrelink's Fraud Investigation Case Management System 97
Fraud Investigation Manual 102
Training and Quality Assurance 105

5. Referral of Cases to the Commonwealth Director of Public Prosecutions 112
Background 112
National Case Selection Guidelines 114
Collecting evidence for possible prosecution action 119
Content and quality of Centrelink's briefs of evidence 122
Feedback and liaison 131
6. Performance Information and Reporting 132
Consistency and reliability of fraud data in Centrelink's systems 132
Target setting 136
Monitoring and reporting fraud activity 139
Cost-effectiveness of fraud programs 144

Appendices 149

Appendix 1: Agencies' responses to the audit 151
Appendix 2: Roles and responsibilities in the Bilateral Management Arrangements between Centrelink, the Department of Human Services and the policy agencies 154
Appendix 3: Previous ANAO audits related to fraud control 155
Appendix 4: Centrelink's Strategic Directions for 2008–09 156
Appendix 5: Centrelink's key industry stakeholder relationships 158
Series Titles 160
Current Better Practice Guides 162

Tables

Table S1 Centrelink's compliance with investigation standards 32
Table 1.1 Fraud investigations and prosecutions activity reported by Centrelink in 2008–09 44
Table 1.2 Centrelink's operational framework 49
Table 1.3 Centrelink's use of its coercive powers and the applicability of the AGIS 52
Table 1.4 Final ANAO sample of Centrelink fraud investigation cases 53
Table 3.1 Cases referred to the CDPP by complexity rating in 2007–08 77
Table 3.2 Performance measures for the Business Integrity Network 2008–10 85
Table 4.1 Centrelink's conduct of Fraud Investigations 91
Table 4.2 Limitations of Centrelink's Fraud Investigation Case Management System 97
Table 5.1 Short form briefs of evidence 123

Figures

Figure S1 Centrelink's compliance model 19
Figure 1.1 The Australian Government's regulatory framework for managing fraud 46
Figure 2.1 Centrelink's enforcement pyramid model for community compliance 60
Figure 2.2 Centrelink successful prosecutions by group in 2007–08 63
Figure 3.1 Detection of fraud and case flows into FICMS in 2008–09 67
Figure 3.2 Outcomes of finalised DMS cases referred to the FITs in 2007–08 68
Figure 3.3 Outcomes of finalised IRS cases referred to the FITs in 2007–08 69
Figure 3.4 Complexity ratings assigned to fraud investigation cases in 2007–08 76
Figure 3.5 Proportion of cases referred to the CDPP by payment type in 2007–08 78
Figure 3.6 Workflow of cases in and out of FICMS in 2008–09 81
Figure 4.1 Overview of Centrelink's fraud investigation process 90
Figure 5.1 Fraud case flows: detection to prosecution 2007–08 115
Figure 5.2 Centrelink fraud prosecution referrals to the CDPP, January 2007 to July 2009 130
Figure 6.1 Centrelink's Annual Report 2008–09 fraud investigations matched with FICMS data 135
Figure 6.2 AFP model to ensure resources are targeted to the highest priority work 146

Abbreviations

ADEX	Explanation of Mainframe Debt
AFP	Australian Federal Police
AGIS	*Australian Government Investigations Standards 2003*
AIC	Australian Institute of Criminology
ANAO	Australian National Audit Office
APS	Australian Public Service
ARC	Administrative Review Council
Archives Act	*Archives Act 1983*
AUSTRAC	Australian Transaction and Reports Analysis Centre
BMAs	Bilateral Management Agreements
BPAs	Business Partnership Agreements
CCO	Case Control Officer
CDPP	Commonwealth Director of Public Prosecutions
CDR	Critical Decision Record
CEO	Chief Executive Officer
CHART	Customer History and Relationships Tool
DEEWR	Department of Education, Employment and Workplace Relations
DHS	Department of Human Services
DOC.	A DOC. is a record of an event or decision recorded on a customer's record in Centrelink's Mainframe system.
DMS	Debt Management System
FMA Act	*Financial Management and Accountability Act 1997*
FaHCSIA	Department of Families, Housing, Community Services and Indigenous Affairs
FAU	Fraud Analyst Unit
FICMS	Fraud Investigation Case Management System

FIM	*Fraud Investigation Manual*
FIT	Fraud Investigation Team
FOI	*Freedom of Information Act 1982*
HOCOLEA	Heads of Commonwealth Operational Law Enforcement Agencies
IA	Intelligence Assessment
ID fraud	Identity fraud
IRS	Integrated Review System
JASCEWG	Joint Agency Strategic Cash Economy Working Group
KPIs	Key Performance Indicators
MOU	Memorandum of Understanding
NCSG	*National Case Selection Guidelines*
NSO	National Support Office
Privacy Act	*Privacy Act 1988*
POI	Proof of Identity
Public Service Act	*Public Service Act 1999*
QAR	Quality Assurance Review
RSS	Random Sample Survey
Social Security (Administration) Act	*Social Security (Administration) Act 1999*
The Guidelines	*The Commonwealth Fraud Control Guidelines 2002*
TORS	Tip-off Recording System

Glossary

Australian Government Investigations Standards 2003 (the AGIS)	The AGIS provides a set of best practice, minimum standards for fraud investigations. All Australian Government agencies that are required to comply with the *Commonwealth Fraud Control Guidelines*, must also comply with the AGIS standards.
Benefit	A benefit is defined in s12 of the *Commonwealth Services Delivery Agency Act 1997* and includes: a pension, allowance, concession or payment; and a card entitling its holder to a concession or a payment of any kind.
Bilateral Management Arrangements (BMAs)	The BMAs set out Centrelink's responsibilities and expectations of policy departments including Key Performance Indicators (KPIs), and the basis for the financial arrangements between the parties. Before 1 July 2009, Centrelink's revenue was primarily derived from its bilateral arrangements with its policy departments known as Business Partnership Arrangements (BPAs) or similar.
Brief of evidence	A brief of evidence is a set of papers containing: • an allegation and reference to the relevant legislation; • a narrative of the facts of the case; and • admissible evidence that proves the elements of the possible offence and any other relevant material, so that the matter may be evaluated and prosecuted.
Business Integrity Division	Centrelink's Business Integrity Division is responsible for ensuring the integrity of Government outlays and services by minimising fraud and customer debt.

Case Control Officer (CCO)	The role of the CCO is to assess all new cases in the Team New Work of the Fraud Investigation Case Management System (FICMS) against Centrelink's *National Case Selection Guidelines* (NCSG). Cases that satisfy the NCSG are allocated for investigation and possible referral for prosecution. Once a case is assessed by the CCO, the outcome may be termination, referral elsewhere or allocated for investigation.
Case Prioritisation Framework (CPF)	The CPF is designed to enable Centrelink staff to make an assessment of the seriousness and priority of fraud investigations.
Commonwealth Fraud Control Guidelines - 2002 (the Guidelines)	Under the Guidelines, the Australian Government requires all agencies governed by the FMA Act and CAC Act to implement effective fraud control practices and procedures.
Compliance reviews	Centrelink conducts customer compliance reviews to assess the eligibility of benefit payments. The reviews are based on information gained from internal and external data sources, including the use of data-matching.
Fraud Analyst Units (FAUs)	The primary function of the FAUs is to develop cases of alleged fraud to a point where Centrelink can identify if there is a likelihood of fraud and criminal activity. FAUs undertake high-level data analysis of internal and external databases and produce case-specific Intelligence Assessment reports to assist the investigation of cases of fraud by Centrelink staff working in Fraud Investigation Teams.
Fraud	The Guidelines define fraud as 'dishonestly obtaining a benefit by deception or other means'.
Fraud Investigation Teams (FITs)	The FITs are part of the Business Integrity Network. They case manage all external fraud investigations and prosecution referrals in 11 locations around Australia.

HOCOLEA Principles	The Heads of Commonwealth Operational Law Enforcement Agencies (HOCOLEA) have agreed to implement overarching principles for selecting cases for investigation, referral for prosecution, and other regulatory activity. Centrelink has adopted the AGIS requirement of using the HOCOLEA Principles as a basis to frame the development of its fraud investigations *Case Prioritisation Framework*.
Investigation	The AGIS defines an investigation as 'inquiries into whether there has been a breach of Commonwealth, State or Territory law, with a primary purpose of gathering admissible evidence for any subsequent action, whether civil, criminal or administrative. An investigation also includes intelligence projects, proceeds of crime and financial investigations'.
Legal Notice	Under s.192 of the Social Security (Administration) Act (the Act), Centrelink staff with the delegated authority, can obtain third party information about customers in relation to social security entitlement by issuing a s.196 written Legal Notice to a person to provide information and produce documents.
Proceeds of Crime	Proceeds of Crime refers to the benefits derived from the committing of criminal offences against Commonwealth laws.
Prosecution Policy of the Commonwealth	The policy provides guidelines for the making of decisions regarding the prosecution process. The policy is a public document based on the principles of fairness, openness, consistency, accountability and efficiency that the Office of the Commonwealth Director of Public Prosecutions seeks to apply in prosecuting offences against the laws of the Commonwealth.
Payment accuracy	Payment accuracy recognises the obligation of customers to advise of changes in their circumstances that may affect their payment entitlements.

Payment error	Payment error can be attributed to an unintentional omission by the recipient customer.
Payment inaccuracy	Payment inaccuracy is a variation to a payment that results from Centrelink, the policy department and/or customer actions.[1]
Payment incorrectness	Payment incorrectness is a variation to a payment that results from decision making processes which are within Centrelink's control.[2]
Payment Accuracy Fraud Risk Assessment Plans	The Guidelines require agencies to undergo a risk assessment process at least every two years and produce a Fraud Control Plan to manage the risks identified. Centrelink's Payment Accuracy Fraud Risk Assessment Plans outline the risks to payment accuracy identified in the assessment process and underpin Centrelink's 2008–10 Fraud Control Plan.
Raised debts	Where payment anomaly(s) are identified in a customer's records that cannot be explained, the amount is confirmed as a legal debt resulting in a debt being raised that is generally required to be repaid by the customer.
Random Sample Survey (RSS)	The RSS is a point-in-time analysis of sampled customers' circumstances, designed to establish whether customers are being paid their correct entitlement.
Serious social security fraud	Centrelink defines serious fraud using the following criteria: the nature of the fraud; how many risks are in the allegation/data; does information support ongoing fraudulent activity; the length of fraudulent activity; and the length of time on payment.

[1] The Allen Consulting Group, *FaCS and Centrelink: Compliance Review,* January 2004, p. vii.

[2] ibid.

Social Security fraud	Social Security fraud (includes the terms welfare and benefit fraud) is generally characterised by deliberate omission or provision of incorrect information in order to secure payments or payment amounts for which the recipient is not entitled. The important factor in characterising fraud is the level of 'intent' reflected in the customer's behavior.
Short form brief of evidence	A short form brief of evidence follows the same format as any other brief of evidence although it will not include all the evidence and exhibits that would otherwise be provided in a full brief such as witness statements. A short form brief of evidence contains: an allegation and reference to the relevant legislation; a narrative of the facts of the case; and admissible evidence that proves the elements of the possible offence.

Summary and Recommendations

Summary

Introduction

1. Centrelink is the Australian Government's principal service delivery agency for delivering a range of social security payments and benefits to eligible customers on behalf of policy departments. In 2008–09, Centrelink delivered social welfare payments totalling $87 billion to 7 million customers,[3] many of whom are the most vulnerable in our society and heavily dependent on Centrelink payments.

2. While improving the economic and social participation of its customers remains a high priority for Centrelink, the integrity of social security outlays is one of the high-level risks to be managed and a key consideration for policy departments including the Department of Education, Employment and Workplace Relations (DEEWR) and the Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA).

Integrity of Outlays

3. In delivering welfare payments and services, Centrelink is responsible for the integrity of Government outlays including the provision of assurance that customer payments are correct and fraud is minimised. In managing the integrity of social security outlays, Centrelink identifies and reports against Centrelink administrative error and payment accuracy. Payment accuracy recognises the obligation of customers to advise of changes in their circumstances that may affect their payment entitlements. While inaccurate payments can be caused by an unintentional omission by the recipient customer, welfare fraud is generally characterised by deliberate omission or provision of incorrect information in order to secure payments or payment amounts for which the recipient is not entitled. The important factor in characterising fraud is the level of 'intent' reflected in the customer's behavior.

[3] *Centrelink Annual Report 2008–09*, p. 4 & p. 11.

Centrelink's Fraud Control Plan

4. Centrelink's *Fraud Control Plan 2008–10* outlines its framework of compliance strategies and activities to prevent, detect and deter payment inaccuracies and fraud. The framework includes:

- prevention—systems and procedures designed to minimise incorrect payment and fraud from occurring, rather than detecting them later;
- detection—systems and procedures designed to discover incorrect payment and fraud when it occurs; and
- deterrence—systems and procedures designed to deal with incorrect payment and respond to potential or actual fraud when it is uncovered.

5. During 2008–09, Centrelink established corporate targets for fraud investigations and prosecution referrals, in order to recover the amount of customer debts and savings required by the policy agencies, under bilateral management arrangements (BMAs).

Bilateral Management Arrangements

6. Until 1 July 2009, Centrelink's revenue was primarily derived from its BMAs or similar with relevant policy departments. The arrangements with DEEWR and FaHCSIA included a suite of Key Performance Indicators (KPIs) and measures in relation to the amount of debts and savings required, mostly through the recovery of customer debts, and a payment correctness target of 95 per cent, to ensure the integrity of social security outlays.

7. Over the past few years, the total amount of customer debt raised by Centrelink as a result of compliance activities has increased from $419 million in 2006–07 to $536 million in 2008–09. During the same period, customer debts identified through fraud investigations, primarily generated from compliance activity, accounted for $127 million and $113.4 million respectively.

8. Since July 2009, Centrelink has received all of its departmental funding through direct appropriation. While policy agencies remain accountable for the oversight of social security payments, Centrelink has an increasing focus on preventative controls to manage the integrity of outlays but necessarily complements this with a range of detective controls designed to identify welfare payments that warrant closer analysis to assess their accuracy. This direction aligns with the Australian Government's new whole-of-government approach to managing social, health and welfare fraud and non-compliance, the core of which is to establish an appropriate balance between fraud

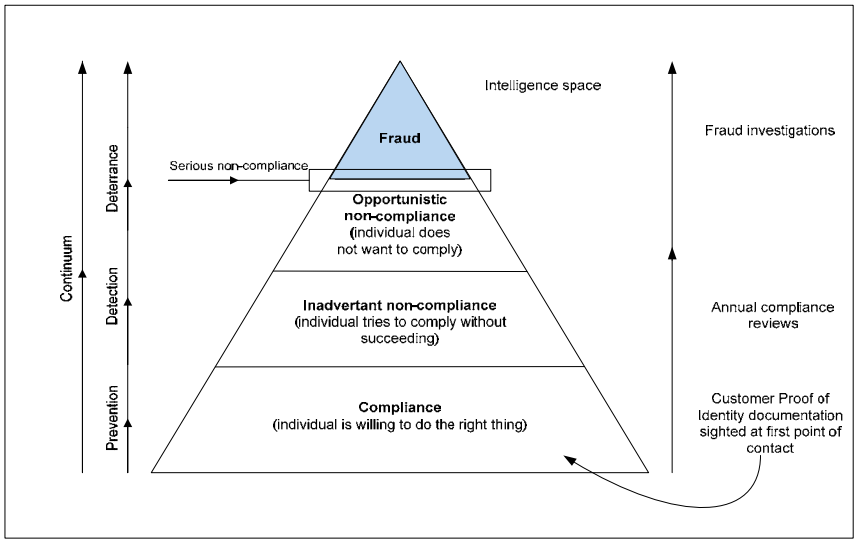
prevention and detection strategies, which focuses on prevention at the service delivery interface.[4]

Centrelink's compliance model

9. Centrelink's approach to defining and understanding the factors that influence the compliance behaviour of its customers is reflected in its compliance model. This model takes a graduated response to customer behaviour, recognising that most customers are willing or trying to comply. Customers at the top of the pyramid are considered to be 'unwilling' to comply, and this component is considered to constitute payment and serious fraud (see Figure S1).

Figure S1

Centrelink's compliance model



Source: ANAO analysis based on Centrelink's audit entry interview presentation, 23 June 2009.

10. Centrelink's compliance program aims to provide fair and appropriate responses to customer behaviour based on the customer's demonstrated ability and willingness to comply with their payment and reporting requirements. Centrelink's compliance model acknowledges each customer's unique circumstances, varying reasons for complying with their payment obligations

[4] The Australian Government's new whole-of-government approach, outlined in the Department of Human Services: *2009–10 Annual Compliance Plan and Performance Report*, is Cabinet-in-Confidence.

and the need for a tailored approach to supporting or correcting customer behaviour respectively.

11. Previous ANAO audit coverage of Centrelink's approach to managing incorrect payments and fraud focused on the agency's prevention and detection strategies.[5] The ANAO's focus in this audit was Centrelink's approach to investigating and responding to external fraud, including how Centrelink prioritises, selects and deals with serious cases of non-compliance.

Fraud investigations

12. Under the *Commonwealth Fraud Control Guidelines 2002* (the Guidelines), Centrelink is authorised to investigate potential cases of fraud and prepare briefs of evidence for consideration of prosecution action by the Commonwealth Director of Public Prosecutions (the CDPP). In 2008–09, Centrelink conducted 26 084 fraud investigations (compared to 35 885 in 2007–08) which led to $113.4 million in customer debts (compared to $140.2 million in 2007–08). Of the 26 084 fraud-related investigations reported in Centrelink's 2008–09 Annual Report, 5082 referrals were made to the CDPP for consideration of prosecution action in relation to fraud, resulting in 2973 convictions (about 11 per cent of the total investigations reported by Centrelink).

13. Centrelink's Business Integrity Division is responsible for investigating fraud on the programs Centrelink delivers including: a Fraud Investigation Network of 11 dedicated Fraud Investigation Teams (FITs) across Australia, supported by an established intelligence capability; a *Fraud Investigation Manual* (the FIM) of investigation policies, procedures and processes; and systems for case managing fraud investigations, performance monitoring and reporting fraud.

14. The scale of Centrelink's detection activities is necessarily large and its investigators are provided with fraud cases from a number of areas including generic and automatic referrals, to be able to meet performance targets for

[5] See, for example, the ANAO reports: *Fraud Control in Australian Government Agencies,* Audit Report No.42, 2009–10; *Centrelink's Tip-off System,* Audit Report No.07, 2008–09; *Management of Customer Debt—follow-up audit,* Audit Report No.42, 2007–08; *Proof of Identity for Accessing Centrelink Payments,* Audit Report No.08, 2007–08; *Assuring Centrelink Payment—The Role of the Random Sample Survey Programme,* Audit Report No.43, 2005–06; and *Management of Fraud and Incorrect Payment in Centrelink*, Audit Report No.26, 2001–02.

savings and prosecutions referrals.[6] The largest proportion of Centrelink's fraud cases are automatically referred debt cases.

Regulatory framework

15. In responding to fraud, Centrelink is governed by the legislation, powers and Directives under which it operates; the Australian Government's regulatory framework for Australian Public Service (APS) agencies managing fraud including the Guidelines; the *Australian Government Investigations Standards* (the AGIS), and other legislated requirements designed to protect the rights of individuals such as the *Freedom of Information Act 1982*, the *Privacy Act 1988* and the *Public Service Act 1988*.

Social Security Law

16. The Social Security Law coercive information-gathering powers are used by Centrelink (among other approaches) to collect internal and external evidence about a customer's circumstances. These coercive powers are determined by the provisions of the *Social Security (Administration) Act 1999* and are primarily used to collect information to establish an individual's eligibility or correct entitlement.[7] For the purpose of investigations, these administrative powers can only be used in limited circumstances to collect evidence. Once fraudulent behaviour is suspected, the powers can no longer be used to collect evidence for criminal purposes.[8] Centrelink has policies and procedural controls in place that are designed to ensure the use of coercive powers by its fraud investigators, is compliant with Social Security legislation.

The Australian Government Investigations Standards

17. In identifying the standards for investigations, the AGIS uses the Heads of Commonwealth Operational Law Enforcement Agencies (HOCOLEA)[9] agreed principle to differentiate between compliance work and fraud investigations. The AGIS standards are identified as the authority to be applied to all investigations, regardless of the outcome of the investigation (whether administrative, civil or criminal) other than audit and compliance work.

---

6 *Business Needs for Fraud Management in Centrelink*, 20 March 2008, p. 9.

7 *Social Security (Administration) Act 1999*, ss.192–195.

8 Centrelink, *Fraud Investigation Manual,* Scope of Powers: s.192–196, 2 June 2008.

9 Centrelink is not a HOCOLEA agency; however, HOCOLEA provides clarification to assist agencies to differentiate compliance review work from fraud investigative work.

18. The AGIS requires agencies to 'have written procedures in place to document decision making so the transition from regulatory/compliance functions to criminal investigation is clearly identified'.[10]

19. Accordingly, Centrelink's *Fraud Investigation Manual* (the FIM) was developed to enable Centrelink to meet the requirements of the AGIS and enhance its ability to provide assurance to Government and Centrelink's policy and partner agencies, that it has the capability to undertake quality fraud investigation activities that accord with the AGIS.[11] Implementation of mandatory work processes and support tools in the FIM were designed to overcome the risk to Centrelink of inconsistent practices.

Audit objective

20. The objective of the audit was to examine the effectiveness of Centrelink's approach to investigating and responding to external fraud.[12] The ANAO's assessment was based on four key criteria. In particular, the ANAO assessed whether Centrelink:

- had established a management framework, business systems and guidelines, that support the investigation, prosecution and reporting of fraud;
- had implemented appropriate case selection strategies and controls to ensure resources are targeted to the cases of highest priority;
- complied with relevant external and internal requirements when investigating fraud and referring cases for consideration of prosecution; and
- had implemented an effective training program that supports high quality investigations and prosecution referrals.

---

[10] Attorney General's Department, *Australian Government Investigations Standards 2002*, AGD, Canberra, September 2003, Chapter 5, Introduction.

[11] Centrelink, *Fraud Investigation Manual*, Questions and Answers, Why was the FIM developed?

[12] In forming the audit objective and scope, the ANAO took into consideration advice from Centrelink that it was implementing a range of measures over the next three years consistent with the Australian Government's new whole-of-government compliance framework for social, health and welfare payments.

Audit scope and methodology

21. The scope of the audit included fraud investigations undertaken by Centrelink during 2008–09. The ANAO's methodology involved randomly selecting a sample of cases for review from Centrelink's Fraud Investigation Case Management System (FICMS). FICMS is a purpose built system for case-managing fraud investigations and prosecution referrals and based on Centrelink's advice, was determined to be the appropriate source for sampling fraud investigation cases.

22. Subsequently, Centrelink advised that owing to systems and structural limitations, FICMS contained some cases that were compliance reviews, not fraud investigations, and Centrelink has limited capacity to distinguish between them. Centrelink considered that these limitations had resulted in the inclusion of compliance review cases in the ANAO's sample.

23. While the ANAO's analysis indicated that most of the initial larger random sample[13] contained activities associated with fraud investigations, the results of the case reviews in the audit report are based on 113 cases that had satisfied Centrelink's *National Case Selection Guidelines* for investigation and possible prosecution. These cases were referred to, and investigated by, fraud investigators in Centrelink's FITs.

24. The ANAO reviewed each of the 113 cases against the Australian Government's policies and Centrelink's internal procedures. This legislative framework and internal Centrelink guidance sets out procedures designed to promote effective prosecution of fraud, including the collection of admissible evidence, while ensuring that cases of fraud are treated fairly and equitably. In examining each case, the ANAO focused on:

- critical decision records, including whether the transition from a compliance review to an investigation was identified, and whether significant decisions and changes in the direction of an investigation were identified;
- the presence and use of investigation plans, that provide assurance of an appropriate approach and oversight of fraud investigations and allow for transparency and review at each stage of the investigation,

[13] Original sample of 275 fraud investigation cases randomly selected by the ANAO from a total population of 14 499 fraud investigations activated and finalised in FICMS in 2008–09.

including proposed approaches such as: witness statements; interviews; the handling of evidence; and the use of surveillance, informants and search warrants; and

- the recording of the outcome of fraud investigations and reconciliation of systems and records.

Overall conclusion

25. The scale and complexity of Centrelink's operations are reflected in the $87 billion in social security payments it delivers annually to approximately 7 million customers, many of whom are vulnerable and heavily dependent on Centrelink payments. Within this environment, encouraging customers to comply and keeping non-compliance to a minimum, is a major and ongoing task for Centrelink. The focus of this audit is Centrelink's approach to identifying, investigating and managing potential cases of external fraud.

26. Key developments recently undertaken by Centrelink to improve its fraud control program include: implementation of an online *Fraud Investigation Manual* (the FIM) designed to support high quality fraud investigations that are conducted in accordance with the *Australian Government Investigations Standards* (the AGIS); use of an intelligence capability to detect fraud; and a restructuring of its Business Integrity Network. In 2008–09, Centrelink met its fraud investigation and prosecution targets but did not achieve the required savings outcomes through the identification of customer debts.

27. Notwithstanding the development of Centrelink's FIM, the results of the ANAO's case reviews indicate that most of these fraud investigations did not comply with the Australian Government's regulated framework for fraud investigations and Centrelink's internal policies and procedures. Typically, these results reflect Centrelink's non-compliance with the requirements of the AGIS and its internal policies and procedures at key points throughout the investigation process, contributing to: deficiencies in case selection and prioritisation practices; and shortcomings in managerial oversight of investigation planning and the necessary deliberation of critical decisions and investigation outcomes. Meeting these key requirements is part of the Government's legislated framework and Centrelink's internal procedural controls that were put in place to promote high quality investigations and prosecution referrals, including the collection of admissible evidence, while ensuring that cases of fraud are treated fairly and equitably. In particular, Centrelink's FIM was developed to provide assurance to Government and

Centrelink's policy and partner agencies, that it undertakes quality fraud investigation activities in accordance with the AGIS.

28. Centrelink refers the largest number of briefs to the Commonwealth Director of Public Prosecutions (the CDPP) of any agency and these briefs generally relate to customers who are receiving social welfare benefits and whom it is alleged, have intentionally misrepresented their circumstances to Centrelink. Although ultimately it is the responsibility of the CDPP to determine which Centrelink cases are prosecuted based on standards such as fairness, consistency and accountability, under the *Prosecution Policy of the Commonwealth,* referral of cases to the CDPP is a decision for Centrelink. Cases that are not referred to the CDPP result in administrative remedies and, generally, this is the outcome of the majority of Centrelink cases investigated. Irrespective of the manner in which cases are handled following investigation, the audit highlighted that Centrelink would benefit from placing stronger emphasis on the quality and consistency of its case management practices, and targeting customers most at risk of committing serious fraud.

29. Until recently, Centrelink advised that its approach to targeting customers most at risk of committing serious fraud has been constrained by the agreed performance measures contained in purchaser/provider funding arrangements under which it operated with the Department of Education, Employment and Workplace Relations (DEEWR) and the Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA) until 30 June 2009. These arrangements focused on the savings to be achieved, mostly through the recovery of customer debts and include quantitative targets for fraud investigations and prosecution referrals. Understandably, this approach influenced actual case prioritisation, selection and processing as it focused fraud investigations on the less complex cases (in order to achieve the targets), at the expense of progressing the more complex, serious fraud investigations.

30. Over time, Centrelink's ability to detect and investigate serious and complex fraud is being enhanced with the introduction of an intelligence capability. This initiative will better position Centrelink to focus its fraud investigation resources on the high risk areas. A key responsibility of Centrelink's Intelligence teams[14] is to support fraud investigation operations

[14] The word 'Intelligence' is capitalised in this report wherever references are made to Intelligence teams and Intelligence staff.

by identifying complex and serious fraud and prioritising cases for investigation. For cases to qualify for investigation and consideration of prosecution action, they must undergo assessment and satisfy Centrelink's *National Case Selection Guidelines* (NCSG). Investigation outcomes can range from an administrative remedy through to referral to the CDPP for consideration of prosecution.

31. While Centrelink's new approach is designed to prioritise and manage serious cases of fraud, it is being overshadowed by the automatic and generic referral of potential fraud cases and the lack of appropriate guidance and oversight of decision-making by fraud investigators throughout the investigative process. The largest proportion of Centrelink's fraud cases are automatically referred debts and these cases also make up the largest proportion of prosecution referrals. The ANAO's reviews of 113 cases identified that while half of Centrelink's fraud investigations had undergone an Intelligence Assessment, the influence of these assessments to progress serious fraud cases to prosecution was negligible. Closer monitoring of decision making by management throughout serious fraud investigations would enable Centrelink's fraud intelligence capability to be more effectively utilised.

32. Overall, compliance with the AGIS and Centrelink's policies and procedures in the FIM, including the required managerial oversight at key points throughout the investigation process, would produce a more consistent and balanced approach to case selection, investigation planning and decision making, and, therefore, improved investigation outcomes. Compliance with these key controls would enhance Centrelink's ability to provide assurance that the investigation process is effective in achieving consistently high quality fraud investigations and prosecution referrals. In conjunction with appropriate training, this approach would improve investigators' skills and encourage a more consistent approach to capturing, recording and documenting critical and other key information and decisions throughout fraud investigations and better align with the AGIS. In particular, appropriate managerial oversight throughout investigations, would provide a greater level of assurance of decision making regarding the use of coercive powers to obtain third party information about customers generally, and more specifically, when an administrative investigation transitions to a criminal investigation.

33. The business systems used by Centrelink to provide ready access to high-quality information upon which they can base their decision-making and fraud reporting also require some attention. For example, the data in

Centrelink's Fraud Investigation Case Management System (FICMS) does not reconcile with the published fraud investigation performance data extracted from its Integrated Review System (IRS). This affects both an internal understanding of the nature, number and status of compliance reviews and fraud investigations managed by Centrelink and, importantly, the reliability of its external reporting. Centrelink's Business Integrity Division also confirmed that FICMS is unreliable and is not used to measure performance against investigation targets.

34. The ANAO made four recommendations that focus on supporting Centrelink's approach to managing external fraud by: more effectively using its intelligence capability; ensuring compliance with external and internal fraud investigation requirements; providing closer oversight of decision making by fraud investigators as well as more targeted and effective training; and improving the integrity and quality of its fraud data.

Key findings

Performance targets

35. During 2008–09, Centrelink had corporate targets in place for investigations (and prosecution referrals) in order to achieve the amount of savings required under the purchaser/provider arrangements that were in place with the responsible portfolio departments. These targets were tied to the dollar savings that would be identified through each fraud investigation and recouped from customers, contributing to the overall required savings amount. Over the past few years, the total amount of Centrelink debt raised as a result of compliance activities has increased from $419 million in 2006–07 to $536 million in 2008–09. During the same period, customer debts identified through fraud investigations, primarily from compliance activity, accounted for $127 million and $113.4 million respectively.

36. In 2009–10, the achievement of Centrelink's fraud-related targets has been tied to individual performance of Centrelink fraud investigators. These measures are primarily quantitative and include: the number of investigations completed (99 per year in 2009–10); the number of prosecutions referred to the CDPP (six per year in 2009–10); and the number of prosecutions accepted by the CDPP (85 per cent in 2009–10). These targets do not distinguish between outcomes by complexity of the fraud, and are not aligned with Centrelink's serious fraud priorities.

37. Centrelink's pursuit of quantitative targets at the officer level, including the selection of less complex cases for investigation, has the potential to compromise the quality of fraud investigations. For example, Centrelink reports on the number, type and age of cases that each investigator has on hand, and these reveal that many serious fraud investigations have been ongoing for up to three years or more. During interviews, stakeholders and Centrelink staff advised that the focus on the existing targets was influencing the case selection towards less complex cases for investigation and prosecution, at the expense of the more complex, serious fraud cases. Centrelink has acknowledged these issues and has since advised that investigation targets are under review.

38. While targets are a feature of a good monitoring and reporting framework, they need to be balanced and measurable. Centrelink's fraud investigation and prosecution targets and performance measures also need to be regularly reviewed to ensure ongoing relevance against Centrelink's intended outcomes. A recent ANAO audit identified the inherent risks, in the capacity of Centrelink's compliance and investigation targets, to measure the performance of compliance review officers and investigators.[15] In response to this audit, Centrelink agreed to develop a more balanced set of measures that assess the conduct and quality of compliance reviews and investigations. This will assist in the development of a stronger focus by Centrelink on priority setting and balanced targets, relevant to combating complex and serious fraud cases.

Case prioritisation and selection

39. Centrelink has a number of detection procedures and activities to identify possible cases of fraud that require further investigation. These include: compliance reviews or 'generic referrals' arising from anomalies identified through customer payment reviews; automatic debt referrals that occur for any customer debt that exceeds a predetermined amount [$5000]; and, increasingly, the use of fraud intelligence to detect and prioritise the more serious cases of fraud for investigation. All cases of alleged fraud referred to Centrelink's fraud investigation teams have to satisfy Centrelink's NCSG for investigation and possible prosecution. The exception is serious fraud cases

[15] Australian National Audit Office, *Centrelink's Tip-off System*, Audit Report No.7, ANAO, Canberra, 2008–09, pp. 74–75.

that have been assessed by Centrelink's Intelligence staff as a high priority and must be investigated.

40. While Centrelink has policies and procedures designed to prioritise and manage serious cases of fraud, this capability is being overshadowed by the automatic and generic referral of potential fraud cases and case selection practices. The ANAO's analysis of 2007–08 fraud data[16] identified that automatically referred customer debt cases were seven times more likely to be detected, investigated and referred to the CDPP than all other cases (including public and internal tip-offs, cash economy and manual fraud case referrals from compliance and other areas within Centrelink).

