The Auditor-General
Audit Report No.26 2001–2002
Performance Audit

Management of Fraud and Incorrrect Payment in Centrelink

Australian National Audit Office

ISSN 1036-7632

ISBN 0 642 80607 1

Australian National
Audit Office

Canberra ACT
14 December 2001

Dear Madam President
Dear Mr Speaker

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

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

Yours sincerely

P. J. Barrett
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. 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 Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

Auditor-General reports are available from Government Info Shops. Recent titles are shown at the back of this report.

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

Steven Lack
Ann Thurley
Alex Wilkinson

Contents

Abbreviations

AAT	Administrative Appeals Tribunal
ABC	Activity Based Costing
ABN	Australian Business Number
ABS	Australian Bureau of Statistics
ACM	Accelerated Claimant Matching
APS	Australian Public Service
AFP	Australian Federal Police
AFPO	Australian Federal Police Outposted Officer
APO	Area Privacy Officer
ARO	Authorised Review Officer
ASIC	Australian Securities and Investment Commission
ASO	Area Support Office
ASX	Australian Stock Exchange
ATO	Australian Taxation Office
BAS	Business Activity Statement
BPA	Business Partnership Agreement
CASPO	Centrelink / ATO Special Project Officers
CRAM	Customer Records Access Monitor
CSDA	*Commonwealth Services Delivery Act 1997*
CEO	Chief Executive Officer
CSA	Child Support Agency
CSC	Customer Service Centre
CSO	Customer Service Officer
DART	Detection and Review Team
DETYA	Department of Education, Training and Youth Affairs
DEWRSB	Department of Employment, Workplace Relations and Small Business
DIMA	Department of Immigration and Multicultural Affairs
DMP Act	*Data-matching Program (Assistance and Tax) Act 1990*

DPP	Director of Public Prosecutions
DSP	Disability Support Pension
EBT	Electronic Benefit Transfer
EII	Enhanced Investigation Initiative
ESD	Electronic Service Delivery
FaCS	Department of Family and Community Services
FBI	Federal Bureau of Investigation
FMA Act	*Financial Management and Accountability Act 1997*
FOI Act	*Freedom of Information Act 1982*
FTR Act	*Financial Transactions Reports Act 1998*
ICEFIT	Inter-agency Cash Economy Field Investigation Team
IFT	Identity Fraud Team
IVR	Interactive Voice Response
MLR	Marriage-like Relationship
MOU	Memorandum of Understanding
NSA	Newstart Allowance
NSO	National Support Office
NSRS	National Selective Review System
OECD	Organisation for Economic Cooperation and Development
OTO	One-to-one initiative
PMIS	Prosecutions Management and Information System
POI	Proof of Identity
PPP	Parenting Payment – Partnered
PPS	Parenting Payment—Single
QOL	Quality On Line
RMU	Records Management Unit
ROAM	Review of Activity Management
SAMS	Security Access Management System
SDM	Service Delivery Model
SLA	Service Level Agreement

TDF	Tax File Declaration Form
TFN	Tax File Number
TORS	Tip-off Recording System
UK DSS	United Kingdom Department of Social Security
WebPo	Web Post Office
YAL	Youth Allowance

Summary and Recommendations

Summary

1. The prevention and management of fraud are important issues for the Australian Public Service (APS). Fraud is defined in the draft Commonwealth Fraud Control Policy as '*dishonestly obtaining a benefit by deception or other means*'.[1] The importance of effective fraud control arrangements has also been recognised in legislative provisions in the *Financial Management and Accountability Act 1997* (FMA Act).

2. This audit of Centrelink is one of a series of fraud control audits, including a survey of fraud control arrangements in the APS[2], undertaken by the Australian National Audit Office (ANAO). A list of these audits is at Appendix 1. The audit discussed in this report is complemented by a separate audit of fraud control arrangements in the Department of Family and Community Services (FaCS) which was tabled in June 2001.[3]

3. In its Report No. 385[4], the Joint Committee of Public Accounts and Audit (JCPAA) highlighted the benefits of agencies developing sub-categories of fraud to provide a better understanding of the nature and significance of various types of fraudulent activity. For instance, inappropriate use of information, travel fraud, and identity fraud. This issue will be more fully considered by the ANAO when it develops its Better Practice Guide on Fraud Control in 2002–03 at the completion of this series of fraud audits. The JCPAA requested the ANAO develop sub-categories of fraud for the purposes of fraud reporting, when preparing the Better Practice Guide on Fraud Control.

4. Centrelink was established on 1 July 1997 as the Australian Government's one-stop shop for social security and employment services.[5] It is responsible for the integrated delivery of a wide range of Commonwealth social and economic payments and services and provides services to 6.4 million customers each year, involving nine million benefit payments and an annual cost approaching $50 billion. It employs over 22 000 staff to deliver these services on behalf of 16 Commonwealth

---

1 Fraud Control Policy of the Commonwealth, Attorney General's Department, Consultation Draft, 2000.

2 ANAO Audit Report No.47 1999–2000 *Survey of Fraud Control in the APS Agencies*.

3 ANAO Audit Report No.45 2000–2001 *Management of Fraud Control,* Department of Family and Community Services 2001.

4 Review of Auditor General's Reports, 2000–01, Second and Third Quarters August 2001 Canberra.

5 The *Commonwealth Services Delivery Agency Act 1997* formally established Centrelink on 1 July 1997.

departments and agencies and all State Housing Authorities under formal purchaser/provider arrangements. Centrelink delivers its services through a distributed network of over 1000 sites including 15 Area Support Offices (ASOs), 310 Customer Service Centres (CSCs), 28 Call Centres and about 350 agency arrangements.

5. Centrelink's major purchasers in terms of the value of payments and services delivered on their behalf by Centrelink in 1999–2000 were the Department of Family and Community Services (FaCS), Department of Education, Training and Youth Affairs, Department of Transport and Regional Services and Agriculture, Fisheries and Forestry—Australia.

6. The size, geographical spread and devolved accountability of Centrelink's operations means that there are inherent fraud risks associated with its business, which need to be properly managed.[6] Fraud against Centrelink can be committed externally by individuals seeking to obtain payments they are not entitled to receive or internally by its staff and contractors. To assist in detecting and treating these fraud risks, Centrelink has separated fraud into three distinct categories: program fraud, information fraud, and administrative fraud. Centrelink reports as fraud only those cases successfully prosecuted in a court of law. In 1999–2000, there were 2960 convictions for program fraud involving over $27 million in debts; two cases of administrative fraud involving a total of $1100 in debts and 488 cases of information fraud.

Audit scope and focus

7. Centrelink is a major provider of services on behalf of FaCS. The funding for these services is appropriated to FaCS. Under the FMA Act, Centrelink and FaCS are responsible for promoting the efficient, effective and ethical use of Commonwealth resources. In addition, the *Commonwealth Services Delivery Agency Act 1997* (CSDA Act) defines an important function of the Centrelink Board as ensuring *'that the Agency's functions are properly, efficiently and effectively performed'*.

---

6 Since it was established in 1997, Centrelink has also had the significant task of merging the fraud control regimes of a number of agencies, including integrating the legacy systems of different agencies, while at the same time seeking to continually improve its fraud control systems and practices. A summary of recent developments in fraud control in Centrelink is presented in Appendix 5.

8. FaCS and Centrelink are dependent on each other for delivering a satisfactory level of performance in the area of fraud control. An outcome for both agencies should include effective measures to prevent, detect and treat fraud in order to maintain the integrity of the social security system. The achievement of this outcome within a purchaser/provider relationship calls for a partnership or collaborative approach to achieve the required results.

9. The relationship between FaCS and Centrelink is governed by a Business Partnership Agreement (BPA) which acknowledges joint responsibility for performance. In relation to the management of fraud, the BPA outlines the roles and responsibilities of the two parties. FaCS is responsible for providing Centrelink with appropriate policy advice, direction and support to enable effective service delivery and Centrelink is responsible for implementing strategies for payment control as part of its approach to service delivery.

10. A challenge for both agencies is to successfully interact with each other in the pursuit of the government's fraud control objectives. While FaCS has the primary responsibility for specifying and providing funding for compliance strategies and Centrelink has the role of implementing these strategies and achieving certain performance benchmarks, there is a joint responsibility to meet the wider outcomes that the government is seeking through the FMA Act and the CSDA Act. For example, without feedback from Centrelink, policy-advisers in FaCS may not benefit from the operational experience of understanding what happens when policies are put into practice. Centrelink is also well placed to identify trends and provide statistical information to FaCS and other client agencies that purchase its services and identify where approaches from different government departments need to be harmonised. This joint responsibility was taken into account in the ANAO's recent fraud audit in FaCS and in this audit in Centrelink.

11. Audit Report No.45, *Management of Fraud Control* in the Department of Family and Community Services was tabled in June 2001. The audit examined the arrangements in place for FaCS to manage internal and external fraud and the mechanisms that FaCS had established to obtain assurance regarding the effectiveness of fraud control and incorrect payment in those agencies which deliver services and/or make payments on its behalf, particularly Centrelink.

12. This audit of the Management of Fraud and Incorrect Payment in Centrelink, focuses on Centrelink's arrangements for the prevention, detection and treatment of incorrect payments as a result of fraud and incorrect payment[7] (program fraud). Given that nearly 90 per cent of total payments and services delivered by Centrelink are on behalf of FaCS, the major focus of this audit was the fraud control arrangements put in place for the services provided for FaCS. The audit also examines Centrelink's arrangements to manage internal fraud committed by its staff and contractors (administrative and information fraud).

Audit objective and criteria

13. The objective of the audit was to assess whether Centrelink had implemented appropriate fraud control arrangements in line with the Fraud Control Policy of the Commonwealth and whether these arrangements were operating effectively in practice.

14. The ANAO established a framework for analysing the effectiveness of Centrelink's fraud control arrangements based on whether Centrelink had:[8]

- robust front-end administrative processes for preventing customers as well as staff from obtaining payments and benefits they are not entitled to receive;
- effective mechanisms for detecting, investigating and dealing with customers and staff that obtain payments and benefits they are not entitled to receive;
- a comprehensive performance assessment framework for the compliance and fraud control function;
- arrangements for protecting the confidentiality of customer information; and
- measures for ensuring that administrative funds and Commonwealth property are not misused by Centrelink staff.

---

7 Centrelink can not currently provide separate information on the level of fraud and incorrect payment.

8 The audit criteria were developed from Attorney General's Department guidelines, the Australian Standard/New Zealand standard (AS/NZS) 4360:1999 on risk management and general better practice that has been identified in earlier fraud control audits. Due consideration was also given to standards outlined in the BPA between FaCS and Centrelink.

15. The framework for analysis also included an examination of Centrelink's governance arrangements that are designed to assist the management of its fraud control framework.

Audit approach

16. To achieve the audit objectives, the audit team:

- interviewed key staff in Centrelink's National Support Office (NSO) in Canberra as well as staff in ASOs and CSCs across Australia with fraud control responsibilities;
- held discussions with external agencies such as the Australian Federal Police (AFP) and the Office of the Director of Public Prosecutions (DPP), which provide services to Centrelink in relation to fraud control;
- reviewed Centrelink documents pertaining to fraud control; and
- undertook detailed compliance testing of some key aspects of Centrelink's controls for program fraud to determine the level of compliance with policies and procedures aimed at detecting and treating program fraud.

17. Compliance testing was undertaken in 10 ASOs and incorporated 33 CSCs across Centrelink's service delivery network during audit fieldwork. The Areas and CSCs were selected following discussions with the Australian Bureau of Statistics (ABS) and with the assistance of Centrelink.

18. The sample of Areas and CSCs visited was not designed to provide statistically significant results because information needed to stratify the sample based on likely levels of error across CSCs and payment types was not available. For this reason the data obtained can not be extrapolated to the population. Nevertheless, the sample sizes were selected in such a way to ensure that there were sufficient files reviewed to allow comparisons across payment types as well as CSCs in relation to new benefit claims and to allow comparison across ASOs for tip-off and compliance reviews.

Overall conclusion

19. The ANAO concluded that Centrelink had implemented appropriate fraud control arrangements in line with the Fraud Control Policy of the Commonwealth. This included having a comprehensive planning regime to guide its fraud control program that was based on an appropriate risk assessment process and Fraud Control Plan.

20. Centrelink had a clear focus on preventing fraud and had established appropriate procedures in relation to Proof of Identity (POI) and had made considerable effort to establish the customers' identity up-front. However, there were POI coding errors in 22 per cent of the claims reviewed which adversely impacts on the quality of Centrelink's electronic records. Because of this incorrect coding, the computer-based detection methodologies will not be necessarily able to detect cases of fraud and error. This also leads to additional administrative costs to correct the coding errors.

21. The ANAO concluded that current compliance activities, including an extensive data-matching program, would detect a significant proportion of fraud and error when they occur. Appropriate processes had been established by Centrelink for ensuring that the data-matching it conducts conforms with the requirements of data-matching and privacy legislation. Centrelink conducts more than one million compliance reviews each year, most of which are triggered by data-matching results.

22. At the time of the ANAO fieldwork, there was no regular assessment of the quality of these reviews to identify any that were sub-standard even though the way they are conducted can significantly affect whether the review detects fraud or error. Centrelink advised that, as part of the Getting it Right strategy launched in November 2000, its on-line quality assurance system (QOL) had been enhanced. As well, QOL was to be supplemented by a secondary checking regime to test the quality of review processes.