41. The ANAO's 113 case reviews also revealed that inconsistent case management practices, and the limited managerial guidance and oversight of decision-making in relation to case selection and at key points in the investigative process, are compromising Centrelink's referral strategies and intelligence work. While 50 per cent of cases reviewed had undergone an intelligence assessment, the influence of this analysis to contribute to higher quality outcomes was not evident in Centrelink cases progressed to the CDPP for consideration of prosecution. For example, only five per cent of investigations with an Intelligence Assessment report resulted in a referral to the CDPP, compared to 77 per cent of debt cases and 86 per cent of all other cases investigated.

42. Once cases are referred to the CDPP for assessment, the CDPP has responsibility for determining which Centrelink cases are prosecuted, in accordance with the *Prosecution Policy of the Commonwealth*. However, the majority of Centrelink fraud investigations are not referred to the CDPP and instead result in an administrative recovery of the identified debt. For example, in 2008–09 less than 20 per cent of Centrelink's fraud investigations resulted in referral to the CDPP, while the remaining 80 per cent received an administrative remedy.

43. While referral of a matter to the CDPP is a decision for Centrelink under the *Prosecution Policy of the Commonwealth*, in matters involving alleged offences of a serious nature that are not referred for consideration of prosecution, Centrelink is required to consult with the CDPP. The ANAO's

[16] The ANAO analysed 2007–08 fraud data because a greater number of cases had been finalised in that year, compared with the number of 2008–09 cases finalised in FICMS at the point in time of the data extraction (which occurred on 9 August 2009).

case reviews identified cases with significant debts and information on file that indicated an 'intent' to defraud the Commonwealth, where Centrelink's decision had been not to refer the case to the CDPP. In these cases, there was no record of consultation occurring between Centrelink and the CDPP, at this stage in the process.

Compliance with the *Australian Government Investigations Standards* and Centrelink's internal requirements

44. All agencies subject to the *Commonwealth Fraud Control Guidelines 2002* (the Guidelines), are required to comply with the minimum standards for investigations as set out in the AGIS. Agencies must have in place 'procedures that are consistent with or exceed' the AGIS, in order to comply.[17] Each agency is also required to comply with the legislation, powers and directives under which it operates; and other legislated requirements designed to protect the rights of individuals such as the *Freedom of Information Act 1982*, the *Privacy Act 1988* and the *Public Service Act 1999*.

45. To provide assurance that its investigation and prosecution referral work is performed consistently across the Business Integrity Network and to meet the AGIS requirements, Centrelink implemented its FIM in September 2007. Centrelink advised that the FIM is its mandated policy and practices manual which all fraud investigators are expected to follow.[18]

46. Under the *Social Security (Administration) Act 1999*, Centrelink exercises coercive information-gathering powers (among other techniques) to collect internal and external evidence about customers throughout the investigative process. However, for the purpose of investigations, these coercive powers can only be used in limited circumstances to collect evidence and once fraudulent behaviour is 'suspected', the powers can no longer be used.[19]

47. Overall, most fraud investigations reviewed by the ANAO did not comply with the Australian Government's regulated framework and Centrelink's internal policies and procedures. The important issues to emerge from the results of the ANAO's case reviews were:

---

[17] Attorney General's Department, *Australian Government Investigations Standards*, AGD, Canberra, September 2003, Chapter 1, p. 4.

[18] 'The FIM [*Fraud Investigation Manual*] is Centrelink's mandated policy and practices manual. All fraud investigators are expected to follow it', Centrelink advice to the ANAO, 15 February 2010.

[19] Centrelink, *Fraud Investigation Manual,* Scope of Powers: ss.192–196, 2 June 2008.

- non-compliance with the AGIS and Centrelink's own polices and processes – increasing the risk of serious and complex fraud cases not being referred for consideration of prosecution and potentially affecting the quality of briefs of evidence referred to the CDPP;
- incomplete information recorded in Centrelink's Fraud Investigation Case Management System (FICMS) and investigation files – affecting Centrelink's ability to provide assurance that the investigative approach was appropriate, and to protect the rights of customers through legislated safeguards such as Freedom of Information; and
- the lack of documented critical decisions and evidence of managerial oversight at key control points in the investigative process including information-gathering processes – making it difficult to determine whether Centrelink used its coercive powers inappropriately to collect evidence after fraud was suspected.

48. Table S1 provides a summary of the results of the ANAO's case reviews in relation to Centrelink's compliance with external and internal investigation standards.

Table S1

Centrelink's compliance with investigation standards

External and internal requirements	Results of the ANAO's case reviews
Overall compliance with the AGIS requirements	Overall, most Centrelink cases examined did not meet the standards in the AGIS and, therefore, the Australian Government's regulatory framework for fraud investigations.
Compliance with specific standards in the AGIS and Centrelink's *Fraud Investigation Manual*	In relation to specific standards and requirements: • more than 30% of cases had no separate investigation file; • 45% of cases had no investigation plan documented on file; and – of the cases with an investigation plan, 30% were not approved and 30% were incomplete • 40% of cases had no recorded outcome.
Recording critical decisions	Both the AGIS and Centrelink's FIM require critical decisions to be comprehensive and documented on file. Centrelink staff are not consistently complying with this important standard including documenting the critical decision when a case transitions from a compliance review to an investigation, and any subsequent significant changes in the direction of an investigation, including when an investigation is terminated. The general lack of documentation and information meant that the ANAO could not always determine the basis of key decisions, including the use of Centrelink's coercive powers, and whether the powers were used lawfully.
Centrelink's *Fraud investigation Manual*	70% of cases had no recorded document (DOC.) in Centrelink's mainframe to clearly alert Centrelink staff that the case was under investigation for fraud.

Source: ANAO analysis.

Oversight of decision-making

49. Centrelink's FIM requires all critical decisions made during an investigation to be approved by a Case Manager and documented on file, to ensure investigation management and decision-making are transparent. However, the ANAO's case reviews identified that Centrelink staff are not consistently complying with this key procedural control in Centrelink's FIM. The absence of documented critical decisions during the investigative process, including when an investigation is terminated, means that Centrelink's single quality control, that is, managerial consideration and approval of decision

making at key points throughout the investigative process, is not effective.[20] General guidance from Case Managers, which is necessary to better inform the overall quality of decision-making throughout the investigation and to provide assurance to Centrelink, was also found to be lacking. Increased guidance and managerial oversight at key stages in the case management process would assist Centrelink to more effectively manage the investigative process and achieve consistent, high quality investigation outcomes, including referrals to the CDPP.[21]

50. The Guidelines encourage the 'specialised training of employees involved in fraud control activities'. For those staff directly responsible for preventing, detecting and investigating fraud, the Guidelines require minimum qualifications and competency standards to be met. Centrelink's Business Integrity Division facilitates two Certificate IV and two Diploma Government workshops in investigations each year to ensure employees obtain their mandatory qualifications within 12 months of commencing in their roles, as per the Guidelines. Centrelink provided evidence of qualifications of staff working in fraud control but was unable to confirm the exact number and stated that Intelligence staff are not required to meet the training standards.[22]

51. Administrative coercive powers are widely used (among other methods) by the Business Integrity Network. The ANAO's case reviews identified that these powers are used to collect evidence from third parties during the assessment of fraud allegations by Intelligence staff and throughout the entire fraud investigative process. Third party checks include credit companies, banks, employers, other Commonwealth agencies databases, real estate agencies and transport authorities.

---

[20] The Ernst and Young report, *Evaluation of Centrelink's Fraud Investigation Case Management System*, identified the need for strong executive leadership and careful case management to ensure fraud investigations and enforcement policy are justified and equitable. The report found, among other issues, that the lack of oversight by executive management was a contributing factor to the problems identified in Centrelink's case management of fraud investigations (Final Report, 2006, p.7 and p.18).

[21] For example, the results of the ANAO's case reviews identified cases with debts of $50 000 or more that were not referred to the CDPP. The CDPP advised that it considers the debt amount of $50 000 to be sufficiently serious as to warrant a hearing in a higher court with more severe penalties (CDPP advice to the ANAO, 11 November 2009).

[22] The Guidelines require all staff working in fraud related areas such as prevention, detection and investigation activities to meet specific competency standards. Equally, the AGIS identifies intelligence projects as fraud investigations and, therefore, the mandatory training requirements of the Guidelines apply to Centrelink intelligence staff.

52. However, the case reviews revealed that there was insufficient evidence on file to support decision making in relation to third party checks generally, and more specifically, when a written Legal Notice was issued. In all instances where a Critical Decision Record (CDR) was required to approve the decision to send written Legal Notices to third parties, there was no evidence documented on file or electronically. During 2008–09, CDRs were the single (mandated) quality control point in the investigative process that had been implemented by Centrelink. Notwithstanding, many cases had: no documented CDR on file (as required by the AGIS); where a critical decision was recorded, in many instances it was not approved or contained insufficient information to enable an informed decision; and CDR templates were not filled out correctly.

53. These results highlight the need for Centrelink to look beyond the minimum training requirements of the Guidelines, to develop a more specialised training program that better supports staff working in fraud control areas and to meet its particular business risks and related skill requirements. A more planned and strategic approach to training for fraud control staff should be based on risks identified in quality assurance and other activities such as feedback from the Australian Federal Police (the AFP) and the CDPP case-related correspondence. During audit fieldwork, Centrelink developed a draft Quality Assurance Program for fraud investigations. Implementation of this program would better enable Centrelink to identify and target the training needs of fraud control staff through issues highlighted in the case reviews and through other assurance activities.

The level of system support and the quality and integrity of fraud data

54. The accuracy of an agency's information provides the basis for monitoring the effectiveness of its fraud control activities and for internal and external reporting purposes. The methods used by Centrelink to monitor, manage and report information are unclear. For example, Centrelink's FICMS was purpose-built for recording and case-managing fraud investigations. However, Centrelink advised that FICMS has limited functionality, the data is not reliable and the system is not used to monitor and report on the performance of its fraud investigation program, except for prosecution-related activity. Instead, Centrelink uses the system that manages its compliance intervention activity, the Integrated Review System (IRS), to report on its fraud investigation performance. There are, however, discrepancies between the data

held in each system. These inconsistencies are reflected in the 26 084 fraud investigations reported in Centrelink's *Annual Report 2008–09* compared with the 39 106 fraud investigations recorded in FICMS for the same period. Of the 26 084 cases reported, 60 per cent were not recorded in Centrelink's system dedicated to case-managing fraud investigations (FICMS).[23] At a minimum, the performance information published by Centrelink needs to be reconcilable in both systems to enable Centrelink to be confident that the information it publicly reports is reliable in terms of: the number of actual fraud investigations; the number of cases referred to the CDPP; and the number of cases prosecuted.

55. An independent evaluation of FICMS commissioned by Centrelink in 2006 also found that the system's operational ability was unable to deliver basic investigation and prosecution functions and does not meet the standards in the AGIS of a case management system.[24]

Summary of agencies' responses

56. The following comments constitute each agency's summary response to the audit. The full responses are at Appendix 1.

Centrelink

57. Centrelink agrees with the recommendations of the audit of its Fraud Investigation Program. These recommendations will assist Centrelink to make further improvements to its framework of compliance strategies and activities to prevent, detect and deter non compliance and fraud.

58. Centrelink is pleased that the ANAO has acknowledged the work already undertaken to address some of the issues raised in the report. These actions will continue in line with the recommendations. Centrelink is committed to delivering cost effective and well managed processes that support good outcomes for customers and ensure the integrity of government outlays.

---

[23] Centrelink has not been able to reconcile this difference.

[24] Ernst and Young, *Evaluation of Centrelink's Fraud Investigation Case Management System*, Final Report, 2006, p.15. This report identified inefficiencies in Centrelink's current systems in relation to fraud investigations and prosecutions referrals, particularly regarding interconnectivity, case management functionality and search capability.

Australian Federal Police

59. I would like to advise you that the Australian Federal Police has studied the proposed findings as referred under Section 19 and has no additional comments to add to them.

Commonwealth Director of Public Prosecutions

60. The Commonwealth Director of Public Prosecutions provided specific comments of an editorial nature.

Recommendations

Recommendation No. 1

Para 3.55

To facilitate the more effective use of its fraud intelligence capability, the ANAO recommends that Centrelink: review its fraud prioritisation and case selection policies; internal targets; and performance indicators for fraud management; so as to better align these polices and measures with its fraud control strategies.

Centrelink response: *Agreed*.

Recommendation No. 2

Para 4.29

The ANAO recommends that Centrelink reviews the support provided to fraud control staff, paying particular attention to:

- the content of its *Fraud Investigation Manual* to ensure investigation guidelines, procedural controls, processes and practices are clearly articulated and consistent with the *Australian Government Investigations Standards* and Social Security legislation;
- managerial oversight of decision making and documenting of critical decisions throughout the investigative process, including when an administrative investigation transitions to a criminal investigation; and
- the efficiency and useability of Centrelink's fraud-related decision support and reporting systems.

Centrelink response: *Agreed*.

Recommendation No. 3

Para 4.40

To improve compliance with external and internal fraud investigation requirements and the quality of its decision-making, the ANAO recommends that Centrelink:

- increase the level of guidance and oversight provided to support decision-making by fraud investigators throughout the investigative process, from the point of case selection through to finalisation of the fraud investigation; and
- develop a rolling program of specialised training for its fraud control staff that includes regular refresher courses on the policies and procedures in its *Fraud Investigation Manual.*

Centrelink response: *Agreed*.

Recommendation No. 4

Para 6.46

To improve the quality and reliability of its fraud management-related systems, the ANAO recommends that Centrelink review its standards and procedural controls for the accurate recording, reporting and evaluation of fraud data, to enable:

- investigation timeframes to be monitored, particularly in regard to serious fraud cases; and
- fraud to be more accurately quantified and the cost-effectiveness of Centrelink's fraud control strategies to be assessed.

Centrelink response: *Agreed*.

Audit Findings and Conclusions

1. Introduction

This chapter provides an overview of Centrelink's environment and the Australian Government's framework for minimising fraud risks. The chapter also outlines Centrelink's approach to fraud control, and the objective of the audit.

Background

1.1 The Australian Government is committed to protecting its revenue, expenditure and property from fraudulent activity by taking a systemic approach to the management of fraud across the Australian Public Service (APS). This commitment is articulated in the provisions of the *Financial Management and Accountability Regulations 1997,* of the *Financial Management and Accountability Act 1997* (the FMA Act). Under the FMA Act, the requirements for agencies are outlined in the *Commonwealth Fraud Control Guidelines 2002* (the Guidelines).

Centrelink

1.2 Centrelink is a statutory agency within the Department of Human Services (DHS) portfolio. It is the Australian Government's principal service delivery agency for a range of social security payments and benefits to eligible customers on behalf of policy departments. Centrelink employs almost 28 000 staff to deliver its services through a dispersed network of over 1000 service delivery points.[25] In 2008–09, Centrelink delivered social welfare payments totalling $87 billion to 7 million customers,[26] many of whom are the most vulnerable in our society and heavily dependent on Centrelink payments.

Integrity of outlays

1.3 In delivering welfare payments and services, Centrelink is responsible for the integrity of Government outlays including the provision of assurance that customer payments are correct and fraud is minimised. In managing the integrity of social security outlays, Centrelink identifies and reports against Centrelink administrative error and payment accuracy.

[25] *Centrelink Annual Report 2008–09*, p. 11.

[26] ibid., p. 4 & p. 11.

1.4 Payment accuracy recognises the obligation of customers to advise of changes in their circumstances that may affect their payment entitlements. While payment error can be attributed to an unintentional omission by the recipient customer, welfare fraud is generally characterised by deliberate omission or provision of incorrect information in order to secure payments or payment amounts for which the recipient is not entitled.

1.5 Inaccurate provision of information by customers can include unintentional errors or omissions, and intentional errors or omissions. As advised in the Guidelines, fraud against the Commonwealth is defined as 'dishonestly obtaining a benefit by deception or other means'. Benefit fraud is generally characterised by deliberate provision of incorrect information (or omission of information) in order to secure payments or payment amounts for which the recipient (customer) is not entitled. The important factor in characterising fraud is the level of 'intent' reflected in the customer's behavior.

Bilateral Management Arrangements

1.6 Until 1 July 2009, Centrelink's revenue was primarily derived from its bilateral arrangements with its policy departments known as Business Partnership Arrangements (BPAs) or similar. These arrangements set out Centrelink's responsibilities, the expectations of the policy departments including Key Performance Indicators (KPIs), and the basis for the financial arrangements between the parties. The arrangements included business assurance relating to fraud control and the investigation of matters of joint interest to both agencies, consistent sharing of information, and effective use of cross-agency resources and taskforces. A payment correctness target was set by the policy agencies at 95 per cent to ensure the integrity of social security outlays. In 2008–09, Centrelink reported a payment correctness rate of almost 97 per cent.

1.7 Over the past few years, the total amount of customer debt identified by Centrelink as a result of its fraud control activities, has increased from $419 million in 2006–07 to $536 million in 2008–09.

1.8 As part of the 2008–09 Commonwealth Budget the Government also announced that, from 1 July 2009, Centrelink would receive all of its departmental funding directly from the Budget. While policy agencies, such as DEEWR and FaHCSIA, remain accountable for the oversight of social security outcomes, Centrelink's funding to deliver income support and benefit payments, is now directly appropriated. Subsequently, separate new arrangements between Centrelink, the DHS and DEEWR and FaHCSIA came

into effect on 24 November 2009. The arrangements define the roles of the agencies in meeting their respective accountabilities (see Appendix 2).

1.9 The DHS is responsible for the Australian Government's new, strategic whole-of-government approach to managing social, health and welfare fraud and non-compliance. A key focus of the approach is the establishment of an appropriate balance between fraud prevention and detection strategies, particularly in regard to prevention at the service delivery end, through increased payment accuracy and earlier detection of debts. The new arrangements with DEEWR and FaHCSIA refer to the DHS Annual Compliance Plan, which is to govern the whole-of-government strategic fraud and non-compliance activities.[27]

Fraud control in Centrelink

Business Integrity Division

1.10 Centrelink's Business Integrity Division, within its National Support Office (the NSO), is responsible for ensuring the integrity of Government outlays and services by minimising fraud and ensuring customer payments are correct. This Division manages Centrelink's Fraud Program and operational framework including: dedicated Fraud and Intelligence teams; policies, procedures and processes; systems, performance monitoring and reporting.

Compliance and fraud activities

1.11 Centrelink's *Fraud Control Plan 2008–10* outlines its program of compliance strategies and activities to prevent, detect and deter payment inaccuracies and fraud. The framework includes:

- prevention—systems and procedures designed to minimise incorrect payment and fraud from occurring, rather than detecting them later;
- detection—systems and procedures designed to discover incorrect payment and fraud when it occurs; and
- deterrence—systems and procedures designed to deal with incorrect payment and respond to potential or actual fraud when it is uncovered.

[27] The Australian Government's new whole-of-government approach, outlined in the Department of Human Services: *2009–10 Annual Compliance Plan and Performance Report*, is Cabinet-in-Confidence.

1.12 Centrelink uses an enforcement pyramid approach to define and understand the factors that influence the compliance behaviour of its customers (see Chapter 2 for more detailed information). The enforcement pyramid model takes a graduated response to customer behaviour, recognising that most customers are willing or trying to comply (see Figure 2.1 in Chapter 2). Centrelink advised that it targets its fraud programs to the top of the pyramid, where customers are considered to be 'unwilling' to comply and this component is considered to constitute payment and serious fraud.

Fraud investigations

1.13 Under the Regulations of the FMA Act, Centrelink is authorised to investigate potential cases of fraud and prepare briefs of evidence for consideration of prosecution action by the Commonwealth Director of Public Prosecutions (the CDPP).[28] In its 2008–09 Annual Report, Centrelink reported 26 084 fraud investigations (compared to 35 885 in 2007–08) which identified $113.4 million in customer debts (compared to $140.2 million in 2007–08). For details relating to Centrelink's fraud investigations and prosecutions in 2008–09, see Table 1.1.

Table 1.1

Fraud investigations and prosecutions activity reported by Centrelink in 2008–09

Investigations	Referred to the CDPP	Prosecuted	Acquitted	Convicted	Offence proven, no conviction recorded
26 084	5082	3388	34	2973	381

Source: *Centrelink Annual Report 2008–09*, pp. 38-39.

1.14 Of the 26 084 fraud-related investigations in 2008–09, 5082 referrals were made to the CDPP for consideration of prosecution action in relation to fraud, resulting in 2973 convictions (about 11 per cent of total investigations reported).

[28] Attorney General's Department, *Commonwealth Fraud Control Guidelines*, issued by the Minister for Justice and Customs as Fraud Control Guidelines under Regulation 19 of the *Financial Management and Accountability Regulations 1997*, AGD, Canberra, May 2002.

Australian Government regulatory framework

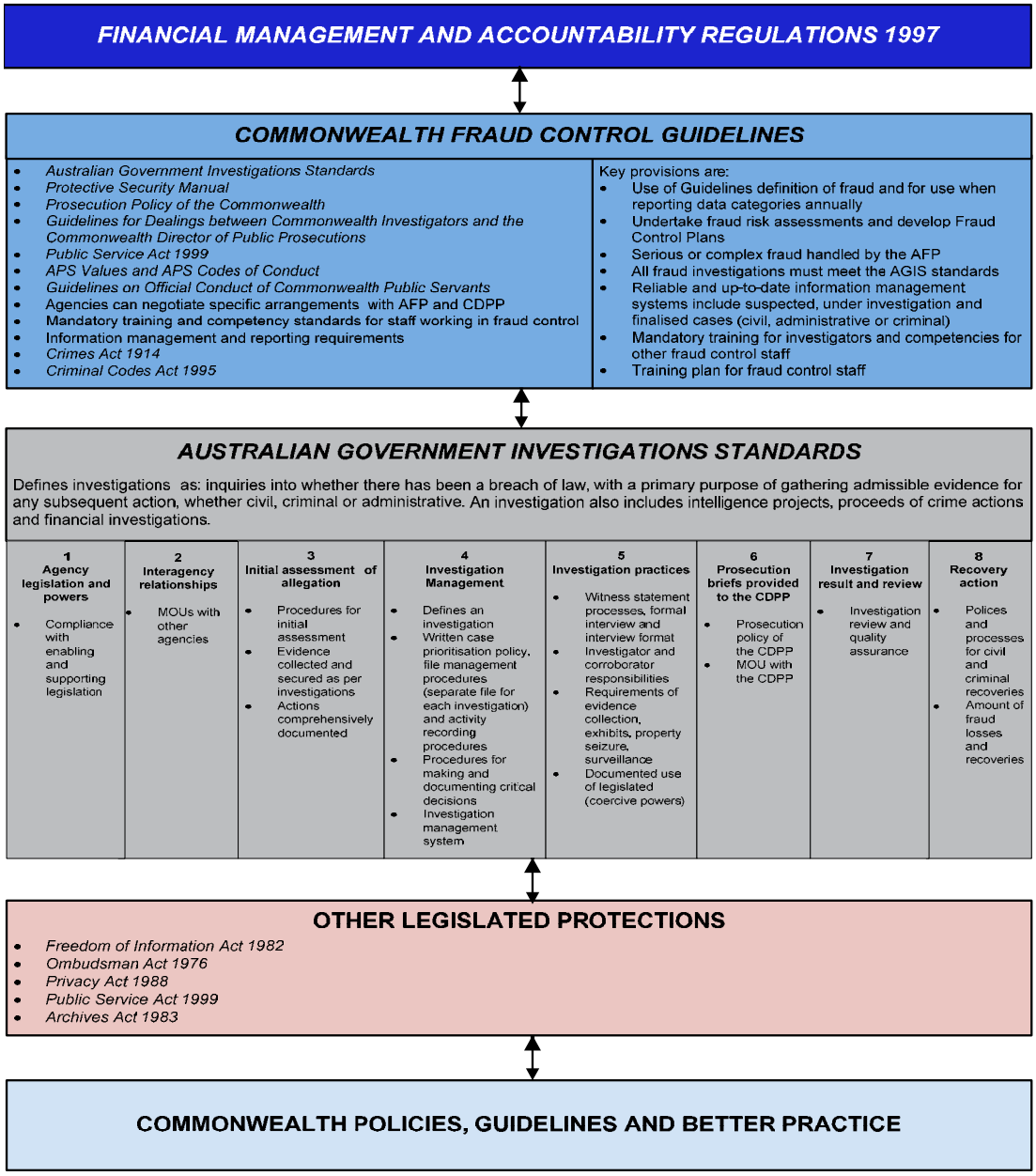
1.15 In responding to fraud, Centrelink is governed by the Australian Government's regulatory framework for APS agencies managing fraud including: the Guidelines; the *Australian Government Investigations Standards* (the AGIS), the legislation, powers and Directives under which it operates; and other legislated requirements designed to protect the rights of individuals such as the *Freedom of Information Act 1982*, the *Privacy Act 1988* and the *Public Service Act 1988*.

1.16 Figure 1.1 provides an overview of the Australian Government's regulatory framework for APS agencies managing fraud. This legislated framework assists APS agencies to effectively prosecute fraud while treating fraud cases equitably.[29]

[29] Australian National Audit Office, *Better Practice Guide–Fraud Control in Australian Government Agencies,* ANAO, Canberra, August 2004, p. 12.

Figure 1.1

The Australian Government's regulatory framework for managing fraud



Source: Attorney General's Department, *Commonwealth Fraud Control Guidelines 2002* and the *Australian Government Investigations Standards 2003,* AGD, Canberra.

Australian Government Investigations Standards

1.17 In identifying the standards for investigations, the AGIS uses the Heads of Commonwealth Operational Law Enforcement Agencies (HOCOLEA)[30] agreed principle to differentiate between compliance work and fraud investigations. The standards in the AGIS are identified as the authority to be applied to all investigations other than audit and compliance work.

1.18 The AGIS defines an investigation as:

> ...inquiries into whether there has been a breach of...law, with the primary purpose of gathering admissible evidence for any subsequent action, whether civil, criminal or administrative. An investigation also includes intelligence projects, proceeds of crime action and financial investigations.[31]

1.19 Therefore, according to the AGIS, the outcome of an investigation does not distinguish between administrative, criminal or civil action and is not a factor in the quality of the investigation. Rather it is the standards applied during an investigation and the capacity of the investigative process to withstand administrative, operational and judicial review.

1.20 Agencies are required to comply with the AGIS to achieve a uniformly high standard of investigation by:

- having up-to-date policies and procedures relevant to their functions and programs and an investigation management system, and file management and activity recording procedures in place;
- complying with the AGIS definition of an investigation and the related primary purpose for gathering admissible evidence for subsequent action;
- documenting their policies and procedures for handling all aspects of the investigation process consistent with AGIS, from initial consideration of an allegation through to successful prosecution of fraudulent crime and recovery of criminal proceeds; and
- clearly identifying the different investigation methodologies for administrative and criminal investigations and the decision-making in relation to the transition from regulatory/compliance functions to criminal investigation.

---

[30] Centrelink is not a HOCOLEA agency; however, HOCOLEA provides clarification to assist agencies to differentiate compliance review work from fraud investigative work.

[31] Attorney General's Department, *Australian Government Investigations Standards*, AGD, Canberra, September 2003, Chapter 5, paragraph 4.

1.21 Accordingly, Centrelink's *Fraud Investigation Manual* (the FIM) was developed to enable Centrelink to meet the AGIS requirements and enhance its ability to provide assurance to Government and Centrelink's policy and partner agencies, that it has the capability to undertake quality fraud investigation activities that accord with the AGIS.[32] Implementation of mandatory work processes and support tools in the FIM were designed to overcome the risk to Centrelink of inconsistent practices.

Social Security Law

1.22 Under Social Security Law, the onus is on the customer to report information to Centrelink about changes in their circumstances that affect their entitlement. Centrelink assists customers to understand and meet their obligations by providing information and other preventative measures, particularly to help those customers who are willing to comply.

1.23 The Social Security coercive information-gathering powers are used by Centrelink (among other techniques) to collect internal and external evidence about a customer's circumstances. These coercive powers are determined by the provisions of the *Social Security (Administration) Act 1999* and are primarily used to collect information to establish an individual's eligibility for entitlement.[33] For the purpose of investigations, these administrative powers can only be used in limited circumstances to collect evidence. Once the investigator 'suspects' fraudulent behaviour, the powers can no longer be used to collect evidence for criminal purposes.[34]

1.24 The AGIS is consistent with this approach, as once criminal behaviour is suspected, the standards require an investigator to use criminal investigation procedures and techniques to obtain further evidence such as witness statements, surveillance, search warrants and formal interviews.[35] Agencies are required to have written procedures in place to document decision-making, so that when an investigation transitions from administrative to criminal, it is clearly articulated.

---

[32] Centrelink, *Fraud Investigation Manual*, Questions and Answers, Why was the FIM developed?

[33] *Social Security (Administration) Act 1999*, ss.192–195.

[34] Centrelink, *Fraud Investigation Manual*, Scope of Powers: Section 192-196, 2 June 2008.

[35] Attorney General's Department, *Australian Government Investigations Standards*, AGD, Canberra, September 2003, Chapters 4 & 5.

Fraud investigation operational framework

1.25 Centrelink's operational framework for managing investigations comprises dedicated fraud investigation and Intelligence teams, legislation, systems, policies, procedures and processes, and targets and performance reporting. Prior to investigation and prosecution consideration, all cases referred to the Business Integrity Network have to satisfy Centrelink's *National Case Selection Guidelines* (NCSG). Table 1.2 provides an overview of the key elements of Centrelink's operational framework for managing fraud against Social Security Programs, which includes external and internal requirements.

Table 1.2

Centrelink's operational framework

Key elements of Centrelink's operational framework	
External requirements:	
Financial Management and Accountability Regulations 1997 (the FMAR)	• Fraud investigations have to be conducted in accordance with the *Australian Government Investigations Standards* (the AGIS) and meet other legislated requirements and Commonwealth polices and guidelines. • Agencies are required to have information systems in place to manage information gathered about fraud against the agency, that are reliable and up-to-date.
Mandatory training and competencies	• Under the FMAR, the *Commonwealth Fraud Control Guidelines* require mandatory training requirements for fraud investigators and these responsibilities extend to meeting the Guidelines competency requirements and *Certificate IV in Government (Investigations)* qualifications for investigators.
Australian Government Investigations Standards (the AGIS)	• The AGIS is the authority to be applied to all investigations and agencies are required to document their policies and procedures for handling all aspects of the investigation process consistent with the AGIS.
Social Security (Administration) Act 1999 - Part V powers	• The use of the powers in Part V of the Social Security (Administration) Act are limited to ensure that customers are or have been paid at the correct rate commensurate with their circumstances. It is also used for debt-related matters. It is not for criminal prosecution.[36] • The Act does not contain criminal powers to obtain evidence. Warrants, surveillance and formal interview techniques are some of the methods used to obtain evidence once fraudulent behaviour is suspected.

[36] Centrelink, *Fraud Investigation Manual*, Third Party Information Gathering Policy, Business case, 16 October 2007.

Key elements of Centrelink's operational framework	
Internal policies, procedures and practices:	
Fraud Investigation Manual (the FIM)	• The FIM is Centrelink's documented online reference tool for all fraud policies and procedures in relation to the management of a fraud investigation and was implemented to ensure the investigative process complies with the AGIS. • The FIM includes legislated requirements, agency Directives, Case Prioritisation and *National Case Selection Guidelines*, investigations management, methodologies and procedures, critical decision guidelines and guidelines for briefs of evidence. Investigation outcomes can range from an administrative remedy through to referral to the CDPP for prosecution consideration.
Fraud Investigation Case Management System (FICMS)	• FICMS is Centrelink's system for case-managing fraud investigations and prosecution referrals. Cases flow or are transferred into FICMS from the Debt Management System (DMS) and the Integrated Review System (IRS) including manual referrals.
Intelligence capability	• A key responsibility of Centrelink's Intelligence teams is to support fraud investigation operations by identifying complex and serious fraud cases and prioritising cases for investigation. • Where a reasonable suspicion of fraud is identified, an Intelligence Assessment report is produced and the seriousness of the case assessed and a 'seriousness' complexity rating assigned. Intelligence Assessments include the complexity rating and an investigation priority rating of low, medium or high.
Source of case referrals for investigation:	
Compliance review outcomes (administrative reviews of payments to customers) make up 70–80 per cent of referrals for investigation and possible prosecution action. Case referrals include: • generic referrals (arising from anomalies identified in compliance reviews) including manually referred cases; • automatic debt referrals of a predetermined amount [of more than $5000]; and • serious fraud referrals generated by Centrelink's intelligence work.	
Formal arrangements with other Commonwealth agencies:	
Australian Federal Police (the AFP)	• Under a Service Agreement, AFP officers are out-posted in Centrelink's Business Integrity Network and have an important role in improving the capabilities and investigative practices of staff working in fraud control, particularly in regard to the provision of forensic and other technical expertise and support for criminal investigations.
Commonwealth Director of Public Prosecutions (the CDPP)	• The Memorandum of Understanding (MOU) with the CDPP is high level and sets out the working relationship between Centrelink and the CDPP for the investigation and prosecution of alleged criminal offences including offences regarding Social Security Programs.

Source: ANAO analysis.

Audit objective, scope and methodology

1.26 The objective of the audit was to examine the effectiveness of Centrelink's approach to investigating and responding to external fraud.[37]

1.27 The ANAO's assessment was based on four key criteria. In particular, the ANAO assessed whether Centrelink:

- had established a management framework, business systems and guidelines, that support the investigation, prosecution and reporting of fraud;
- had implemented appropriate case selection strategies and controls to ensure resources are targeted to the cases of highest priority;
- complied with relevant external and internal requirements when investigating fraud and referring cases for consideration of prosecution; and
- had implemented an effective training program that supports high-quality investigations and prosecution referrals.