23. Centrelink has a number of remedies available to treat fraud and error when detected, including breaches, formal warning letters and prosecution. However, the ANAO concluded that breaches and warning and obligation letters were used inconsistently. Centrelink advised the ANAO that a coordinated training package would be delivered during 2001 to assist staff who are unclear about the legislative requirements for imposing breaches to gain the understanding to use such mechanisms consistently. In July 2001, Centrelink also reviewed the content of its warning and obligation letters in conjunction with the Director of Public Prosecutions (DPP) and made appropriate changes to assist consistent usage and Centrelink's ability to follow-up in relation to any subsequent failures on the part of customers to advise Centrelink of changes in circumstances.

24. Centrelink is contracted to implement fraud compliance strategies on behalf of FaCS and to achieve certain performance benchmarks. The performance indicators and targets in the BPA between FaCs and Centrelink should enable Centrelink to monitor and report on the level

and results of its fraud review activity. While the current performance indicators were an improvement on indicators contained in earlier BPAs, the ANAO concluded that the performance indicators continue to place too much emphasis on the number of compliance and fraud reviews conducted rather than on the results of reviews and the effect of review activity.

25. FaCS and Centrelink have recognised the need to shift the focus to reducing fraud and incorrect payment (preventative measures) rather than just detecting it once it has occurred. The ANAO concluded that, deriving an estimate of the level of fraud and error by income support payment type, could also assist Centrelink, in conjunction with FaCS, to develop more meaningful indicators to demonstrate the impact of compliance activities and other relevant factors on the level of losses from fraud and error.

26. Centrelink had only undertaken limited analysis of the large amount of data relating to the review results it collects and of the strategies used to prevent and detect fraud. Work to trial risk profiling of customers was, however, announced in the 2001–02 Budget. Risk of incorrect payment will be one of the key aspects of profiles, which should enable customer contact and reviews to be better targeted at minimising and preventing incorrect payment.

27. The impact of penalties on compliance had not been assessed and it was not possible to determine whether the value of penalties and the circumstances in which they were imposed provided an effective deterrent to non-compliance. This lack of assessment reduced the effectiveness of the targeting of activities to encourage voluntary compliance and thereby improve fraud prevention. Following the fieldwork for this audit, a review of the fraud deterrence framework was announced by FaCS as part of the 2001–02 Budget.

28. The ANAO also considered that only limited action had been taken to evaluate the effectiveness of Centrelink's customer education program. Such evaluation would provide information to allow FaCS and Centrelink to determine whether they had been jointly effective in achieving desired outcomes, such as increased voluntary compliance. This is particularly important given the high incidence of payment cancellations, reductions and debts raised annually as result of customers failing to comply with their obligations. The ANAO noted that FaCS recently conducted a survey on voluntary compliance involving Centrelink customers in four payment categories.

Centrelink response

29. In responding to the Section 19 draft report, Centrelink requested that the final report highlight more directly the nature and operation of the relationship between Centrelink and its client agencies. In particular, it should be emphasised that Centrelink is contracted to implement compliance strategies on behalf of its client agencies and to achieve certain performance benchmarks.

30. Centrelink also wished to emphasise that while there was generally scope for some negotiation with client agencies on implementation strategies, Centrelink is ultimately responsible for acting in accordance with client agency requirements and targets, as specified and funded by client agencies. Hence, Centrelink is not primarily responsible for the design of those compliance strategies or targets. Similarly, Centrelink wished to see the report recognise the reality of Centrelink's existing funding model, that is, there is no direct appropriation from the Budget, including for systems development. Centrelink's activities are funded through the BPA arrangments, with funds provided to Centrelink by its client agencies.

ANAO comment

31. The final report and recommendations recognise the joint role that FaCS and Centrelink have in maintaining the integrity of the social security system. In particular, the ANAO has taken into account that Centrelink implements compliance strategies, activities and performance benchmarks on behalf of its client agency FaCS, as provided for under the BPA with them.

Preventing Identity Fraud and Incorrect Payment (Chapter 2)

32. The ANAO found that while Centrelink had a clear focus on prevention of fraud and had established appropriate procedures in relation to Proof of Identity (POI), there were coding errors in 22 per cent of the claims reviewed. Inaccurate information held on Centrelink systems adversely affects the quality of Centrelink's electronic records. This, in turn, affects the efficiency of existing computer-based identity fraud detection methodologies and results in additional administrative costs for Centrelink.

33. In addition to formal POI procedures, Centrelink had developed and implemented a wide range of mechanisms to enhance its ability to prevent, as well as detect, identity fraud. This includes the development of a new model for POI. This should assist Centrelink to better manage risks associated with the proliferation of digital technologies that make it easier to create false documents and perpetrate identity-related fraud.

34. The ANAO found that processes implemented by Centrelink to prevent incorrect earnings declarations by its customers could be improved by requiring high risk customers to verify income and earnings from employment[9] to assist to reduce the number of debts raised due to honest mistakes made by customers.[10] The ANAO noted that, as part of the Australians Working Together Initiative, Centrelink is also exploring more cost effective means of facilitating customers declaring earnings and of enabling automated background verification of key information with third parties.

9 Existing procedures require only customers in exceptional circumstance to verify earnings they declare while receiving a benefit payment.

10 The announcement in the 2001–2002 Federal Budget to introduce an income bank for customers could also reduce the number of debts raised as a result of incorrect earnings declaration.

35. To ensure all customers have access to relevant information, Centrelink aims to encourage voluntary compliance of customers through education targeted to particular customer sub-groups. However, only a limited evaluation had been undertaken of the various products to determine their effectiveness in achieving increased voluntary compliance. Centrelink considers that measurement of the effect of education strategies and products on the level of customer compliance is a matter for Centrelink's client agencies. This is illustrated by, for example, reference to the fact that FaCS recently conducted a survey on voluntary compliance involving Centrelink customers in four payment categories.

Review Activity (Chapter 3)

36. The ANAO found that Centrelink had maintained an effective compliance function and had a range of controls for detecting fraud and incorrect payment. This included the use of an extensive data-matching program that matches data with a large number of Commonwealth, State and Territory agencies. This is guided by business rules and risk parameters designed to enable higher risk cases to be identified based on key criteria, such as recent employment history. Appropriate processes had been established by Centrelink for ensuring that the data-matching it conducts conforms with the requirements of data-matching and privacy legislation.

37. While Centrelink has actively sought to identify additional opportunities and sources of information to strengthen the coverage of its data-matching particularly in detecting new areas of risk, there are inherent limitations of data-matching, such as the type and quality of information held by external agencies, that result in a number of residual risks. However, Centrelink had developed a number of strategies to manage residual risks and improve its ability to deal with more complex cases of welfare fraud, for example, using surveillance to obtain information on fraudulent activity.

38. Centrelink collects and stores large amounts of data and intelligence relating to review results, but it had not fully analysed this compliance information to ensure that it effectively targets higher risk customers for its more complex review activities. An improved understanding of customers could be obtained by developing customer risk profiles. Better targeting of customers would also assist Centrelink to implement cost-effective preventative compliance measures. Work to trial risk profiling of customers was announced in the 2001–02 Budget. Risk of incorrect payment will be one of the key aspects of profiles, which should enable customer contact and reviews to be better targeted at minimising and preventing incorrect payment.

39. The ANAO found that current compliance activities, including an extensive data-matching program, would detect a significant proportion of fraud and error when it occurs. Appropriate processes had been established by Centrelink for ensuring that the data-matching it conducts conforms with the requirements of data-matching and privacy legislation. Centrelink also conducts more than one million compliance reviews each year, most of which are triggered by data-matching results. At the time of the audit fieldwork, the ANAO also found that there was no evidence of the use of a regular quality assurance program aimed at identifying sub-standard review practices even though the quality of reviews can significantly influence review outcomes. Centrelink advised that, as part of the Getting it Right strategy launched in November 2000, its QOL had been enhanced. As well, QOL was to be supplemented by a secondary checking regime to test the quality of the review process surveillance.

Dealing with Fraud and Incorrect Payment (Chapter 4)

40. The ANAO found that a number of remedies available to deal with fraud and error such as activity test breaches and caution letters, were used inconsistently across the Centrelink network. However, Centrelink advised the ANAO that a coordinated training package would be delivered during 2001 to assist staff who are unclear about the legislative requirements for imposing breaches to gain the understanding to use such mechanisms consistently. As well, in July 2001, Centrelink in conjunction with the DPP reviewed and made appropriate changes to the content of the warning and obligation letters.

41. Centrelink had developed an appropriate prosecution process for addressing both routine and serious cases of welfare fraud and, in 1999–2000, met the prosecution referral target specified in its Business Partnership Agreement (BPA) with FaCS. While this indicates the high quality of referrals that are provided by the agency to the DPP, improvement could be made to the automatic referral process to assist prosecution units to identify all cases that should be considered for referral to the DPP.

42. While Centrelink had developed guidelines for the collection and storage of records and documentation, the ANAO found that there was a low level of awareness among staff of these guidelines and compliance with the guidelines required improvement. Since the audit fieldwork was completed, Centrelink released its Getting it Right initiative in November 2000, which included a mandatory minimum standard for on-line documentation of decisions, including details of information provided to customers and information received from customers.

43. The ANAO found that the impact of penalties on compliance had not been assessed. As well, it was not possible to determine whether the value of penalties and the circumstances in which they were imposed provided an effective deterrent to non-compliance. This reduced the effectiveness of the targeting of activities to encourage voluntary compliance and thereby improve fraud prevention. A review of the fraud deterrence framework was announced by FaCS as part of the 2001–02 Budget initiatives.

Performance Assessment Framework for Compliance Activities (Chapter 5)

44. Centrelink had a range of performance indicators and targets, specified in BPAs, designed to allow Centrelink to provide regular management reports to its client agencies on the level and results of review activity.

45. Centrelink's National Selective Review System (NSRS) provided relevant data to enable Centrelink to monitor and report on outcomes of its review activity. However, there were questions about the reliability of adjustments to customer payments recorded on the system as a result of review activities and consequently the level of savings recorded and reported by Centrelink.[11] The ANAO therefore found that the implementation of a validation process (used by several ASOs visited during the fieldwork for this audit) would result in more accurate recording and reporting of review results.

46. Centrelink is contracted to implement fraud compliance strategies on behalf of FaCS and to achieve certain performance benchmarks. The performance indicators and targets in the BPA between FaCs and Centrelink should enable Centrelink to monitor and report on the level and results of its fraud review activity. While the current performance indicators were an improvement on indicators contained in earlier BPAs, the ANAO found that the performance indicators continue to place too much emphasis on the number of compliance and fraud reviews conducted rather than on the results of reviews and the effect of review activity. As a consequence, the focus has been on discovering fraud and error rather

[11] The ANAO sampled 17 program review cases to determine whether the results recorded on NSRS provided an accurate reflection of the outcome from the review. Of the cases sampled, three (18 per cent) were incorrectly recorded on NSRS.

than reducing them. As well, the new indicators have offered little incentive for Centrelink to reduce fraud and error through preventative measures and do not encourage the pursuit of more complex cases which are more time consuming and difficult to prove. Notwithstanding these deficiencies in the performance indicators, the ANAO noted that Centrelink has dedicated specialist teams in its National and Area Support Offices which deal with complex and serious frauds. These teams are subject to performance measures specific to their own work and their resources are not available to be diverted to routine and less serious fraud.

47. The ANAO found, that deriving an estimate on the level of fraud and error by income support payment type, could assist both FaCS and Centrelink to develop more meaningful indicators to demonstrate that they have been jointly successful in reducing consequent losses. Changes over time in this estimate may be useful in showing that Centrelink compliance efforts (encompassing debt prevention, customer education and review activity) are influencing customer behaviour.[12] The ANAO noted that other factors may also affect the level of losses from fraud and error. However, such an estimate could also assist to quantify the costs to the Government and the community of fraud and incorrect payment.

48. Centrelink did not have costing information available in a sufficient level of detail to enable the cost effectiveness of compliance activities to be assessed. Centrelink could not, therefore, make informed decisions regarding resource allocation for different review activities; determine the most effective compliance strategies for reducing the level of fraud and incorrect payment; or accurately price compliance strategies. Centrelink advised the ANAO that it is currently undertaking an Output Pricing Review and negotiating a new Funding Model. The Output Pricing Review provides an opportunity to improve the transparency of pricing as well as improving internal strategic cost management initiatives. The Output Pricing Review will support the development of the new Funding Model in relation to a better understanding of outputs in terms of price, quantity, quality and risk.

---

[12] The ANAO acknowledges that other factors, such as public perceptions on the likelihood of fraudulent activity being detected, may also affect the levels of losses from fraud and error.

Governance and Management Arrangements (Chapter 6)

49. The ANAO found that Centrelink had generally taken appropriate action to promote a fraud control culture among its staff. However, there were still a number of aspects where CSOs demonstrated a lack of knowledge in relation to fraud matters. These should be addressed by implementing an evaluation process to ensure that awareness-raising and training sessions are delivering the desired outcomes.

50. Centrelink had undertaken detailed fraud risk assessments of the major programs that it administers for client agencies. Recently introduced risk management guidelines should improve this process by promoting a holistic approach to risk management across all segments of the agency. As well, the fraud risk assessment framework for administrative fraud has been updated to ensure greater consistency in approach across areas dealing with these fraud risks.

51. A Fraud Control Plan, as required by the Fraud Control Policy of the Commonwealth, had been developed and was supported by lower level action plans that contained specific details regarding actions to be taken to address risks.

52. Centrelink had increased its focus on ensuring investigation staff had achieved, or are working towards attaining, the fraud investigation competency level prescribed in the latest draft on the new Commonwealth Fraud Control Policy and has specifically provided information for staff on privacy awareness.

53. The ANAO found that Centrelink had established appropriate procedures to prevent and detect administrative fraud but there was a diversity of approaches being used across its service delivery network. As well, the roles and responsibilities of the various Areas with an administrative fraud control function in relation to quality assurance were not clearly understood. However, Centrelink was undertaking a range of initiatives to address these problems.