Audit scope

1.28 The scope of the audit included fraud investigations undertaken by Centrelink during 2008–09. While the audit did not encompass an examination of Centrelink's compliance activity, the ANAO did review the assignment of suspected fraud cases identified during compliance reviews that had satisfied Centrelink's *National Case Selection Guidelines* for investigation and possible prosecution.

1.29 An important consideration for Centrelink is to be able to clearly identify when it is undertaking a compliance review and when it is undertaking a fraud investigation. For instance, the use of legislated powers, such as coercion, should only be used by Centrelink for administrative determinations and not for criminal investigations (see Table 1.3).

[37] In forming the audit objective and scope, the ANAO took into consideration advice from Centrelink that it was implementing a range of measures over the next three years consistent with the Australian Government's new whole-of-government compliance framework for social, health and welfare payments.

Table 1.3

Centrelink's use of its coercive powers and the applicability of the AGIS

	Coercive Powers	AGIS	Comment
Compliance Reviews	✓	×	When undertaking a compliance review, it is appropriate for Centrelink staff to use coercive powers under the Social Security Law to gather information and/or documents to ensure that customers are being, or have been paid the correct rate of entitlement.
Fraud Investigations	×	✓	The investigation of fraud involves complex interventions and the adherence of Centrelink staff to relevant legislation and standards including the *Commonwealth Fraud Control Guidelines*, and the *Australian Government Investigations Standards* (AGIS).

Source: ANAO analysis of Social Security Law and the *Australian Government Investigations Standards*.

Audit methodology

1.30 The ANAO initially selected a random sample of 275 cases for review from Centrelink's Fraud Investigation Case Management System (FICMS). FICMS is a purpose built system for case-managing fraud investigations and prosecution referrals and Centrelink agreed that it was the appropriate system from which to sample fraud investigation cases. Cases flow, or are transferred, into FICMS from Centrelink's Debt Management System (DMS) and its Integrated Review System (IRS), including manually referred cases.

1.31 Following the ANAO's initial analysis, Centrelink considered that 162 cases within the ANAO's random sample of 275 cases were not, in fact, fraud investigations because the outcome of the investigation was an administrative remedy.

The ANAO's final sample of fraud investigation cases

1.32 While the ANAO's analysis identified that most of the initial 275 cases contained activities associated with fraud investigations, the results of the case reviews are based on the 113 cases that the ANAO determined had:

- met Centrelink's *National Case Selection Guidelines* for investigation and prosecution consideration;
- been referred to a fraud investigator in a Fraud Investigation Team (FIT); and

- been activated as a fraud investigation in Centrelink's dedicated Fraud Investigation Case Management System (FICMS).

1.33 Using this methodology did not substantially change the results of the ANAO's case reviews and Centrelink's overall compliance rate. Unless otherwise stated in the report, the ANAO's findings and conclusions are based on the sample of 113 fraud investigations as explained in the following table.

Table 1.4

Final ANAO sample of Centrelink fraud investigation cases

Source	Final Sample	ANAO Comment
Debt Management System (DMS)	15	Of the 15 DMS cases, Centrelink confirmed that: all 15 had progressed to investigation; of these, 5 were subsequently forwarded to the Commonwealth Director of Public Prosecutions for potential prosecution; and 3 of these cases were convicted.
Integrated Review System (IRS)	98	Based on the ANAO analysis of Customer Record Numbers (CRNs): 92 of the 98 IRS cases were reported as fraud investigations in Centrelink's 2008–09 Annual report.
Total	113	All 113 cases met Centrelink's *National Case Selection Guidelines* and were referred for investigation and prosecution consideration to the Fraud Investigation Teams. The audit results are indicative of the total population of Centrelink's 2008–09 fraud investigation data.

Source: ANAO.

1.34 The ANAO consulted with key stakeholders including DEEWR and FaHCSIA, the Commonwealth Ombudsman's Office, the Department of Finance and Deregulation, the National Welfare Rights Network, the Attorney General's Department, the DHS and the Office of the Privacy Commissioner.

1.35 The ANAO developed a structured approach to interviewing key Centrelink Business Integrity personnel and other stakeholders including: Privacy Officers, Freedom of Information Officers; Social Workers; the Australian Federal Police (the AFP) and out-posted AFP Officers in Centrelink; and senior CDPP staff. The interviews consisted of set questions developed around key themes and were conducted in Canberra and seven of the 11 Business Integrity Network areas.

Previous audits

1.36 There are many recent and earlier ANAO audit reports that have content relevant to this audit. The most recent reports conducted over the past

two years include: *Fraud Control in Australian Government Agencies*, ANAO Audit Report No.42, 2009–10; *The Australian Taxation Office's Management of Serious Non-Compliance*, ANAO Audit Report No.34, 2008–09; and *Centrelink's Tip-off System*, ANAO Audit Report No.7, 2008–09. For a complete list of previous ANAO audit reports with relevant content to this report, see Appendix 3.

Structure of the report

1.37 The report structure consists of:

- Fraud Management Framework (Chapter 2);
- Referrals Leading to Case Selection (Chapter 3);
- Investigating and Responding to External Fraud (Chapter 4);
- Referral of Cases to the Commonwealth Director of Public Prosecutions (Chapter 5); and
- Performance Information and Reporting (Chapter 6).

2. Fraud Management Framework

This chapter examines Centrelink's fraud management framework including its Fraud Control Plan, fraud risk assessment and compliance framework.

Background

2.1 Governance is a set of responsibilities, practices, policies and procedures exercised by an agency's executive to provide strategic direction, ensure the agency's objectives are achieved, and risks are managed and resources used responsibly and with accountability.[38]

2.2 Under the Regulation 19 of the *Financial Management and Accountability Regulations 1997* of the *Financial Management and Accountability Act 1997* (the FMA Act), Chief Executive Officers (CEOs) are responsible for ensuring their agencies have effective fraud control arrangements in place.[39]

2.3 The ANAO examined Centrelink's:

- governance framework as it relates to fraud control; and
- compliance framework as it relates to fraud control.

Governance framework

2.4 Centrelink has a documented governance framework, with defined areas of accountabilities and responsibilities, and processes to facilitate communication and reporting between the CEO and the Centrelink Executive, the Minister, and the Centrelink Strategic Committees.[40] Centrelink's Annual Report states that the Audit Committee provides independent assurance and assistance to the CEO on Centrelink's risks, controls and compliance framework and on its external accountability responsibilities.[41]

---

[38] Australian National Audit Office, *Better Practice Guide–Implementation of Programme and Policy Initiatives,* ANAO, Canberra, October 2006, p. 13.

[39] Australian National Audit Office, *Better Practice Guide–Fraud Control in Australian Government Agencies*, ANAO, Canberra, 2004, p. 17.

[40] *Centrelink Annual Report 2007–08*, p. 2.

[41] ibid., p. 12.

Risk management framework

2.5 Risk management is an inherent part of an agency's controls framework to manage business risks, as it involves identifying and analysing risks and consistently working towards mitigating these in a timely manner.[42] The *Commonwealth Fraud Control Guidelines 2002* (the Guidelines) state that fraud control risk management should be integrated into the agency's practices and business plans, to ensure it becomes the business of everyone in the organisation.

2.6 Centrelink has a Risk Management Plan for the agency that was developed following a risk management workshop with Centrelink's Executive in July 2008. Each Division prepared a Business Plan for 2008–09 which identified risks to the achievement of key priorities and deliverables. Divisional risk plans were then collated in a risk register and risks identified as high or very high were incorporated into Centrelink's overall Risk Management Plan.

Centrelink's business planning and reporting

2.7 Centrelink has a high-level Business Integrity Strategic Plan for 2007–10. The purpose of this plan is to progress business integrity within Centrelink through key strategic activities required to improve its business integrity framework.[43] Centrelink's Strategic Directions for 2008–09 are the foundations for the organisational, group, division, branch and local area business planning.[44] The Strategic Directions are outlined in Appendix 4.

Business Integrity Division

2.8 Centrelink's Business Integrity Division located in Centrelink's National Service Office (NSO) is responsible for ensuring the integrity of Centrelink outlays and services by minimising fraud and ensuring customer payments are correct. The Business Integrity Division manages Centrelink's business integrity activities including policies, programs and activities relating to prevention and deterrence, detection and its response to fraud. Under

---

[42] *Australian/New Zealand Standards on Risk Management–AS/NZS ISO 31000:2009 Risk Management*.

[43] Centrelink, *Business Integrity Strategic Plan 2007–2010*, Final, June 2007.

[44] *Centrelink Annual Report, 2008–09*, p. 17.

Centrelink's Strategic Planning and Reporting Framework it is a requirement for the Business Integrity Division to annually produce business plans.[45]

2.9 The Business Integrity Division identifies a risk in Centrelink's Risk Management Plan[46] which relates to 'staff failing to follow documented policy and procedures'. This risk relates to the fraud investigation function specifically, and related policies and procedures. The risk is linked to the strategic theme of 'Service delivery/Business Continuity' and the overarching risk of 'Centrelink Service Delivery System does not contribute to the achievement of Government objectives'.

2.10 The strategies to treat this risk include documenting the end-to-end functions for all Business Integrity portfolio functions, and implementing a decision support tool and a three-tiered Quality Assurance process. Not all of these treatments have been implemented.[47] For example, in June 2009 when this Plan was most recently revised, the three-tiered Quality Assurance Framework was not documented, although a draft program was developed during the audit, and was to be implemented on 30 November 2009. Related issues are examined in Chapters 4 and 6.

Fraud Control Plan 2008–10

2.11 Centrelink has a Fraud Control Plan in place for 2008–10 which sets out its commitment to fraud control and commits staff to the highest ethical standards of values and behaviours. The Fraud Control Plan refers to the collective responsibility for identifying and addressing fraud and business integrity risks.[48]

2.12 Centrelink's Fraud Control Plan is based on: prevention; detection and deterrence (includes prosecutions and other penalties and recovering proceeds of crime); awareness training; specialised training to staff working in fraud

---

[45] On 16 October 2009, Centrelink advised the ANAO that it could not provide a business plan for the Business Integrity Division and Network for 2008–09 but it could provide the history of the Division's business planning arrangements. On 16 February 2010, a copy of a 2008–09 business plan was provided to the ANAO, the status of which is unknown.

[46] Centrelink was unable to provide a risk management plan for the period of the ANAO's case reviews (2008–09). During the ANAO's audit, Centrelink's Business Integrity Division advised that it was developing a risk management plan, which was awaiting Executive sign-off.

[47] The ANAO notes that during the audit fieldwork a Quality Assurance Program was being developed by Centrelink. Once implemented, this will represent a positive step in Centrelink's management and oversight of fraud investigations and prosecutions.

[48] Centrelink, *Fraud Control Plan 2008–2010*, p. i.

control; and reporting and accountability. Whilst some of the information is out-of-date, the Fraud Control Plan provides a comprehensive overview of Centrelink's commitment to fraud control and business integrity for 2008–10 and outlines the responsibilities of employees in upholding Centrelink's ethical behaviours, and for reporting fraud. Centrelink's Fraud Control Plan is underpinned by biennial risk assessments.

Biennial Fraud Risk Assessments

2.13 The Guidelines state that fraud control risk management should be integrated into the agency's practices and business plans from the ground up, to ensure that it becomes the business of everyone at all levels within the organisation. Centrelink has identified four key areas of fraud risk which are incorporated into three fraud risk assessments that underpin the Fraud Control Plan, in relation to internal and external fraud. These include administrative and staff fraud, information fraud and payment fraud. As the focus of this audit is on external fraud, the ANAO reviewed the Payment Accuracy Fraud Risk Assessment Plans (payment risk assessments) for welfare payments.

Payment fraud

2.14 Centrelink provided payment risk assessments for the key payment types that contribute to its biennial risk assessment process. Each plan is updated as risks change, which is consistent with the Guidelines. The specific risks identified are comprehensive and generally identify the level of risk by rating, and the existing controls and treatments to detect and deter fraud.

2.15 The payment major risks identified are weighted in terms of the effect on government outlays, to differentiate between the different types of risk as is required by the Guidelines. However, for sub-risks, from which policies or initiatives are developed, there are no risk weightings. For example, some risks require different risk mitigation strategies depending on the cause of the overpayment, such as a customer's misunderstanding of their reporting obligations, ranking equally with the provision of false information by a customer.

2.16 Centrelink would benefit from expanding its analysis of fraud data, from particular types of special fraud operations and Budget measures, to identify a broader range of risks. Better use could also be made of the data analysis undertaken by Centrelink's Intelligence teams. This should better position Centrelink to develop appropriate measures to treat the risks, that

translate into effective fraud mitigation strategies 'on the ground', in terms of service delivery.

Compliance framework

2.17 Centrelink uses elements of the Heads of Commonwealth Operational Law Enforcement Agencies (HOCOLEA) *Overarching Principles for Selecting Cases for Investigation and Administrative, Civil and Criminal Sanctions* (the HOCOLEA Principles). The HOCOLEA Principles state that 'each agency will have a compliance strategy…[that]…will encourage [customer] compliance with the laws the agency enforces by making full use of all appropriate means'[49] including:

> education programs; intelligence assessments, risk management and strategic targeting;...applying strategies including administrative penalties; strategic use of available sanctions (administrative, civil and criminal)…[50]

2.18 The important factor in characterising fraud is the level of 'intent' reflected in the customer's behavior. The Guidelines define fraud as dishonestly obtaining a benefit by deception or other means and Centrelink uses this definition in its *Fraud Control Plan 2008–10*. However, Centrelink's Fraud Control Plan does not refer to the term (and use by Centrelink) of 'serious fraud', which was introduced in 2006 as part of a new Budget initiative and is the focus of Centrelink's fraud programs.

2.19 Fraud control fits within Centrelink's broader compliance framework of measures to prevent, detect, investigate and report fraud. Within this framework, Centrelink has adopted the Braithwaite enforcement pyramid approach to understanding the factors that influence the compliance behaviour of its customers.[51] Centrelink's enforcement pyramid approach takes a graduated response to customer behaviour, recognising that most customers are willing or trying to comply.

---

[49] Attorney-General's Department, HOCOLEA, *Overarching Principles for Selecting Cases for Investigation and Administrative, Civil and Criminal Sanctions*, AGD, Canberra, undated, p. 1.

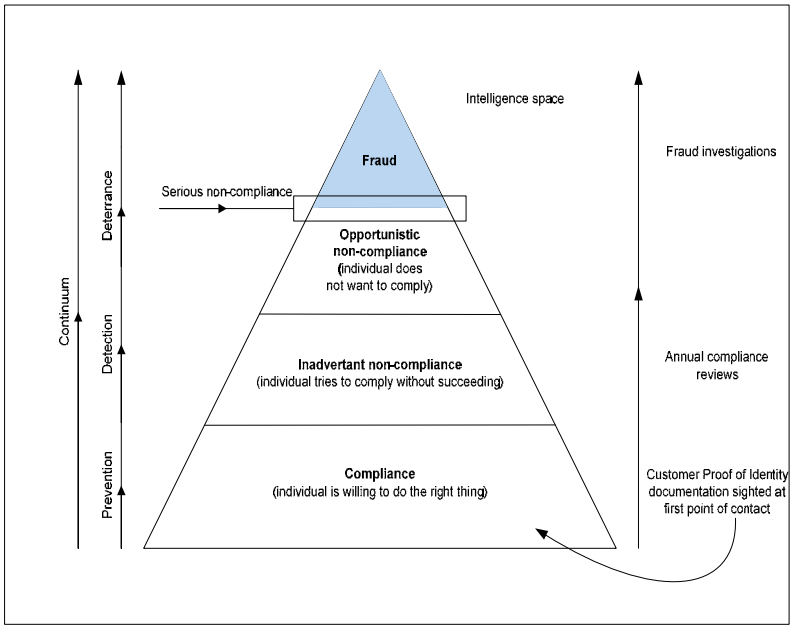
[50] ibid.

[51] This approach is based on directing information and other preventative measures towards customers at the bottom of the pyramid who are willing to comply (see Figure 2.1) and progressively targeting compliance at the top of the pyramid, particularly to those customers Centrelink has identified as deciding not to comply.

2.20 Encouraging compliance and ensuring that non-compliance is kept to a minimum is a major and ongoing task for agencies such as Centrelink, where there is a high exposure to external fraud and a close relationship between compliance strategies for customers and fraud control.[52] Centrelink advised that it targets its fraud programs to the top of the pyramid, where customers have decided not to comply (see Figure 2.1).

Figure 2.1

Centrelink's enforcement pyramid model for community compliance



Source: Centrelink audit entry interview, 23 June 2009.

2.21 Centrelink assists customers at the bottom of the pyramid that are willing to comply, by providing information and other preventative measures to help customers understand and meet their obligations. These measures include community media campaigns and other online communication initiatives. In order to raise public awareness of social security fraud and Centrelink's response to fraudulent behaviour, its Communications Strategy focuses on successfully prosecuted cases.

[52] Australian National Audit Office, *Better Practice Guide – Fraud Control in Government Agencies*, ANAO, Canberra, 2004, p. 18.

2.22 Centrelink stated that its compliance activities are progressively targeted towards the top of the pyramid, particularly to those customers it has identified as deciding not to comply. Centrelink considers this component to constitute payment and serious fraud and targets its fraud investigation activity to this group.[53] Centrelink advised that compliance reviews are the most efficient and effective activity in detecting and targeting non-compliance.[54] Centrelink's compliance work for 2008–09 was undertaken by a dedicated business team: Payment Review. Compliance work is desk-based with reviews actioned by compliance review staff, using internal and external data and information sources. Compliance work ultimately forms the bulk (70–80 per cent) of referred cases of alleged fraud to Centrelink's Fraud Investigation Teams (FITs), which may also be selected for investigation and possible prosecution action.[55]

2.23 While Centrelink has not formally documented its overarching compliance framework for 2008–09 and 2009–10,[56] it does have a program of compliance strategies and activities in place that are intended to control, prevent and detect payment inaccuracies and fraud. The nature of fraud control in Centrelink is that many cases detected are either found to have a legitimate explanation or lack the criminality for a substantial prosecution outcome.[57]

Compliance strategies and activities to control fraud

2.24 Centrelink's program of compliance strategies and activities to prevent, detect and deter payment inaccuracies and fraud are outlined in its *Fraud Control Plan 2008–10*. These activities are designed to provide a graduated response to payment risks as illustrated in Centrelink's enforcement pyramid approach in Figure 2.1 and include:

- Prevention—systems and procedures designed to minimise incorrect payment and fraud from occurring, rather than detecting them later. A

[53] ANAO audit entry interview with Centrelink, 23 June 2009.

[54] ANAO audit entry interview with Centrelink, 23 June 2009. From 2002–03 to 2006–07, 90 per cent of Centrelink's debts raised directly resulted from compliance review activity, ANAO Audit Report No.42, 2007–08, *Management of Customer Debt Centrelink, Follow-up Audit*, Canberra, p.77.

[55] Centrelink, *Fraud Investigation Strategy 2008–09: Blueprint for Managing our Current Program of Activity More Effectively*, v0.5, p. 14.

[56] Centrelink meetings with the ANAO.

[57] Centrelink, *Business Needs for Fraud Management in Centrelink*, 20 March 2008, p. 9.

key Centrelink preventative control is the requirement for customers to provide proof of identity (POI) documents as part of establishing their eligibility for most Centrelink payments and benefits. Correct application of the POI guidelines is Centrelink's most important preventative control to ensure benefits are provided to the correct person (see Chapter 5 for further discussion on POI);[58]

- Detection—systems and procedures designed to discover incorrect payment and fraud when it occurs. Techniques used by Centrelink to detect incorrect payments and fraud include: identity checks; compliance activities and data-matching of information from other agencies; public 'tip-offs'; and selecting customers for review based on their circumstances, duration of payments, or a specific event; and
- Deterrence—systems and procedures designed to deal with incorrect payment and respond to potential or actual fraud when it is uncovered. When potential or actual fraud is uncovered, Centrelink takes corrective action through activities such as debt recovery, fraud investigations and prosecution referrals. Fraud investigations, including the gathering of evidence to support the prosecution of customers who decide to not comply, are integral to Centrelink's approach to managing fraud.

2.25 The scale of Centrelink's detection activities is necessarily large and its investigators are provided with fraud cases from a number of areas including generic and automatic referrals, to be able to meet performance targets for savings and prosecutions referrals.[59] The largest proportion of Centrelink's fraud cases and prosecution referrals are automatically referred debt cases, that is, arising from debts of more than $5000. The ANAO's analysis of fraud data from 2005–09 showed that 60 per cent of cases prosecuted over that period were debt referrals. The impact of debt referrals on Centrelink's enforcement pyramid approach, as well as its case selection practices and the oversight of decision-making during the investigative process, are examined in the remaining chapters.

---

[58] COAG, National Identity Security Strategy [Internet], 2007, available from <http://www.coag.gov.au/coag_meeting_outcomes/2007-0413/docs/national_identity_security_strategy.pdf> [accessed 5 November 2009].

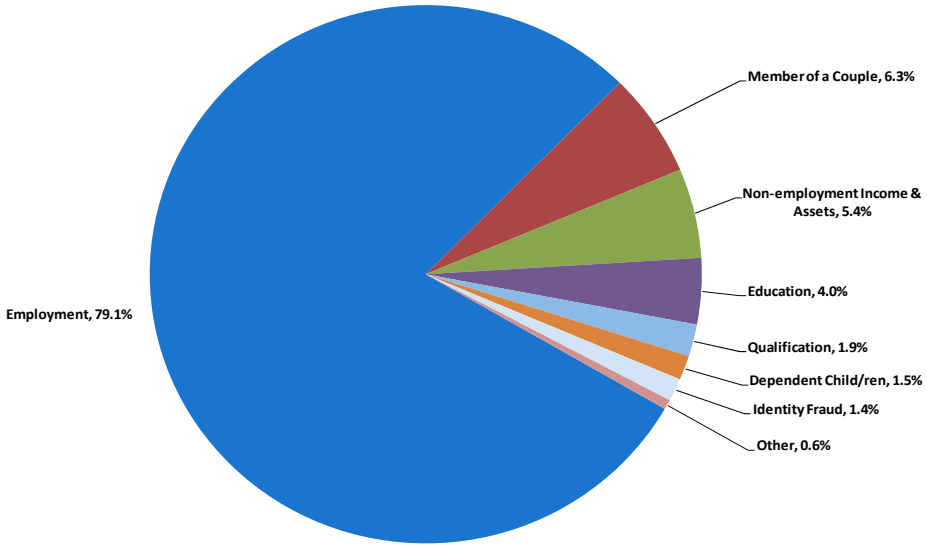
[59] Centrelink, *Business Needs for Fraud Management in Centrelink*, 20 March 2008, p. 9.

Types of external fraud detected by Centrelink

2.26 Centrelink detects a range of fraud offences (alleged and substantiated), of which the largest group are employment-related offences. These include under-declaring casual earnings; failure to declare part-time and full-time earnings; and failure to declare partner income. Figure 2.2 provides an overview of offence groups that were successfully prosecuted in 2007–08 (extracted from Centrelink's Fraud Investigation Case Management System (FICMS) case data.[60]

Figure 2.2

Centrelink successful prosecutions by group in 2007–08



Source: ANAO analysis.

Trend in customer debt

2.27 Over the past few years Centrelink has reported a steady increase in customer debt arising from compliance activities. For example, in 2004–05 debts totaling $390.5 million were raised through Centrelink compliance activities and by 2008–09 the debt amount had increased to $536 million. Following a recent ANAO audit into the management of customer debt,

[60] At the date of the ANAO's data extraction (6 August 2009) only 59 per cent of the 2008–09 cases were finalised compared to 86 per cent of cases finalised in 2007–08.

Centrelink has agreed to analyse the underlying drivers of its debt base[61] (see Chapter 3 for further discussion).

The operation of Centrelink's compliance framework to control fraud

2.28 Centrelink's compliance strategies and activities to prevent, detect and deter payment inaccuracies and fraud are identified in its *Fraud Control Plan 2008–10*. While not formally documented, these compliance strategies and activities align with the Braithwaite model and were designed to provide a graduated response to payment risks and to focus Centrelink's fraud effort on serious cases of non-compliance, that is, actively prioritising and selecting for fraud investigation, those customers considered to be 'unwilling' to comply.

2.29 In the following chapters of this report, the ANAO examined Centrelink's approach to putting its compliance framework into practice, as it relates to fraud investigations. In particular, the ANAO assessed whether Centrelink's case management practices and decision-making at the operational level were consistent with the agency's case prioritisation strategies, and procedures for selecting, investigating and managing serious fraud cases.

[61] Australian National Audit Office, *Management of Customer Debt—follow-up audit*; ANAO, Canberra, Audit Report No.42, 2007–08.

3. Referrals Leading to Case Selection

This chapter examines the effectiveness of Centrelink's activities for selecting and prioritising suspected cases of external fraud after it has occurred.

Background

3.1 Centrelink has a number of measures that generate referrals of fraud cases to its Business Integrity Network including:

- generic referrals (arising from anomalies identified in compliance reviews) including manually referred cases;
- automatic referrals (arising from debts of more than $5000); and
- serious fraud referrals generated by Centrelink's intelligence work.

3.2 The ANAO examined these referral mechanisms with a view to determining how they integrated with Centrelink's: fraud case prioritisation and categorisation policies; *National Case Selection Guidelines* (NCSG); and fraud-related targets.

Generic referral of fraud cases

3.3 Centrelink's compliance activities are wide-ranging and focus on cases considered to be at high risk of inaccurate payment as a result of fraud, misrepresentation, error, or omission on the part of the customer. Compliance review activities are generally desk-based and include internal and external data matching and information sources.[62] The bulk of cases of alleged fraud referred for investigation and prosecution consideration to the Fraud Investigation Teams (FITs) are generated by Centrelink's compliance review work.

3.4 The key compliance strategies and activities utilised by Centrelink include: data matching with external agencies; service profiling, which is the use of a set of characteristics that enables Centrelink to better target groups of customers to determine the level of service and support they require; desk-based data analysis focusing on debt prevention; use of an intelligence-led capability to detect and investigate serious and complex fraud

[62] The Allen Consulting Group, *FaCS and Centrelink: Compliance Review*, 2004, pp. 16–17.

and investigations of payment fraud; and special skills and techniques to identify Identity Fraud. The Fraud Control Plan states that Centrelink rigorously pursues identity crime in conjunction with the Australian Federal Police (the AFP) and the Commonwealth Director of Public Prosecutions (the CDPP), with all cases being referred to the CDPP for consideration of prosecution.[63]

3.5 Centrelink's *Fraud Investigation Strategy for 2008–09*[64] states that the work undertaken by the Payment Review team formed the most significant proportion of detected cases of alleged fraud in 2008–09. Centrelink refers to these compliance reviews as 'generic referrals', which comprised 70–80 per cent of detected and investigated cases of alleged fraud referred to the CDPP for consideration of prosecution action.[65] Centrelink confirmed that compliance reviews are the most efficient and effective method to detect and target non-compliance.[66]

Automatic referral of fraud cases

3.6 During 2008–09, Centrelink had an automatic case referral system in place, whereby all debts raised against customers (that exceeded $5000) were automatically referred from its Debt Management System (DMS) into its Fraud Investigation Case Management System (FICMS) for assessment against the NCSG (see Figure 3.1).

[63] Centrelink, *Fraud Control Plan 2008–10*, pp.24–25.

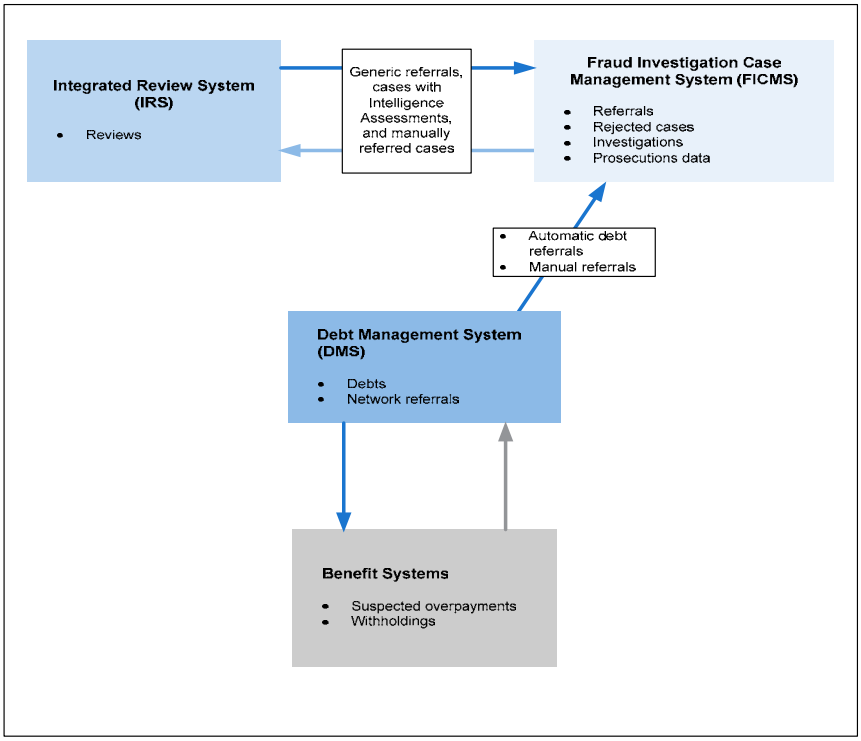
[64] On 16 February 2010 Centrelink informed the ANAO that the document reviewed by the ANAO (see footnote 65) was not endorsed by Centrelink's Executive and was a 'proposed model for managing the current program of fraud activity more effectively'. Centrelink subsequently provided part of a Ministerial brief that is not as comprehensive as the strategy document at footnote 65 and its status is unknown.

[65] Centrelink, *Fraud Investigation Strategy 2008–09*: *Blueprint for Managing our Current Program of Activity More Effectively,* v0.5, p. 14.

[66] Centrelink advice to the ANAO, 23 June 2009.

Figure 3.1

Detection of fraud and case flows into FICMS in 2008–09



Source: ANAO analysis based on information provided by Centrelink.

3.7 Debt referred cases, mainly from debts raised as a result of a compliance review, ultimately form the basis of a large proportion of detected cases of alleged fraud. The ANAO's analysis of 2007–08 and 2008–09 data identified that 60 per cent of fraud investigations in FICMS were debt referrals.[67] Many of these detected debt cases are referred to the CDPP for prosecution action.[68] Furthermore, the ANAO's analysis revealed that in 2007–08, debt cases were seven times more likely to be referred to the CDPP than other fraud cases sourced from Centrelink's Integrated Review System (IRS).[69] IRS cases include public and internal tip-offs, cash economy, manual

[67] In February 2010, Centrelink advised that debt referrals are not fraud investigations and are now considered to be just another form of intelligence. However, legal debts are only raised in circumstances where anomalies identified in customer records are unable to be explained.

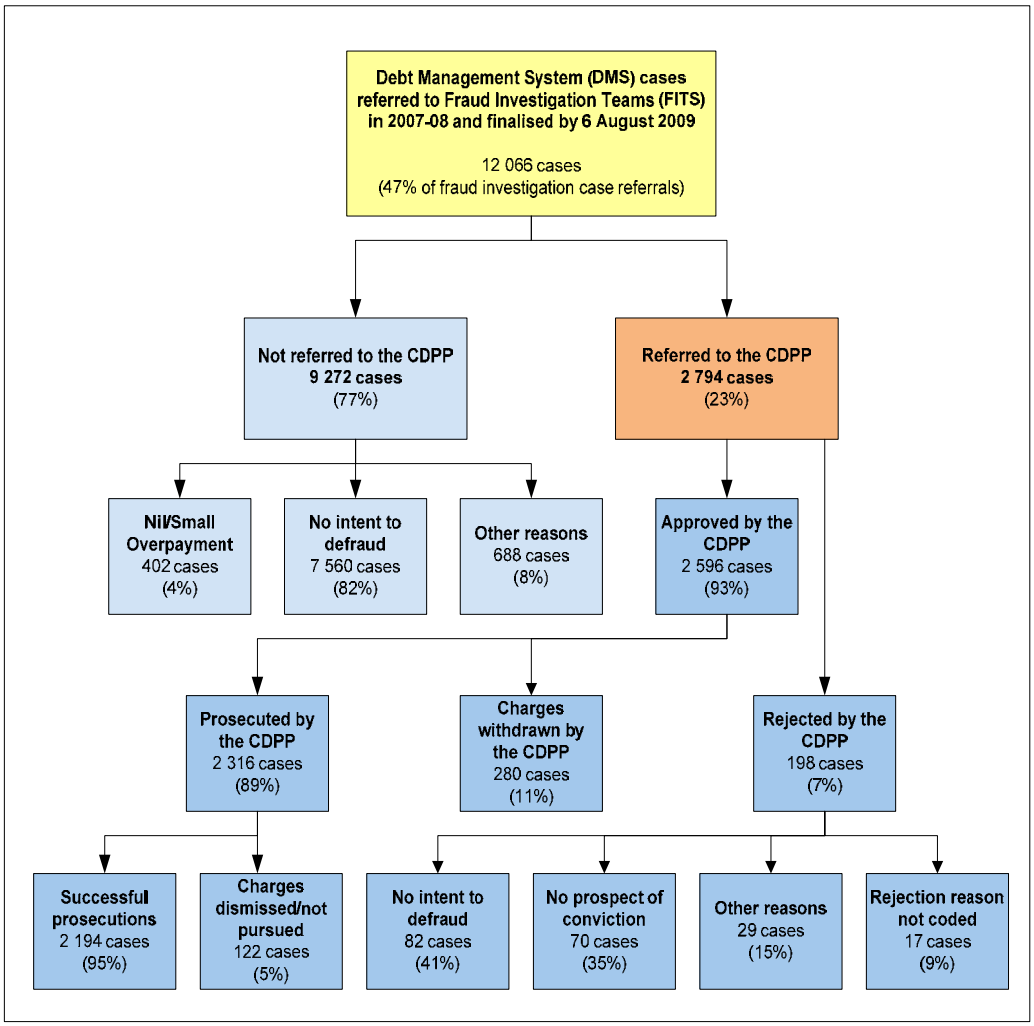
[68] Centrelink, *Fraud Investigation Strategy 2008–09: Blueprint for Managing our Current Program of Activity More Effectively*, v0.5, p. 14.