54. Centrelink had taken action on all recommendations in the recent ANAO audit *Managing Data Privacy in Centrelink*[13] and had implemented a number of technological measures to prevent unauthorised access to information stored electronically, particularly confidential customer information. In addition, processes, such as records or logs of access, have also been implemented to monitor staff access to systems which enables Centrelink to investigate and report on alleged privacy breaches, whether inadvertent or deliberate.

---

[13] ANAO Audit Report No.8 1999–2000, *Managing Data Privacy in Centrelink.*

Recommendations

Set out below are the ANAO's recommendations aimed at improving Centrelink's management of fraud and incorrect payment.

In recommending that Centrelink undertake work in collaboration with FaCS and/or other client agencies, the ANAO has taken into account that Centrelink implements compliance strategies, activities and performance benchmarks on behalf of its client agencies, as provided for under Business Partnership Agreements with them. This recognises the primary role that client agencies have in relation to specifying and providing funding for compliance strategies and activities in relation to their programs.

Recommendation No. 1 Para. 2.41

The ANAO recommends that Centrelink, in collaboration with FaCS as client agency, measure and/or assess the effects of the various education strategies and products on the level of customer compliance.

Centrelink response: Agreed.

FaCS response: Agreed.

Recommendation No. 2 Para. 3.71

The ANAO recommends that Centrelink quickly conclude its current negotiations, with its client agencies, aimed at obtaining an improved Business Assurance Framework, to help ensure that all reviews meet established standards and provide the best possible results.

Centrelink response: Agreed.

FaCS response: Agreed.

Recommendation No. 3 Para. 5.19

The ANAO recommends that Centrelink, in collaboration with FaCS as client agency, quickly conclude the current negotiations aimed at an improved Business Assurance Framework, to provide an estimate of losses from fraud and error by income support payment type in order to better assess the impact of compliance activities on the level of losses from fraud and error. The estimates should distinguish between losses from Centrelink error and those resulting from customer error and fraud.

Centrelink response: Agreed.

FaCS response: Agreed.

Recommendation No. 4 Para. 5.20

To facilitate the effective targeting of compliance to areas of highest risk, the ANAO recommends that Centrelink request FaCS, as client agency, to develop performance indicators that provide more incentive for Centrelink to reduce losses from fraud and error as well as discovering fraud.

Centrelink response: Agreed.

FaCS response: Agreed.

Recommendation No. 5 Para. 5.30

The ANAO recommends that Centrelink, in collaboration with its client agencies, assess the cost-effectiveness of developing its business systems to record and report on the preventive effect of compliance activities and their impact on voluntary disclosures, initially assessing whether the National Selective Review System (NSRS), or its replacement system could record whether payment adjustments were attributable to voluntary disclosures due to an impending review.

Centrelink response: Agreed.

FaCS response: Agreed.

Audit Findings and Conclusions

1. Background

This chapter sets out the background to the audit, its objectives, scope and methodology. It also outlines the structure of the rest of the report.

Introduction

1.1 The prevention and management of fraud is an important issue for the Australian Public Service (APS). The Federal Government demonstrated its ongoing commitment to the protection of its revenue, expenditure and property from fraudulent activity through the release of its first Fraud Control Policy in 1987. There was a subsequent update in 1994 and in the latest Consultation Draft fraud is broadly defined as *'dishonestly obtaining a benefit by deception or other means.'*[14]

1.2 The importance of agencies establishing effective fraud control arrangements has also been recognised in legislative provisions in the *Financial Management and Accountability Act 1997* (FMA Act). Under Section 45 of the FMA Act, Chief Executive Officers (CEOs) are responsible for the implementation of a fraud control plan and for reporting to the Portfolio Minister on fraud control within their agencies.

1.3 This audit of Centrelink is one of a series of audits, including a survey of fraud control arrangements in the APS[15], undertaken by the Australian National Audit Office (ANAO). A list of these audits is at Appendix 1. The audit discussed in this report is complemented by a separate audit of fraud control arrangements in the Department of Family and Community Services (FaCS) which was tabled in June 2001[16].

1.4 In its Report No. 385[17], the Joint Committee of Public Accounts and Audit (JCPAA) highlighted the benefits of agencies developing sub-categories of fraud to provide a better understanding of the nature and significance of various types of fraudulent activity. For instance, inappropriate use of information, travel fraud, and identity fraud. This issue will be more fully considered by the ANAO when it develops its Better Practice Guide on Fraud Control in 2002–03 at the completion of this series of fraud audits. The JCPAA requested the ANAO develop sub-categories of fraud for the purposes of fraud reporting, when preparing the Better Practice Guide on Fraud Control.

---

14 Fraud Control Policy of the Commonwealth, Attorney Generals Department, Consultation Draft, No.2 April 2001.

15 ANAO Audit Report No.47 1999–2000 *Survey of Fraud Control in the APS Agencies*.

16 ANAO Audit Report No.45 2000–2001 *Management of Fraud Control*, Department of Family and Community Services.

17 Review of Auditor General's Reports, 2000–01, Second and Third Quarters August 2001 Canberra.

Centrelink

1.5 Centrelink was established on 1 July 1997 as the Australian Government's one-stop shop for social security and employment services.[18] It is responsible for the integrated delivery of a wide range of Commonwealth social and economic payments and services and provides services to 6.4 million customers each year, involving nine million benefit payments and an annual cost approaching $50 billion. It employs over 22 000 staff to deliver these services on behalf of 16 Commonwealth departments and agencies and all State Housing Authorities under formal purchaser/provider arrangements. Centrelink delivers its services through a distributed network of over 1000 sites including 15 Area Support Offices (ASOs), 310 Customer Service Centres (CSCs), 28 Call Centres and about 350 agency arrangements.

1.6 Centrelink's major purchasers in terms of the value of payments and services delivered on their behalf by Centrelink in 1999–2000 were FaCS, the Department of Education, Training and Youth Affairs, the Department of Transport and Regional Services and Agriculture, Fisheries and Forestry—Australia.

Fraud control in Centrelink

1.7 The size, geographical spread and devolved accountability of Centrelink's operations means that there are inherent fraud risks associated with its business, which need to be properly managed.[19] Fraud against Centrelink can be committed externally by individuals seeking to obtain payments they are not entitled to receive or internally by its staff and contractors. To assist in detecting and treating these fraud risks, Centrelink has separated fraud into three distinct categories: program fraud, information fraud and administrative fraud. Centrelink reports as fraud only those cases successfully prosecuted in a court of law. In 1999–2000, there were 2960 convictions for program fraud involving over $27 million in debts; two cases of administrative fraud involving a total of $1100 in debts and 488 cases of information fraud.

---

18 The *Commonwealth Services Delivery Agency Act 1997* formally established Centrelink on 1 July 1997.

19 Since it was established in 1997, Centrelink has also had the significant task of merging the fraud control regimes of a number of agencies, including integrating the legacy systems of different agencies, while at the same time seeking to continually improve its fraud control systems and practices. A summary of recent developments in fraud control in Centrelink is presented in Appendix 5.

1.8 Centrelink focuses on program fraud and this is reinforced in its Business Partnership Agreement (BPA) with FaCS that requires Centrelink to implement arrangements aimed at preventing, detecting and deterring fraud and incorrect payments. This is appropriate given that the services it delivers for FaCS are around 90 per cent of all Centrelink business. To illustrate the level of compliance activity specified by FaCS that Centrelink needs to undertake, Table 1.1 lists the target number of reviews to be conducted in 2000–2001.

Table 1.1

2000–2001 performance targets for controlling program fraud as defined in the Centrelink-FACS BPA

Level of review activity	Compliance reviews	Number of compliance reviews	1 100 000
	Program reviews	Number of program reviews	2 303 850
	Rent assistance reviews	Number of Rent Assistance specific compliance reviews	125 000
	Child Care Benefit reviews	Number of outreach visits	500
		Review of providers ceasing operation	100%
		Review of providers from public information	100%
Effective focussing of activity in compliance reviews		Percentage of compliance reviews in which incorrect payment is identified.	30%
Quality of prosecution referrals		Percentage of cases referred to the Director of Public Prosecutions that can be actioned[1].	80%

[1] Includes cases in which the Director of Public Prosecutions decides in the public interest not to proceed.

Audit objective and criteria

1.9 The objective of the audit was to assess whether Centrelink had implemented appropriate fraud control arrangements in line with the Fraud Control Policy of the Commonwealth and whether these arrangements were operating effectively in practice.

1.10 The ANAO established a framework for analysing the effectiveness of Centrelink's fraud control arrangements based on whether Centrelink had:[20]

- robust front-end administrative processes for preventing customers from obtaining payments and benefits they are not entitled to receive;
- effective mechanisms for detecting, investigating and dealing with, in a timely manner, customers and staff that obtain payments and benefits they are not entitled to receive;
- a comprehensive performance assessment framework for the compliance and fraud control function;
- arrangements for protecting the confidentiality of customer information; and
- measures for ensuring that administrative funds and Commonwealth property are not misused by Centrelink staff.

1.11 The framework for analysis also included an examination of Centrelink's governance arrangements that are designed ensure proper management of its fraud control framework.

Audit scope and focus

1.12 Centrelink is a major provider of services on behalf of FaCS. The funding for these services is appropriated to FaCS. Under the FMA Act, Centrelink and FaCS are responsible for promoting the efficient, effective and ethical use of Commonwealth resources. In addition, the *Commonwealth Services Delivery Agency Act 1997* (CSDA Act), defines an important function of the Centrelink Board as ensuring *'that the Agency's functions are properly, efficiently and effectively performed'*.

1.13 FaCS and Centrelink are dependent on each other for delivering a satisfactory level of performance in the area of fraud control. An outcome for both agencies should include effective measures to prevent, detect and treat fraud in order to maintain the integrity of the social security system. The achievement of this outcome within a purchaser/provider relationship calls for a partnership or collaborative approach to achieve the required results.

---

[20] The audit criteria were developed from guidelines relating to fraud control arrangements provided by the Attorney-General's Department, the Australian /New Zealand Standard 4360:1999 on risk management and general better practice that has been identified in earlier fraud control audits. Consideration was also given to standards outlined in the BPA between FaCS and Centrelink.

1.14 The relationship between FaCS and Centrelink is governed by a Business Partnership Agreement (BPA) which acknowledges joint responsibility for performance. In relation to the management of fraud, the BPA outlines the roles and responsibilities of the two parties. FaCS is responsible for providing Centrelink with appropriate policy advice, direction and support to enable effective service delivery and Centrelink is responsible for implementing strategies for payment control as part of its approach to service delivery.

1.15 A challenge for both agencies is to successfully interact with each other in the pursuit of the government's fraud control objectives. While FaCS has the primary responsibility for specifying and providing funding for compliance strategies and Centrelink has the role of implementing these strategies and achieving certain performance benchmarks, there is a joint responsibility to meet the wider outcomes that the government is seeking through the FMA Act and the CSDA Act. For example, without feedback from Centrelink, policy-advisers in FaCS may not benefit from an understanding of what happens when policies are put into practice. Centrelink is also well placed to identify trends and provide statistical information to FaCS and other client agencies that purchase its services and identify where approaches from different government departments need to be harmonised. This joint responsibility was taken into account in the ANAO's recent fraud audits in FaCS and Centrelink.

1.16 Audit Report No.45, *Management of Fraud Control* in the Department of Family and Community Services was tabled in June 2001. The audit examined the arrangements in place for FaCS to manage internal and external fraud and the mechanisms that FaCS had established to obtain assurance regarding the effectiveness of fraud control and incorrect payment in those agencies which deliver services and / or make payments on its behalf, particularly Centrelink.

1.17 This audit of the Management of Fraud and Incorrect Payment in Centrelink, focuses on compliance reviews and Centrelink's arrangements for the prevention, detection and treatment of incorrect payments as a result of fraud and incorrect payment[21] (program fraud). Given that nearly 90 per cent of total payments and services delivered by Centrelink are on behalf of FaCS, the major focus of this audit was the fraud control arrangements put in place for the services provided for FaCS. The audit also examines Centrelink's arrangements to manage internal fraud committed by its staff and contractors (administrative and information fraud).

---

[21] Centrelink can not currently distinguish between fraud and incorrect payment.

1.18 Centrelink investigates many cases where customers have obtained benefits that they were not entitled to receive. However, it defines, and subsequently reports, program fraud as only those cases which are proven in the courts. The ANAO determined at an early stage, in relation to program fraud, that limiting the audit to only those cases that were successfully prosecuted in the courts would not be adequate. Therefore, in reviewing Centrelink's control framework for program fraud, the ANAO assessed the compliance arrangements that were in place to manage instances where a customer, or staff member, had obtained a payment or benefit they were not entitled to receive and not just those cases successfully prosecuted for welfare fraud in a court of law.

Audit methodology

1.19 The ANAO reviewed Centrelink documents relating to compliance and fraud control and undertook detailed compliance testing of some key aspects of Centrelink's controls for program fraud. Compliance testing was undertaken in 10 ASOs and incorporated 33 CSCs across Centrelink's service delivery network during audit fieldwork. A list of these Areas and CSCs is provided at Appendix 2.

1.20 The main purpose of the testing was to determine the level of compliance with policies and procedures aimed at preventing, detecting and treating program fraud. Specifically, the testing involved the examination of random samples of:

- new benefit claims, for selected payment types[22], that were granted between 1 January 2000 and 31 August 2000 to assess compliance and adherence with current Proof of Identity (POI) policies and procedures;
- tip-off reviews conducted in each ASO visited to assess, among other things, the timeliness of investigations, breaches being applied (in those benefits where breaches are applicable) and data relating to tip-offs received; and
- compliance reviews completed during the past year in each ASO, to determine timeliness and imposition of breaches as well as to obtain information regarding prosecution referrals to gauge their quality.