[69] ANAO analysis.

case referrals and referrals from compliance reviews. The relatively low rate of referral to the CDPP of cases sourced from Centrelink's IRS compared to debt cases from the DMS is evident in Figure 3.2 and Figure 3.3.

Figure 3.2

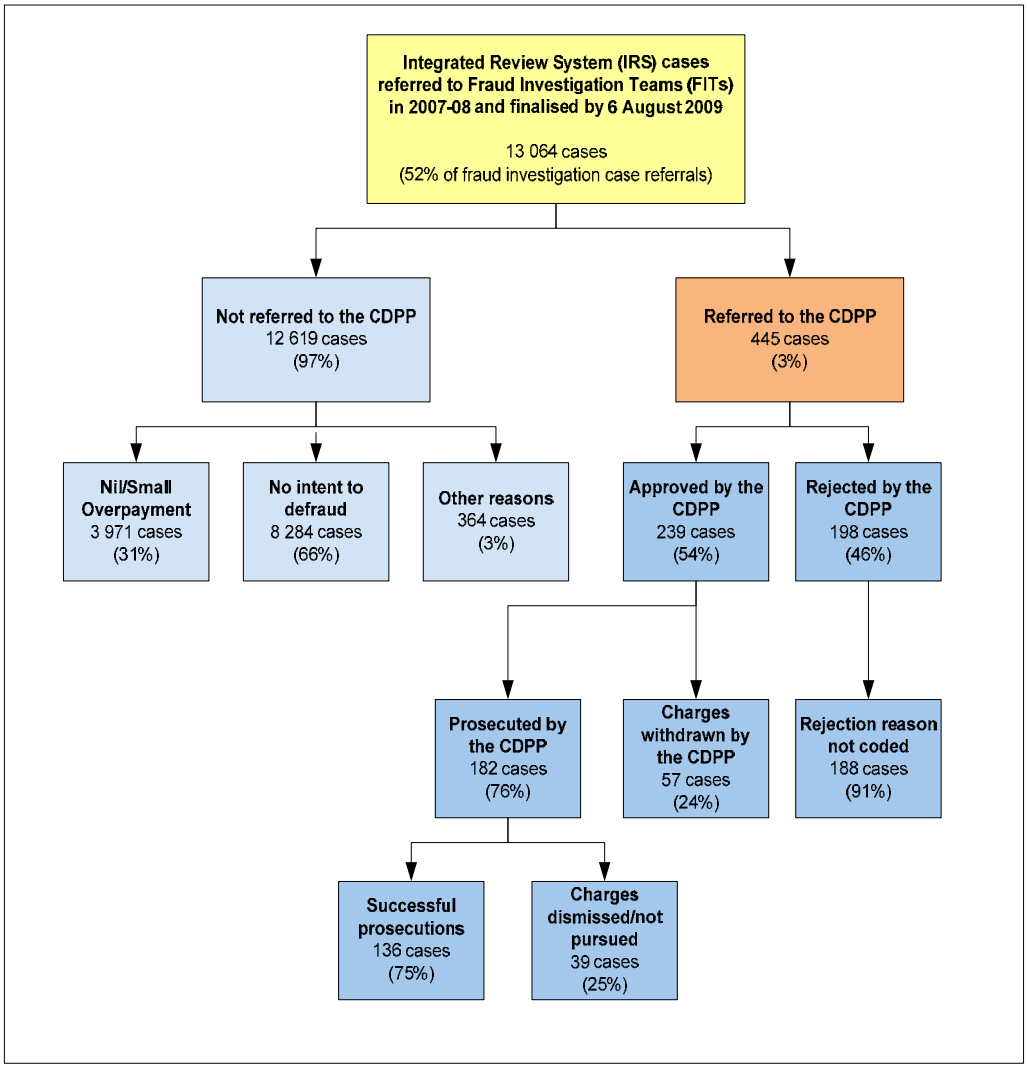
Outcomes of finalised DMS cases referred to the FITs in 2007–08



Source: ANAO analysis.

Figure 3.3

Outcomes of finalised IRS cases referred to the FITs in 2007–08



Source: ANAO analysis.

Intelligence Assessments generated by Centrelink's intelligence capability

3.8 During 2008–09, Centrelink used an Intelligence Model to facilitate the detection of fraud. Centrelink's National Intelligence Model is designed to facilitate the 'acquisition, processing and dissemination' of information that

enables the better detection of fraud cases, and to provide advice for the development of risk management policy.[70] The Intelligence Model is also designed to incorporate the analysis of emerging fraud trends.[71] For example, Centrelink now operates with Strategic, Operational and Tactical Intelligence teams that undertake high-level analysis and detection of fraud. Other elements of Centrelink's intelligence capability include: fraud tip-offs; new approaches to detect and combat identity fraud; the use of risk profiling to improve cash economy intelligence; and cross-agency information sharing.

Fraud tip-offs: reporting allegations of fraud to Centrelink

3.9 Each Australian Government agency must specify in its Fraud Control Plan details of how employees, contractors and members of the public can report fraud against the agency'.[72] During 2008–09 Centrelink introduced a new Tip-off Recording System (TORS) to record allegations of fraud received from the public. The TORS is also designed to record internal Centrelink staff tip-offs relating to the detection of customer fraud. Centrelink employee-generated tip-offs are referred to by Centrelink as 'office referrals' and may include a wide range of suspected customer fraud.[73] Where a tip-off is deemed to warrant either referral to a FIT or to a compliance review team, Intelligence staff in the Fraud Analyst Units (FAUs) load the case into Centrelink's IRS for action. Where the tip-off involves a referral to a FIT, the FAU will also produce an Intelligence Assessment which is distributed to a FIT for allocation to an appropriate investigator.[74]

Identity fraud

3.10 Centrelink is developing new approaches to detect and combat identity fraud (ID fraud). The approaches include specific reports that are designed to be used to improve detection techniques such as data-matching and understanding how ID fraud occurs. The reports are comprehensive and include *Post-Case Analysis Reports* and *Strategic Analysis Reports*. Centrelink produces detailed ID fraud *Post-Case Analysis Reports* on a monthly basis. The

---

70 Centrelink, *Fraud Investigation Strategy 2008–09: Blueprint for Managing our Current Program of Activity More Effectively*, v0.5, p. 14.

71 Centrelink, *Intelligence Plan 2008–09*: *Supporting Fraud Investigations*, p. 5.

72 Attorney-General's Department, *Commonwealth Fraud Control Guidelines*, AGD, Canberra, 2002, paragraph 3.15.

73 Centrelink, *e-Reference 110.40430–Report a Suspected Fraud Office Referrals*, October 2008, p. 1.

74 Centrelink, *Fraud Investigation Manual*: Tip-off Processing –Revise and Review Process Diagram, 2007.

ANAO found that Centrelink's *Post-Case Analysis Reports* and *Strategic Intelligence Reports* were of good quality and that the information contained in these reports offer Centrelink an ability to track and analyse the risks that it faces from ID fraud to its programs. Both types of reports could readily be expanded to cover most types of payment fraud that Centrelink experiences and if this occurred Centrelink would be better placed to analyse a broader range of risks.

Cash economy operations and intelligence

3.11 Centrelink uses high-level intelligence, including data mining of its old and new TORS, to detect suspected cash economy employers.[75] Centrelink conducts both 'field operations' (usually involving the assistance of State and other Commonwealth agencies) and 'desk-based' investigations of customer payments. These investigations are associated with the use of Centrelink's administrative coercive information-gathering powers under s195 of the *Social Security (Administration) Act 1999*, which gives Centrelink the power to coercively gather information on classes of persons. Centrelink uses risk profiling to detect fraud through intelligence that is fed back into cash economy operations, including the identification of customers that are likely to under-declare, or not declare their income.[76] In 2008–09, Centrelink carried out 124 cash economy operations that involved the investigation of 7923 customers.[77]

Cross-agency information sharing

3.12 During 2008–09, Centrelink was engaged in several cross-agency information-sharing networks that supported its intelligence-led capability. These included: the Australian Crime Commission led Financial Intelligence Assessment Team; the Joint Agency Strategic Cash Economy Working Group (JASCEWG);[78] the Department of Human Services Strategic Fraud and Non-compliance Steering Committee;[79] and an internal reference group to coordinate planning of Centrelink's fraud intelligence activities in 2008–09.[80]

---

75 Centrelink, *Intelligence Plan 2008–09: Supporting Fraud Investigations,* p. 8.

76 Centrelink advice to the ANAO, 16 February 2010.

77 Centrelink, *Annual Report 2008–09*, p. 39.

78 Centrelink, *Fraud Intelligence Plan 2008–09*: *Supporting Fraud Investigations*, p. 5.

79 Department of Human Services advice to the ANAO, 26 June 2009.

80 Centrelink, *Fraud Intelligence Plan 2008–09: Supporting Fraud Investigations*, p. 5.

Appendix 5 provides a list of Centrelink's key industry stakeholder relationships.

Fraud case prioritisation and categorisation policy

3.13 The *Australian Government Investigations Standards* (the AGIS) stipulate that agencies are required to have a case prioritisation policy in place that assists staff with responsibility for acting on detected cases of alleged fraud.[81] The AGIS directive is multifaceted and the development of a case prioritisation policy ultimately determines the focus that an agency will maintain when detecting and selecting cases for investigation.

3.14 To ensure a consistent approach to the application of case selection processes at the operational level, the ANAO assessed the extent of Centrelink's National Intelligence Model to:

- identify and prioritise more complex and serious fraud cases through Intelligence Assessment reports to enhance investigations;
- detect trends, and new and emerging risks to program outlays and inform a range of activity, beyond identified special fraud operations and Budget measures, through its analysis of Centrelink's broad range of fraud data; and
- ensure serious fraud cases are processed and delivered to the Business Integrity Network promptly, in line with serious fraud timeliness standards.

Centrelink's *Case Prioritisation Framework*

3.15 Centrelink has adopted the AGIS requirement of using the Heads of Commonwealth Operational Law Enforcement Agencies Principles (HOCOLEA Principles) as a basis to frame the development of its *Case Prioritisation Framework*. In response to the serious fraud Budget measure implemented in 2006, Centrelink uses the HOCOLEA Principles as a basis of its definition and approach when responding to serious fraud.[82]

---

[81] Attorney-General's Department, *Australian Government Investigations Standards*, AGD, Canberra, 2003, paragraph 4.1.

[82] Centrelink is not a designated law enforcement agency.

Serious fraud

3.16 Centrelink uses the HOCOLEA definition of serious crime to define 'seriousness' in terms of fraud investigations.

Serious fraud:

- involves a significant degree of criminality on the part of the offender; and
- the Commonwealth or the community expect it (serious fraud) will be dealt with by a prosecution which is conducted in public before a court and usually carries the risk of imprisonment in serious cases;
- either produces significant, real or potential harm to the Commonwealth or the community; or
- is of such a nature or magnitude, that it is important to deter potential offenders and prosecution will act as a very effective deterrent.[83]

3.17 Centrelink defines serious fraud using the following criteria: the nature of the fraud; how many risks are in the allegation/data; does information support ongoing fraudulent activity; the length of fraudulent activity; and the length of time on payment.[84]

Case Prioritisation Framework

3.18 During 2008–09, Centrelink had in place a *Case Prioritisation Framework* (CPF) designed to enable the assessment of the priority and seriousness of cases of alleged fraud from low, medium and high priority. Centrelink's CPF also included an assessment of priority in relation to: ministerial directives and policy department priorities; the value and nature of the alleged offence; the response required; and whether there is evidence of recidivist activity; and the impact of the alleged fraud on Centrelink.[85] The assessment and application of a case prioritisation rating is undertaken by fraud analysts working in the FAUs. Where the likelihood of fraud or criminal behavior is identified a case-specific Intelligence Assessment is provided. This process is designed to provide clear guidance to FIT staff who undertake the investigation.[86]

3.19 Centrelink's CPF states that cases of detected fraud involving a debt of a 'value of [an] alleged offence' over $30 000 requires an immediate response

---

[83] Centrelink, *Fraud Investigation Manual*, Interpretation Guide of Serious Fraud, 26 September 2007.

[84] ibid.

[85] Centrelink, *Fraud Investigation Manual*, Case Prioritisation Framework, October 2007, p. 1.

[86] Centrelink, *Fraud Investigation Manual,* Case Prioritisation Framework Guide, October 2007, p. 2.

from Centrelink.[87] The ANAO's case reviews identified that there were many cases with debts over $30 000 that did not initiate an immediate response, and higher debts with evidence of fraudulent behavior that were not referred to the CDPP. This is an inconsistent practice and ultimately has a flow-on effect for the types of debts that are investigated and referred to the CDPP for prosecution action.

Intelligence Assessments and case complexity ratings

Fraud Analyst Units

3.20 The FAUs were introduced in 2007 after Centrelink received an appropriation relating to the 2006–07 Budget measure *Enhanced Focus on Serious Social Security Fraud*. The FAUs are designed to enable staff to detect external fraud through a range of techniques including: the analysis of internal and external data systems; and sourcing background information on the status of customer financial and asset records through the use of paid third party service providers. The primary function of the FAUs is to develop cases to a point where Centrelink can identify if there is a likelihood of fraud and criminal activity.

3.21 The work undertaken by the FAUs is desk-based. Examples of internal Centrelink databases from which intelligence about suspected cases of fraud is detected include: the Customer History and Relationships Tool (CHART); the TORS (which may include tip-offs from staff working in Customer Service Centres); and the Mainframe (the IRS). The main source of external intelligence is data provided by the Australian Transaction and Reports Analysis Centre (AUSTRAC).[88] Notwithstanding these tools, high-level internal and external data-matching is also taking place.[89]

3.22 A key responsibility of Centrelink's Intelligence teams is to support fraud investigation operations by identifying the complexity and seriousness of fraud and prioritising cases for investigation. Accordingly, fraud analysts produce case-specific Intelligence Assessment reports to assist with the

---

[87] Debts initially examined and identified by intelligence staff may differ to the amount of debt determined when an investigation is finalised - *Fraud Investigation Manual*, Case Prioritisation Framework, October 2007.

[88] Centrelink, *Fraud Investigation Manual:* Tactical Analysis Information Sources Process Area Diagram, 2007.

[89] ibid.

detection of suspected cases of fraud for investigation by the Fraud Investigation Teams.

3.23 Separate to the application of case prioritisation ratings that prioritise the investigation of cases of alleged fraud, fraud analysts also apply complexity ratings of the seriousness of the alleged fraud and include a rating of each case in the Intelligence Assessment reports. The application of case complexity ratings stems from the 2006–07 *Legal Action on Serious Fraud* Budget measure that was designed to increase Centrelink's focus on higher profile and more difficult fraud cases and increase the number of complex cases referred to the CDPP for prosecution action.[90]

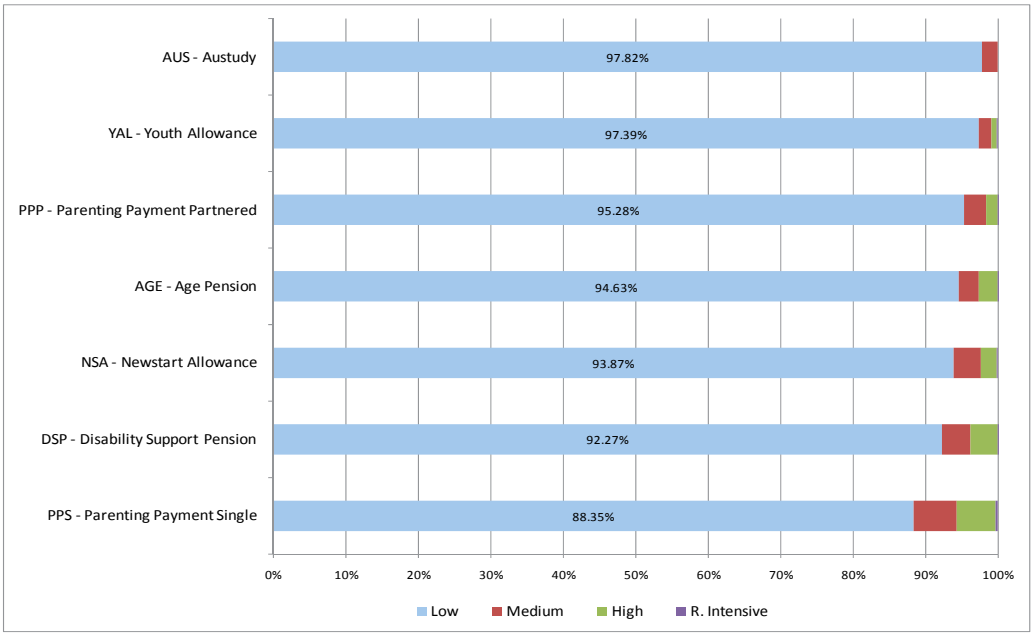
3.24 The ANAO's analysis of Centrelink FICMS data revealed that in 2007–08, the range of complexity ratings assigned during the investigation of alleged cases of fraud varied from 92 per cent of cases rated as low complexity, compared to 8 per cent of medium, high and resource-intensive rated cases.[91] Figure 3.4 identifies Centrelink's complexity ratings assigned by major payment types for 2007–08.

[90] Centrelink, *Fraud Investigation Manual*, Complexity Assessment for Fraud Cases with Intelligence Assessments, October 2008, p. 1.

[91] ANAO analysis of 2007–08 FICMS data.

Figure 3.4

Complexity ratings assigned to fraud investigation cases in 2007–08



Source: ANAO analysis.

3.25 Accordingly, the approach may have resulted in the limited detection and investigation of serious fraud cases with higher complexity ratings. The ANAO also considered the effect of the complexity ratings on investigation outcomes regarding cases referred to the CDPP for consideration of prosecution action. Of the cases referred to the CDPP in 2007–09, 92 per cent were cases with a low complexity rating.[92]

[92] Fraud investigations can take time to finalise. The proportion of 2007–08 investigations that had been finalised on the 6 August 2009 (when the data was extracted from FICMS) was 86 per cent, compared to 59 per cent for 2008–09, which is why 2007–08 data is used.

Table 3.1

Cases referred to the CDPP by complexity rating in 2007–08

Complexity code	Not referred to the CDPP	Referred to the CDPP	Total	Per cent referred to the CDPP
Low	22 740	4594	27 334	17%
Medium	869	355	1224	29%
High	691	285	967	29%
Resource intensive	24	25	49	51%
Total	24 324	5259	29 583	

Note: The ANAO analysed 2007–08 fraud data because a greater proportion of cases had been finalised in that year, compared with the number of 2008–09 cases finalised at the point in time of the data extraction (9 August 2009).

Source: ANAO analysis.

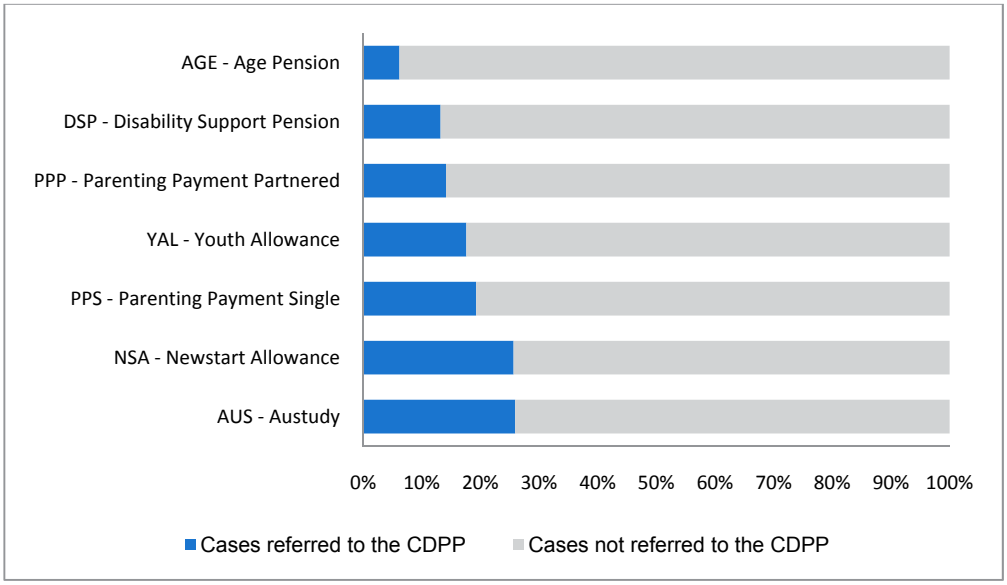
3.26 Low complexity fraud cases represented 92 per cent (27 334/29 583) of Centrelink's fraud-related investigations and 87 per cent (4594/5259) of cases referred to the CDPP by Centrelink in 2007–08. The detection and referral of most Centrelink fraud cases related to less complex employment type offences: under-declaring casual earnings (37 per cent); failure to declare part-time employment (30 per cent); failure to declare full-time employment (17 per cent); and failure to declare partner income (8 per cent). This trend was confirmed during structured interviews with Centrelink fraud staff, the CDPP and the AFP.

3.27 However, as illustrated in Table 3.1, while low complexity fraud cases represented 87 per cent of cases referred to the CDPP by Centrelink, the relative referral rate to the CDPP did increase according to the complexity of the case.

3.28 The ANAO's analysis also revealed that the payment type with the most cases of a high complexity rating was Parenting Payment Single, followed by Disability Support Pension and Newstart Allowance. The actual payment with the highest average debt referred to the CDPP was the Age Pension. Figure 3.5 shows the proportion of cases referred to the CDPP by payment type in 2007–08. The range of referral rates varies from six per cent of Age Pension cases to 26 per cent of Austudy cases. While the referral rate is lowest for Age Pension cases, the average debt recovered is highest for Age Pension cases.

Figure 3.5

Proportion of cases referred to the CDPP by payment type in 2007–08



Note: Each percentage in the graph is by the 'proportion' of a payment type that is referred to the CDPP for prosecution. For example, in 2007–08, 26% of Austudy fraud cases were referred to the CDPP.

Source: ANAO analysis.

3.29 Although the Age Pension had the highest average debt referred to the CDPP in 2007–08, only 6.2 per cent of Age Pension cases referred to the FITs resulted in referral to the CDPP, compared with more than 25 per cent of Austudy and Newstart Allowance payment cases.

3.30 Centrelink does not undertake post-case analysis on the range of fraud case types that it detects and investigates as currently this type of analysis is limited to specific Budget measures. Such analysis would involve Centrelink modeling different approaches to treating the fraud risks to the programs it delivers.

3.31 The Intelligence Assessment reports reviewed by the ANAO were generally determined to be of a high quality. However, the influence of this analysis to contribute to achieving higher quality outcomes, including referral of serious fraud cases to the CDPP, was neither evident in the results of the ANAO's case reviews, nor in the analysis of four years of FICMS data (across 2005–09). For example, the ANAO's reviews of Centrelink cases in 2008–09 determined that less than 50 per cent of cases had undergone an Intelligence Assessment by the FAU and of these cases, 95 per cent were not referred for

consideration of prosecution action, compared to 77 per cent of debt referred cases, and 86 per cent of all other referred cases.

Centrelink's National Case Selection Guidelines

3.32 Centrelink has *National Case Selection Guidelines* (NCSG) in place to assist staff to make consistent decisions about when to select cases of suspected fraud for investigation and possible prosecution:

> In consultation with the CDPP, Centrelink has case selection guidelines on the types of cases it will investigate and refer to the CDPP in order to meet standards of quality, consistency and timeliness. These guidelines are intended to promote national consistency in the making of decisions that arise in the institution and conduct of prosecutions...[93]

3.33 Under Centrelink's NCSG all cases which meet any of the following four criteria are to be investigated: recidivist behaviour; where a warning letter has been previously issued; debts over $5000; and serious misconduct requiring the community to be informed.[94]

3.34 All cases, including those with Intelligence Assessment reports, flow into FICMS Team New Work and are assessed against Centrelink's NCSG for investigation and prosecution consideration (except for cases with Intelligence Assessment reports with a 'high' priority rating which must be investigated). Case Control Officers (CCOs) in the fraud investigation network play an important role in assessing each case for suitability of investigation against the NCSG before assigning the case to an appropriate investigator, referring cases elsewhere, or terminating the case.[95]

---

93 Centrelink and the CDPP, *Memorandum of Understanding*, 1999, paragraph 3.3.

94 Centrelink, *Fraud Investigation Manual*, National Case Selection Guidelines, October 2007, p. 1.

95 During the audit, Centrelink advised that all cases, including debt cases, needed a Critical Decision Record outlining the reasons for terminating the investigation and approved by a Case Manager. This is consistent with the FIM and the AGIS. Subsequently, Centrelink informed the ANAO that DMS debt referrals are not considered to be fraud investigations and, therefore, are not required to meet the AGIS and mandatory FIM requirements for critical decisions. The ANAO notes, however, that debt referrals make up a significant percentage of Centrelink cases that are referred to the CDPP and prosecuted.

3.35 In the FIM, all cases assigned for investigation by the CCO are regarded as:

> Inquiries into whether there has been a suspected criminal fraud perpetuated against law administered by Centrelink's programs, with a primary purpose of gaining admissible evidence for any subsequent criminal action.[96]

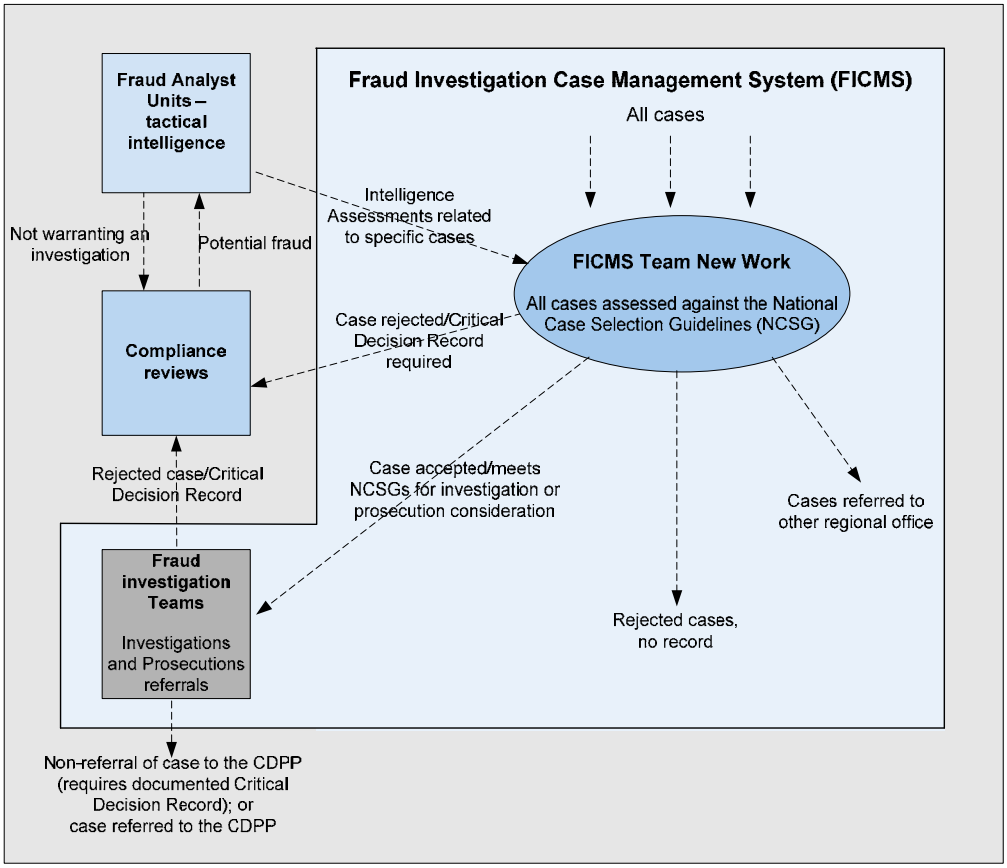
3.36 The application of the NCSG also effectively acts as a control mechanism, as the CCOs determine whether or not some debt cases are appropriate for direct referral to Centrelink's prosecutions team (without an investigation being conducted)[97] (see Chapters 4 and 5 for related issues). The outcomes of fraud investigations can range from an administrative remedy through to referral to the CDPP for prosecution consideration. Figure 3.6 provides an overview of the case workflows in and out of FICMS.

[96] Centrelink, *Fraud Investigation Manual*, Investigation Planning Guidelines, 28 November 2007, p. 2.

[97] This practice is not consistent with the AGIS or Centrelink's FIM. On 15 February 2010, Centrelink advised that the 'FIM is Centrelink's mandated policy and practices manual. All fraud investigators are expected to follow it'.

Figure 3.6

Workflow of cases in and out of FICMS in 2008–09



Source: ANAO analysis.

Fraud-related targets

3.37 Targets and performance measures are a feature of a good reporting framework and they need to be balanced, measurable, and regularly reviewed to ensure they are compliant with Centrelink's policies and processes and effective in achieving the desired outcomes. The Business Integrity Network is allocated yearly quantitative targets in relation to the number of fraud investigations and prosecutions the network needs to achieve each year to contribute to the savings required by the policy agencies.

Timeliness standards in actioning debt referrals

3.38 Timely actioning of fraud investigations is important to ensure agencies deal with fraud quickly to facilitate a successful outcome. When matters are

not dealt with promptly, there is an increased chance of an unsuccessful prosecution or charges being withdrawn. The CDPP advised that an investigation that faces long delays heightens the risk of an unsuccessful prosecution due to evidence and the offences becoming stale.

3.39 The AGIS requires that agencies deal with allegations of fraud promptly:

> Agencies are to have a procedure covering…time frames for initial consideration of the allegation. Agencies need to be mindful of the difficulties caused when matters are not dealt with or referred promptly. These can include loss of evidence, further damage caused by the continuation of the offence, and an increased chance of an unsuccessful prosecution or charges being withdrawn.[98]

3.40 Centrelink guidelines state 'that there are no timeliness standards in respect of actioning debt referrals, except that the FICMS will not process a backlog of over 300 referrals, and accordingly the number of referrals must be monitored and activated daily'.[99] This is not consistent with the AGIS[100] and the implications of not acting promptly when cases of alleged fraud are detected are detrimental to Centrelink, the alleged offender and legal proceedings.

3.41 The ANAO identified instances of deficiencies in the timeframes surrounding the referral of compliance review activities for investigation. This is evident in circumstances where a debt is raised against a customer as a result of a compliance review and where the debt amount meets criteria established in Centrelink's NCSG.[101] These cases of alleged fraud are automatically referred into FICMS Team New Work from the DMS.

3.42 Centrelink advised that from 21 January 2010, debt cases now undergo a (brief) assessment process by the FAUs. While the ANAO acknowledges the difficulty in balancing limited resources and case work, the new process

---

98 Attorney-General's Department, *Australian Government Investigations Standards*, September 2003, AGD, Canberra, paragraph 3.2(iv).

99 Centrelink, *Fraud Investigation Manual*, Receipt of, and Initial Assessment of, Allegation in FICMS, May 2009, p. 3.

100 On 16 February 2010, Centrelink advised that a new procedure was implemented on 21 January 2010 whereby automatic debt referrals are now considered to be 'intelligence' and will be assessed by the Fraud Analyst Units prior to referral of those debt cases to the FITs that are deemed to warrant a fraud investigation.

101 Under Centrelink's NCSG, all cases which meet any of the following four criteria are to be investigated: recidivist behaviour; where a warning letter has been previously issued; debts over $5000; and serious misconduct requiring the community to be informed.

implemented in January 2010 for debt cases may resolve some of the issues identified.[102]

Timeframes for serious fraud

3.43 Centrelink has implemented timeliness requirements for its serious fraud cases. The timeliness standards for the serious fraud cases commence through activation of the case in the IRS, yet the actual investigation start date does not commence until the case is activated in the FICMS. The time difference between activating a case in these two systems can be more than 12 months and this issue is not identified as a risk or documented in the FIM. The use of two systems to report performance information internally and externally, which were designed for different purposes, limits Centrelink's ability to present accurate and reliable reporting for both decision-making and external consumption and is not efficient.

3.44 There was also evidence of cases facing significant investigative delays, particularly in the detection of alleged 'Member of a Couple' fraud cases, among other case types. Evidence in Centrelink's 'Comptime' reports revealed that there are significant delays in commencing, investigating and finalising serious fraud cases. The 'Comptime' reports show that most of Centrelink's fraud investigations that are ongoing for more than 12 months are the more 'serious' fraud cases with some ongoing for more than three years.[103] Centrelink advised the ANAO that the contributing factors in this issue were the complexity of the cases and delays in prosecution proceedings. While the ANAO acknowledges the complexity of these cases, the 'Comptime' reports do not include cases that had been finalised and referred to the CDDP. Additionally, an investigation that faces long delays heightens the risk of an unsuccessful prosecution due to stale evidence and offences. The CDPP confirmed 'older' cases can be problematic in getting a successful prosecution and locating a customer's whereabouts can also be difficult. These timeliness issues are not consistent with internal and external requirements.

3.45 Centrelink's case prioritisation and selection is influenced by Centrelink's corporate targets for the Business Integrity Network. During

[102] On 15 February 2010, Centrelink provided updated FIM procedures and an implementation plan for the strategy and subsequently advised that no system changes were required to implement this change.

[103] Centrelink, '*Comptime' Reports*, 2008–09. These reports show active investigations, type of fraud, serious fraud cases, the age of the cases from the date the investigation commenced, to the date the information was retrieved.

2008–09, Centrelink had corporate targets in place for investigations (and prosecution referrals) in order to contribute to the achievement of the amount of savings required under purchaser/provider arrangements with its policy departments.

Targets for the Business Integrity Network

3.46 Centrelink's Business Integrity Network targets were tied to the dollar savings that would be generated from each fraud investigation and recouped from customers, contributing to the overall required savings amount. Over the past few years, the total amount of customer debt raised by Centrelink as a result of compliance activities has increased from $419 million in 2006–07 to $536 million in 2008–09. During the same period, customer debts recovered through fraud investigations, primarily from compliance activity, accounted for $127 million and $113 million respectively.

3.47 In 2009–10, the achievement of fraud-related targets was tied to the individual performance of Centrelink fraud investigators. These measures are primarily quantitative targets and include: the number of investigations completed (99 per year in 2009–10); the number of prosecutions referred to the CDPP (6 per year in 2009–10); and the number of prosecutions accepted by the CDPP (85 per cent in 2009–10).

3.48 The Business Integrity Network is allocated these yearly quantitative targets in relation to the number of fraud investigations and prosecutions individual staff have to achieve each year to contribute to the savings amount required by the policy agencies. Following the restructure of the FITs in 2008–09, targets have now been tied to individual investigator performance agreements for 2009–10.

3.49 Table 3.2 provides the current and previous financial years' targets. Centrelink maintained or marginally increased the targets in some categories in 2009–10 (see Chapter 5 for an examination of prosecution targets).

Table 3.2

Performance measures for the Business Integrity Network 2008–10

Staff	2008–09 targets	2009–10 targets
Fraud Investigation Teams (FIT)		
Investigators (APS 5)		
Number of Complete Reviews (High – Medium)	96 per year	99 per year
Prosecution Numbers	6 per year	6 per year
CDPP Acceptance Rate	85%	85%
Investigators (APS 4)		
Number of Complete Reviews (High – Medium)	99 per year	99 per year
Legal Action on Serious Fraud Prosecution Numbers	6 per year	6 per year
CDPP Acceptance Rate	85%	85%
Prosecution Officers (APS 4 & 5)		
Number of Referrals	60 per year	55 per year
CDPP Acceptance Rate	85%	85%
Fraud Analyst Units (FAUs)		
Tactical analysts		
Intelligence Assessment (IA) and serious fraud Tip-Off processing	In 2008–09 Centrelink did not have set targets for the FAU analysts' for the production of IAs or Tip-Offs.	In 2009–10 there is weekly 'performance expectations' of the number of IAs produced as a function of APS level. However, unlike FIT staff, Centrelink advised that this is not a benchmark or target level staff must achieve.

Source: Centrelink advice October 2009, and 10–11 December 2009.

3.50 These fraud investigation and prosecution targets do not distinguish between outcomes by complexity of the fraud, and are not aligned with Centrelink's serious fraud priorities in its CPF. Centrelink has acknowledged the inherent risks associated with pursuing quantitative targets; however, issues remain around the selection of the less complex cases for investigation, and the potential to compromise the quality of fraud investigations generally. Centrelink's 'Comptime' reports detail the number, type and age of cases that each investigator has on hand and these risks are reflected in the many serious fraud investigations that have been ongoing for up to three years or more. During interviews, stakeholders and Centrelink staff indicated that the focus on existing targets was influencing the case selection towards less complex

cases for investigation and prosecution, at the expense of the more complex, serious fraud cases. During interviews, the CDPP regional offices consistently raised the issue of old Centrelink cases with stale evidence being difficult to prosecute (see Chapter 5 for further discussion).

3.51 While targets and performance measures are a feature of a good reporting framework, they need to be balanced, measurable and regularly reviewed to ensure they are not compromising compliance with Centrelink's policies and processes and are effective in assessing the quality of investigations and prosecution referrals.

3.52 A recent ANAO audit identified the risks around Centrelink's capacity to rely on investigation and compliance targets as measures of investigator and compliance review officer performance. In response to this audit, Centrelink agreed to develop a more balanced set of measures that assess the conduct and quality of compliance reviews and investigations.[104] This will assist in the development of a stronger focus on priority setting and balanced targets, relevant to combating complex and serious fraud.

3.53 Centrelink acknowledges that the performance targets for investigations and prosecutions are driving behaviors' to achieve the targets as the priority, rather than investigators focusing on qualitative fraud outcomes, that is, the more complex cases of serious fraud. This is not consistent with Centrelink's enforcement pyramid approach to tackling fraud in terms of prioritising, selecting and dealing with complex and serious fraud cases (see Chapter 2, Figure 2.1 and related text).

3.54 Centrelink acknowledges this dilemma and informed the ANAO that it is reconsidering the targets provided to the Business Integrity Network in October 2009 for 2009–10. On 10 December 2009, Centrelink advised that it is also considering targeting resources to where fraud is more likely to occur and directing serious cases of fraud to those FITs where there is a high level of expertise. Centrelink indicated that debt referrals can be handled in any location.

[104] Australian National Audit Office, *Centrelink's Tip-off System*, Audit Report No.7, ANAO, Canberra, pp. 74–75.

Recommendation No.1

3.55 To facilitate the more effective use of its fraud intelligence capability, the ANAO recommends that Centrelink: review its fraud prioritisation and case selection policies; internal targets; and performance indicators for fraud management; so as to better align these polices and measures with its fraud control strategies.

3.56 Centrelink response: *Agreed*.

Centrelink commenced this process in January 2009 and continues to implement changes in line with this recommendation.

4. Investigating and Responding to External Fraud

This chapter assesses Centrelink's approach to investigating external fraud including compliance with the Australian Government Investigations Standards.

Background

4.1 Centrelink is authorised to conduct its own investigations and prepare briefs of evidence for referral to the Commonwealth Director of Public Prosecutions (the CDPP) under the *Commonwealth Fraud Control Guidelines 2002* (the Guidelines). Agencies managing their own fraud programs, that are subject to the *Financial and Management and Administration Act 1997* (the FMA Act), must comply with the Guidelines.

4.2 In order to assess Centrelink's compliance with the Guidelines, the *Australian Government Investigations Standards* (the AGIS), and Centrelink's policies and procedures for managing fraud investigations, the ANAO assessed:

- Centrelink's fraud investigations against the Australian Government's and Centrelink's requirements;
- the reliability of Centrelink's Fraud Investigation Case Management System (FICMS);
- Centrelink's compliance with its *Fraud Investigation Manual* (the FIM); and
- training and quality assurance arrangements in place to support Centrelink staff and good decision-making.

Fraud investigations

Australian Government Investigations Standards

4.3 The AGIS articulates case handling standards for all fraud investigations and charts the various stages of a fraud investigation including investigation management, methodologies and practices such as: witness statements; interviews; evidence handing; the use of surveillance; the use of informants; and the use of legislated powers such as coercion and the execution of search warrants.

4.4 Under the AGIS, the primary purpose of evidence-gathering during an investigation is to determine the subsequent action, whether civil, administrative or criminal. The AGIS also outlines the written procedures and guidelines that an agency should have in place and follow in order to perform an effective and efficient fraud investigation. Under the Guidelines, it is a requirement that Centrelink's fraud investigators meet minimum mandatory training requirements, and conduct investigations in line with the standards in the AGIS.

4.5 The Commonwealth's regulatory framework assists agencies to investigate and appropriately prosecute fraud, while treating fraud cases fairly and equitably. For the purpose of conducting investigations, the AGIS defines an 'investigation' as:

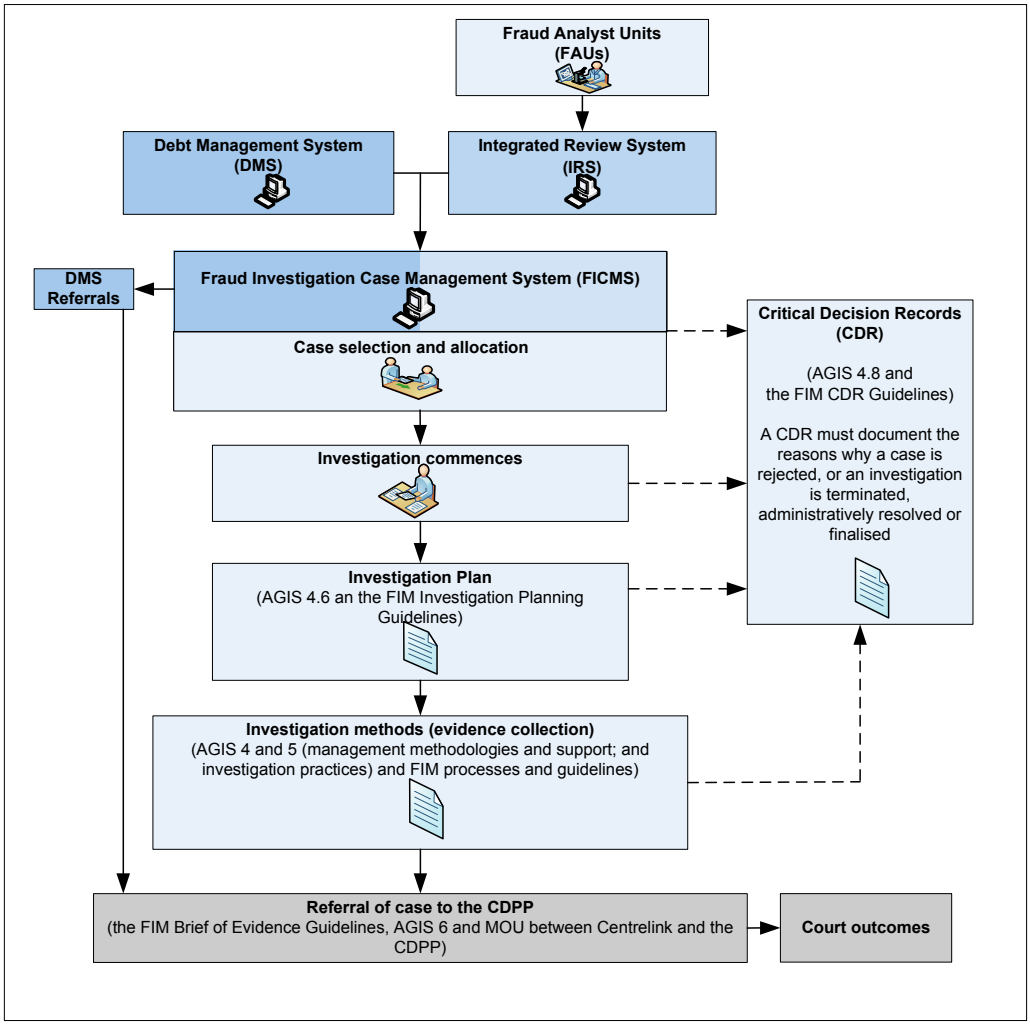
> …inquiries into whether there has been a breach of…law, with the primary purpose of gathering admissible evidence for any subsequent action, whether civil, criminal or administrative. An investigation also includes intelligence projects, proceeds of crime action and financial investigations.[105]

4.6 As well as testing for compliance with the AGIS, the ANAO assessed whether Centrelink followed its internal polices and processes for investigating fraud. Figure 4.1 provides a broad overview of the stages in Centrelink's fraud investigation processes and practices in 2008–09.

[105] Attorney General's Department, *Australian Government Investigations Standards*, AGD, Canberra, September 2003, Chapter 4, p. 7.

Figure 4.1

Overview of Centrelink's fraud investigation process



Source: ANAO analysis.

4.7 The ANAO's audit methodology included analysis of a random sample of 275 cases that were activated and finalised in FICMS in 2008–09 and review of a sample of 113 (of the 275) cases that the ANAO determined had the characteristics of fraud investigations. Where applicable, relevant Centrelink policies, the results of the ANAO's analysis of FICMS data across four financial years (2005–09) and evidence collected during the ANAO's structured interviews, are also discussed in Table 4.1 and Table 4.2.

Centrelink's conduct of fraud investigations

4.8 The results of the ANAO's 113 case reviews of Centrelink's conduct of fraud investigations are outlined in Table 4.1.

Table 4.1

Centrelink's conduct of Fraud Investigations

External and internal requirements	Findings	Implications for fraud case management
Lawful and transparent use of coercive powers in decision making.	Coercive powers are being used throughout the investigative process and after fraud is 'suspected' and in some instances after a formal caution and interview.	While the exercise of information-gathering powers for the purpose of administering Social Security legislation is utilised by a range of areas in Centrelink to determine a person's correct entitlement, these powers cannot be used once a case has been referred for investigation and/or prosecution consideration. The Social Security (Administration) Act coercive information-gathering powers are being used to collect evidence after fraud is 'suspected' in many instances and, in some cases, after the customer has been cautioned.
Investigations must have an investigation plan.	45% of cases had no investigation plan documented on file. Of the 55% of cases with an investigation plan: 30% had not completed the investigation stages and methodology; and 30% had not been approved by a Case Manager.	Investigation plans are required to enable Centrelink staff to take a considered approach to planning and conducting fraud investigations and to allow for transparency and review at each stage of the investigation. Approval of the investigation plan by a Case Manager is a mandatory requirement of the FIM. Approval of this plan enables the investigation to commence and provides assurance to Centrelink and its stakeholders that the investigative approach is appropriate to the alleged fraud and situation such as: the handling of evidence and witness statements and the use of interviews, informants, surveillance and warrants. The absence of an adequate investigation plan makes it difficult for Centrelink to demonstrate that its investigation practices met legislated requirements.

External and internal requirements	Findings	Implications for fraud case management
Legal Notices using coercive powers to gather third party information, and other third party checks, must be documented.[106]	100% of written Legal Notices to gather information from third parties did not have a Critical Decision Record approving the decision; and most third party checks were not recorded.	Centrelink's FIM outlines the range of methods investigators can use to obtain third party information such as through the processes outlined in an established agreement. However, the FIM requires the reasons for obtaining third party information by Legal Notice to be outlined (and signed) in a Critical Decision Record and approved by a Case Manager, prior to the issuing of the notice. Procedural controls, practices and managerial oversight are not appropriate to ensure compliance with the AGIS, Social Security legislation and Centrelink's FIM in relation to: the requirement for management approval of the critical decision to issue written Legal Notices to third parties and documenting the approved Critical Decision Record on file; other third party checks; the use of coercive powers; and consistent identification of the delegated authorised officer and powers in correspondence when requesting third party information.
A document (DOC.) has to be recorded on the customer record notifying of the current investigation or investigation outcome.	Most cases had no recorded DOC. alerting staff that the case was undergoing a fraud investigation.[107] 46% had no recorded DOC. clearly advising of the investigation outcome.	Most cases had no clearly recorded DOC. on the customer record to inform staff at service delivery points that the customer was under investigation for alleged fraud (and not under review). Furthermore, almost half of the cases did not clearly document the outcome of the investigation (that is, whether the investigation outcome was administrative or the case was referred to the CDPP).[108]

[106] Under s.196 of the *Social Security (Administration) Act 1999* the use of coercive information-gathering powers under Division 1 of the Act must take place via the issuing of a written notice.

[107] In June 2010, Centrelink provided further information in relation to DOC.s recorded in customer records in the Mainframe from a sample of the cases reviewed by the ANAO. These did not meet the specific FIM requirements of a DOC. such as recording the 'commencement of the investigation' or 'referral of the brief of evidence for prosecution'. Instead the records mainly referred to compliance review activity.

[108] Centrelink stated that many fraud investigations, case managed in FICMS, are actually compliance reviews and are not required to meet the requirements of the AGIS and Centrelink's FIM and, therefore, it is not necessary to identify in a DOC. that the case is under investigation for fraud. Instead the DOC. may refer to a review. However, this practice is not consistent with the AGIS or Centelink's FIM and, in any case, Centrelink compliance reviews are actioned and saved in a different system to fraud investigations (that is, the IRS)

External and internal requirements	Findings	Implications for fraud case management
Compliance with legislated safeguards, such as Freedom of Information and Privacy legislation.	Lack of transparency in investigation due to the inconsistent recording of information. Information requested and disclosed did not consistently comply with the Privacy Act.	Lack of documentation in records does not support legislated requirements including Freedom of Information.[109] Information unrelated to investigations and inconsistent with the Privacy Act was found on files. Information on file unrelated to the investigation included real estate information and names on Medicare cards. The CDPP has also advised Centrelink that the release of Tax File Numbers (in referred briefs of evidence) is a criminal offence and that the practice should cease.
Investigations must have a separate investigation file.	More than 30% of cases had no separate investigation file.	The integrity and confidentiality of investigations is not being upheld because investigation documents are loosely placed in customer files where no separate investigation file exists. Cash economy files usually have one file created for an entire operation involving many individuals.[110]
Records Management Policies and legislation should be complied with.	Many cases did not have sufficient evidence on file upon which decision-making was based.	Key information required to support decision-making was missing, which is not consistent with document handling and other requirements in the FIM, or Freedom of Information and Archival legislated requirements.[111] Centrelink's record-keeping policy in the FIM is contradictory and incomplete.

[109] A recent Commonwealth Ombudsman's report (May 2010) found the existence of information critical to an investigation and subsequent prosecution was unable to be provided by Centrelink in response to a request for documents under Freedom of Information. The Ombudsman found Centrelink had batch-stored the customer's records, including records of interview and noted that 'Significant documents of this type should be stored on the customer file, where they would not be subject to destruction after 12 months.' See *Centrelink and Commonwealth Director of Public Prosecutions, Review of Circumstances Leading to a Conviction*, May 2010, Parts 1 & 2, paragraphs 1.9, 1.10, 2.21 & 2.23.

[110] The ANAO's case reviews identified that some cash economy cases either have no investigation file created or one file and one FICMS record (that covers many individuals). Centrelink's FIM does not differentiate between the requirements for cash economy and all other investigations and the AGIS also requires an investigation plan for each individual.

[111] In July 2010, Centrelink provided the ANAO with further case documentation in relation to a sample of 20 of the 113 cases reviewed. However, much of this information had been saved in shared drives or elsewhere and, in most instances, was not recorded on the investigation file or in FICMS at the time of the ANAO's case reviews. Centrelink staff reported that fraud investigation documents are often saved in shared drives, personal cabinets and elsewhere which does not comply with the AGIS, the FIM and other legislation. Ernst and Young reported a similar finding regarding local practices in its report, *Evaluation of Centrelink's Fraud Investigation Case Management System*, Final Report, Ernst and Young, 2006.

External and internal requirements	Findings	Implications for fraud case management
Fraud investigations should undergo quality assurance.	Centrelink had no Quality Assurance Program in place for fraud investigations in 2008–09.[112]	Serious and complex fraud cases, with significant debts (of more than $100 000[113]) contained evidence of 'intent' to defraud but there was insufficient evidence of management approval of critical decisions made throughout the investigations and reasons for non-referral to the CDPP were either missing, not clearly stated, or not approved by a Case Manager.[114] Third party information requests are not consistently documented or approved, and the process followed to obtain the information was not transparent. Investigation outcomes revealed that cases were not treated consistently and equitably. For example, cases with smaller debts could be referred to the CDPP whereas cases with significant debts and evidence of fraud, often received an administrative remedy. Furthermore, there was no indication that the CDPP had been consulted in those matters resolved administratively by Centrelink that involved alleged offences of particular seriousness where there was information to suggest 'intent' to defraud.[115]

[112] During the audit, Centrelink developed a Quality Assurance Program and advised the ANAO that it was to be implemented on 30 November 2009.

[113] In the ANAO's original sample of 275 cases, four cases of more than $100 000 were resolved administratively and in one case, investigated and resolved in a day. The AFP advised that their expectation of debts this size would require approval not to refer the case to the CDPP, at the Senior Executive Service officer level in Centrelink. The ANAO identified many debts of a substantial amount, particularly in the original sample where the reasons for non-referral to the CDPP were not clearly stated, and were not approved at the Senior Executive level.

[114] The size of these debts is the key issue and Centrelink's ability to provide assurance that it is managing the associated risks by ensuring appropriate management oversight of decision making at key mandatory points throughout an investigation, as required by the AGIS and Centelink's FIM. This was not the situation, as there was little, if any evidence, of management oversight throughout the investigations reviewed and reasons for non-referral to the CDPP were either missing, not clearly stated, or not documented or approved.

[115] Under the *Prosecution Policy of the Commonwealth*, (November 2008) while the decision to refer a matter to the CDPP is one for Centrelink, where matters involve alleged offences of particular seriousness and are resolved through action other than prosecution, agencies are required to consult with the CDPP. The ANAO's case reviews did not identify evidence of these particular types of consultations occurring.

External and internal requirements	Findings	Implications for fraud case management
Serious fraud is targeted.	Inconsistent approach to remedying serious fraud cases with significant debts.	Clearer guidance and closer oversight is needed to ensure a more consistent approach to case managing serious fraud cases including the need for cases to meet the serious fraud timeframes imposed by Centrelink. Most critical and other key decisions made throughout investigations were not documented or clearly recorded on file or in FICMS as required by the FIM, and critical decisions were not approved by a Case Manager at key points in the process. This includes the point at which the critical decision is made when a fraud investigation transitions from an administrative to a criminal investigation.

Source: ANAO analysis.

4.9 The results of the ANAO's case reviews identified that 87 per cent of Centrelink's 113 fraud investigations did not comply with the AGIS and Centrelink's mandatory policies and procedures. The impetus for Centrelink implementing the FIM was to provide assurance to government and other stakeholders that the investigative and prosecution referral work undertaken by Centrelink is performed consistently across the Business Integrity Network and to ensure investigation case management practices comply with the AGIS.[116] However, the ANAO's case reviews identified inconsistencies with: the case management of investigations and decision-making; recording of activities during investigations; practices around third party checks and insufficient oversight of decision-making at key points in the process; polices and procedures regarding the purpose and lawful use of coercive information-gathering powers; and Centrelink practices and the AGIS in relation to investigation outcomes (whether civil, administrative or criminal).[117]

4.10 The limited review and quality assurance of decision-making, including the lack of managerial oversight of decisions made throughout investigations and Centrelink's approach to record keeping, is affecting the transparency and accountability of its decision-making and compliance with

[116] 'The FIM [*Fraud Investigation Manual*] is Centrelink's mandated policy and practices manual. All fraud investigators are expected to follow it', Centrelink advice to the ANAO, 15 February 2010.

[117] In June 2010, Centrelink provided additional case-related material in response to the results of a sample of 20 cases reviewed by the ANAO. This material did not change the overall results of the ANAO's case reviews.

legislated safeguards such as the *Freedom of Information Act 1982* (Freedom of Information), the *Privacy Act 1988* and Archival legislation.

4.11 The Commonwealth Ombudsman reported similar findings to those identified in this report in regard to a Centrelink customer's request for copies of her records under Freedom of Information. The Ombudsman's report raised a number of issues and also questioned '…the quality control measures employed by Centrelink to ensure proper oversight of its fraud investigations'.[118]

4.12 Most investigations undertaken by Centrelink are desk-based, using administrative coercive information-gathering powers to collect evidence. The ANAO's case reviews found that only a small proportion of fraud investigation cases referred to the CDPP had used criminal investigative techniques such as surveillance (five per cent) or formal customer interviews (23 per cent). Furthermore, there was insufficient evidence on file to support third party checks including when a written Legal Notice was issued. In all instances there was no supporting Critical Decision Record (CDR - a mandatory requirement in the FIM) approving the decision to send the Legal Notice. During 2008–09, CDRs were the single quality control point in the investigative process that Centrelink had implemented.

4.13 Most of Centrelink's controls in the investigative process are procedural and designed to ensure that Centrelink staff adhere to both written standards and internal policy advice. However, the absence of appropriate oversight of decision-making throughout fraud investigations and lack of hard-coded controls in FICMS means the capacity of the FIM and the FICMS to control workarounds and non-compliance are limited.[119] This situation, coupled with the poor documentation to support decision-making, undermines Centrelink's ability to be confident that its practices meet legislated requirements and that external fraud is being effectively managed.[120]

---

[118] Commonwealth Ombudsman, *Centrelink and Commonwealth Director of Public Prosecutions, Review of Circumstances Leading to a Conviction*, May 2010, Part 2, paragraph 2.45 available from <http://www.ombudsman.gov.au/files/onlineCentrelink-DPP_fraud-conviction.pdf> [accessed 8 June 2010].

[119] This is consistent with the findings of an Ernst and Young independent evaluation of FICMS conducted in 2006, *Evaluation of Centrelink's Fraud Investigation Case Management System, Final Report*, Ernst & Young, 2006.

[120] This is consistent with the findings of an Ernst and Young independent evaluation of FICMS; *Evaluation of Centrelink's Fraud Investigation Case Management System, Final Report*, Ernst & Young, 2006.

Centrelink's Fraud Investigation Case Management System

4.14 The Guidelines require agencies to have a system in place to manage fraud information that is reliable and up-to-date to support sound decision-making. The AGIS also requires agencies to have a case management system in place to record allegations of fraud and to ensure investigations are managed in a uniform, systemic manner. Centrelink implemented FICMS in 2005 to ensure consistency and transparency throughout the investigative process and to meet the AGIS requirements of a case management system. The FICMS was designed to record data and documents, and to enable statistical analysis of investigation issues and trends.

4.15 Centrelink's policy for initial receipt and assessment of allegations that was in place in 2008–09 states that all cases that satisfy the *National Case Selection Guidelines* (NCSG) are to be investigated, thus accepted into and activated in FICMS, and this creates a case record for the investigation in FICMS.[121] Table 4.2 outlines the results of the ANAO's case reviews in regard to both the reliability of the data, and the limitations of FICMS, Centrelink's tool for case managing fraud investigations.

Table 4.2

Limitations of Centrelink's Fraud Investigation Case Management System

External and internal requirements	Findings	Impact on fraud case management
Fraud investigation case management should comply with the AGIS and Centrelink's business processes.	The FICMS does not align with Centrelink's business processes. Decisions made during investigations were not consistently recorded.	There was insufficient information recorded in most cases in the FICMS and accordingly, decision-making was not transparent and did not consistently comply with the AGIS or Centrelink's business processes in the FIM.

[121] Centrelink, *Fraud Investigation Manual*, Receipt of, and Initial Assessment of, Allegation in FICMS, May 2009, p. 2. This policy document was redrafted in January 2010.

External and internal requirements	Findings	Impact on fraud case management
Fraud investigations are case-managed in a uniform and consistent manner.	Fraud investigation case management practices were not consistent resulting in unreliable information in FICMS.	The outcomes of fraud investigations were often inconsistent in regard to the seriousness of the alleged fraud, and the evidence on file and the reasons for decisions were in many cases, undocumented and unclear.
Fraud investigations are subject to control and an appropriate level of managerial oversight.	40% of cases had no recorded outcome in FICMS.	More than a third of cases had not recorded whether the case was referred or not referred to the CDPP.[122] FICMS controls are limited and mainly procedural. Critical decision quality control points (the single established quality control point in the investigative process in 2008–09) are not being adhered to throughout the investigation and oversight of decision-making is limited.

[122] Centrelink stated that this is because many of the investigations case-managed in FICMS by fraud investigators are actually compliance reviews (not fraud investigations) and a DOC. (document that outlines the outcome in the customer's record in the Mainframe) is either not required for these compliance reviews, or the information advising of the outcome of the reviews can be saved in another system (e.g., the IRS). This is not consistent with the Commonwealth's regulatory framework for managing fraud investigations including the AGIS, or Centrelink's own policies and procedures in its FIM.

External and internal requirements	Findings	Impact on fraud case management
Record keeping should be of a standard that supports decision making.	Many cases had minimal information recorded in FICMS.	FICMS case note entries are limited to 250 characters and, therefore, are not always clear or comprehensive. This includes the lack of contemporaneous notes such as records of correspondence sent, discussions, decisions, events such as telephone and other informal interviews and actions as they occur, which are not consistently recorded in FICMS.[123] FICMS records were not created for every customer (e.g., cash economy operations were generally a single file for several customers).[124]
Fraud investigations should be supported by reliable and quality data.	45% of cases that undertook customer interviews had not recorded the date of interview in FICMS.[125] The FICMS case note field has a limited recording capacity.	FICMS data was incomplete and unreliable. In many instances, free text FICMS letters were not saved (or documented on file). The content of most critical decisions uploaded did not meet the standards in the AGIS, were unsigned and/or undated, or not approved by a Case Manager. FICMS case notes were not comprehensive and did not identify the complexities of different cases. For example, debt cases that Centrelink claimed were not fraud investigations were indistinguishable from other cases recorded in FICMS.

[123] In July 2010, Centrelink advised the ANAO that as most investigations are desk based, contemporaneous notes are not generally required and when they are, FICMS case notes are used for this purpose (unless recording cash economy field activities which must be recorded using notebooks). However, many fraud investigations have minimal information recorded in FICMS case notes. This has the potential to impact on investigators who are called upon to give evidence in court, upon which they can rely and requires notes to be recorded when the events are fresh in the investigator's mind (which is consistent with the requirements of the AGIS and the FIM).

[124] Centrelink advised that its current practice is to develop a single investigation plan for each desk based cash economy investigation (that can involve many individual people including Centrelink customers). The ANAO's case reviews identified that some cash economy cases either have no investigation file created or only one file and one FICMS record (covering many individuals). Centrelink's FIM does not differentiate between the requirements for cash economy and all other investigations and the AGIS also requires an investigation plan for each individual.

[125] Centrelink stated that some of these interviews were enquiry interviews rather than formal interviews, which are not required to be recorded in FICMS and do not require the customer to be formally cautioned. However, evidence collected during an interview without a caution being administered and the customer being advised that they have a right to legal representation, will lead to the evidence collected being inadmissible in court proceedings. This issue is relevant to the discussion in footnote 123 also.

External and internal requirements	Findings	Impact on fraud case management
Fraud investigations in FICMS should undergo regular review and quality assurance.	Centrelink had no review or quality assurance processes in place in 2008–09.	There was insufficient information in the FICMS to determine whether decisions were justified and equitable (as required under the *Commonwealth Fraud Control Guidelines 2002*) and a lack of robust review processes supporting quality control and continuous improvement.[126]
Level of financial and human resources should support the investigation.	Most cases had no record of financial and human resource information.	FICMS does not allow for the identification of the appropriate level of financial and human resources that should be allocated to each investigation.[127] Centrelink does not estimate the level of financial and human resources required to efficiently and effectively undertake individual investigations.

Source: ANAO analysis.

4.16 The analysis in Table 4.2 illustrates Centrelink's limitations and the unreliability of the information recorded in the FICMS. In 2006, Centrelink engaged Ernst and Young to conduct an independent evaluation of FICMS, a key component of which was to test FICMS compliance with the AGIS. The evaluation found that the system's operational ability was inefficient and unable to deliver basic investigation and prosecution functions and did not meet the *Australian Government Investigations Standards* (the AGIS).[128] The findings of the evaluation are consistent with the issues identified in this audit report by the ANAO. The Ernst and Young Report used 22 requirements to test the level of FICMS compliance with the AGIS. Of the 22 requirements, FICMS met two. The Ernst and Young Report found:

> ...strong anecdotal and empirical evidence that demonstrates that FICMS is non-compliant with the AGIS. This raises serious governance concerns relating

[126] In 2006, an independent Ernst and Young evaluation of FICMS found that '...the lack of comprehensive 'cradle to grave' case management and of any effective accumulated assessment and review process in relation to fraud investigations significantly affects the quality and accuracy of statistical reporting', *Evaluation of Centrelink's Fraud Investigation Case Management System, Final Report*, Ernst & Young, 2006.

[127] One Centrelink fraud investigation examined in the ANAO's broader sample of 275 case reviews identified the resources required to conduct the investigation. However, Centrelink considers that this is not required as it stated that the resources for individual fraud investigations are costed, approved and allocated through its budget process.

[128] *Evaluation of Centrelink's Fraud Investigation Case Management System*, Final Report, Ernst and Young, 2006, p. 15.

to the current case management of fraud investigations and accurate reporting of outcomes.[129]

4.17 Following the recommendations in the Ernst and Young report—which were designed to provide some immediate improvement in the functionality and useability of FICMS—funding to address the issues was provided in Centrelink's 2006–07 Budget. However, this work did not proceed because Centrelink considered that more effective options might be available.[130] While some changes have since been implemented, the key findings of the Ernst and Young report have not been addressed. Centrelink would benefit from implementing a case management system for fraud investigations, with the functionality and capability to meet the minimum standards for investigations in the AGIS, particularly in regard to investigation management methodologies, more efficient search capabilities, support and monitoring, and quality assurance and reporting.

4.18 The ANAO's case reviews found that many of the shortcomings in Centrelink's FICMS arise because Centrelink staff do not follow internal guidance provided in Centrelink's FIM (and, therefore, the standards in the AGIS). The quality of information in the FICMS would be improved by more robust administrative controls, and an increase in the guidance and oversight of decision-making throughout the investigation process.

4.19 The ANAO interviewed key Centrelink staff with knowledge and experience in the use of the FICMS. Centrelink's Business Integrity area in the National Support Office (NSO) confirmed that FICMS is unreliable and is not used to measure performance against investigation targets. Fraud control staff working in Centrelink's Business Integrity Network described the FICMS as a case management system that is clearly not able to meet Centrelink's business needs in terms of record keeping and data analysis of investigations.[131]

---

[129] *Evaluation of Centrelink's Fraud Investigation Case Management System*, Final Report, Ernst and Young, 2006, pp. 25–27.

[130] Centrelink, *Business Needs for Fraud Management in Centrelink*, 20 March 2008, p. 7.