---

[22] The payment types reviewed were clustered into 3 categories:

- Newstart (NSA) and Youth Allowance (YAL);
- Disabilities Support Pension; and
- Parenting Payment Single (PPS) and Parenting Payment Partnered (PPP).

These payment types were chosen because the ANAO had already reviewed elements of the Special Benefit and Age Pension payments in previous audits.

1.21 The ASOs and CSCs examined, as well as the sample sizes for each of the compliance tests, were determined with reference to advice provided by the Australian Bureau of Statistics (ABS) and in consultation with Centrelink. Centrelink randomly selected the files for examination based on sample sizes specified by the ANAO. The process for sample selection is detailed in Appendix 3. Results of the compliance testing are presented throughout the report.

1.22 The ANAO also conducted an extensive program of interviews with key staff in Centrelink's National Support Office (NSO) in Canberra as well as with staff in ASOs and CSCs across Australia. In addition, discussions were held with external agencies such as the Australian Federal Police (AFP) and the Office of the Director of Public Prosecutions (DPP), which provide services to Centrelink in relation to fraud control.

Environmental factors impacting on fraud control in Centrelink

1.23 There have been a number of recent government policy initiatives that could impact on Centrelink's compliance and fraud control activities, including:

- simplification of the social security system—there has been a growing acceptance that some of the problems with compliance occur because the complexity of the *Social Security Law*[23] makes it difficult for people to understand their obligations and entitlements;
- increasingly, the Government is adopting the concept of mutual obligation[24], placing emphasis on Centrelink's Customer Service Officers (CSOs) understanding the full circumstances of a customer, developing a plan with that customer to ensure that they meet their obligations to the community and being firm about breaching customers where they fail to meet their obligations; and
- delivery of government services online has focused attention on electronic authentication of customer identity and security of information to safeguard customer's rights.

1.24 As well, Centrelink is aiming to progressively introduce a range of new service delivery strategies that could impact on payment control. These strategies are part of a broader transition in Centrelink towards a

---

23 The *Social Security Law* comprises the *Social Security Act 1991*, the *Social Security (Administration) Act 1999* and the *Social Security (International Agreements) Act 1999*.

24 McClure, P., March 2000, *Participation Support for a More Equitable Society: Reference Group on Welfare Reform Report to the Minister for Family and Community Services.*

new model of service delivery based on the life events of a customer.[25] The aim of this new service delivery model (SDM) is to remove the complexity for customers and allow Centrelink to deliver a more focused and holistic service to customers. The key underlying principle is that the customer will not be expected to know or name the various products or services to which they may be entitled when they initially (or subsequently) access Centrelink. Instead, all they will have to do is advise Centrelink of the life event(s) they are experiencing. The onus will be on Centrelink to match the customer's circumstances with the products and services that have been legislated and made available by client agencies.

1.25 To support the shift to a life event's approach Centrelink has introduced, to varying degrees, a range of other initiatives that combine to form the new SDM. These include:

- the one-to-one (OTO) initiative whereby customers are allocated to one CSO who will be responsible for their initial and ongoing business, rather than having to continually deal with different staff;
- a wide range of access options for customers to interact with Centrelink, including face-to-face, over the phone, Internet, kiosk facilities and integrated voice response systems guided by integrated channel management; and
- once only POI for customers that may involve a customer authentication mechanism.

1.26 As well, Centrelink implemented the Getting it Right strategy in November 2000, which sets the framework for improving accuracy and accountability in Centrelink.

Structure of the Report

1.27 Chapter 2 examines Centrelink's arrangements for preventing identity fraud and incorrect payment. Chapter 3 outlines the review activity undertaken to detect fraud and incorrect payment. Chapter 4 assesses the application of the various remedies available to Centrelink to deal with fraud and incorrect payment once it has been detected. The performance assessment framework for compliance activities is discussed in Chapter 5. Chapter 6 outlines Centrelink's governance arrangements for managing its fraud risks and issues, including in relation to administration and information fraud.

1.28 The audit was conducted in compliance with ANAO auditing standards at a cost to the ANAO of $420 000.

---

[25] A life event is defined as a significant change or changes that affect a person and/or their family and/or their community.

2. Preventing Identity Fraud and Incorrect Payment

This chapter discusses the controls that have been implemented by Centrelink to prevent fraud and incorrect payment in the programs that it administers. It reviews arrangements for preventing identity fraud and also assesses Centrelink approaches for verifying customer eligibility to receive payments and services and for educating customers about their obligations when receiving Centrelink payments and services.

Introduction

2.1 Centrelink's responsibility for establishing a comprehensive framework for maximising correct payments and outlays is clearly specified in its Business Partnership Agreement (BPA) with the Department of Family and Community Services (FaCS). The 2000–2001 BPA identifies three key strategies for maximising correct payments and outlays – prevention, detection and deterrence. Of these, it gives priority to prevention, stating that '*the primary aim of control strategies, as far as possible, will be to prevent incorrect payments, rather than detect them later*'.

2.2 Establishing the true identity of a Centrelink customer provides a fundamental starting point for the prevention of fraud. Therefore, the ANAO examined whether:

- Centrelink had established Proof of Identity (POI) procedures and that they were operating effectively in practice; and
- a review of POI procedures had been undertaken to address new and emerging risks for identity fraud and improve current practices.

2.3 As well as assessing POI procedures, the ANAO examined the range of other controls Centrelink had in place to prevent and detect identity fraud. Another key element of a comprehensive strategy for the prevention of fraud and incorrect payment relates to establishing customer eligibility to receive payments. Therefore, the ANAO examined whether Centrelink had arrangements in place for verifying income declared by its customers.

2.4 Centrelink encourages customers to comply voluntarily with POI and eligibility requirements. This means that it is important that education programs are in place to encourage voluntary compliance among customers.

2.5 Each of these is discussed under separate headings.

Proof of Identity procedures

2.6 One of the most frequently used strategies to perpetrate fraud is the creation of false identities through the falsification of identity documents.[26] The introduction of digital technologies and their increased availability has made it easier to create false documents and perpetrate identity-related fraud. Once a false identity has been created it is then possible for an individual to act illegally in other ways and avoid detection, investigation and arrest.[27] This is a significant issue for public and private sector agencies in Australia. The United States Federal Bureau of Investigation has described identity fraud as the fastest growing crime in the nation.[28]

2.7 Over recent years Centrelink has been exposed to numerous fraud related crimes committed by both customers and staff seeking to obtain payments that they were not entitled to receive. These range from opportunistic to well-organised and sophisticated cases of identity fraud. The level of identity fraud detected by Centrelink over the last two years is provided in Table 2.1

Table 2.1

Number of Identity fraud cases detected over the last two financial years

	1998–99	*1999–2000*
External		
Detected	110	168
Finalised	93	92
Internal		
Detected	41[1]	18
Finalised	8	28
Estimated Savings ($)	11.6 million	14.4 million

1 The high incidence of internal identity frauds perpetrated during 1998–99 coincided with the introduction of Electronic Benefit Transfer (EBT) cards resulted in the large number of internal frauds. Controls for the issue of EBT cards have been improved.

26 ANAO Audit Report No.37 1998–99, *Management of Tax File Numbers*, noted the ease with which false identity documents can be obtained and the difficulties this poses for government organisations in terms of their POI processes.

27 Smith, Russell, Identity-related Economic Crime: Risks and Countermeasures (1999), Trends and Issues in Crime and Criminal Justice Series, No.129, Australian Institute of Criminology, September, p. 1.

28 Theft of Identity: The Consumer X-files, CALPRIG AND US PIRG, August 1996, pp. 14–15 cited in Occasional Paper No. 2/00, The Criminal Exploration of Identity, Office of Strategic Crimes Assessments, Canberra 2000.

Current POI procedures

2.8 The ANAO found that Centrelink had developed formal procedures that set out the minimum POI requirements for customers claiming payments or services delivered by Centrelink. POI procedures are based on verifying the identity of customers by reference to evidence, primarily in the form of acceptable documents.[29] The procedures are made available to all staff via Centrelink's intranet and cover all aspects of the POI process, including:

- the types of documents that can be accepted as POI for new claims and abridged claims.[30] Customers are informed at the claim stage that assistance is subject to Centrelink being provided with adequate documentation to establish the identity of the individual;
- procedures for customers using a previous Centrelink record as POI. Where a previous record is used for POI, a signature check is required to verify identity;
- retaining POI documents provided by customers on a customer's file;[31] and
- recording details of the documents used as POI onto the Centrelink mainframe database.

29 Centrelink guidelines require that original POI documents be presented with an application for payment. Customers must supply at least three POI documents, one of which is a primary document. This is referred to as standard POI. Alternatively, if claimants are unable to satisfy standard POI requirements they may provide a combination of documents which provides an 'identity history' of the claimant.

30 Abridged claims include those where a customer is reclaiming a benefit within a prescribed timeframe, usually 13 or 26 weeks of the previous claim or customers who transfer between benefits delivered by Centrelink.

31 The requirement to retain copies of documents on the claimant's file is necessary for accountability as well as to meet legal requirements, such as evidentiary standards for prosecution cases.

2.9 While the procedures generally provide sound guidance on the POI process, there were two areas where the procedures for the use of non-standard documents should be improved, as follows:

- non-standard documents.[32] Three or more of these documents, combined with two secondary documents are currently attributed a value as a POI document equal to that of a primary document[33] even though the non-standard documents are of considerably lower integrity; and
- POI requirements for abridged claims. Currently any POI document can be presented with an abridged claim to verify identity. The provision of one of the original POI documents used by the customer to initially make a claim should be used to verify identity.[34]

2.10 Since the audit was carried out, Centrelink has introduced a new POI model (September 2001) which removes the non-standard POI option so that only approved documents are acceptable as POI. Customers who are initially unable to meet normal POI requirements have access to alternative POI processes which allow for payments to commence based on the CSO verifying identity information provided by the customer. Also under the new model, for abridged, claims the CSO is now required to conduct a signature check between the new claim and a document supplied with the previous claim. In addition, the customer must supply a document from an improved list which contains a photo or signature of the customer. These changes to POI procedures should assist to reduce the risk of the use of false documentation to prove identity and thereby reduce the potential for fraud and error.

---

32 These documents are used when a customer is unable to meet standard POI requirements (for example, one primary and two secondary documents) but can provide a combination of documents that together prove the existence of the identity for a reasonable period of time.

33 A distinction is made between primary, secondary and non-standard documents based on the relative reliability and integrity of the document and its issuing agency as well as the length of time that the document has been held by the bearer:

- primary documents are those which are regarded as sound because of the stringent conditions which are satisfied before they are issued, their obvious importance to the holder and the fact that they are difficult to duplicate; and
- secondary documents are those which are issued without the need for the holder to prove their identity but which establish a reasonable history of use of the name and/or address.

34 The POI requirements for Abridged Claims now require the CSO to conduct a signature check between the new claim and a document supplied with the previous claim. In addition the customer must supply a document from the approved list which contains a photo or signature of the customer.

Effective Operation of POI procedures

2.11 In December 1998, a Centrelink internal audit report into POI practices,[35] found, among other things, that:

- for the period 1995–96 to 1997–98, 75 to 80 per cent of detected identity fraud cases would have been prevented had POI guidelines been correctly applied; and
- a significant proportion of cases reviewed did not comply with Centrelink's POI standards and procedures.

2.12 The internal review concluded that:

> *Current standards and procedures for [proof] of identity… focus attention of staff on mechanistic sighting, copying and recording of documents, rather than on critical consideration of claimant identity. As a result of that focus, where acceptable documents are not provided, compliance is often compromised to allow claim processing to proceed.*

2.13 To follow-up on this internal review, the ANAO conducted an assessment of current POI practices in CSCs. The results of the ANAO's examination are presented in Table 2.2. It should be noted that errors by Centrelink staff in applying POI procedures do not necessarily mean that identity fraud has occurred. Centrelink advised that a subsequent re-examination of the POI casework carried out after this audit validated all identities initially defined as warranting closer examination, and no cases of possible identity fraud were detected as a result of the follow-up examination.

---

[35] Audit and Evaluation, *Proof of Identity*, December 1998.

Table 2.2
National POI compliance results

POI processing error	*Number*	*Percentage*	*Cumulative percentage*
POI not fully established at time of claim[1]	5	0.4	0.4
Coding[2]	272	22.0	22.4
Administrative[3]	660	53.4	75.8
No error[4]	298	24.2	100.0
Total claims assessed[5]	1235	100.0	

1 Cases where the information provided at the time of claim was not sufficient to determine with any degree of confidence that the claimant is who they purport to be.

2 Those errors where the POI documents and personal information presented by a customer at the time of claim is not accurately recorded on Centrelink's mainframe system by staff.

3 Administrative errors are minor in nature and would not have an adverse impact on current data-matching detection methodologies. Examples of these errors include failure to apply the correct procedures for entering bank account or previous record details onto the mainframe.

4 Cases where all POI procedures were correctly applied.

5 Of the 1375 files reviewed, only 1235 were assessed for compliance with POI procedures as 3 files were not able to be assessed due to system restrictions protecting the confidentiality of those files and there was no application on 91 (6.6 per cent) files reviewed (the ANAO did not assess these files as it could not be assured of the accuracy of the details recorded on the system).

2.14 While the errors identified in the table do not mean that fraud has occurred, poor front-end practices can affect community perceptions about the integrity of programs and increase the opportunity for fraud and error to occur. As well, weaknesses in front-end processes can also result in a less than efficient use of back-end mechanisms that Centrelink has in place for detecting identity fraud.

2.15 The commitment to systematically applying most POI procedures meant that there were only five cases in the files reviewed where Centrelink staff had not fully established the customer's identity.[36] However, there remained a significant degree of non-compliance with POI procedures relating to the coding of identity document details. In particular, there were coding errors in 22 per cent of the claims reviewed. This adversely affects the quality of Centrelink's electronic records and can impact on the efficiency of existing computer-based identity fraud detection methodologies such as data-matching. It also results in additional administrative costs for Centrelink and impacts on decision-making in regard to cases requiring further investigation.

36 Minimising these errors is particularly important given that, in a pilot exercise conducted by Westpac and New South Wales Registry of a Certificate Validation Service, 13 per cent of birth certificates that had been tabled to the bank as part of identification documentation were found to be false.

2.16 The rate of administrative errors shown in Table 2 reflected a departure from expected practice based on Centrelink's guidelines and included:

- documents used to verify identity not photocopied and placed on a customer's file;
- significant levels of non-compliance with procedures for customers using a previous record as POI;
- tax file numbers (TFNs) not being removed as required by Privacy legislation and guidelines;
- a high incidence of cases where the documents recorded on the computer system did not match the documents that had been placed on the customer's file (in many cases POI provided in previous claims was duplicated on the system); and
- lack of detailed information on the mainframe system regarding non-standard documents, such as serial number and date of issue.

2.17 These administrative errors, while not significant in terms of a customer's qualification and payability requirements, reflected poor work practices. Following the completion of the fieldwork, Centrelink advised that the introduction of the Getting it Right strategy in November 2000 and the new POI model in September 2001, should address these problems.

2.18 As well as the above issues in relation to the potential for identity fraud, the ANAO noted that Centrelink is able to provide customers with payments in the absence of sufficient POI documentation where hardship would otherwise result. The ANAO sought to determine the incidence of individuals claiming and receiving payments and services prior to providing adequate POI documentation. While Centrelink procedures allow for such payments being granted, recipients must subsequently provide appropriate POI documents within two fortnights. The ANAO found that Centrelink was unable to provide details regarding the number of claims granted with insufficient POI that did not subsequently provide the appropriate documentation and as a result had payment cancelled. The ANAO considers this information to be important for Centrelink and its client agencies to assess whether opportunistic identity fraud is being perpetrated against program funds at a less complex level.[37]

---

[37] Data on the number of cases which are granted payment based on alternative POI and which are subsequently cancelled due to non-provision of documents is available with the introduction of the new POI model.

Review of POI procedures

2.19 Centrelink had undertaken a range of activities in relation to POI to address recent internal and external audit findings and new and emerging risks of identity fraud. This included a new model for POI procedures, involvement in inter-governmental forums and the evaluation of the effectiveness of electronic POI approaches. The ANAO also reviewed relevant controls, other than those set out in the POI procedures. These are also discussed below.

New POI Model

2.20 The new POI model was developed in conjunction with client agencies following a full review of Centrelink's POI procedures and standards, including a formal risk assessment and quantitative analysis of POI information. It was due to be implemented later in 2001.

2.21 The new POI model has a number of important features including:

- a risk management approach to POI based on the potential payment of program funds to a customer. Individuals claiming a long-term benefit, such as age or disability support pension, will be required to submit full POI documentation while customers claiming services not involving a direct payment, such as a Health Care Card, will be subject to lesser POI requirements;
- 'once only POI', whereby customers would only need to prove their identity once to Centrelink, saving time for customers and Centrelink staff;
- POI document points allocation system similar to that required by the *Financial Transaction Reports Act 1988* (FTR Act);[38]
- system enhancements for validating data entered onto the mainframe by staff. These include system checks that will test the validity of registration/serial numbers entered for certain types of identification such as driver's licences, birth certificates and previous Centrelink record numbers; and
- the new POI model introduced in September 2001 has incorporated systems changes which through use of field edits and the use of a selection screen for valid POI documents will reduce the incidence of coding errors.

---

[38] The FTR Act requires account signatories to provide sufficient identification to meet the prescribed verification procedure, known generally as the 100 point check.

2.22 The new POI model has potential efficiency gains for staff and that the 'once only POI' approach, if implemented should assist in simplifying the re-claim process for customers.

Inter-governmental forums

2.23 Centrelink has been actively involved in POI discussions and forums across government aimed at identifying common risks relating to false identity, such as the expansion of electronic service delivery, with a view to developing a Whole-of-Government approach to POI. For example, Centrelink has participated in the AUSTRAC-facilitated Whole-of-Government Proof of Identity Steering Committee that is investigating ways of improving Australia's POI framework for all organisations across both the public and private sectors.[39] It is anticipated that this work will assist all agencies to tighten POI processes through a higher standard of document validation and reach some level of consistency in POI processes across Commonwealth agencies.

Electronic POI approaches

2.24 Centrelink was evaluating the effectiveness and reliability of a number of mechanisms to authenticate the identity of customers electronically accessing its services and maintain the integrity of POI process using a variety of technologies. This is in line with the Australian Government's commitment to have all appropriate government services able to be delivered via the internet by 2001.

Controls

2.25 In addition to POI procedures,[40] Centrelink had developed a wide and sophisticated range of mechanisms by which identity fraud can be prevented and detected. These controls include the following:

- the National Index, which linked Centrelink's 11 separate online customer environments. This national integration of mainframe systems transformed Centrelink into an organisation with a national focus and provides it with a high level of assurance that customers are not lodging and being paid on multiple claims submitted at different sites;

---

39 Continually improving the means of reducing false POIs is important for example, for Centrelink the Health Care Card requires a lower level POI but provides access to a wide range of Federal, State and local services.

40 Centrelink advised that POI procedures alone will generally fail to prevent well organised identity fraud being committed. Therefore, complementary tools are required to ensure robust measures are in place to effectively mange identity fraud.

- Accelerated Claimant Matching (ACM). This system is the front-end of Centrelink processing where all new customer information entered onto the mainframe is automatically checked overnight for anomalies against existing information held by Centrelink. ACM is an important tool for stopping duplicate claims and detecting instances of duplicated tax file numbers; and
- the establishment of the Identity Fraud Team (IFT), a specialist section that aims to detect individuals who have deliberately set out to defraud the welfare system by creating a false identity or assuming the identity of another person. The IFT uses a computer-based identity matching process to match data from a number of sources and derive an identity score for all customers. This score indicates how closely the customer record matched with the identity records from other sources and assists to identify cases requiring closer examination. The IFT also uses data-mining and transaction analysis to detect possible cases of identity fraud.

2.26 These approaches rely on accurate data entry. This emphasises the need for coding errors identified in Table 2.2 to be minimised so that these additional controls to work effectively in practice.

Eligibility

2.27 As well as proving identity, customers receiving Centrelink payments are required to inform Centrelink of their employment and income details to allow an assessment of their eligibility. Procedures for Centrelink to verify these details include:

- customers providing employment separation certificates to prove they are no longer employed; and
- arrangements for verifying income declared by customers.[41]

Separation certificates

2.28 Obtaining separation certificates from customers who have recently ceased employment is a key control for ensuring applicants still in employment are not granted payments inappropriately. The ANAO found that CSOs adhered to procedures for new claimants who had recently left work by ensuring that separation certificates were obtained from the claimant's former employer.

---

[41] Centrelink has sophisticated mechanisms for detecting people who have commenced work or earned income above threshold limits during the year.

Verification of income

2.29 Incorrect declaration by customers[42] does not necessarily mean that they are trying to defraud Centrelink. However, non-declaration or incorrect declaration of income by customers, generally from employment, continue to be the largest source of debt for Centrelink.

2.30 Centrelink had a number of specific prevention strategies to address this risk, such as;

- improving processes for customers to accurately declare earnings and educating customers on the correct way to declare earnings; and
- the Debt Prevention and Monitoring Officer (DPMO) initiative,[43] the aim of which is to reduce the incidence of preventable debt.

2.31 However, national procedures for the verification of income declared by customers at the time of claim and subsequent contact had not yet been developed by Centrelink. Existing procedures require only those customers in exceptional circumstances to verify earnings they declare while on payment. The inherent risk of this self-assessment approach was highlighted by the ANAO's examination of compliance reviews and tip-off investigation cases that resulted in income-related debts being raised.[44] In the majority of these cases, there was no verification of income details that had been declared by customers, even where declared income had been close to threshold limits.

---

42 The level of payment received by a customer is affected by the level of income earned by the customer in the corresponding period and debts can be incurred where:

- the customer's income periods overlap their Centrelink payment period; and
- the customer does not receive their pay until some time after it is earned.

43 Funding for DPMOs for each CSC was provided as part of the 1996 Budget initiative, 'Simplification of the Debt Creation Provision'. The main role of DPMOs is to identify and implement debt prevention strategies.

44 This issue is discussed in Chapter 4 under the heading *Activity test breaches*.

2.32 It was noted that Centrelink had recently conducted Earnings Verification pilots aimed at establishing procedures to verify customer income details and consequently reduce debt levels with a view to national implementation. The findings from these pilots could lead to significant benefits for both Centrelink and its customers including:

- more accurate customer income information which could potentially reduce the number of compliance reviews required for incorrect earnings declarations;
- assisting payment correctness on an ongoing basis and minimising the incidence of debts being raised due to honest mistakes made by customers; and
- reducing compliance costs incurred by employers in meeting their legislative obligations to respond to Centrelink requests for information as part of its review activity.

2.33 As well, Centrelink, as part of the Australians Working Together initiative[45] is also exploring more cost-effective means of facilitating customers declaring earnings and of enabling automated background verification of key information with third parties.

2.34 As entitlement to allowance is on a fortnightly basis customers may be penalised if they have some lumpy payments that exceed income test free areas as opposed to smooth payments that do not.[46] In the 2001–02 Budget, the government announced the introduction of Working Credits which people on income support payments can accumulate to effectively increase their income test free area. This measure is aimed at providing an incentive for people to participate in the workforce. Therefore, this measure could also encourage greater declaration of income. A $1000 limit applies to accumulated credits.

Education of customers

2.35 The Organisation for Economic Cooperation and Development (OECD) has recognised that the ability of social security customers to understand the rules and their obligations is a major factor influencing compliance. It has recently stated that a separate necessary condition for compliance is:

---

45 The Australians Working Together—Helping People to Move Forward Initiative was announced in the 20001–02 Budget. This initiative contains important changes to Australia's welfare and employment services and provides new funding for employment and community services to expand and improve the assistance available to people looking for work.

46 The current income test free areas are $62 per fortnight for Newstart recipients and $106 per fortnight for single workforce age pensioners, without children.

> *…knowledge or comprehension by the target group of the rules—non-compliance will result when requirements are too complex to know and understand.*[47]

2.36 The ANAO therefore examined whether Centrelink had taken appropriate steps to provide relevant and timely information to encourage voluntary compliance by customers with their obligations, particularly in relation to changes in circumstances.[48]

2.37 Centrelink had developed a comprehensive range of education products that are delivered through a variety of channels aimed at ensuring that sufficient information is available to customers to assist them to understand their rights and responsibilities when receiving government payments and services. Examples of these included:

- issuing pamphlets to customers at the new claim stage advising customers of their obligations, including to notify Centrelink of changes in their circumstances;[49]
- requiring Newstart customers to attend a pre-claim seminar outlining their rights and responsibilities and Preparing for Work Agreements are negotiated with every claimant of Newstart and Youth Allowance;
- developing a range of written material from direct mail outs to pamphlets and posters in CSCs informing and reminding customers of their rights and obligations;[50]
- providing press releases or other information through regular communication outlets such as *Age Pension News*, *Update* and SBS radio;[51] and
- implementing the *Outreach*[52] program that aims to make Centrelink more visible to segments of the community that may not be aware, or have access to relevant information, through the normal channels.

---

47 *'Reducing the risk of policy failure: Challenges for regulatory compliance'*, OECD Working Party on Regulatory Management and Reform, March 2000. Extract taken from *'Factors affecting voluntary compliance'*, paper presented to the six countries benefit fraud conference, Department of Family and Community Services, September 2000, Ireland.

48 Senator Vanstone in a Media Release entitled 'Cooperation and Compulsion Both Needed for Compliance' stated that survey data revealed that failure to notify Centrelink of changes in circumstances was the main cause of incorrect payments to welfare recipients.

49 One issue raised during the audit was whether customers are provided with too much information at the new claim stage.

50 The information is provided in a number of foreign languages through translated written material or interpreters.

51 *Age Pension News* and *Update* are targeted publications regularly provided for age pension and unemployed customers respectively.

52 DPMOs located within in each ASO are responsible for managing the *Outreach* program in their Areas.

2.38 Electronic versions of most Centrelink educational material are also available on the Centrelink website, at www.centrelink.gov.au.

2.39 Changes being introduced as part of the new Service Delivery Model (SDM), including the implementation of the one-to-one contact model, are intended to reduce the complexity of administrative arrangements for Centrelink customers. To assist in preventing incorrect payments leading to customers having debts raised against them, the most important message that Centrelink should be giving its customers is that they should advise Centrelink of any changes in personal and financial circumstances.

2.40 The ANAO found that Centrelink had developed a broad customer education strategy. However, Centrelink, and its client agency FaCS, had only taken limited action to evaluate the effectiveness of its customer education program. This evaluation would provide information to allow Centrelink to determine whether it had been effective in achieving desired outcomes, such as increased voluntary compliance. This is particularly important given the high incidence of payment cancellations, reductions and debts raised annually as a result of customers failing to comply with their obligations.