[131] The 2006 Ernst and Young evaluation of FICMS made 12 recommendations, the first of which recommended that Centrelink implement: a holistic corporate case management system that ensures every fraud investigation case is assessed comprehensively, is managed to a consistent standard, is conducted in a fair and expeditious manner, and is subject to rigorous continuing quality assurance, *Evaluation of Centrelink's Fraud Investigation Case Management System*, Final Report, Ernst and Young, 2006.

Fraud Investigation Manual

4.20 Centrelink's FIM is an online reference tool containing guidelines, policies and procedures with diagrams showing the options available to investigators, depending on the type of fraud under investigation and the stages in each process. The FIM was primarily implemented to assist Centrelink to meet the requirements of the AGIS and the Guidelines and its legislative and other obligations. The major results of the ANAO's 113 case reviews in regard to compliance with the key elements of Centrelink's FIM and, therefore, the standards in the AGIS and other legislated safeguards included:

- 87 per cent of cases did not meet the FIM and other Commonwealth requirements;
- 100 per cent of cases with a written Legal Notice that require a critical decision to be approved by a Case Manager and documented on file, did not meet this mandatory requirement;
- administrative powers are being used after fraud is *suspected* and in some instances, after the customer has been formally cautioned and interviewed; and
- fraud investigations with clear evidence of criminality and substantial debts are being undertaken under the guise of administrative reviews.

4.21 The administrative controls in Centrelink's FIM were designed to assist Centrelink's fraud investigations to consistently meet external and internal standards. For this reason, they should accurately reflect the requirements prescribed in the Guidelines, the AGIS, the FIM, the *Social Security (Administration) Act 1999* and other legislated requirements. While the FIM is comprehensive, it is unwieldy and not efficient in locating information and processes, and some information is out of date or incomplete.

4.22 Inconsistent case management practices, limitations in the functionality and reliability of the FICMS, the inadequate level of oversight of decision-making throughout the investigative process and non-compliance with the FIM, are factors contributing to the poor results of the ANAO's case reviews. A recent Commonwealth Ombudsman's report highlighted similar issues to this audit, stressing the importance of managing staff that conduct Centrelink fraud investigations and questioning the quality control measures

employed by Centrelink that ensure the proper oversight of its fraud investigations.[132]

Authority and use of Social Security coercive powers

4.23 Under the *Social Security (Administration) Act 1999*, coercive information gathering powers enable Centrelink staff to collect evidence about customers from internal and external sources. Coercive powers can be intrusive and require strict controls around their usage. The Commonwealth Ombudsman has identified the importance of appropriate safeguard controls and oversight when agencies exercise coercive powers, including:

> …the exercise of significant powers is underpinned by high quality internal systems, rigorous decision making, clear policy guidance, effective training, active oversight and quality assurance…[133]

4.24 The case reviews identified that Centrelink staff are using the Social Security coercive powers to gather evidence throughout the investigative process, including after fraud is 'suspected'. The ANAO's case reviews found that coercive powers are being used by Centrelink following acceptance of a case under the NCSG 'where there is sufficient evidence of an offence…for prosecution action'. While this is consistent with the AGIS, this approach and the processes become inconsistent with the AGIS when Centrelink: does not adhere to the formal investigative processes applied to all investigations that are mandated in the FIM; gathers evidence coercively without meeting the standards in the AGIS that apply to collecting and securing evidence; and uses the coercive powers beyond the point at which fraud is suspected (see Chapter 5 for discussion of the use of Centrelink's coercive powers for prosecution purposes).

Debt referrals

4.25 In relation to debts referred for fraud investigation, Centrelink's current guidelines in the FIM state that once 'a suspicion is held…as to the existence of

---

[132] Commonwealth Ombudsman, *Centrelink and Commonwealth Director of Public Prosecutions, Review of Circumstances Leading to a Conviction*, May 2010, Part 2, paragraph 2.45, available from <http://www.ombudsman.gov.au/files/onlineCentrelink-DPP_fraud-conviction.pdf> [accessed 8 June 2010].

[133] Commonwealth Ombudsman, *Lessons for Public Administration: Ombudsman investigation of the referred immigration cases*, Report No.11, 2007, Commonwealth Ombudsman, Canberra. Lesson 1. 'Maintain accurate, comprehensive and accessible records' available from <http://www.ombudsman.gov.au/files/investigation_2007_11.pdf> [accessed 3 March 2010].

criminal conduct', it would be inappropriate to continue to use the powers to collect evidence.[134] In order for cases to satisfy Centrelink's NCSG, including referred debt cases, fraud has to be 'suspected'. Therefore, once cases satisfy the NCSG, Centrelink should not be using its coercive powers, given the current policy framework. Centrelink's oversight of decision-making in regard to this process is not sufficiently robust to provide an appropriate level of assurance.

Scope and use of coercive powers

4.26 During fieldwork interviews with the ANAO, a number of Centrelink investigators reported uncertainty in regard to administrative versus criminal investigations and their role, that is, whether they are review officers or criminal investigators. Centrelink's Litigation area advised that:

> ...the case officer has to use their judgement. It goes back to the experience of investigators and their intuition…Its driven by policy not law…This is a hard thing to train people in.[135]

4.27 The business case for using coercive powers is clearly articulated in Centrelink's FIM and refers to *Scope of Part V of Social Security (Administration) Act 1999 Powers*. However, other related Centrelink advice is not as clear including that covering: the *Scope of Powers: Section 192-196* guidelines and *Third Party Information Gathering Policy* and the scope of powers document should be updated to align with Centrelink's business case and procedural controls. The Scope of Powers guidelines in the FIM were to be updated by 2 June 2008 to include the use of State-based privacy legislation as the appropriate authority for the collection of information, when officers could no longer use the powers in s.192 and s.196. However, Centrelink advised that issues have since arisen with some State Departments and their privacy laws, which have yet to be resolved.

4.28 During interviews with the ANAO, Centrelink staff noted that training is required in the use of the FIM and that the FIM needs to be streamlined to make it simpler and less time-consuming to use. Many staff interviewed consistently reported that they do not use the FIM for these reasons. Stakeholders raised similar issues in regard to the need for Centrelink to

---

[134] Centrelink, *Fraud Investigation Manual,* Third Party Information Gathering Policy, p. 5, 16 October 2007.

[135] Centrelink advice to the ANAO, 13 August 2009.

embrace a more consistent approach to achieving high-quality investigations and prosecution referrals.

Recommendation No.2

4.29 The ANAO recommends that Centrelink reviews the support provided to fraud control staff, paying particular attention to:

- the content of its *Fraud Investigation Manual* to ensure investigation guidelines, procedural controls, processes and practices are clearly articulated and consistent with the *Australian Government Investigations Standards* and Social Security legislation;
- managerial oversight of decision making and documenting of critical decisions throughout the investigative process, including when an administrative investigation transitions to a criminal investigation; and
- the efficiency and useability of Centrelink's fraud-related decision support and reporting systems.

4.30 **Centrelink response:** *Agreed*.

Training and Quality Assurance

Training and qualifications

4.31 All Australian Government agencies managing fraud programs must comply with the Guidelines in meeting mandatory training requirements for fraud investigators and conducting fraud investigations in accordance with the AGIS to ensure all staff working in fraud control programs meet the recognised standards. These responsibilities extend to meeting the Guidelines' competency requirements and *Certificate IV in Government (Investigations)* qualifications for investigators and others working in fraud control.

4.32 Centrelink's Business Integrity Division facilitates two Certificate IV and two Diploma Government workshops in investigations each year to ensure employees obtain their mandatory qualifications within 12 months of commencing in their roles, as per the Guidelines.[136] Notwithstanding, there is

[136] Centrelink was unable to confirm the exact number of staff working in its fraud programs with the required qualifications, or how many were in the process of obtaining a qualification. The staff related data that Centrelink provided in response to the ANAO's survey regarding the audit *Fraud Control Australian Government Agencies,* Audit Report No.42, ANAO, Canberra, 2009–10 and the staff related data provided in response to this audit, were not consistent.

considerable scope to enhance the effectiveness of Centrelink's current fraud control training beyond the requirements of the Guidelines, to improve the controls and practices in order to achieve high-quality fraud investigations and prosecution referrals.

4.33 The Australian Federal Police (the AFP) out-posted officers in Centrelink's Business Integrity Network were consistent in their views about the working practices of Centrelink's Fraud Investigation Teams (FITs). They stated that further training and clarification is needed to fully utilise Centrelink's available resources for fraud investigations. Areas identified by the AFP for consideration were: the implications of an environment where the less complex cases are being referred to the CDPP; the investigation of debt cases that involve low levels of debt and criminality; the formulaic investigative techniques in the FIM and in practice; and occasions when serious criminal behaviour is not followed up because investigation targets have already been met.

4.34 During interviews, stakeholder and Centrelink staff stated that staff working in fraud control would benefit from specialised training in investigation processes and techniques, which will also improve the quality of prosecution briefs referred to the CDPP.[137] Areas of training need identified included: investigation techniques in Centrelink's FIM; ethics, Privacy and Freedom of Information legislated requirements; FICMS and records management practices; required checks and balances in the processes to obtain third party information and documenting evidence; interview techniques; and clarification and training on the use of coercive powers and quality control around the transition from administrative to criminal investigations. Centrelink would benefit from adopting the Administrative Review Council's (ARC) advice that 'for an agency with a large number of officers exercising coercive information gathering powers, development of an accredited training

[137] Areas requiring continued targeted training for Centrelink investigators were identified in the CDPP's and Centrelink's evaluation report of Legal Action on (Centrelink) Serious Fraud cases in 2005–06 including: the evidence required to establish fault elements of the offence; conducting complex investigations such as 'Member of a Couple' relationships; active investigation and interrogation of information; Centrelink systems and interpreting Centrelink data; obtaining evidence by legal compulsion; and conducting a record of interview, *Evaluation Report of Cases Rejected by the Commonwealth Director of Public Prosecutions Based on Lack of Evidence in the 2005–2006 Financial Year*, p. 4.

program specific to the agency would represent good administrative practice'.[138]

4.35 The restructure of Centrelink's Business Integrity Network provides an environment more conducive to improving the level of control around decision-making and to identifying gaps in skills and the corresponding training needs of individuals. Also, the new Business Integrity Network performance agreements introduced in October 2009 include some assessment of an officer's compliance with the requirements of the FIM and the FICMS.

4.36 During the audit, Centrelink advised that it has commenced a review of its current learning and development program for fraud investigators and Intelligence staff and that the purpose of this review is to ensure staff receive ongoing, up-to-date, post-Certificate IV training in Government Investigations or Diploma training. However, the results of the ANAO's case reviews highlight the need for Centrelink to look beyond the minimum training requirements of the Guidelines and to develop more specialised training tailored to Centrelink's operational needs, including key business risks and skill requirements.

4.37 Shortcomings identified in Centrelink's operational practices and skill levels are undermining its controls and guidelines put in place to meet the AGIS and to minimise its exposure to risk. A more planned and strategic approach to training is required for fraud control staff, based on risks identified through quality assurance and other avenues such as internal feedback from fraud investigators and Case Managers, and external feedback such as from the AFP, and in the CDPP case-related correspondence. Stakeholder feedback can help to identify skill gaps and training needs and promote better practice to assist Centrelink in its delivery of consistent and equitable high quality fraud investigations and prosecution briefs. This approach would also help to address the issue of outdated qualifications and skills as the audit fieldwork revealed currency of qualifications to be an issue. The development of a more thoughtful, planned and regular program of specialised training for fraud control staff, including a review of the currency, content and clarity of the policy guidelines in the FIM, will further support these activities.

[138] Administrative Review Council, *The Coercive Information Gathering Powers of Government Agencies*, May 2008, p. xiii, available from <http://www.deewr.gov.au/WorkplaceRelations/Policies/BuildingandConstruction/WilcoxReport/Documents/GatheringPowersGovAgenciesMay08.pdf> [accessed 5 March 2009].

4.38 Centrelink developed a Quality Assurance Program for fraud investigations during the audit, which was to be implemented by 30 November 2009. Implementation of this program will better enable Centrelink to identify and target the training needs of fraud control staff through issues highlighted in the results of the case reviews and other assurance activities.

Training standards for Intelligence staff

4.39 Centrelink advised that the role of its Intelligence teams is not to investigate alleged fraud, rather, it 'is to disprove' the allegations and, therefore, they are not required to meet the training standards in the Guidelines for fraud investigators.[139] However, the Intelligence Assessments in the case reviews revealed that this work involves third party checks with other government agencies and credit companies for which delegated authority is required under the Social Security (Administration) Act. Intelligence Assessment activities can be as intrusive as other investigations and include information such as a detailed personal assessment of a couple's relationship and their financial circumstances. The AGIS also requires evidence collected during initial inquiries to be secured as per fraud investigation standards. Intelligence projects also fall within the meaning of an investigation in the AGIS.[140] There may be benefit in Centrelink's Intelligence teams adopting the key features and better practices of the Guidelines and the AGIS so as to provide a greater level of clarity and assurance around their role.

[139] The term to 'disprove the allegations' suggests there has to be an allegation of fraud that requires investigation in the first instance. If the allegation is found to have substance, the case is referred to the Business Integrity Network for assessment by a Case Control Officer or Manager against Centrelink's *National Case Selection Guidelines*.

[140] The AGIS states that 'an investigation includes intelligence projects, proceeds of crime and financial investigations'.

Recommendation No.3

4.40 To improve compliance with external and internal fraud investigation requirements and the quality of its decision-making, the ANAO recommends that Centrelink:

- increase the level of guidance and oversight provided to support decision-making by fraud investigators throughout the investigative process, from the point of case selection through to finalisation of the fraud investigation; and
- develop a rolling program of specialised training for its fraud control staff that includes regular refresher courses on the policies and procedures in its *Fraud Investigation Manual*.

4.41 **Centrelink response:** *Agreed*.

Quality Assurance Framework

4.42 The Guidelines require agencies to comply with the AGIS. The AGIS sets out the standards required for internal review of investigations. In order to meet the standards in the AGIS, Centrelink is required to have a written procedure in place outlining the internal review process that investigations will undergo whether it involves internal review, evaluation or quality assurance. The purpose of the internal review is to promote continuous improvement and achieve better practice. Agencies are required to publicise the procedures to the relevant areas of the organisation and fraud investigators are to be familiar with, and apply and comply with, the agency's standards.[141]

4.43 At the commencement of the audit, Centrelink advised that it had a three-tiered Quality Assurance Framework in place for fraud investigations. Centrelink advised that this consists of the AFP Quality Assurance Reviews (QARs); critical decision points in an investigation (where approval is required by a Case Manager or equivalent before the investigator can proceed); and a Quality Assurance Program that was still in the early formative stage (in May 2009).[142]

[141] Attorney General's Department, *Australian Government's Investigations Standards*, Introduction, AGD, Canberra, September 2003, pp 4–5.

[142] On 16 February 2010, Centrelink advised the ANAO that its Quality Assurance Program was implemented in November 2009 but Centrelink has yet to provide supporting evidence.

4.44 Under the Guidelines, the AFP is tasked with providing a rolling review of agencies' investigations.[143] The Guidelines also require agencies to comply with the AGIS, which require agencies to implement a Quality Assurance or equivalent process, to achieve continuous improvement and promote better practice.[144]

4.45 The AFP has not conducted a QAR of a Centrelink investigation since May 2007. Prior to this, two QARs (of two separate investigations) were conducted in 2002, which is three AFP QARs in eight years. The AFP conducts around 10 QARs of fraud investigations across APS agencies per year although agencies can negotiate with the AFP if they wish a QAR to be undertaken on a particular investigation.

4.46 During the audit, Centrelink developed a Quality Assurance Program for investigations which was still to be implemented in November 2009. The initial draft indicated that two per cent of investigations would be randomly selected for review. However, Centrelink subsequently advised that the random sample has been revised down to 0.2 per cent. The implementation of a Quality Assurance Program will improve Centrelink's capability to monitor and identify where the significant risks are in achieving Centrelink's focus on serious fraud. The ANAO suggests the Quality Assurance Program be trialled and evaluated after a 12-month period to ensure it is achieving its objectives and to assess whether the sample of 0.2 per cent provides an appropriate level of assurance.

4.47 Other areas of quality control, such as critical decisions, need to have better controls and increased oversight and guidance during decision-making, in order to more effectively manage the process. Centrelink's mandated critical decision policy was part of the suite of information tools implemented in the FIM in September 2007 and during the ANAO's case reviews was the only quality control point in the investigative process that had been implemented by Centrelink. However, the ANAO's case reviews found very few investigation files contained documented critical decisions, or when they did, they were often not approved, were incomplete, or the information was not sufficient to provide the required level of assurance to the approving officer. AGIS requires all agencies investigating cases of fraud to clearly document the

[143] Attorney General's Department, *Commonwealth Fraud Control Guidelines 2002*, AGD, Canberra, p. 26.

[144] Attorney General's Department, *Australian Government's Investigations Standards*, AGD, Canberra, September 2003, paragraph 7.5.

critical decisions. However, the case reviews found Centrelink is not consistently complying with this important standard. Staff would benefit from targeted training in the required processes, content and documentation of critical decisions. More clearly documented critical decisions would better inform the Case Managers (who have responsibility for approving critical decisions) to make reasoned judgements about the decisions and progress of investigations.

5. Referral of Cases to the Commonwealth Director of Public Prosecutions

This chapter examines the effectiveness of Centrelink's referral of fraud cases to the Commonwealth Director of Public Prosecutions for assessment and possible prosecution action.

Background

5.1 The *Commonwealth Fraud Control Guidelines 2002* (the Guidelines) sets out the legislative framework for fraud investigations and case referral standards for the referral of cases to the Commonwealth Director of Public Prosecutions (the CDPP) for consideration of prosecution action.

Prosecution Policy of the Commonwealth

5.2 The independence of the CDPP is grounded through the legislative provisions of the *Director of Public Prosecutions Act 1983*. The CDPP does not have an investigative role. The *Prosecution Policy of the Commonwealth* underpins all of the decisions made by the CDPP and was designed to promote consistency in decision-making.[145] This policy also provides the CDPP with discretion to prosecute or not to prosecute, while seeking to meet standards of fairness, openness, consistency, accountability and efficiency in prosecuting offences and in maintaining public confidence.[146] The *Prosecution Policy of the Commonwealth* guidelines for decision-making state that:

> A prosecution should not be instituted or continued unless there is admissible, substantial and reliable evidence that a criminal offence known to the law has been committed by the alleged offender.[147]

5.3 The CDPP advised that Centrelink referrals make up the largest proportion of its work, around 80 per cent of referrals in 2008–09,[148] which amounts to 75 per cent of all referrals prosecuted 'summarily' and 12 per cent

[145] Commonwealth Director of Public Prosecutions, *Annual Report 2008–09*, p. 5.

[146] Attorney General's Department, *Prosecution Policy of the Commonwealth*, AGD, Canberra, 2008, p. 4.

[147] ibid.

[148] CDPP advice provided to the ANAO, 11 November 2009.

of cases prosecuted on 'indictment'. Centrelink's Annual Report for 2008–09 indicates that 5082 cases were referred to the CDPP. Of these, 3388 were prosecuted and 2973 convicted.[149] Most Centrelink customers plead guilty (98 per cent) and of the cases prosecuted in 2008–09, almost 100 per cent were successful.[150,151]

Memorandum of Understanding

5.4 During 2008–09, Centrelink and the CDPP had a Memorandum of Understanding (MOU) in place which set out each agency's respective roles and responsibilities. The MOU refers to the CDPP's *Centrelink Investigator Manual* which has been superseded by Centrelink's *Fraud Investigation Manual* (the FIM).[152]

5.5 In order for a case to be accepted for referral for prosecution action by the CDPP, briefs of evidence must prove 'intent' beyond reasonable doubt, and have a reasonable prospect of securing a conviction. Accepted case referrals must also be deemed to be in the public interest.

5.6 Centrelink liaises with the CDPP at the national and regional levels and both agencies advise that the relationship is good at the national level. Regional CDPP officers also have productive relationships with their counterparts in Centrelink, particularly since the restructure of the Fraud Investigation Teams (FITs) last year. These relationships are facilitated by the regular liaison meetings between the two agencies. At the regional level, Centrelink fraud staff consult with the CDPP about specific cases and their prospect of being accepted for referral, which is generally on an informal basis, although it can take the form of a formal written request and response.[153] The CDPP provides considerable guidance and assistance to Centrelink fraud staff.

---

149 Another 381 cases resulted in the offence being proven, but no conviction was recorded.

150 *Centrelink Annual Report 2008–09*, p. 39.

151 Data analysis highlights differences in the number of Centrelink fraud prosecutions by State, and the number of convictions applied by the courts – reflecting, in part, the propensity of some magistrates not to record convictions.

152 Centrelink and the CDPP, *Memorandum of Understanding: Centrelink and Commonwealth Director of Public Prosecutions*, August 1999, paragraph 6.1.

153 ibid., paragraph 10.7.

5.7 In order to assess Centrelink's effectiveness in facilitating successful prosecution action, the ANAO examined:

- Centrelink's use of its *National Case Selection Guidelines* (NCSG) and the basis for decisions to select cases for prosecution action;
- Centrelink's collection of evidence for possible prosecution;
- the content and quality of Centrelink briefs of evidence; and
- the feedback and liaison arrangements between Centrelink and the CDPP.

National Case Selection Guidelines

5.8 The ANAO examined the relationship between the decision by Centrelink to select cases for investigation and potential prosecution action. To assist fraud staff in the process of selecting appropriate cases for referral to prosecution, Centrelink, in consultation with the CDPP, developed the NCSG. Under Centrelink's NCSG, all cases which meet any of the following four criteria are to be investigated: recidivist behaviour; where a warning letter has been previously issued; debts over $5000; and serious misconduct requiring the community to be informed.[154]

5.9 The NCSG also refer to 'alleged offenders', implying there must be a suspicion that an offence has been committed for an investigation to be initiated.[155] Centrelink applied its NCSG to cases that were sourced predominately from two of its IT systems: the Integrated Review System (IRS); and the Debt Management System (DMS). Those cases that met the NCSG were then investigated, with some cases referred to the CDPP for consideration of prosecution. Figure 5.1 identifies the fraud case flows (that meet Centrelink's NCSG) from the detection of fraud through to investigation and prosecution. Of the 25 308 cases referred to the FITs in 2007–08 and finalised by 6 August 2009:

- 52 per cent (13 064) were IRS referrals, of which only 3.4 per cent were referred to the CDPP for prosecution; and
- 47 per cent (12 066) were debt referrals, of which 23.2 per cent were then referred to the CDPP for prosecution.

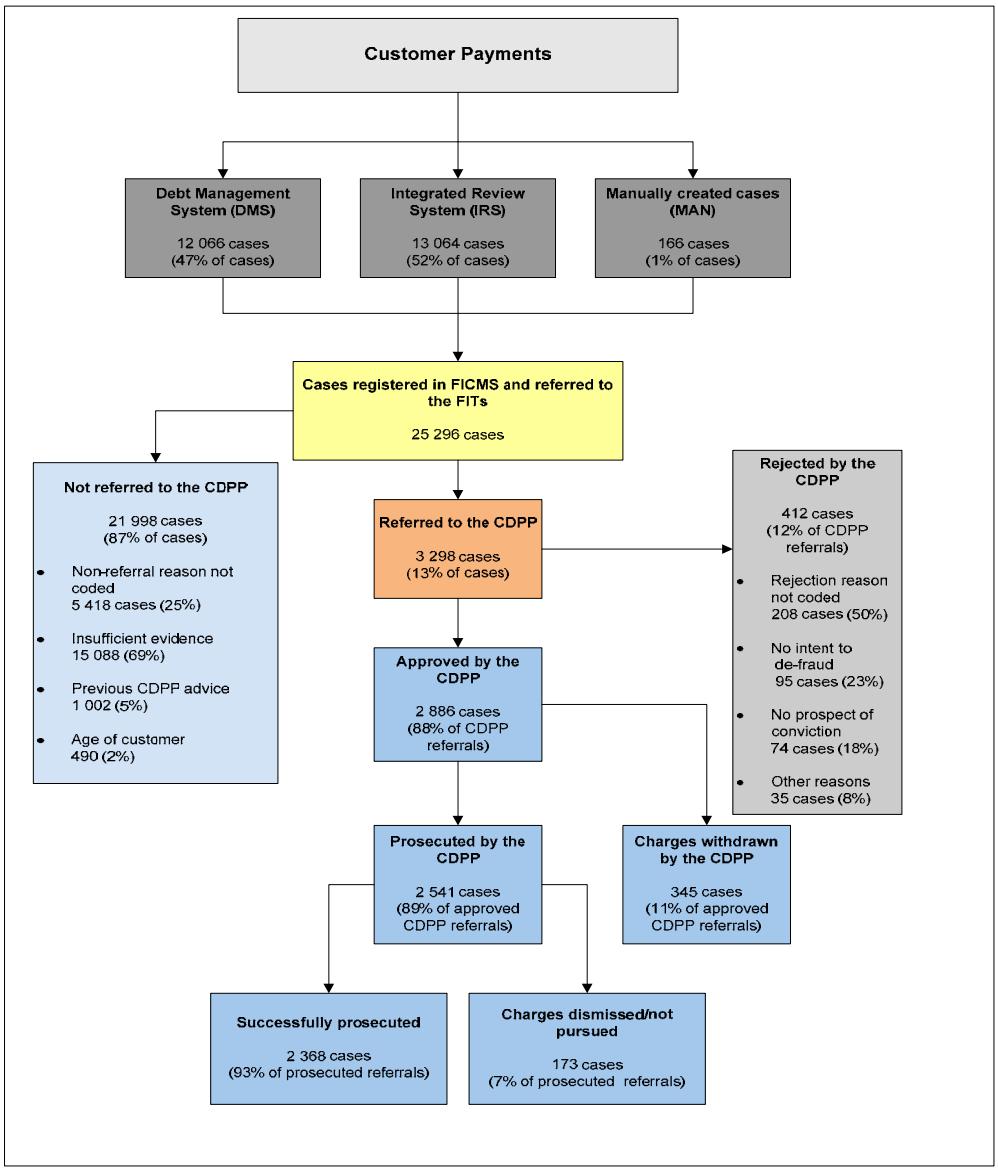
---

[154] Centrelink, *Fraud Investigation Manual*, National Case Selection Guidelines, October 2007, p. 1.

[155] ibid., p. 2.

Figure 5.1

Fraud case flows: detection to prosecution 2007–08



Note: Percentages may not add-up to 100 per cent because of rounding.

Source: ANAO analysis of cases referred for investigation in 2007–08 and finalised by 6 August 2009.

5.10 The ANAO's analysis identified that debt cases were almost seven times more likely to be referred to the CDPP compared to IRS cases. Moreover, 78 per cent of DMS debt cases referred to the CDPP resulted in

successful prosecutions compared with only 23 per cent of IRS cases referred to the CDPP.[156] Consequently, of the 13 064 IRS cases referred to the FITs in 2007–08 and finalised by the date of extraction, only 136 (one per cent) resulted in a successful prosecution where a charge was found to be proved against a defendant. By comparison, of the 12 066 debt cases referred to the FITS in 2007–08 and finalised by the date of extraction, 2184 (18 per cent) resulted in a successful prosecution.

Referring cases for consideration for prosecution by the CDPP

5.11 Until recently, Centrelink fraud investigations were case-managed in stages by different teams. That is, the investigation phase was managed by an officer in one FIT, while the preparation and referral of the prosecution brief of evidence phase was managed by a prosecutions team.[157] Centrelink advised that since late 2008, a Business Integrity Division policy change resulted in all fraud investigations having to be conducted end-to-end by FIT investigators.[158]

5.12 Centrelink's prosecutions teams (in the FITs) are now responsible for investigating and preparing briefs of evidence for the referral of debt cases (and not IRS cases) to the CDPP. Centrelink recently advised that it does not consider DMS debt cases (of suspected fraud) to be fraud investigations and accordingly, staff working in prosecution teams do not have to consistently comply with all of the requirements of Centrelink's FIM and, therefore, the standards in the *Australian Government Investigations Standards* (the AGIS).[159]

5.13 The prosecution teams receive referrals of DMS customer debts to assess their suitability for prosecution action[160] and these are case-managed in Centrelink's Fraud Investigation Case Management System (FICMS) by FIT staff. Debt referrals are generally less complex and are more efficient to process

[156] A 'successful prosecution' is one where a charge/or charges are found proved against a defendant.

[157] Both teams were FITs but each team either had an investigative role or a prosecutions-related role.

[158] On 19 July 2010, Centrelink advised that activities are still transitioning to this model. However, according to the Ernst and Young evaluation of FICMS in 2006, implementation of this model began in 2006, *Evaluation of Centrelink's Fraud Investigation Case Management System, Final Report*, Ernst & Young, 2006.

[159] Centrelink advice to the ANAO, 16 February 2010.

[160] On 16 February 2010 and after the audit fieldwork had been completed, Centrelink advised that it implemented a new procedure on 21 January 2010 (which supersedes this process), whereby automatically detected debt referrals are now considered to be 'intelligence' and will be assessed by Intelligence staff, prior to referral of those debt cases to the FITs that are deemed to warrant a fraud investigation.

than cases directly sourced from the IRS, because they are not subject to the same checks and balances as IRS investigations, particularly in regard to determining 'intent' to defraud even though the outcome for the customer may be the same, that is, prosecution and a conviction for fraud. However, the ANAO's initial sample of 275 cases revealed that while cases can be less complex, debt amounts can be significant.

5.14 The current status of debt referrals contributes to Centrelink's uncertainty around compliance work versus fraud investigation work. The ANAO's data analysis shows that the number of DMS debt cases referred to the CDPP for prosecution action is increasing each financial year. For example, in 2006–07, about a third of Centrelink referrals to the CDPP were debt cases. In 2007–08 debt referrals made up half of all referred cases, and in 2008–09, two-thirds of all cases referred to the CDPP were debt referrals. This situation is considered to be influenced by Centrelink's quantitative fraud targets for investigations and prosecutions designed to meet the savings required by the policy agencies, as these cases are usually less complex to process.

5.15 Once cases are referred to the CDPP for assessment, the CDPP has responsibility for determining which Centrelink cases are prosecuted, in accordance with the *Prosecution Policy of the Commonwealth* and in doing so, seeks to meet principles of fairness, openness, consistency, accountability and efficiency in order to maintain public confidence.[161] However, the ANAO's case reviews identified many cases with significant debts that were resolved through an administrative remedy and were not referred to the CDPP. Instead the outcome of these cases was an administrative recovery of the debt by Centrelink. For example, in 2008–09 less than 20 per cent of Centrelink's fraud investigations resulted in referral to the CDPP, while the remaining 80 per cent were resolved administratively.

5.16 The results of the ANAO's original sample of 275 identified many cases of alleged serious fraud, some with considerable information that suggested 'intent' on the part of the customer. At least one of the cases reviewed met the threshold of each of the 'five pillars'[162], which is considered necessary for a

[161] Attorney General's Department, *Prosecution Policy of the Commonwealth*, AGD, Canberra, 2008, paragraph 1.4.

[162] The 'five pillars' refer to five criteria that need to be proved by Centrelink in order to substantiate that a customer(s) is in a 'Member of a Couple' relationship (previously known as a 'Marriage Like Relationship').

successful prosecution of an allegation of a customer failing to declare that he or she is a 'Member of a Couple'. While these cases received an administrative remedy, they involved high levels of customer fraud and significant debts: in several instances above $100 000.[163] Centrelink subsequently provided additional information in relation to four cases with debts in excess of $100 000, advising that there were extenuating circumstances in some of these cases regarding the investigation outcomes, that is, the decision not to refer the matters to the CDPP. At the time of the ANAO's case reviews, this information was not clearly documented on the relevant investigation files or electronically recorded in FICMS. Given the size of the debts involved, the basis and approval of the decision of non-referral to the CDPP and any extenuating circumstances, should have been clearly documented in all instances.

5.17 While the ANAO understands that all cases will not result in a referral to the CDPP and referral of a matter to the CDPP is a decision for Centrelink, under the *Prosecution Policy of the Commonwealth*, in those matters involving alleged offences of a serious nature that are not referred for consideration of prosecution, the policy requires Centrelink to consult with the CDPP. The ANAO's case reviews identified cases with significant debts and information suggesting 'intent' to defraud the Commonwealth, where Centrelink had made the decision not to refer the case to the CDPP. In these cases, there was no record of this type of consultation occurring between Centrelink and the CDPP after the decision not to refer the case to the CDPP had been made.

5.18 The MOU between Centrelink and the CDPP, also outlines the expectation that Centrelink will seek the advice of the CDPP about the decision of whether to pursue charges where evidence of criminal offences exit, or where there is uncertainty about the existence of a criminal offence.

5.19 The MOU between the agencies states:

> If a matter has been investigated by Centrelink and the investigation has established prima facie evidence of criminal offences, Centrelink will refer the matter to the DPP for a decision on whether charges should be made.

[163] In regard to the AGIS standards, the AFP considered a debt of this dimension should at least be approved 'not to proceed to the CDPP' by an officer at the Senior Executive Service level in Centrelink. See also Footnotes 113 & 114.

> If Centrelink is unsure whether an investigation has established prima facie evidence of criminal offences, it will refer the matter to the DPP for advice.[164]

5.20 Where Centrelink considers that seeking approval from the CDPP is not appropriate in a particular circumstance, this needs to be clearly documented in the critical decision and approved by a Case Manager.