Recommendation No.1

2.41 The ANAO recommends that Centrelink, in collaboration with FaCS as client agency, measure and/or assess the effects of the various education strategies and products on the level of customer compliance.

Centrelink response:

Agreed.

FaCS Response:

Agreed.

Getting it Right

2.42 A key element in Centrelink's renewed focus to improve payment accuracy by ensuring front-end processes are undertaken in accordance with policies and procedures is the recently released Getting it Right strategy. Getting it Right is supported by a CEO instruction mandating minimum standards that must be applied by all Centrelink staff when performing their duties. These minimum standards apply to processes and procedures where weaknesses have been identified, either through internal or external reviews, in Centrelink operations.[53] If implemented and evaluated appropriately, the Getting it Right strategy should assist Centrelink in improving the prevention of fraudulent activity.

Conclusion

2.43 The ANAO concluded that while Centrelink had a clear focus on prevention of fraud and had established appropriate procedures in relation to POI, there were coding errors in 22 per cent of the claims reviewed. Inaccurate information held on Centrelink systems adversely affects the quality of Centrelink's electronic records. This, in turn affects the efficiency of existing computer-based identity fraud detection methodologies and results in additional administrative costs for Centrelink.

2.44 In addition to formal POI procedures, Centrelink had developed and implemented a wide range of mechanisms to enhance its ability to prevent, as well as detect, identity fraud. This includes the development of a new model for POI. This should assist Centrelink to better manage risks associated with the proliferation of digital technologies that make it easier to create false documents and perpetrate identity-related fraud.

2.45 The ANAO concluded that processes implemented by Centrelink to prevent incorrect earnings declarations by its customers could be improved by requiring high risk customers to verify income and earnings from employment[54] to assist to reduce the number of debts raised due to honest mistakes made by customers.[55] The ANAO noted that, as part of the Australians Working Together Initiative, Centrelink is also exploring

---

53 Items covered by the minimum standards are POI, on-line docs, records management, recording reasons for decisions, skills and check the checking.

54 Existing procedures require only customers in exceptional circumstance to verify earnings they declare while on payment.

55 The announcement in the 2001–2002 Federal Budget to introduce an income bank for customers could also reduce the number of debts raised as a result of incorrect earnings declaration.

more cost-effective means of facilitating customers declaring earnings and of enabling automated background verification of key information with third parties.

2.46 To ensure all customers have access to relevant information, Centrelink aims to encourage voluntary compliance of customers through education targeted to particular customer sub-groups. However, only a limited evaluation had been undertaken of the various products to determine their effectiveness in achieving increased voluntary compliance. Centrelink considers that measurement of the effect of education strategies and products on the level of customer compliance is a matter for Centrelink's client agencies. This is illustrated by, for example, reference to the fact that FaCS recently conducted a survey on voluntary compliance involving Centrelink customers in four payment categories.

3. Review Activity

This chapter discusses Centrelink arrangements for detecting fraud and incorrect payment including data-matching, investigation of community tip-offs, inter-agency compliance activities and the use of optical surveillance. It also discusses Centrelink's approach to targeting review activities and improving the quality of reviews.

Introduction

3.1 Under the *Social Security Law*, customers are required to disclose information about changes in their personal and financial circumstances that affect their entitlement. However, there are risks associated with a reliance on voluntary disclosure by customers as people can fail to report relevant changes when they occur either through lack of understanding of their obligations, omission, mistake, or deliberately misrepresenting their circumstances.

3.2 Activities directed at ensuring compliance and detecting non-compliance, have a number of benefits for Centrelink, including:

- recovery of losses from incorrect payments as a result of fraud and incorrect payment;
- providing a level of assurance to the community and client agencies that customers who receive incorrect payments, particularly as a result of fraudulent conduct, will be detected and brought to account (this can act as a visible deterrent and encourage voluntary compliance); and
- strengthening the community's perception of the effectiveness of Centrelink in ensuring that only those who are eligible to, actually receive assistance and that these people receive the correct entitlement.

Overall review activity

3.3 Currently, the level of review activity to be undertaken by Centrelink in relation to program fraud is agreed with client agencies and specified in relevant Business Partnership Agreements (BPA). Under the BPA with FaCS, Centrelink is required to conduct two types of reviews, program reviews and compliance reviews.

3.4 Centrelink is required to conduct program reviews across all payment types. Program reviews generally have multiple objectives[56], are conducted by CSOs as part of their customer service role[57] and are generally undertaken by mail or by interview.[58] As the main focus of these reviews is not on detecting fraud and incorrect payment, the ANAO did not examine them during the audit. The ANAO did, however, sample 17 program review cases to determine whether the results recorded on NSRS provided and accurate reflection of the outcome from the review.

3.5 Compliance reviews examine a customer's circumstances where there is a perceived risk of incorrect payment or fraud. Centrelink undertakes more than one million compliance reviews on behalf of FaCS each year. The Detection and Review Team (DART) in the National Support Office (NSO) has primary responsibility for managing this work and reporting on outcomes. The aim of compliance reviews is to detect an error, omission, misrepresentation or fraud on the part of the customer. There are two types of compliance reviews—general and complex. Centrelink characterises complex reviews as those which either involve complexity in customer's circumstances, particularly their financial arrangements, or which involve complexity in the nature of the fraud carried out (including the difficulty of detection). Reviews which do not involve either of these complexities could be described as simple or general. Data-matching is used to generate both general (which represent about 90 per cent of all reviews) and complex reviews.

3.6 The ANAO examined the effectiveness of the following Centrelink detection compliance mechanisms used to detect fraud and incorrect payment:

- data-matching;
- community tip-offs;[59]
- inter-agency compliance review initiatives; and
- the Enhanced Investigation Initiative (EII).

---

56 The objectives include determining whether additional assistance through referral to specialist services is required, provision of information to customers and encouraging workforce participation.

57 These reviews are either periodic or cyclical in nature (for example, three monthly or annual) or based on significant life events of the customer (for example, a change in living arrangements).

58 For example, the three-month review of Newstart customers involves a variation of the standard form that is forwarded to customers fortnightly seeking additional information on a customer's circumstances. A proportion of these customers (40 per cent) is invited to Centrelink for a follow-up interview. The interview is used to assess on-going entitlement and to determine whether the customer requires additional assistance.

59 Members of the public often provide Centrelink with information, known as community tip-offs, about people who may be incorrectly receiving a social security payment.

3.7 As well, the ANAO assessed whether review activity was appropriately targeted to areas of higher risk and the quality of reviews undertaken.

3.8 Table 3.1 provides an overview of the main detection mechanisms implemented by Centrelink with an assessment of their effectiveness in detecting fraud and incorrect payment. A more detailed discussion of the effectiveness of each strategy follows the table.

Table 3.1

Centrelink tools for detecting and investigating fraud and incorrect payment

Centrelink tools or information sources	*Assessment of effectiveness*		*Comment*
	Incorrect payments and opportunistic fraud	*Complex fraud*[1]	
Data-matching[2]	✓	Partial	Provides significant benefits where relevant information is held by other agencies to: • uncover and reduce fraud and incorrect payment; • encourage better compliance; and • improve the quality of data held on Centrelink systems.
Community tip-offs	✓	Partial	Important source of intelligence, particularly where data-matching capacity is limited.
Inter-agency partnerships	✓	✓	Improvements in inter-agency cooperation demonstrate a more integrated whole-of government approach to dealing with fraud against the Commonwealth.
Enhanced Investigations	✓	✓	Useful tool to assist the review process and provide additional evidence of fraudulent activity.

✓ = ANAO considers effective Partial = ANAO considers to be on partially effective in relation to complex fraud.

1 Complex fraud includes cases where income is derived from the cash economy, collaboration between customers and staff and other systemic frauds designed to circumvent existing detection mechanisms.

2 Includes more sophisticated computerised techniques such as data mining and transaction analysis which are primarily used in the identification of identity fraud.

Data-matching

3.9 Data-matching is the main tool used by Centrelink for preventing and detecting fraud and incorrect payment. Centrelink has a sophisticated and comprehensive data-matching program and matches data with a large number of Commonwealth and State organisations. The main data-matching projects conducted by Centrelink, together with the payment risks being addressed and the agencies with which information is matched are outlined in Appendix 4.

3.10 In 1999–2000, more than 60 per cent of data-matches occurred as a result of Centrelink information matched with data held by the Australian Tax Office (ATO) indicating cases where customers had recently commenced employment.[60] Overall, data-matching with the ATO (including that which showed employment had commenced) accounted for nearly 80 per cent of all data-matching conducted by Centrelink, generating 68 per cent of savings and 83 per cent of debts raised from data-matching in 1999–2000. Table 3.2 outlines the results from each of the main data matches conducted by Centrelink for the last two years and provides an indication of the level of data-matching activity that takes place.

Table 3.2
Results of Centrelink data-matching for last 3 years

	1998–99			*1999–2000*		
	Number of reviews	*Savings[1] ($'000)*	*Debts ($'000)*	*Number of reviews*	*Savings[1] ($'000)*	*Debts ($'000)*
Tax File Declaration Form (TDF)	575 150	7005	123 207	532 325	6323	123 428
Data-Matching Program (DMP)	178 308	1993	80 954	146 070	1852	75 708
Immigration	71 985	1415	8364	53 872	663	7662
Enrolment	12 765	184	2679	50 897	713	22 860
Corrective services	18 565	1127	4172	23 190	1543	3928
Other[2]	48 906	1400	13 155	76 833	1299	19 931
Total	**905 679**	**13 124**	**232 531**	**883 097**	**12 393**	**253 517**

1 Annualised fornightly savings.

2 Other included 21 781 Australian Stock Exchange (ASX) data matches and 24 169 rent assistance data matches for 1999–2000.

60 Tax File Number Declaration Form matches (TDF) using employee data sent to the ATO by employers at the time a new employee commences work. This matching was previously undertaken using details from Employment Declaration Forms (EDF), however, these were replaced by the TDF on 1 July 2000 as part of the new tax system. This matching process now incorporates matching on both the TFN and on the customer's other identity details (for example, customer's name). It is anticipated that using the TFN to match data will provide tighter, more correct matches than previously under EDF matching based on the customer's name.

3.11 The ANAO examined Centrelink's data-matching to see whether:

- it was guided by business rules and legislation;
- it was conducted in a timely fashion;
- new areas of coverage were being examined; and
- residual risks resulting from data-matching were addressed.

3.12 The ANAO also assessed whether there were any further opportunities for data-matching and identified the use of country of birth information for testing. Each of these matters is discussed under separate headings below.

Business rules and legislation

3.13 Centrelink had established business rules and risk parameters for its data-matching that were designed to ensure high quality selections for review.[61] This approach is aimed at identifying higher risk cases on the basis of key criteria such as recent employment history and level of income declared in tax returns. As well, a formal evaluation program had been developed to:

- delete projects which address obsolete risks;
- ensure data-matching projects are run at optimum times; and
- change project parameters to more accurately reflect, among other things, income limits for payments.

3.14 Data-matching undertaken with external organisations is governed primarily by the:

- *Data-matching Program (Assistance and Tax) Act 1990;* and
- the Privacy Commissioner's Guidelines for *The Use of Data-Matching in Commonwealth Administration*.

3.15 The ANAO found that Centrelink had implemented appropriate processes for ensuring that the data-matching it conducts conforms with legislative requirements and that data obtained as a result of a match is subsequently destroyed as required by the Privacy Commissioner's Guidelines.

---

[61] Business rules specify the type of records to be matched; the matching criteria (or match keys) used to match one record against another; and the refining criteria (sub-sets) to be applied to match keys in order to further eliminate cases where there is no need for review. The matching parameters for the different matching projects conducted are selected on a risk- based approach.

Timeliness of data-matching reviews

3.16 The timeframes that have been established for conducting data-matching are based on an assessment of risk, legislative requirements and the availability of information being matched from source agencies. For example, the high number of customers who fail to notify Centrelink that they have obtained employment, full-time or casual, has resulted in Centrelink conducting Tax File Declaration Form (TDF) matching on a weekly basis. The frequency of data-matching ensures that Centrelink is able to recover incorrect payments in a timely manner. It also ensures that debts are minimised for customers who had not reported changes in their circumstances.

3.17 The ANAO's analysis of compliance reviews found that every effort was made by Centrelink to conduct them in a timely manner. In most cases data match reviews were completed within three months of the information being matched and released.

3.18 In relation to TDF matching, the ANAO considered that Centrelink should, jointly with the ATO, examine the opportunities for TDFs to be lodged by employers directly with Centrelink for processing and data entry. This would assist to improve timeliness of reviews and help reduce the size of all debts incurred by the customer.

Coverage of Centrelink's data-matching capability

3.19 Centrelink's main focus over recent years has been to identify additional opportunities and sources of information for data-matching, based on an assessment of risk, to broaden the coverage of its detection capability,[62] particularly in the areas of detecting undisclosed income[63] and assets.[64] Identifying cost effective detection mechanisms for emerging risks, such as overseas investments, was not, however, as advanced.

3.20 For each new data-matching opportunity identified Centrelink had, in consultation with client agencies, conducted a formal pilot and assessed the results achieved to determine the cost-benefit ratio and the capacity of the project to help manage previously unaddressed risks. Centrelink had also consulted with the Privacy Commissioner in relation to new data-matching proposals that involve the handling of personal information and privacy issues.

---

62 A particular emphasis has been on better leveraging information provided to the ATO in tax returns.

63 Especially in relation to income from self-employment and investments.

64 These include undisclosed assets such as property, shares, companies and trusts.

3.21 Some of the trials included:

- electronic Pay As You Go (PAYG) Payment Summary matching to identify customers earning income but not lodging tax returns;[65]
- identifying customers with undisclosed assets, primarily beneficial interests in trusts, shareholdings in private companies and undisclosed investment properties. Data-matching programs were being developed with ATO trust data and Australian Securities and Investment Commission (ASIC) private company data;
- matching against ATO's Annuity and Superannuation Pension declarations and Reasonable Benefit Limits data; and
- the planned Australian Business Number (ABN) matching pilots to help identify self-employment income in a timely manner.[66] A proposal was approved in the 2001–02 Budget to undertake a pilot based on this data.

New areas of coverage

3.22 The correct coding of country of birth details is an important aspect of Centrelink's identity fraud capability. The ANAO found in those Centrelink Areas where a higher proportion of customers required country of birth verification that there was a lower error rate than where the need to code country of birth details was not common.[67]

3.23 To assist Centrelink's Identity Fraud Team to refine its suspected identity fraud case selection list, the ANAO facilitated a pilot data-matching exercise between Centrelink and the Department of Immigration and Multicultural Affairs (DIMA) during the audit. It was also anticipated that indirect benefits would accrue from the pilot, including improved data quality for both Centrelink and DIMA and the identification of overstayers who were incorrectly receiving benefits. The pilot matched DIMA last movements for the past 10 years with customer information held on Centrelink payment systems.

---

65 A proposal was approved in the 2001–02 Budget to undertake a pilot based on matching this data.

66 This is a particular issue for FTB where customers are required to estimate their, or their partner's, earnings, and reflects a focus by Centrelink on ensuring that customer debts are minimised.

67 At the time of audit fieldwork some Areas had error rates exceeding 20 per cent. An inappropriate default which coded country of birth to Australia has subsequently been corrected. This default was responsible for some of the errors detected.

3.24 Prior to conducting the data-match Centrelink's IFT had identified and recorded on its systems nearly 40 000 high risk suspected identity fraud records. Of these, 44 per cent had their country of birth recorded as Australia and 56 per cent were recorded as overseas born. The suspected identity fraud cases recorded on IFT systems require substantial resources to be applied to investigate whether actual fraud has occurred in these cases.[68] Table 3.3 shows the results of the data-match.

Table 3.3

Reduction in the number of high risk cases as a result of pilot data match exercise

High risk cases	*Before data-match*	*After data-match*	*Per cent reduction (%)*
Country of birth—Australia	17 526	6041	65.5
Country of birth—other	22 293	8184	63.3
Total	39 819	14 225	64.3

3.25 This Table shows the benefit of data-matching. It means that resources which would have been directed at reviewing and investigating the approximately 40 000 cases identified as being at high risk to determine whether identity fraud had actually been committed can be more effectively allocated to the 14 000 cases remaining after the data-match occurred. This should improve the potential to detect actual cases of fraud.

3.26 The pilot also identified substantial scope for improvement in the quality of data held by both Centrelink and DIMA. Centrelink advised that, in consultation with DIMA, processes would be established with the aim of improving the quality of data held on relevant systems.

3.27 Given the potential benefits identified during the pilot for improving case selections for suspected identity fraud cases and improving data quality, Centrelink should investigate opportunities for conducting similar matching on a regular basis.

Residual risk areas

3.28 While Centrelink had been active in expanding its data-matching capability, there are a number of areas of risk that are currently not adequately addressed through existing data-matching. These areas include:

- self-employment and investment income—Centrelink is examining a

[68] It must be noted that these 40 000 cases are the highest risk cases recorded on IFT databases. A substantial number of proven frauds are from lower risk categories that are also recorded by the IFT as part of its data mining and other analytical analysis of customer records.

range of data-matching strategies to improve its ability to identify and accurately assess such income;[69]

- undisclosed assets (including overseas investments)—during 2000, Centrelink commenced matching with the ASIC to detect undeclared interests in private companies and the ATO to detect undeclared interests in trusts and companies;
- the cash economy—Centrelink's main means of detecting such earnings is through community tip-offs and inter-agency partnerships[70]; and
- marriage-like relationships (MLRs) as specified in legislation[71]—Centrelink relies on risk based algorithms including an automatic review of new births nine months or more after grant for Parenting Payment Single customers and by some data-matching (for example, ACM Rent Assistance and Defence Housing matching). As well, community tip-offs aid the detection of non-compliance associated with MLRs.

3.29 Centrelink had implemented a number of measures to improve its ability to effectively, detect and investigate non-compliance relating to the cash economy. It had established procedures for working more closely with the ATO and DIMA to gather intelligence and targets its optical surveillance capability, through the Enhanced Investigation Initiative (EII—discussed further below), to such cases.

3.30 Centrelink conducts program reviews of all customers receiving Parenting Payment Single (PPS) payments at predetermined intervals. However, its primary detection mechanism for fraud and incorrect payment is information received through community tip-offs.[72] Centrelink reviews all community tip-offs, including where a MLR is alleged resulting, at times, in a less than effective use of resources.

---

69 A new initiative was announced in the 2001–02 Budget to undertake 18 000 investment property reviews over the next two years.

70 Centrelink is currently piloting an initiative to work with the AFP, DIMA and the ATO to identify and review customers working in high risk cash economy industries.

71 Under current legislation, Centrelink must demonstrate that two people meet five specific criteria to consider them as a member of a couple and living in a marriage-like relationship with no one factor being determinative. In particular, Centrelink must have regard to and assess the financial aspects of the relationship; the nature of the household; the social aspects of the relationship; any sexual relationship between the people; and the nature of the people's commitment to each other.

72 Some data-matching can also identify the existence of undeclared MLRs such as Defence Housing matching.

3.31 During the audit, the ANAO identified a number of measures that could improve Centrelink's targeting of reviews to establish the existence of MLRs:

- making better use of information gathered during program reviews;
- better use of information gathered from its customers in relation to Family Tax Benefit payments (internal data-matching); and
- introducing data-matching, or otherwise improving sharing of information with the Child Support Agency (CSA).

3.32 The ANAO considered that Centrelink was making a significant effort to address areas of residual risk but could further improve its targeting of review activity in relation to MLRs as specified above.

Community tip-offs

3.33 Community tip-offs are a valuable source of information in identifying abuses of the income support system and play an important part in contributing to improved customer compliance. Tip-offs are received through CSCs and Call Centres, other agencies who receive allegations of fraud relevant to Centrelink payments, the Minister's Office and through the mail.[73]

3.34 Centrelink's stated policy is to investigate all tip-offs where the person named in the allegation can be identified as a customer. Table 3.3 provides details on the numbers of reviews conducted as a result of tip-offs and results recorded for the last three financial years.

Table 3.3
Tip-offs results for last three financial years

Year	*Total reviews*	*Cancellations No. (%)*	*Downward adjustment No. (%)*	*Fortnightly savings ($)*	*Debts raised No. (%)*	*Debt ($)*
1997–98	55 456	5337 (9.62)	9 555 (17.23)	3 316 548	7 957 (14.35)	23 898 717
1998–99	49 052	4924 (10.04)	10 428 (21.26)	3 183 283	10 406 (21.21)	29 896 405
1999–00	55 009	3911 (7.11)	10 602 (19.27)	2 900 602	1 035 (18.82)	29 915 566

3.35 National procedures for handling and recording community tip-offs had been developed and aim to ensure Centrelink responds efficiently and effectively to information provided by the public. To support the management of community tip-offs Centrelink had implemented a

[73] Centrelink will be developing an internet site that will allow members of the public to record and send tip-off information to Centrelink for investigation. This initiative is in line with the Government's policy on electronic service delivery.

nationally accessible electronic tip-off recording system (TORS). This system provides a standard format for the collection of data. Links had been established between TORS and Centrelink's payment systems to ensure that tip-off information is recorded against a customer's record.

3.36 Recently, Centrelink and the ATO implemented measures to improve the exchange of information between the two agencies in relation to community tip-offs. Of the cases currently recorded on CISCO (the ATO's tip off recording system) nearly 25 per cent have been identified by the ATO as having potential Centrelink implications.

Investigating community tip-offs

3.37 Effective handling of tip-offs is a key element in maintaining confidence in the integrity of income support payments. Teams have been established in ASOs dedicated to investigating community tip-offs and Centrelink had developed policies and procedures to assist teams with prioritising community tip-offs and ensuring cases were investigated in a timely manner.

3.38 There were also clear guidelines for deleting tip-offs[74] where the alleged offender was not a Centrelink customer or inadequate information had been provided to Centrelink. The ANAO's analysis found that the tip-off deletion process could benefit from a broader quality assurance process to provide further assurance to key stakeholders that all tip-offs are receiving appropriate attention and are not inappropriately being set aside. To address this issue Centrelink advised that, as part of a 2001–02 Budget initiative, it would be establishing a specialist tip-off processing unit to ensure tip-offs are deleted appropriately on all occasions.

3.39 During 2000–2001, Centrelink had a performance indicator requiring tip-off review investigations to be completed within 42 days (from the date of receipt to the completion of a tip-off investigation) in 90 per cent of cases. The sample of tip-off investigation files reviewed by the ANAO found that 44 per cent of tip-off investigations were not completed within the 42 day timeframe. Furthermore, 39 cases (13.5 per cent) took more than six months to complete with the investigation of five of these cases taking more than one year.[75]

---

74 Deleted tip-offs represent more than 10 per cent of all tip-offs recorded on TORS.

75 The ANAO noted that timeliness information could be improved, as currently such information is not collected about deleted tip-offs.

3.40 Centrelink recognised the need to not just focus on timeliness, and that target compliance officers must understand the need to (and have the opportunity to do so) undertake reviews in a way that identifies fraud and incorrect payment rather than being driven only by a target.

Inter-agency compliance initiatives

3.41 Over recent years Centrelink had placed considerable emphasis on improving inter-agency cooperation with regard to compliance issues.

3.42 Two key initiatives established by Centrelink to foster effective inter-agency compliance activity are:

- Centrelink / ATO Special Project Officers (CASPOs),[76] and
- Inter-agency Cash Economy Field Investigation Team (ICEFIT), involving Centrelink, working with the ATO, AFP and DIMA.[77]

3.43 Results from CASPO activities show that CASPOs have been successful in identifying larger debts compared with debts identified by other Centrelink compliance activities. The average debt raised nationally for 1999–2000 was in excess of $2700 but averages achieved by individual CASPOs have exceeded $6000.[78] Of the 1154 debts raised across all compliance activities in excess of $10 000 for 1999–2000, CASPOs identified 108, representing approximately 9.4 per cent of all such debts even though the number of CASPO reviews accounted for less that 0.2 per cent of all reviews conducted by Centrelink. This indicates the value of CASPO activities.

---

[76] Guidelines have been developed for the communication of information from the ATO to Centrelink that sets out in detail the type of information that can be provided to CASPO's. The legal authority for the ATO to communicate information to Centrelink is provided in the *Income Tax Assessment Act 1936* Sections 16(4)(e), (ea) and (eb). The guidelines also make reference to the relevant Information Privacy Principles contained in the *Privacy Act 1988.*

[77] Centrelink established the inter-agency cash economy field investigation team (ICEFIT), a new two-year pilot project, which commenced on 1 January 2001 and was funded as a budget initiative in the 2000–01 Budget, to address the important strategic issues of extending links and seeking opportunities in emerging areas of cross agency interest. The primary objectives of the pilot are to:

- identify customers who fail to declare cash income earned from employment in high risk cash economy industries;
- assess the feasibility using field teams to enhance Centrelink's capability to detect customers operating in the cash economy;
- assess the feasibility of enhanced inter-agency cooperation in detecting customers operating in the cash economy; and
- identify program savings arising from investigation of these customers and their partners.

[78] The average debt raised for all compliance reviews for 1999–2000 was $883.45.

3.44 Centrelink has used the results of particular CASPO initiatives to improve its detection mechanisms. For example, the PAYG pilot announced in the 2001–02 Budget was based on a successful CASPO initiative.

3.45 Similarly, the ANAO found that initial piloting of the ICEFIT concept prior to its formal implementation provided good returns in high risk areas where traditional detection techniques such as data-matching are generally not very effective. Joint investigations involving Centrelink, the ATO and DIMA[79] have resulted in illegal entrants being removed from Australia and the detection of systematic tax and welfare offences. The ANAO considers that it will be important that the results derived from the projects undertaken by ICEFIT in conjunction with other agencies, are recorded in a way that identifies the results achieved for all of the agencies involved. This would demonstrate the value of a collaborative approach.

3.46 Centrelink has also extended inter-agency activities beyond joint investigations to also include joint prosecution activity. Joint prosecutions have been conducted in partnership with the ATO involving both tax evasion and welfare fraud.

Relationship with the Australian Federal Police (AFP)

3.47 The AFP is responsible for investigating cases of serious and complex fraud against the Commonwealth.[80] Centrelink had developed an effective working relationship with the AFP at both the national and local level. Centrelink's liaison with the AFP primarily revolves around two key issues, that is investigation and training. A Service Agreement (SA) has been developed that clarifies the roles and responsibilities of the two agencies as well as provides detailed guidance on the types of cases that should be referred to the AFP for investigation.

Enhanced Investigation Initiative

3.48 The Enhanced Investigation Initiative (EII) is concerned with the management of Centrelink's optical surveillance[81] capability.

---

79 Joint investigation can also involve State Police and the AFP.

80 Fraud Control Policy of the Commonwealth.

81 Optical surveillance primarily involves the observation of person/s suspected to be committing acts of social security fraud for the purpose of gathering evidence to prove that fraud has occurred. The use of optical surveillance to assist Centrelink fraud investigations was approved by Cabinet in November 1998.