5.21 The ANAO's case reviews also identified cases with debts of around $50 000 and considerably higher that were not referred to the CDPP. The ANAO sought clarification from the CDPP and was advised that it considers the debt amount of $50 000 to be sufficiently serious as to warrant a hearing in a higher court with more severe penalties.[165] The ANAO acknowledges the complexities around investigating cases of serious fraud; however, some of the cases reviewed had the characteristics of being serious fraud at face value and could have been referred to the CDPP for consideration or advice.[166]

Collecting evidence for possible prosecution action

5.22 As indicated in Chapter 4, the *Social Security Act 1991* and the *Social Security (Administration) Act 1999* govern all social security benefit payments made by Centrelink. The Social Security (Administration) Act determines Centrelink's coercive information-gathering powers. This forms an important part of the Centrelink's investigative approach, whereby evidence of customer fraud is gathered.[167]

5.23 Under the legislation governing the use of coercive information-gathering powers, a person can be required to provide information or produce a document that could be relevant to their eligibility to

---

[164] Centrelink and the CDPP, *Memorandum of Understanding: Centrelink and Commonwealth Director of Public Prosecutions*, August 1999, paragraphs 5.1 & 5.2.

[165] CDPP advice to the ANAO, 11 November 2009.

[166] Regular liaison and consultation between Centrelink and the CDPP in more complex cases for pre-brief or legal advice, was a recommendation in the CDPP's and Centrelink's evaluation report of *Legal Action on (*Centrelink*) Serious Fraud* cases in 2005–06, *Evaluation Report* of Cases Rejected by the Commonwealth Director of Public Prosecutions Based on Lack of Evidence in the 2005–2006 Financial Year, p. 4.

[167] *Social Security (Administration) Act 1999*, ss.192–195. Centrelink also has access to coercive information-gathering powers under: *A New Tax System (Family Assistance) (Administration) Act 1999*; the *Student Assistance Act 1973*; and the *Farm Household Support Act 1992*.

receive a social security payment.[168] Failure to provide information to Centrelink once the powers have been exercised is an offence and can potentially result in criminal penalties. The ANAO examined Centrelink's use of coercive information-gathering powers and how the use of these powers affected Centrelink's ability to refer cases of fraud to the CDPP for prosecution action.

5.24 Centrelink FITs are using the full suite of coercive powers under the Social Security (Administration) Act to investigate cases of alleged fraud. However, in some instances, these powers (under ss.192–196) are being used to conduct administrative reviews and investigation of fraud cases simultaneously, and the Business Integrity Network reported considerable uncertainty around the point where an administrative investigation becomes a criminal investigation, and the role of investigators in terms of the use of these powers.

5.25 Once an investigator suspects criminal behavior, information gathered under ss.192–196 Legal Notices cannot continue to be used for criminal prosecution purposes and the various related documents reflect the need for greater clarification in, and consistency between, the FIM guidelines and the business case for fraud staff in relation to this important issue. There is a view that the scope of powers contained in ss.192–196 and their use is permitted for administrative reviews only and should not be used to gather evidence once criminal conduct is suspected. Furthermore, the use of other social security coercive powers to collect evidence from customers may be viewed by a court as inadmissible; due to the fact that a customer could unknowingly incriminate themselves without being made aware (cautioned) that the information provided to Centrelink may be used in criminal proceedings against them. Conversely, if the customer is made aware that the information they provide may be used against them and they refuse, they may be subject to further criminal sanctions for upholding their right to remain silent, while refusing to comply with the coercive powers.

5.26 The Administrative Review Council (ARC) has questioned the validity of the use of coercive information-gathering powers if a person exercises the

[168] Administrative Review Council, *The Coercive Information-Gathering Powers of Government Agencies*, Report No. 48, ARC, Canberra, May 2008, p. 7, available from <http://www.deewr.gov.au/WorkplaceRelations/Policies/BuildingandConstruction/WilcoxReport/Documents/GatheringPowersGovAgenciesMay08.pdf> [accessed 5 March 2009].

common law right of claiming privilege against self-incrimination. The ARC states that the rationale of a claim to privilege:

> …[W]as originally seen as a curb on state power, but the prevailing rationale for it in modern times has expanded to embrace the human rights principles of personal freedom, privacy, dignity and protecting individuals from the power of the state. Among other rationales are preventing abuse of power, maintaining the adversarial system, preventing conviction based on a false confession, protecting the quality of evidence, and avoiding self-accusation, perjury and contempt.[169]

5.27 In regard to this issue, it is the ARC's opinion that the Legal Notices issued by agencies using coercive powers should 'inform notice recipients of their rights in relation to privilege'.[170] The ANAO's case reviews found that in many instances the original, or copies, of the Legal Notices sent to customers were not documented on file, and that the Notices did not provide any information about the customer's right in relation to privilege. For example, the ANAO's case reviews identified cases where investigators informally contacted customers by telephone to clarify issues during fraud investigations, including customers who had previously required an interpreter during meetings with Centrelink. During the audit fieldwork, Centrelink redrafted the relevant policy and instructed staff to cease this practice.

5.28 Centrelink would benefit from adopting the ARC's advice that 'for an agency with a large number of officers exercising coercive information gathering powers, development of an accredited training program specific to the agency would represent good administrative practice'[171] (see Chapter 4 regarding training for staff working in Centrelink's fraud control areas).

5.29 The ANAO's case reviews also found that in many instances the original, or copies, of the written Legal Notices sent to third parties were not documented on the investigation file. In all instances, there were no critical decisions documented on file that approved the decision for a written Legal Notice to be sent to banks, employers and others. In most cases, the response from the recipient to Centrelink was the only evidence on file that a Legal

---

169 Administrative Review Council, *The Coercive Information Gathering Powers of Government Agencies*, Report No. 48, ARC, Canberra, May 2008, p. 46.

170 ibid., p. xv.

171 Administrative Review Council, *The Coercive Information Gathering Powers of Government Agencies*, Report No.48, ARC, Canberra, May 2008, p. xiii.

Notice had been sent. Centrelink would benefit from considering its current practices in relation to the use and scope of its coercive-information gathering powers under ss.192–196 of the Social Security (Administration) Act. Additionally, the legal basis of administrative reviews and fraud investigations being conducted simultaneously, while continuing to interact with customers, needs to be considered in light of better practice and natural justice principles.

Content and quality of Centrelink's briefs of evidence

Short form briefs

5.30 Although Centrelink is not a member of the Heads of Commonwealth Law Enforcement Agencies (HOCOLEA), it uses HOCOLEA policy as a basis in the formation of its own policies.[172] HOCOLEA sets out better practice expectations for agencies in relation to criminal and prosecution action. Similarly, the AGIS also provides agencies with better practice guidance in the preparation and referral of briefs of evidence to be provided to the CDPP.

[172] This is consistent with the directive in the *Australian Government Investigations Standards* that agencies use HOCOLEA policy in the formulation of criminal investigation and prosecution policies.

Table 5.1

Short form briefs of evidence

External and internal requirements	Findings	Implications
Specific agreements about the format and content of short form briefs[173] can be made between the CDPP and Centrelink (the AGIS).	The MOU between the CDPP and Centrelink is high level and does not specify the format and content for Centrelink short form briefs of evidence or the differing jurisdictional requirements of each State and Territory. Centrelink and the CDPP advised that they have negotiated a short form brief, the requirements of which are outlined in the FIM.	There is a risk that the requirements of the FIM in regard to short form briefs of evidence, is not sufficiently robust to protect the rights of the individual and this is compounded by the lack of managerial oversight of the related decision-making throughout investigations. Current Centrelink practices are affecting the transparency related to certain material which may or may not be included and accepted in short form briefs of evidence.[174]
The referral of short form briefs of evidence to the CDPP must contain evidence that is admissible, substantial and reliable (*Prosecution Policy of the Commonwealth,* the AGIS and the FIM).	Admissible evidence, including records of interview and witness statements, are generally not obtained and submitted with short form briefs of evidence, because most customers plead guilty.	Evidence collected using coercive powers may be viewed by a court as inadmissible due to the fact that the customer could have unknowingly incriminated themselves without being made aware. The practice of submitting inadmissible evidence in short form briefs because most customers plead guilty could be perceived as impacting on a customer's right to due process.

[173] Briefs of evidence made to the CDPP can differ in format and content. The AGIS advises that a short form brief should follow the same format as any other brief but unlike full briefs of evidence, short form briefs do not include all of the evidence and exhibits that are required in a full brief. Centrelink and the CDPP have an agreement in place and the FIM outlines the required format and content of both short and full briefs of evidence.

[174] A recent Commonwealth Ombudsman's report (May 2010) questioned the basis of the CDPP's case that resulted in a prosecution of a Centrelink customer, stating that there were flaws in Centrelink's submission to the CDPP and the subsequent decision of the CDPP to prosecute, based on incomplete evidence—*Centrelink and Commonwealth Director of Public Prosecutions, Review of Circumstances Leading to a Conviction*, May 2010.

External and internal requirements	Findings	Implications
Customers should always be offered an interview prior to the referral of their case to the CDPP and there are strict procedures in how these interviews are to be conducted (the FIM, the AGIS and better practice).	The ANAO's case reviews identified five per cent of cases where the customer was formally interviewed.[175] The case reviews also revealed that most interviews were informal and while some records showed the interview occurred (and in some instances brief notes were recorded), there was no caution recorded or comprehensive record of interview.	Centrelink customers facing referral for prosecution action should be provided with the opportunity to attend an interview, wherever possible, prior to referral of the brief to the CDPP. However, requesting an interview prior to referral of a matter to the CDPP appears to be a discretionary decision by Centrelink investigators.[176] The risk of informal notes and conversations (untaped) without a caution has ramifications for the disclosure of the material to the CDPP.[177] Centrelink has a responsibility to ensure the suspect clearly understands the implications of the caution given to them (as required by the *Crimes Act 1914*). Community standards for similar interviews by the police, prior to charges being laid, would generally involve the suspect obtaining legal representation.
All agencies are to have access to up-to-date policies and procedures (the AGIS).	Centrelink's FIM does not contain the different jurisdictional brief of evidence disclosure rules for each State and Territory.	Fraud investigation staff may not clearly understand the evidence disclosure rules for the State or Territory in which they operate. This may affect the quality of the evidence collected and referred to the CDPP.
Witness statements are to be provided with the full form briefs (the FIM).	The CDPP reported that Centrelink has difficulty in producing full form briefs of evidence to the standard of quality that is required including obtaining witness statements.	When a customer pleads 'not guilty', Centrelink must provide the CDPP with a full form brief, as it is disclosed to the defence. This requires witness statements to be obtained in order to support the evidence upon which a case is founded.[178]

Source: ANAO analysis of the results of 113 fraud investigation case reviews.

[175] On 16 February 2010, the CDPP advised the ANAO that in most instances a Centrelink customer facing referral for prosecution action will be provided with the opportunity to attend an interview conducted by Centrelink. However. the CDPP also advised that an offer to attend an interview is usually only accepted by customers in a small percent of cases.

[176] Centrelink, *Fraud Investigation Manual*, Review Finalisation: Customer Notification Policy, 22 May 2009.

[177] Material Centrelink must disclose to the CDPP includes: 'a copy or note of conversations between the investigator and the suspect, whether it was recorded on tape and whether it was accompanied by a caution', Centrelink, *Fraud Investigation Manual*, Brief of Evidence Guidelines, 19 March 2008, p. 5.

[178] Centrelink had to be contacted by the CDPP eight times, before the witness statements were provided in one case, CDPP correspondence to Centrelink, 12 August 2009.

5.31 The standards in the AGIS provide guidance to agencies preparing their own briefs of evidence, as do the CDPP *Guidelines on Brief Preparation.* The short form brief section in both documents states that a short form brief may be provided 'where the defendant has made full admissions in an admissible record of interview'.[179] However, Chapter 6 of the AGIS is subject to any overriding agreement between the CDPP and the agency as to the 'format and content of briefs if there is a conflict between them'. The CDPP informed the ANAO that there is such an agreement in place with Centrelink where the content of briefs can contain admissible as well as inadmissible evidence and full admissions by a defendant are not required.[180] This is not, however, explicitly articulated in the *Brief of Evidence Guidelines* in Centrelink's FIM[181] or the MOU between Centrelink and the CDPP.

5.32 The ANAO's case reviews identified short form briefs on file that consisted of Centrelink debt-related system printouts and third party evidence. This material did not meet the AGIS standard of a fraud investigation, nor the Commonwealth Prosecution Policy of a short form brief where the alleged offender had made full admissions in an admissible record of interview. FICMS data indicates that the most common reason that the CDPP rejected Centrelink cases referred to it in 2007–08 was 'insufficient evidence to establish intent' (around one quarter of referral rejections were for this reason). However, around one half of rejected referrals did not have the reason for rejection recorded in FICMS.

5.33 The minutes of Centrelink's liaison meetings with the CDPP and in CDPP correspondence, issues in regard to the quality of Centrelink briefs of evidence are consistently raised including: incorrect debt schedules; insufficient evidence to support a prosecution; the provision of inconsistent documentation; and the reluctance of Centrelink staff to pursue further evidence in support of a case, after it has been submitted to the CDPP.[182]

---

[179] Commonwealth Director of Public Prosecutions, *Brief of Evidence Guidelines*, April 2003, p. 3; *Australian Government Investigation Standards*, paragraph 6.1.2, 2003.

[180] CDPP advice to the ANAO, 16 February 2010.

[181] The provisions of the *Prosecution Policy of the Commonwealth (*November 2008), and the FIM identify the steps that the CDPP follows in deciding whether to prosecute a case, which states: 'there must be admissible, substantial, and reliable evidence that the alleged offender has committed a criminal offence'.

[182] The ANAO reviewed CDPP case-related correspondence, and nine sets of minutes from the joint Centrelink and CDPP liaison meetings (held between March and August 2009).

5.34 This supports advice provided to the ANAO by Senior CDPP Officers regarding systemic issues in relation to the quality of Centrelink briefs of evidence, particularly debt referred cases. During interviews, the CDPP consistently informed the ANAO that they have to bring Centrelink briefs up to an acceptable standard in many instances, with further evidence often having to be requested. The CDPP's National Office subsequently advised that as well as requesting further material from the investigator, this activity is limited to reorganising briefs of evidence to assist in the analysis of the brief or to fulfil court presentation requirements.[183]

Admissibility and reliability of Centrelink's customer debt records

5.35 Centrelink's short form briefs generally consist of evidence in the form of Centrelink system documentation (screen dumps) of customer records and in many instances, some evidence collected with the use of coercive information-gathering powers. Documents that record a customer's interaction with Centrelink are also included, which are usually admissible (see Table 5.1). However, debt-related documents that are sourced from Centrelink's systems, which in most instances are inadmissible as evidence in court, are also included. Some documentation in the short form briefs related to debt cases does not meet the policy thresholds required of other cases because of the inadmissibility of some of the documents.

5.36 The ANAO's review of Centrelink's internal policies and procedures, CDPP correspondence and minutes of its liaison meetings with Centrelink, the 113 fraud investigation cases and fieldwork interviews found that:

- some of the documents provided in Centrelink's short form briefs are not admissible;
- in most cases, Centrelink refers the total debt amount for all debt(s) raised to the CDPP for prosecution consideration;
- the CDPP often has to recalculate Centrelink-referred debts to determine the actual charge amount based on 'intent'[184];

[183] CDPP advice to the ANAO, 16 February 2010. The ANAO notes that AGIS states that it is the role of the investigator, not the CDPP, to organise the brief of evidence.

[184] The CDPP advised that this is because Centrelink refers the total administrative debt to the CDPP in its prosecution briefs (rather than the actual debt amount where 'intent' has been proved beyond reasonable doubt that is relevant to the alleged offence and supported by the evidence).

- Centrelink's key tool for calculating debts, the Explanation of Mainframe Debt (ADEX) was not designed to calculate debt amounts for prosecution purposes and its use for this purpose is not appropriate; and
- many Centrelink staff working in fraud control do not have the tools and skills to calculate debts, which can be complicated and a time-consuming task.[185]

5.37 According to the *Prosecution Policy of the Commonwealth*, a prosecution should not be instituted unless there is admissible, substantial and reliable evidence that a criminal offence has been committed. The ANAO's analysis suggests that material contained in Centrelink's briefs of evidence is not consistently meeting the requirements of the *Prosecution Policy of the Commonwealth*. This has the potential to severely limit the prospect of defendants, who may be successfully convicted for fraud, being treated in a fair, open and accountable manner. The ANAO notes that almost all of Centrelink fraud defendants plead guilty.

5.38 A recent report by the Commonwealth Ombudsman (May 2010) found that information potentially relevant to an individual fraud case was not presented to the CDPP as part of the prosecution process. In particular, the Ombudsman's view was that 'the information provided by Centrelink was not complete – the CDPP received an incomplete claim form and the electronic records indicated that Centrelink held other documents relevant to…' the case.[186]

5.39 The current Centrelink case management practices in relation to investigation of debt cases and referral of these to the CDPP calls into question whether Centrelink investigators are meeting the AGIS standards of establishing 'intent' in regard to each and every debt raised against allegations of fraud, prior to referring the matter to the CDPP. This is particularly important, given so few suspects are interviewed by Centrelink prior to their case being referred to the CDPP.

---

[185] Centrelink staff reported that the calculation of historical debts requires a client's social welfare payments, including fluctuating income and relationships over time, to be correctly factored in, and that most Business Integrity staff do not have the required level of skill to perform this task adequately.

[186] Commonwealth Ombudsman, *Centrelink and Commonwealth Director of Public Prosecutions, Review of Circumstances Leading to a Conviction*, May 2010, Part 3, paragraph 2.55, available from <http://www.ombudsman.gov.au/files/onlineCentrelink-DPP_fraud-conviction.pdf> [accessed 8 June 2010].

5.40 Where offenders are successfully prosecuted and penalised, any reparation amount is subtracted from the customer's total Centrelink debt. The remaining debt is considered to be administrative and is required to be repaid to the Commonwealth.

5.41 The CDPP's recalculated debt charge amounts can vary widely from the debt amount initially referred by Centrelink. Centrelink fraud investigators should only be referring debt details for the CDPP's consideration that are relevant to the alleged offence,[187] that is, where 'intent' is proven by the supporting evidence. It is not efficient for the CDPP to be recalculating Centrelink debts and Centrelink investigators need to have the appropriate tools and skills to both ensure the evidence obtained proves the elements of the possible offence and to effectively calculate the related debt. The Queensland Office of the CDPP reported that the quality of debt calculations in its State has improved over the past five years owing to the thoroughness of Centrelink's debt calculations in that State.

5.42 To improve the quality of Centrelink briefs of evidence to the CDPP, the ANAO has made four recommendations in this audit (in Chapters 3, 4 and 6) designed to enhance fraud investigators' practices and skills and to improve Centrelink's overall compliance with the AGIS.

Establishing Proof of Identity to support prosecution action

5.43 Establishing the identity of a customer is Centrelink's most important preventative control to ensure benefits are correctly provided. Centrelink uses a tiered Proof of Identity (POI) Model designed to improve deterrence controls for payment integrity in accordance with the *National Identity Security Strategy*.[188]

5.44 The ANAO's case reviews included a check of POI on the 113 customer files, most of which were older files and in poor condition. The case reviews identified that almost one quarter (22 per cent) of the 113 fraud investigation cases it reviewed had insufficient POI to meet Centrelink's POI guidelines and to support informed decision-making regarding eligibility for welfare payments (prior to Centrelink's POI policy change in April 2009).

---

[187] This is consistent with the *Fraud Investigation Manual*, Brief of Evidence Guidelines, 19 March 2008.

[188] COAG, National Identity Security Strategy [Internet]. COAG, 2007, available from <www.coag.gov.au/coag_meeting_outcomes/2007-04 13/docs/national_identity_security_strategy.pdf> [accessed 5 November 2009].

5.45 In April 2009, Centrelink changed its POI policy in order to streamline the POI process and create efficiencies. As a result, POI documents are generally no longer required to be photocopied, certified and placed on the customer file. Instead, customer POI information and photographic identity documents are sighted and directly recorded on the system by the Centrelink officer. The Australian Federal Police (the AFP) has expressed reservations regarding this change to POI procedures, which they believe could significantly increase the risk of ID fraud, and diminish Centrelink's ability to prevent identity fraud in the future. However, Centrelink notes that the new process and the controls put in place were carefully considered to ensure ID fraud did not increase. The CDPP also expressed reservations about the policy change, raising concerns that ceasing to photocopy and retain POI documents on Centrelink customer files at the time of social security claim, will make establishing proof of identity much more difficult, and in some cases impossible, at court appearances. On this basis, the CDPP believe there may be a heightened risk for successful identity fraud prosecutions and recovery of Proceeds of Crime. However, Centrelink advised that its targets are not linked to prosecution outcomes, rather prosecution referrals, and it is the CDPP's responsibility to recover the Proceeds of Crime.

5.46 Centrelink advised that it is continually monitoring the new POI procedures and that the number of ID fraud cases detected and referred for prosecution to the CDPP each year is relatively low (less than three per cent of all referrals).[189] According to Centrelink, the initial results of monitoring the new POI procedures over a four-month period indicates that there will be no adverse effects on Centrelink's ability to trace POI claims.[190] Centrelink also stated that its new approach to sighting and recording POI documentation was designed to provide efficiencies, and improve effectiveness of the control. There is merit in Centrelink continuing to periodically monitor the new policy change over time to determine: whether the change increases the risks of identity and payment fraud; and whether it has any tangible impacts on prosecution outcomes.

[189] Centrelink, *National Prosecution Performance: 2008–09 Referrals to the CDPP*, July 2009, p. 1.

[190] Centrelink advice to the ANAO, 16 February 2010.

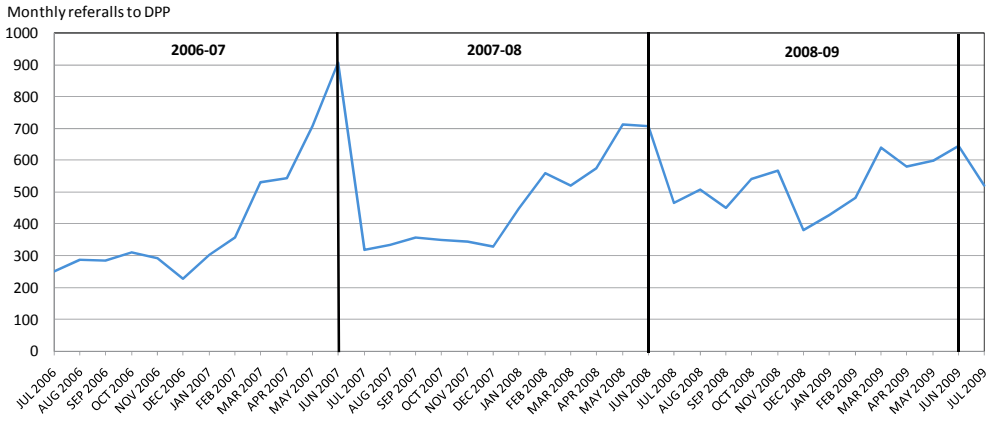
Prosecution referral targets

5.47 The ANAO examined whether Centrelink had targets for referring cases to the CDPP for consideration of prosecution. Table 3.2 in Chapter 3 outlines the numeric prosecution targets. Fraud investigation staff are allocated yearly targets in relation to the number of fraud investigations and prosecutions they need to achieve. During interviews, the CDPP consistently reported that there is a significant spike in the number of referrals to the CDPP from Centrelink towards the end of each financial year.

5.48 Figure 5.2 shows the number of Centrelink fraud prosecution referrals to the CDPP (per month) over the period January 2007 through July 2009. Consistent with advice provided by the CDPP, Figure 5.2 shows that the number of Centrelink referrals to the CDPP rose sharply over the second half of the 2006–07 and 2007–08 financial years, before dropping sharply in the month of July. While an increase in Centrelink referrals to the CDPP was also evident over the second half of 2008–09 (followed by a drop in the month of July 2009), this cyclical pattern was significantly less pronounced than in the preceding years. This is consistent with CDPP feedback provided to the ANAO that Centrelink has improved its management of fraud investigation and referral work flows over recent years.

Figure 5.2

Centrelink fraud prosecution referrals to the CDPP, January 2007 to July 2009



Source: ANAO analysis.

Feedback and liaison

5.49 Feedback provided to the ANAO during the audit indicated that, overall, Centrelink and the CDPP have a good working relationship at the national level while regional liaison is improving at the management level, particularly since the restructure of Centrelink's Business Integrity Network.

5.50 Formal feedback takes place between the CDPP regional offices and respective Centrelink FITs in the form of written correspondence that accompanies a brief of evidence rejected by the CDPP, or when further evidence is required or feedback is provided following prosecution. This advice from the CDPP provides information about the grounds on which the CDPP has made its decision. Centrelink files these letters on the Centrelink investigation file in most FITs. However, there was no mechanism in place to collectively record the substantive reasons for the rejection of cases. This means Centrelink is not utilising the CDPP feedback for continuous improvement purposes such as training and improving the quality of briefs of evidence submitted to the CDPP.

5.51 In one State, Centrelink utilises Technical Officers who evaluate and, in some cases, enhance the standard of briefs of evidence before they are submitted to the CDPP. While the ANAO did not examine the effectiveness of this process, the practice has a range of potential benefits that include improving the effectiveness of liaison and the relationship between both agencies, and familiarising investigators with local jurisdictional requirements and the clearance process for briefs.

6. Performance Information and Reporting

This chapter examines Centrelink's reporting framework for monitoring and improving its performance in managing external fraud. It includes the use of business systems to provide reliable performance information, and examines the effectiveness of Centrelink's performance indicators and targets.

Introduction

6.1 Centrelink's Business Integrity Division is responsible for managing fraud and compliance programs and for having effective information systems in place to collect information and to measure, monitor and report on the performance and effectiveness of Centrelink's fraud programs.

6.2 The ANAO examined the effectiveness of Centrelink's mechanisms that assess and measure its fraud functions and activities. To this end, the ANAO assessed whether Centrelink could demonstrate that:

- fraud data across its systems was consistent and reliable;
- target setting was appropriate and effective;
- the monitoring and reporting of fraud activity was accurate and effective; and
- its fraud programs, including investigations, were cost effective.

Consistency and reliability of fraud data in Centrelink's systems

6.3 Centrelink uses a number of electronic and paper-based systems to collect management information on fraud-related activities. The electronic systems include the:

- Fraud Investigation Case Management System (FICMS);
- Debt Management System (DMS); and
- Integrated Review System (IRS).

6.4 The ANAO considered the links and information flows between FICMS, a purpose built system for recording and case-managing fraud investigations 'whenever situations arise that require direct investigation of

suspected fraud',[191]'[192] and the IRS and the DMS. As illustrated in Figure 3.1, case referral information flows into FICMS from these two sources, with manually referred cases and other cases having to be retrieved from the IRS or DMS respectively.

6.5 These systems provide statistical and other performance reporting information in regard to Centrelink's internal and external reporting requirements. All referrals that satisfy Centrelink's *National Case Selection Guidelines* (NCSG) for investigation and prosecution consideration are activated in FICMS, thus creating a FICMS record.

Ability to account for rejected case referrals

6.6 Centrelink's *Fraud Investigation Manual* (the FIM) policy in relation to the initial receipt of a case in the FICMS Team New Work highlights the risks associated with the work that is rejected out of FICMS at the very first point in the process (prior to assessment) under Centrelink's NCSG. Centrelink's policy in the FIM states that:

> …Due to FICMS capacity limitations, it is not viable to have FICMS records created for all allegations. The…numbers of cases rejected out of FICMS Team New Work cannot be calculated. Some estimates place this as high as 70,000 cases per annum.[193]

6.7 This process undermines the accuracy and integrity of the data and Centrelink's ability to provide assurance around the reliability of the data and its performance reporting. Centrelink advised that FICMS has limited functionality, the data is not reliable and the system is not used to monitor and report on the performance of its fraud investigation program, except for prosecution-related activity.[194]

---

[191] Centrelink, Applications Architecture, *Architectural Review of Business Integrity and Compliance Systems*, v0.7, 1 August 2007, p. 54.

[192] FICMS was developed in-house over four years from 2003, at an estimated cost to Centrelink of more than $3 million. In November 2006, it was evaluated by Ernst and Young. This evaluation found FICMS was not an effective or efficient case management tool for fraud investigations, *Evaluation of Centrelink's Fraud Investigation Case Management System*, Final Report, Ernst and Young, 2006.

[193] Centrelink, *Fraud Investigation Manual*, Receipt of, and Initial Assessment of, Allegations in FICMS, 20 May 2009, p. 2. This policy was subsequently redrafted in January 2010 and the reference to FICMS limitations removed.

[194] In 2006, Centrelink commissioned Ernst and Young to undertake a detailed evaluation of Centrelink's FICMS. The major findings of the report found that FICMS 'is non-compliant with the *Australian Government Investigation Standards* and that there are serious governance concerns relating to 'the... accurate reporting of outcomes', *Evaluation of Centrelink's Fraud Investigation Case Management System*, Final Report, Ernst and Young, 2006.

6.8 While some improvements have since been implemented by Centrelink, the ANAO's analysis of FICMS data confirmed the major findings of the Ernst and Young Report 2006, that is, that FICMS does not support the investigation and prosecution functions and does not meet the standard in the *Australian Government Investigations Standards* (the AGIS) of a case management system for fraud investigations and accurate reporting of outcomes. Funding to address the issues in FICMS was provided in the 2006–07 Budget; however, Centrelink did not proceed with the enhancements because it considered that more effective options may have been available.[195]

6.9 Centrelink uses its IRS system to manage its compliance intervention activity and to report on its fraud investigation performance. While both IRS and FICMS were designed for different purposes, there are discrepancies between the data held in both systems.

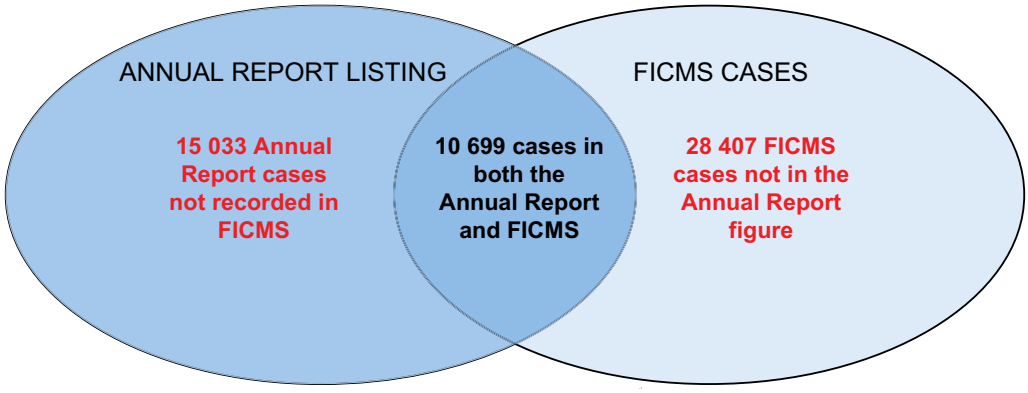
6.10 These inconsistencies are reflected in the 26 084 fraud investigations reported in Centrelink's *Annual Report 2008–09* compared with the 39 106 fraud investigations recorded in FICMS (finalised cases in 2008–09). Of the 26 084 cases reported in 2008–09, 60 per cent were not recorded in Centrelink's dedicated system for case-managing fraud investigations (FICMS).[196] At a minimum, the performance information published by Centrelink needs to be reconcilable in both systems. The inconsistencies between the FICMS and the IRS data are demonstrated in Figure 6.1.

[195] Centrelink, *Business Needs for Fraud Management in Centrelink*, 20 March 2008, p. 7.

[196] Centrelink has not been able to reconcile this data difference.

Figure 6.1

Centrelink's Annual Report 2008–09 fraud investigations matched with FICMS data



Source: ANAO analysis.[197]

6.11 Figure 6.1 illustrates that there are 15 033 'fraud investigations' in the Annual Report listing that do not appear in FICMS, and 28 407 cases in FICMS that are not included in the Annual Report listing. Centrelink advised that fraud investigations are managed from within FICMS but reported from IRS, except for the prosecution reporting that is exclusively from FICMS.[198] Based on this advice from Centrelink, every fraud investigation reported in the Annual Report should be recorded in FICMS.

6.12 In regard to the ANAO's review of 113 investigations, most cases were included in Centrelink's Annual Report listing for 2008–09. However, the 15 DMS cases (in the 113 reviews) that Centrelink had advised were 'fraud investigations' were not included in the Annual Report listing. Of the 15 DMS cases, five were forwarded to the Commonwealth Director of Public Prosecutions (the CDPP) for consideration of prosecution and three were

[197] The ANAO compared the customer record numbers (CRNs) listings that underpinned Centrelink's fraud investigation reporting in its 2008–09 Annual Report and Centrelink's FICMS data which includes the CRN associated with each 'fraud investigation' case recorded in the FICMS.

[198] On 10 March 2010, Centrelink advised that fraud investigation data in IRS (the data used to report the number of fraud investigations in its Annual Reports) that is not recorded in FICMS includes compliance reviews and customers of interest in cash economy operations. This raises further issues for many cash economy customers identified in the case reviews such as the absence of any evidence to warrant a fraud investigation being recorded and reported in Centrelink publications. However, the key differential between the data bases is that they record and report different data, that is, FICMS records fraud investigations and prosecutions, whereas IRS records compliance review activity.

successfully prosecuted for fraud and recoveries were made. This indicates that Centrelink is not accurately reporting fraud investigation activity in its Annual Report.

Target setting

6.13 Performance targets and Key Performance Indicators (KPIs) are a feature of a good reporting framework. Agencies should use well-researched targets that are valid, accurate and measurable and these need to be regularly evaluated to ensure they are targeting customers most at risk of committing serious fraud.[199] The Business Integrity Division is responsible for calculating targets for fraud investigations and prosecution referrals for the Business Integrity Network.

Internal targets

6.14 In 2008–09, Centrelink's targets for the detection and investigation of fraud investigations and the proposed dollar savings to be generated, were calculated via a methodology that included:

- expectations outlined in Budget measures;
- a Resource Allocation Model primarily based on the average staffing level within each Fraud Investigation Team (FIT);
- the use of an electronic 2008–09 Serious Fraud Benchmark Calculator that incorporated formulae including the Government's efficiency dividend and expected dollar savings identified in inter-agency arrangements with program policy departments; and[200]
- pilot projects to measure how many customers needed to be targeted to meet dollar savings and investigation target benchmarks.[201]

[199] Australian National Audit Office, *ANAO Better Practice in Annual Performance Reporting,* ANAO, Canberra, 2004, p. 8.

[200] Centrelink advice to the ANAO, 25 August 2009. On 9 September and 25 November 2009, the ANAO requested an electronic version of Centrelink's Serious Fraud Budget Calculator, which was subsequently provided by Centrelink on 21 July 2010.

[201] Centrelink advice to the ANAO, 25 August 2009.

External targets

6.15 In the setting of targets in 2008–09, Centrelink operated under the previous purchaser/provider arrangements and was required to deliver on the requirements outlined by policy departments.[202] While the policy agencies set the KPIs and savings amount in previous financial years, the ANAO notes that Centrelink developed internal quantitative targets to meet the monetary value of the savings required.

6.16 In 2008–09, Centrelink's Business Integrity Network achieved the dollar savings amount required by the policy agencies without meeting its targets. Since direct appropriation in July 2009, Centrelink has more control over its target setting, and informed the ANAO that it is proposing to be more assiduous in addressing the risks of serious non-compliance. The ANAO notes, however, some categories of the new 2009–10 fraud targets are marginally higher than in the previous financial year. For example, in 2009–10, investigators at the APS 4 and 5 levels have a target of 99 completed fraud investigations per annum, compared to a target of 96 in 2008–09 (see Chapters 3, 4 and 5 for further discussion regarding these targets).

Effectiveness of current targets

6.17 Most of the older cases in Centrelink's 'Comptime' reports are serious fraud cases. Many of these cases are up to one year old, with some more than three years old yet to be finalised. While serious fraud investigations are generally more complicated and take more time to complete, these cases also require the collection of admissible evidence (as discussed in Chapter 3). However, in order to meet targets, Centrelink focuses on the less complex fraud cases.[203] This incentive may explain why many of the old cases in the 'Comptime' reports are the more serious cases of fraud. These circumstances are not consistent with Centrelink's programs and its compliance model, which were designed to focus resources towards the serious end of fraud. These cases are usually more complicated, such as proving a 'Member of a Couple' relationship.

---

[202] Centrelink advice to the ANAO, 16 February 2010. Centrelink also advised that the development of internal targets was required to ensure Centrelink understood targets for both administered and annualised expectations. These methods use different formulae to calculate the targets but are based on the same assumptions

[203] During interviews of Centrelink staff and meetings, including the ANAO's meeting with Centrelink's Executive on 9 October 2009, Centrelink confirmed that the less complex cases are being selected in order to meet targets and, therefore, the required savings.

6.18 The current focus on quantitative targets, rather than qualitative outcomes, is not consistent with Centrelink's compliance model, serious fraud intelligence priorities, case prioritisation and selection policies and its documented approach to fraud control generally.[204] Centrelink has been aware of this situation for several years, that is, the risks of current practices in perpetuating a level of customer intervention that is not aligned with customer behavior. In 2006, an independent evaluation of FICMS found:

> The lack of appropriate systems and processes within FICMS make it impossible to deliver the desired management outcome reports. The problems result from a mix of poor procedures and processes; an excessive focus on auditing investigations with performance measures that often provide little information about the outcomes actually being delivered; limited management flexibility; and lack of oversight by executive management.[205]

6.19 During the ANAO's interviews, both the Australian Federal Police (the AFP) and the CDPP were consistent in articulating concerns about the impacts of the targets which are limiting the types of fraud referred to the CDPP. Moreover, Centrelink's Executive acknowledge that the current focus on quickly finalising less complex cases has the potential to downgrade investigators' skills.[206]

6.20 The recent structural changes to the FITs include greater oversight of decision-making and closer supervision, which have the potential to improve compliance by fraud staff with the FIM and the AGIS. Centrelink has also recently implemented comprehensive performance agreements to improve the quality of investigation outcomes and individual compliance with the FIM, in particular, in relation to the quality and correctness of decision-making. However, to achieve a 'fully effective' performance rating, fraud staff have to achieve their individual performance targets.[207] During ANAO interviews with fraud staff and stakeholders, consistent views were expressed that this

---

[204] On 16 February 2010, Centrelink informed the ANAO that the Business Integrity Division has been progressively seeking to better achieve this balance over the previous years.

[205] *Evaluation of Centrelink's Fraud Investigation Case Management System*, Final Report, Ernst and Young, 2006, p. 18.

[206] ANAO meeting with Centrelink's Executive, 9 October 2009.

[207] On 16 February 2010, Centrelink advised the ANAO that it is not an absolute for staff to meet their targets to achieve a rating of fully effective. However, this requirement is articulated in the individual staff members' 2009–10 performance agreements.

situation is likely to maintain the focus on the less complex cases, at the cost of tackling the more complex, serious fraud cases.[208]

6.21 Many of Centrelink's fraud programs are driven by previous Budget measures that are targeted at a suite of compliance and fraud detection activities. However, it is difficult to determine how Centrelink's current fraud investigation activities relate to those it was originally funded to deliver.[209] Centrelink would benefit from evaluating these programs and analysing the data to measure its effectiveness in achieving the Government's intended outcomes, ensuring new and emerging risks identified through data analysis by the Intelligence teams, are taken into account. In line with this, targets also need to be reviewed to ensure they are effective in targeting serious fraud and achieving the intended outcomes. This will assist the FITs to focus on cases of serious and complex fraud.

6.22 The Business Integrity Division in the National Support Office (NSO) acknowledges these issues and advised it was reconsidering the targets for 2009–10 (provided to the Business Integrity Network in October 2009) and the related staff performance agreements. On 10 December 2009, Centrelink advised that it is considering targeting resources to where fraud is more likely to occur and directing serious cases of fraud to where investigator expertise is located, while DMS debt referrals can be handled by all staff in any location (see also Chapters 3, 4 and 5).

Monitoring and reporting fraud activity

6.23 The *Commonwealth Fraud Control Guidelines 2002* (the Guidelines) require agencies to have a system in place to manage information gathered about fraud against the agency and outlines the types of information agencies are to collect. Reliable performance information, assessment and reporting are critical tools for monitoring and improving performance as they assist agencies

[208] On 16 February 2010, Centrelink advised that a new process for handling DMS debt cases will limit the possibility of staff choosing less complex cases over the more serious cases.

[209] The ANAO requested a list of Centrelink's current and ongoing fraud Budget measures. Centrelink advised that this information is contained in the Department of Human Services *2009–10 Annual Compliance and Performance Plan* which is Cabinet-in-Confidence, so the information is unable to be released.

to identify and address systemic issues relevant to fraud. Reliable information also assists agencies to meet internal and external reporting requirements.[210]

6.24 Centrelink's Business Integrity Division advised that it contributes to three performance related reports a month to Centrelink's Executive and the Chief Executive Officer.[211] To coincide with the audit scope, the ANAO requested these reports for the period November 2008 to January 2009 (that is, nine reports in total). Centrelink could only produce three reports for the period requested. The information related to fraud in these agency reports is minimal and limited to fraud Budget measures.

6.25 The CDPP also provides a monthly report to Centrelink on the status of fraud cases submitted to the CDPP for prosecution consideration.

Internal reporting

6.26 Centrelink's Business Integrity Division also monitors performance through the analysis and preparation of monthly and year-to-date achievements of fraud investigation and prosecution activities, against quantitative performance targets designed to meet the savings amount required by policy agencies. These reports are provided to the Business Integrity Network to keep them informed of their performance against their targets.

'Comptime' reports

6.27 'Comptime' reports are produced by Centrelink's NSO to monitor the number of fraud investigations on hand and the age and type of investigation. These reports are a useful tool for Centrelink's Business Integrity Division and the Network. They provide information on the number of cases each investigator has on hand, the case types and the age of the investigation. The 'Comptime' report of November 2009 shows that most of Centrelink's fraud investigations that are ongoing for more than 12 months are the 'serious' fraud cases, with some cases ongoing for more than three years. This has implications for debts, as they have the potential to accumulate during this period, and is not consistent with the AGIS timeframe standards.

---

[210] Australian National Audit Office, *Better Practice Guide–Annual Performance Reporting*, ANAO, Canberra, 2004, p. 3.

[211] Centrelink advice to the ANAO, 15 February 2010.

6.28 In regard to monitoring the timeliness of fraud investigations Centrelink advised that the 'Comptime' reports are not reliable as the start date of an investigation in IRS may not be accurate. This is based on the start date being triggered in IRS to meet the serious fraud timeliness measures for when a case has to be actioned (which are seven and fourteen days depending on the seriousness of a case). Centrelink advised that this 'start date' in IRS is not a reliable indicator and further checks need to be conducted in the FICMS in order to establish the 'real' start date of the investigation. In addition, there can be a disparity of a year or more, between the 'start' date recorded in IRS (when the case was actioned) and the actual 'start' date the investigation commenced, which is recorded in FICMS. The disparity between the two systems has implications for the transparency and accuracy of internal and external performance reporting in achieving serious fraud timeframes because IRS data is used to report fraud statistics (including those statistics reported in Centrelink's Annual Report) and this information could be misleading.

External reporting

6.29 The Australian Government considers reliable and up-to-date data 'collection on fraud and fraud control activities to be essential to controlling fraud against the Commonwealth'.[212]

6.30 To facilitate the process of annual reporting by the Australian Institute of Criminology (AIC) on fraud control activities (required by the *Commonwealth Fraud Control Guidelines*), agencies have to collect statistical information on fraud for inclusion in the AIC's annual report to the Government. Key information required to be provided by Centrelink includes the outcome of cases investigated such as: the number of cases referred to the CDPP; reasons for non-referral of cases to the CDPP and other outcomes such as administrative remedy; and the outcomes of cases referred to the AFP.[213]

6.31 The ANAO's case studies revealed that key information required to be reported externally and for other reporting purposes, is not consistently captured and recorded in FICMS, such as referral and non-referral of a case to the CDPP. Recording this information in FICMS is a requirement of the

[212] Attorney General's Department, *Commonwealth Fraud Control Guidelines 2002*, AGD, Canberra, p. 28.

[213] In May 2009, the ANAO requested the number of 2008–09 Centrelink case referrals to the AFP. On 26 February 2010, Centrelink advised the ANAO that 37 cases were referred to the AFP during 2007–08 and 25 cases referred in 2008–09. This information is not consistent with the information provided by Centrelink in 2009 in its response to the AIC's survey.

Guidelines and a mandatory requirement of Centrelink's FIM. Of the 113 cases reviewed in FICMS by the ANAO, 40 per cent had no record of whether the case was referred or not referred to the CDPP.

6.32 Centrelink advised the ANAO that fraud statistics from the IRS are used for fraud performance and other reporting, which has to be updated with FICMS data.[214] This is not considered to be an efficient solution. Much of the data required for reporting external fraud to the AIC each year is recorded in FICMS. While FICMS was originally designed to enable statistical analysis and identify trends and systemic issues at both the local and national levels, it is not reliable, accurate, or capable of monitoring and reporting fraud, or providing a complete picture of the effectiveness of Centrelink's fraud control. Centrelink acknowledges that FICMS has limitations[215] and is not an effective information management tool. An independent evaluation of FICMS in 2006 also concluded that FICMS is not an effective case management tool.[216]

6.33 DMS debt referrals make up about 60 per cent of the cases in FICMS. While recorded and case-managed in FICMS, Centrelink does not include most debt referrals in published fraud statistics as investigations, although the majority of Centrelink cases referred to the CDPP and prosecuted are debt cases.

6.34 Centrelink also uses data in FICMS to report the numbers of cases referred to the CDPP and the outcomes, including successfully prosecuted cases. The ANAO examined the 2007–08 FICMS data relating to prosecution referrals and outcomes, and compared it to the figures published in Centrelink's *2007–08 Annual Report*. There is a marked difference between the published and recorded figures, with FICMS recording 3298 referrals to the CDPP in 2007–08 and 2368 prosecutions, compared with the published figures of 5312 referrals and 2658 prosecutions in Centrelink's *Annual Report 2007–08*.[217]

---

[214] Centrelink advice to the ANAO, 10 December 2009.

[215] Centrelink advice to the ANAO, 16 February 2010.

[216] *Evaluation of Centrelink's Fraud Investigation Case Management System*, Final Report, Ernst and Young, 2006, p. 4.

[217] The Ernst and Young report found that the lack of a focused mechanism for fraud management and information reporting compromised the integrity and accuracy of Centrelink's investigation and prosecution statistics and management outcomes, *Evaluation of Centrelink's Fraud Investigation Case Management System*, Final Report, Ernst and Young, 2006.

Performance reporting

6.35 Payment fraud and compliance performance measures are set out in Centrelink's Fraud Control Plan. The performance regime for payment fraud and compliance performance in 2008–09 relates to Centrelink's performance against a range of KPIs contained in the then Business Partnership Agreements (BPAs) with its policy agencies, in particular, BPAs with the Departments of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA) and Education, Employment and Workplace Relations (DEEWR).

6.36 Under the previous BPAs in 2008–09, Centrelink produced Annual Assurance Statements for DEEWR and FaHCSIA that included performance information against KPIs and provided assurance to government, policy departments, stakeholders and customers that Centrelink was meeting performance expectations.[218] The 2007–08 Annual Assurance Statements for FaHCSIA and DEEWR in relation to fraud and compliance showed that Centrelink achieved $1.5 billion in program savings, which was close to its savings benchmark of $1.6 billion, and exceeded the number of fraud and compliance reviews required by both agencies.

6.37 The 2008–09 Assurance Statements showed that Centrelink almost achieved the review targets but was down on the amount of savings it achieved compared to the previous financial year. Furthermore, Centrelink was either close to achieving or exceeded its target for: the number of debts raised; the number of debts under recovery; and the amount of dollars recovered as a proportion of the debts raised.

6.38 The new Bilateral Management Arrangements (BMA) between Centrelink, the Department of Human Services (DHS) and DEEWR, and between Centrelink, DHS and the FaHCSIA, were signed into effect on 24 November 2009. Other than the continued requirement for '95 per cent payment accuracy' using Centrelink's Random Sample Survey (RSS) data, the new set of arrangements with the policy agencies offers no quantitative measures relating to the prevention or deterrence of fraud but rather provides overarching statements of expectations for Centrelink. These include the requirement to implement policies and procedures that focus on and address fraud prevention and deterrence.

[218] Centrelink, *Annual Report 2008–09*, p. 25.

Cost-effectiveness of fraud programs

6.39 The Australian Government invests considerable funding into Centrelink's compliance and fraud detection activities. Sound financial information on the costs associated with fraud control is an important tool for management and accountability purposes. It can provide, alongside non-financial data, a picture of how an agency's fraud control program is operating, including the efficiency of operations and cost-effectiveness. Information on costs can also be used to satisfy external accountability requirements by providing knowledge on what is being delivered and at what cost.

6.40 Practical information on fraud control activities includes: direct and indirect costs when allocated by program; activity costs related to management, prevention, detection, investigation activities and training; costs involved in debt recovery; and recovered debts and savings from fraud and non-compliance activities. Centrelink requires this information in order to measure the cost-effectiveness of its fraud control programs and activities against its KPIs and targets.

6.41 The DHS advised the ANAO that Centrelink spends over $405 million on fraud-related activities.[219] However, Centrelink was unable to confirm this advice or produce an estimated cost of its fraud control program and related activities. Centrelink provided departmental costs for its Business Integrity Division, which has been stable for the past two financial years at around $217 million. Centrelink's Business Integrity Division stated that it does not have a clear understanding of the costs involved in delivering its compliance and fraud control programs, the cost of each program, and does not have a system in place to effectively measure the cost-effectiveness of its fraud programs.[220]

6.42 Centrelink's Business Integrity Division also advised that it cannot provide a definitive breakdown of data such as recovered debts and savings. The ANAO requested specific information previously provided by Centrelink that underpins the DHS *2009–10 Annual Compliance Plan and Performance*

[219] Department of Human Services advice to the ANAO, 4 June 2009.

[220] Centrelink advice to the ANAO, 26 May 2009.

Report.[221] An estimate of debt data was subsequently provided by Centrelink. However, this information was inconsistent with information published in Centrelink's 2007–08 and 2008–09 Annual Reports.

6.43 Centrelink would be better placed to evaluate the effectiveness of its fraud programs if it collected and monitored a breakdown of the costs involved in each program and the savings generated. Such an approach would allow Centrelink to target resources to the most cost-effective outcome. For example, it would allow Centrelink to make informed decisions regarding the most effective strategies for reducing the level of complex and serious fraud, including the relative success of fraud prevention strategies (reducing the potential losses from fraud in the first instance) compared with fraud detection strategies (discovering fraud after it has occurred). This approach would also include Centrelink effectively costing its investigations, in particular, the more complex, resource-intensive operations targeting serious fraud, and reviewing its investigation and prosecution targets to align with its serious fraud priorities.

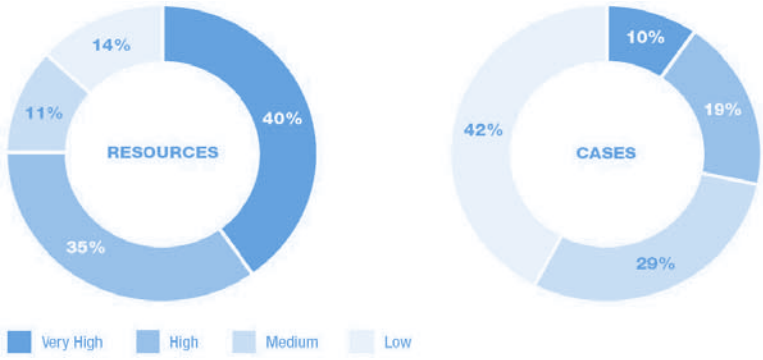
6.44 The AFP uses a Case Categorisation and Prioritisation Model (CCPM) to ensure resources are effectively targeting the highest priority investigations (see Figure 6.2).[222] In deciding to investigate a particular case, the AFP considers: target allocations; AFP investigative and financial resources against identified criminal activity; and related issues.

[221] Department of Human Services, *2009–10 Annual Compliance Plan and Performance Report,* Strategic Fraud and Non-compliance, Canberra, 2009. The department advised that the document remains Cabinet-in-Confidence and it is working on a new compliance plan for 2010–11.

[222] Australian National Audit Office, *ANAO Better Practice–Annual Performance Reporting,* ANAO, Canberra, 2004, p. 15.

Figure 6.2

AFP model to ensure resources are targeted to the highest priority work



Source: *ANAO Better Practice in Annual Performance Reporting,* 2004, p. 15.

6.45 Two of the recommendations in the ANAO's audit report of Centrelink's Tip-off System in 2008–09 identified similar issues with Centrelink's inability to cost its fraud programs and recovered savings and debts. Centrelink, its policy departments and the Department of Finance and Deregulation agreed to the ANAO's recommendations at the time, one of which was to develop a savings methodology that more accurately estimates the savings from fraud programs and improves the reliability of the information required for reporting purposes.

Recommendation No.4

6.46 To improve the quality and reliability of its fraud management-related systems, the ANAO recommends that Centrelink review its standards and procedural controls for the accurate recording, reporting and evaluation of fraud data, to enable:

- investigation timeframes to be monitored, particularly in regard to serious fraud cases; and
- fraud to be more accurately quantified and the cost-effectiveness of Centrelink's fraud control strategies to be assessed.

6.47 **Centrelink response:** *Agreed*.

Ian McPhee
Auditor-General

Canberra ACT
30 September 2010

Appendices

Appendix 1: Agencies' responses to the audit

Centrelink

Centrelink agrees with the recommendations of the audit of its Fraud Investigation Program. These recommendations will assist Centrelink to make further improvements to its framework of compliance strategies and activities to prevent, detect and deter non compliance and fraud.

Centrelink is pleased that the ANAO has acknowledged the work already undertaken to address some of the issues raised in the report. These actions will continue in line with the recommendations. Centrelink is committed to delivering cost effective and well managed processes that support good outcomes for customers and ensure the integrity of government outlays.

Attachment A – Centrelink's response to each of the audit's recommendations

Recommendation No.1
Para 3.54

To facilitate the more effective use of its fraud intelligence capability, the ANAO recommends that Centrelink: review its fraud prioritisation and case selection policies; internal targets; and performance indicators for fraud management; so as to better align these polices and measures with its fraud control strategies.

Centrelink response – Agreed.
Centrelink commenced this process in January 2009 and continues to implement changes in line with this recommendation.

Recommendation No. 2
Para 4.29

The ANAO recommends that Centrelink reviews the support provided to fraud control staff, paying particular attention to:

- the content of its *Fraud Investigation Manual* to ensure investigation guidelines, procedural controls, processes and practices are clearly articulated and consistent with the *Australian Government Investigations Standards* and Social Security legislation;
- managerial oversight of decision making and documenting of critical decisions throughout the investigative process, including when an administrative investigation transitions to a criminal investigation; and

- the efficiency and useability of Centrelink's fraud-related decision support and reporting systems.

Centrelink response – Agreed.

Recommendation No. 3
Para 4.40

To improve compliance with external and internal fraud investigation requirements and the quality of its decision-making, the ANAO recommends that Centrelink:

- increase the level of guidance and oversight of decision-making provided to fraud investigators throughout the investigative process, from the point of case selection through to finalisation of the fraud investigation; and
- develop a rolling program of specialised training for its fraud control staff that includes regular refresher courses on the policies and procedures in its *Fraud Investigations Manual*.

Centrelink response – Agreed.

Recommendation No. 4
Para 6.46

To improve the quality and reliability of its fraud management-related systems, the ANAO recommends that Centrelink review its standards and procedural controls for the accurate recording, reporting and evaluation of fraud data, to enable:

- investigation timeframes to be monitored, particularly in regard to serious fraud cases; and
- fraud to be more accurately quantified and the cost-effectiveness of Centrelink's fraud control strategies to be assessed.

Centrelink response: – Agreed

Australian Federal Police

I would like to advise you that the Australian Federal Police has studied the proposed findings as referred under Section 19 and has no additional comments to add to them.

Commonwealth Director of Public Prosecutions

The Commonwealth Director of Public Prosecutions provided specific comments of an editorial nature in relation to Chapter 5 of the proposed report.

Appendix 2: Roles and responsibilities in the Bilateral Management Arrangements between Centrelink, the Department of Human Services and the policy agencies

Bilateral Management Arrangement between Centrelink, DHS and DEEWR

FaHCSIA	As a policy department providing policy advice and legislative clarification, also engaging with DHS/Centrelink to ensure that service delivery and program design and development are complementary for the achievement of program outcomes. The Minister for FaHCSIA is responsible for its administered appropriation and related outcomes.
DHS	As the policy department responsible for developing service delivery policy; and as a partner with Centrelink in the delivery of payments and services, it also has a role in monitoring and reporting on Centrelink's performance against its operating budget and expected service delivery outcomes.
Centrelink	As the service delivery agency for payments and related services in accordance with policy and legislative requirements; including the correct application and use of administered appropriation. It also, through its engagement with policy departments jointly with DHS, ensures that service delivery and policy design and development are complementary for the achievement of program outcomes.

Bilateral Management Arrangement between Centrelink, DHS and FaHCSIA

DEEWER	As a policy department responsible for its policy outcomes, policy design and legislative clarification, engaging with DHS/Centrelink to ensure that service delivery approaches and program design and development are complementary for the achievement of policy and program outcomes. DEEWR sets out the service delivery approaches for its employment services and other program providers. Due to the close connection between Centrelink and employment services, DEEWR has a role in describing what is required of Centrelink in relation to its interactions with providers to give certainty about provider business operations and to ensure policy objectives are met. DEEWR's Portfolio Minister is responsible for its administered appropriation and related outcomes.
DHS	As the policy department responsible for developing service delivery policy; and as a partner with Centrelink in the delivery of payments and services, it also has a role in monitoring and reporting on Centrelink's performance against its operating budget and expected service delivery outcomes.
Centrelink	As the service delivery agency for payments and related services in accordance with policy and legislative requirements; including the correct application and use of administered appropriation. It also, through its engagement with policy departments jointly with DHS, ensures that service delivery and policy design and development are complementary for the achievement of program outcomes.

Note: These arrangements were not dated and some of the parts were still in draft or yet to be drafted as at 23 November 2009.

Appendix 3: Previous ANAO audits related to fraud control

- Australian National Audit Office, *Fraud Control in Australian Government Agencies,* Audit Report No.42, ANAO, Canberra, 2009–10;
- Australian National Audit Office, *The Australian Taxation Office's Management of Serious Non-Compliance,* Audit Report No.34, ANAO, Canberra, 2008–09;
- Australian National Audit Office, *Centrelink's Tip-off System*, Audit Report No.7, ANAO, Canberra, 2008–09;
- Australian National Audit Office , *Management of Customer Debt-Follow-up Audit*, Audit Report No.42, ANAO, Canberra, 2007–08;
- Australian National Audit Office, *Proof of Identity for Accessing Centrelink Payments*, Audit Report No.8, ANAO, Canberra, 2007–08;
- Australian National Audit Office, *Assuring Centrelink Payment – The role of the Random Sample Survey Programme*, Audit Report No.43, ANAO, Canberra, 2005–06;
- Australian National Audit Office, *Integrity of Electronic Customer Records (Centrelink)*, Audit Report No.29, ANAO, Canberra, 2005–06;
- Australian National Audit Office, *Management of Customer Debt (Centrelink)*, Audit Report No.4, ANAO, Canberra, 2004–05; and
- Australian National Audit Office , *Survey of Fraud Control Arrangements in APS Agencies*, Audit Report No.14, ANAO, Canberra, 2003–04.

Appendix 4: Centrelink's Strategic Directions for 2008–09

Purpose

The Purpose describes the organisation's reason for being. It goes beyond making decisions, delivering services or being cost effective and is not limited to our current capacity or capability. Centrelink's purpose is*: serving Australia by assisting people to become self-sufficient and supporting those in need.*

Core Values

Core values are the essential and enduring building blocks of an organisation. Centrelink is bound by and actively supports the APS Values. Values shape the way we think, the things we do, and how we are perceived. They are the things we stand for. We value:

- Responsiveness to the Government of the day

Actively work with Government, directly and through our client agencies and other stakeholders to deliver the government's agenda.

- Excellence in service delivery

Constantly striving to improve our service delivery to be part of the world's best Government service delivery system.

- Respect for customers and each other

Behaving professionally and impartially in all interactions.

- Accountability

Accepting responsibility for what we do and are transparent in our conduct.

Strategic Themes

The high level of focus that integrates issues, opportunities and information from the internal and external environment. A theme is a succinct statement that provides a medium to long-term focus for Centrelink's strategic implementation efforts.

- Building confidence in Centrelink

To provide assurance to Government, clients and customers that services are fairly, effectively and efficiently delivered.

- Strengthening our customer focus in line with Government direction

To build and leverage off our strong customer focus when delivering government policies and agendas.

- Developing a networked organisation

To link with others inside and outside the organisation to provide quality outcomes and seamless service for our customers.

- Building capability for Government

To have the right resources and underlying capability to progress the Government's agenda on an ongoing basis and in times of crisis.

- Demonstrating value for money

To be accountable for the efficient use of resources and ensuring the best service offer at the best price.

Strategic Priorities

At all levels there are priorities that we have to work on to achieve our purpose. It is important we ensure our priorities are understood and progressed to support the Government's agenda through our strategic themes.

The Strategic Priorities reflect the most important things at an organisational level that need to be done. These are variable and current and for this reason are reviewed regularly.

The 2008–09 Strategic Priorities are:

- build capability and support our people to deliver the Government's priorities;
- improve the customer experience;
- support the Minister and the Department of Human Services to improve service delivery;
- demonstrate united leadership;
- prepare for increasing integration with Human Services agencies;
- ensure effective and efficient delivery of services; and
- strengthen relationships with local communities.

Appendix 5: Centrelink's key industry stakeholder relationships

Agency	Frequency of meetings	Purpose
Department of Education, Employment & Workplace Relations	Quarterly	Joint Agency Strategic Cash Economy Working Group (JASCEWG)
Australian Crime Commission	Bi Monthly	Joint Agency Strategic Cash Economy Working Group (JASCEWG) Financial Intelligence Analysis Team – Joint Management Group
Child Support Program	Monthly	Joint Agency Strategic Cash Economy Working Group (JASCEWG) Portfolio data acquisition working group Portfolio intelligence cell working group
Department of Immigration and Citizenship	Quarterly	Joint Agency Strategic Cash Economy Working Group (JASCEWG) Senior Intelligence Officers Group
Australian Fisheries Management Authority	Quarterly	Joint Agency Strategic Cash Economy Working Group (JASCEWG)
Medicare Australia	Monthly	Joint Agency Strategic Cash Economy Working Group (JASCEWG) Portfolio data acquisition working group Portfolio intelligence cell working group
Australia Federal Police	Bi Monthly	Financial Intelligence Analysis Team – Joint Management Group AFP out-posted Officers Conference Senior Intelligence Officers Group
Australian Securities and Investments Commission	Bi Monthly	Financial Intelligence Analysis Team – Joint Management Group Senior Intelligence Officers Group
Australian Taxation Office	Bi Monthly	Financial Intelligence Analysis Team – Joint Management Group Joint Agency Strategic Cash Economy Working Group (JASCEWG) Senior Intelligence Officers Group
Australian Customs Service	Quarterly	Financial Intelligence Analysis

		Team – Joint Management Group Senior Intelligence Officers Group
Department of Veteran Affairs	Monthly	Portfolio data acquisition working group Portfolio intelligence cell working group
Department of Human Services	Monthly	Portfolio data acquisition working group Portfolio intelligence cell working group
New South Wales Crime Commission	Bi Monthly	Senior Intelligence Officers Group
AUSTRAC	Bi Monthly	Senior Intelligence Officers Group
New South Wales Police	Bi Monthly	Senior Intelligence Officers Group
Commonwealth Director Public Prosecutions	Monthly	National liason/issues
Australian Federal Police	Bi Monthly	AFP out-posted officers
Criminal Assets Liaison Group	Proceeds of Crime	Proceeds of Crime matters

Source: Centrelink advice 10 November 2009.

Series Titles

ANAO Audit Report No.1 2010–11
Implementation of the Family Relationship Centres Initiative
Attorney-General's Department
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.2 2010–11
Conduct by Infrastructure Australia of the First National Infrastructure Audit and Development of the Infrastructure Priority List
Infrastructure Australia

ANAO Audit Report No.3 2010–11
The Establishment, Implementation and Administration of the Strategic Projects Component of the Regional and Local Community Infrastructure Program
Department of Infrastructure, Transport, Regional Development and Local Government

ANAO Audit Report No.4 2010–11
National Security Hotline
Australian Security Intelligence Organisation
Attorney-General's Department
Australian Federal Police

ANAO Audit Report No.5 2010–11
Practice Incentives Program
Department of Health and Ageing
Medicare Australia

ANAO Audit Report No.6 2010–11
The Tax Office's implementation of the Client Contact - Work Management - Case Management System
Australian Taxation Office

ANAO Audit Report No.7 2010–11
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2009 Compliance)

ANAO Audit Report No.8 2010–11
Multifunctional Aboriginal Children's Services (MACS) and Crèches
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.9 2010–11
Green Loans Program
Department of the Environment, Water, Heritage and the Arts
Department of Climate Change and Energy Efficiency

Current Better Practice Guides

The following Better Practice Guides are available on the Australian National Audit Office website.

Strategic and Operational Management of Assets by Public Sector Entities –	
Delivering agreed outcomes through an efficient and optimal asset base	Sep 2010
Implementing Better Practice Grants Administration	June 2010
Planning and Approving Projects	
an Executive Perspective	June 2010
Innovation in the Public Sector	
Enabling Better Performance, Driving New Directions	Dec 2009
SAP ECC 6.0	
Security and Control	June 2009
Preparation of Financial Statements by Public Sector Entities	June 2009
Business Continuity Management	
Building resilience in public sector entities	June 2009
Developing and Managing Internal Budgets	June 2008
Agency Management of Parliamentary Workflow	May 2008
Public Sector Internal Audit	
An Investment in Assurance and Business Improvement	Sep 2007
Fairness and Transparency in Purchasing Decisions	
Probity in Australian Government Procurement	Aug 2007
Administering Regulation	Mar 2007
Developing and Managing Contracts	
Getting the Right Outcome, Paying the Right Price	Feb 2007
Implementation of Programme and Policy Initiatives:	
Making implementation matter	Oct 2006
Legal Services Arrangements in Australian Government Agencies	Aug 2006
Administration of Fringe Benefits Tax	Feb 2006

User–Friendly Forms Key Principles and Practices to Effectively Design and Communicate Australian Government Forms	Jan 2006
Public Sector Audit Committees	Feb 2005
Fraud Control in Australian Government Agencies	Aug 2004
Better Practice in Annual Performance Reporting	Apr 2004
Management of Scientific Research and Development Projects in Commonwealth Agencies	Dec 2003
Public Sector Governance	July 2003
Goods and Services Tax (GST) Administration	May 2003
Building Capability—A framework for managing learning and development in the APS	Apr 2003
Performance Information in Portfolio Budget Statements	May 2002
Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	June 2001
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Commonwealth Agency Energy Management	June 1999
Controlling Performance and Outcomes	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997