3.49 The ANAO found that Centrelink had taken appropriate steps to ensure that all privacy principles are met when selecting cases for surveillance and in conducting surveillance.[82] Centrelink has developed two sets of comprehensive guidelines, one for EII officers referring cases for surveillance and one for the service providers contracted by Centrelink to conduct the surveillance.[83] Service providers are also required to adhere to the *Guidelines for the Conduct of Covert Optical Surveillance in Commonwealth Administration*, published by the Privacy Commissioner in 1992 and the Information Privacy Principles in the *Privacy Act 1988*.

3.50 Optical surveillance is only used as a tool to support the review process. The decision to request optical surveillance to assist in the investigation of a case is mainly based on the following two criteria which are specified in Centrelink's *Guidelines for Referring Cases for Surveillance Activity*:

- where there is a reasonable suspicion that an offence or an unlawful act is being, or has been, committed; and
- where other forms of investigation have been considered and assessed to be unsuitable or other forms of investigation have been tried and found to be inconclusive.

3.51 Trained EII officers have been established by Centrelink to manage the initiative at the Area level. They are responsible for approving cases for referral to service providers so that surveillance can be conducted and for monitoring the performance of providers to ensure compliance with the EII guidelines and the specific instructions that are issued for each case.

3.52 The ANAO's review of selected case files against Centrelink's internal Guidelines showed that documentation and exhibits were appropriately referenced, project officers documented all communications with service providers and other related parties and reports prepared on the surveillance activity clearly summarised the surveillance conducted (for example date and time of surveillance) and what was observed. To facilitate effective project management, EII officers interviewed by the ANAO had established a secure database to monitor progress of cases and reporting of outcomes.

---

82 A separate file is maintained for each case referred for surveillance. These files are distinct from the customer's payment file and are stored in lockable filing cabinets as prescribed in Part IV of the Commonwealth of Australia Protective Security Manual.

83 In selecting service providers, Centrelink undertook a rigorous tender process for private surveillance firms to provide optical surveillance services to the agency, with a total of 21 service providers being selected nationwide. These providers are appropriately licensed and were approved by Centrelink following vetting through the Australian Security Vetting Service (ASVS).

3.53 The initiative has also highlighted inter-agency benefits. Of the cases finalised by Centrelink a number were referred to other agencies for examination. These included 179 cases to the ATO for consideration and three to DIMA. As well, 51 cases have been referred to the AFP and 77 to the DPP for consideration.

3.54 The ANAO found that the evidence-gathering power of the EII has made a positive contribution to Centrelink's review capability in that it has provided evidence that would not have otherwise been available. The use of optical surveillance has proven particularly effective in investigations relating to failure to declare earnings, including income arising from the cash economy, and disability cases where video evidence can often be conclusive in proving whether an alleged offence or fraud is being committed. Consequently, Centrelink has sought to ensure that EII resources are targeted to these types of alleged offences, with other cases prioritised on the basis of risk.

Targeting review activity

3.55 With limited resources, an effective means of targeting review activities is essential. The 1999–2000 and the 2000–2001 BPA between Centrelink and FaCS specifies that 30 per cent (compared with 10 per cent for the preceding period) of compliance reviews conducted by Centrelink should result in an incorrect payment being identified.

3.56 The ANAO found that Centrelink's targeting of compliance review activity could be enhanced further as there are still a significant proportion of cases that are selected for review where no fraud or incorrect payment is identified. Current review arrangements mean that there is limited integration between program reviews and compliance reviews or between reviews conducted in the various payment groupings. This can result in some customers being subject to multiple reviews where such activity may not be warranted. A recently completed joint review conducted by Centrelink and FaCS, known as the Review of Review Activities (RORA), also recognised that improved integration and better targeting of review activities was required.

3.57 By improving its knowledge of specific customers and groups of customers Centrelink could improve the targeting and cost-effectiveness of its compliance activities. Within this context, the ANAO assessed whether Centrelink was using the customer information it collects and stores to improve its knowledge of customers and subsequently improve the targeting of review activities.

3.58 Centrelink acknowledged that each contact with the community can be classified as an opportunity to learn about customers and associated compliance issues. To date, significant effort and emphasis has been placed on creating a service delivery culture in Centrelink. The focus has been to increase understanding of customer needs to better align Centrelink service delivery with community expectations.

3.59 The ANAO noted that Centrelink did have risk-based algorithms, to target incorrect payment that were based on data from a random sample of previously conducted field reviews. However, the results achieved from these review types demonstrate the difficulties Centrelink has had in developing a reliable method for targeting high risk customers.[84]

3.60 In the 2001–02 Budget provision was made for the conduct of a risk profiling pilot that will use available data on customer characteristics to develop profiles of customers at high risk of incorrect payment. If developed successfully, customer risk profiling could assist in targeting high risk customers and groups of customers as well as identifying emerging compliance and fraud risk exposures. Profiling could also act as a deterrent for customers who currently believe Centrelink is unlikely to detect their non-compliance.

3.61 As well, projects have been commenced by FaCS, with the assistance of Centrelink, which have the potential to yield useful information about customers, particularly in relation to fraud and incorrect payment. These projects include research into voluntary compliance and random sample surveys.[85] While these projects are not specifically targeted at developing compliance profiles, information gathered could help both organisations to identify areas of non-compliance; better understand compliance risks; and develop strategies to ensure long term voluntary compliance.

3.62 The ANAO recognises that data-matching projects had been largely derived on the basis of identified risk exposures. However, more detailed analysis of tip-offs and results from random samples[86] could

---

84 For 1999–2000, 16 622 Masterfile selection reviews were conducted that resulted in payment cancellations or reductions in only 8 per cent of cases and debts in only 0.9 per cent of cases.

85 The surveys, which are undertaken by Centrelink on behalf of FaCS, aim to derive a reasonable measure of the per centage of incorrect payment for the selected programs that are reviewed. They also provide useful information on reasons for incorrectness.

86 Centrelink and FaCS are currently conducting random samples to determine the reason incorrect payment is not being detected by the existing control framework, and to identify new and emerging risks of incorrect payment that need to be controlled by new initiatives.

enable Centrelink to develop a clearer understanding of the causes of fraud and incorrect payment, provide Centrelink with significant opportunities to enhance its detection mechanisms, better target its review activity, including refining its data-matching strategies, and identify emerging fraud trends. Centrelink advised that, as part of the 2001–02 Budget, resources would be allocated to analyse tip-off information.

Quality of reviews

3.63 The quality of reviews significantly influences the review outcome. Poor review practices may result in Centrelink failing to detect and properly investigate cases of fraud and incorrect payment. They may also signal to the community a deficiency in Centrelink's ability to detect such activities and thus undermine the integrity of the welfare system. An integrated quality review program involves:

- promulgation of review standards; and
- systematic monitoring of the quality of reviews aimed at identifying sub-standard review activity with reference to standards.

3.64 Centrelink had developed and promulgated review standards in a wide range of documents that are available on its intranet, including a comprehensive Guide to Reviews, an investigators manual and other manuals covering related topics such as guidelines for surveillance, prosecutions. As well, DART had its own site on the intranet that contains appropriate links to other relevant sites to assist review staff and investigators.

3.65 A recurrent theme from feedback received from Centrelink staff during fieldwork was that there was a strong focus on achieving performance targets related to the number of reviews and levels of savings. This focus has at times led to inadequately completed reviews, with evidence being overlooked, little attention paid to determining the reasons for particular review outcomes and action that could be taken to reduce the risk of re-offence. The main reasons provided for this included:

- resource and time constraints did not permit a thorough review of a customer's circumstances to be conducted in all cases; and
- an office interview was not adequate to obtain sufficient evidence of a customer's circumstances.

3.66 Given the reliance on review processes for ensuring maximum return from data-matching this is an area requiring improvement.

3.67 As well, the ANAO's analysis of community tip-offs suggested that performance targets associated with the timeliness of reviews may have adversely influenced the quality of some reviews and investigations undertaken. Failure to conduct quality reviews could result in incorrect payments remaining undetected for long periods, impacting on the level of debt incurred by customers as well as undermining community perceptions about Centrelink's ability to maintain the integrity of the social security system.

3.68 The ANAO did note that informal feedback was sometimes provided to review staff by prosecution staff where a file forwarded for prosecution was inadequate. However, this process was not consistent across the network.

3.69 At the time of the ANAO fieldwork, there was no regular assessment of the quality of these reviews to identify any that were sub-standard even though the way they are conducted can significantly affect whether the review detects fraud or error. Centrelink advised that, as part of the Getting it Right strategy launched in November 2000, its on-line quality assurance system (QOL) had been enhanced. As well, QOL was to be supplemented by a secondary checking regime to test the quality of review processes.

3.70 Under the current BPA (2001–04), Centrelink and FaCS will review the control and business partnership assurance framework for payment correctness during 2001–02. Centrelink, and FaCS envisage that this review will result in improved quality and assurance processes, as well as improvements to processes that provide information on correctness of payments.[87] Centrelink advised the ANAO that negotiations relating to the review of the assurance framework are presently being undertaken.

Recommendation No.2

3.71 The ANAO recommends that Centrelink quickly conclude its current negotiations, with its client agencies, aimed at obtaining an improved Business Assurance Framework, to help ensure that all reviews meet established standards and provide the best possible results.

Centrelink response:

Agreed.

FaCS response:

Agreed.

---

87 Business Partnership Agreement between Centrelink and FaCS 2001–2004.

Conclusion

3.72 The ANAO concluded that Centrelink had maintained an effective compliance function and had a range of controls for detecting fraud and incorrect payment. This included the use of an extensive data-matching program that matches data with a large number of Commonwealth, State and Territory agencies. This is guided by business rules and risk parameters designed to enable higher risk cases to be identified based on key criteria such as recent employment history. Appropriate processes had been established by Centrelink for ensuring that the data-matching it conducts conforms with the requirements of data-matching and privacy legislation.

3.73 While Centrelink has actively sought to identify additional opportunities and sources of information to strengthen the coverage of its data-matching particularly in detecting new areas of risk, there are inherent limitations of data-matching, such as the type and quality of information held by external agencies, that result in a number of residual risks. However, Centrelink had developed a number of strategies to manage residual risks and improve its ability to deal with more complex cases of welfare fraud, for example, using surveillance to obtain information of fraudulent activity.

3.74 Centrelink collects and stores large amounts of data and intelligence relating to review results, but it had not fully analysed this compliance information to ensure that it effectively targets higher risk customers for its more complex review activities. An improved understanding of customers could be obtained by developing customer risk profiles. Better targeting of customers would also assist Centrelink to implement cost-effective preventative compliance measures. Work to trial risk profiling of customers was announced in the 2001–02 Budget. Risk of incorrect payment will be one of the key aspects of profiles, which should enable customer contact and reviews to be better targeted at minimising and preventing incorrect payment.

3.75 The ANAO concluded that current compliance activities, including an extensive data-matching program, would detect a significant proportion of fraud and error when it occurs. Appropriate processes had been established by Centrelink for ensuring that the data-matching it conducts conforms with the requirements of data-matching and privacy legislation. Centrelink also conducts more than one million compliance reviews each year, most of which are triggered by data-matching results. At the time of the ANAO fieldwork, there was no regular assessment of the quality of these reviews to identify any that were sub-standard even though the way they are conducted can significantly affect whether the

review detects fraud or error. Centrelink advised that, as part of the Getting it Right strategy launched in November 2000, its on-line quality assurance system (QOL) had been enhanced. As well, QOL was to be supplemented by a secondary checking regime to test the quality of review processes.

4. Dealing with Fraud and Incorrect Payment

This chapter examines Centrelink's use of penalties and remedies for dealing with fraud and incorrect payment when it is discovered. The major focus was on Centrelink's application of activity test breaches and formal cautions as well as the use of prosecutions for dealing with more serious cases of welfare fraud.

Introduction

4.1 Once a fraud or incorrect payment has been detected, investigated and been found to have occurred, it is important that Centrelink takes appropriate action to deal with the offence. The *Social Security Law* provides the legislative basis for the imposition of a range of penalties and sanctions where fraud or incorrect payment is detected.

4.2 By their very nature, penalties are intended to treat a particular offence and act as a deterrent to those customers who otherwise may not comply with their obligations. Penalties imposed on customers who fail to comply with their obligations are an important aspect of Centrelink's overall compliance strategy. The main mecahanisms available to Centrelink include:

- adjusting payments, raising and recovering debts;
- imposing activity test breaches;
- issuing formal cautions; and
- prosecuting offenders.

4.3 The ANAO also examined whether Centrelink could assess the deterrent effect of these mechanisms.

4.4 In order to ensure that these measures to deal with fraud and incorrect payments fairly, customers have the opportunity to object to penalties imposed by Centrelink. Centrelink has established Authorised Review Officers (AROs) to provide an internal independent review of decisions made by Centrelink officers. Customers can also seek review of decisions through the Social Security Appeal Tribunal (SSAT), the Administrative Appeals Tribunal (AAT) and the courts. These review processes were not considered during this audit.

Adjusting payments and raising debts

4.5 Adjusting payments, raising and recovering debts is the major method used by Centrelink to deal with overpayments. It should be noted that when conducting reviews to identify overpayments Centrelink does not, in most cases, seek to determine whether a failure by a customer to meet their obligations and report changes in their circumstances is fraudulent or not, even though such notification is required by customers under legislation.[88] Rather, it deals with the majority of these cases in the most efficient manner available, by either reducing or cancelling the customer's payment[89] as well as raising and recovering a debt where necessary. This is appropriate given that the proof of intent to defraud is often difficult to establish and the capacity to undertake prosecutions is limited by resources. The ANAO did not therefore review this particular treatment.

Activity test breaches

4.6 The ANAO examined whether activity test breaches and formal cautions were applied consistently in line with legislation and internal procedures and guidelines.

4.7 The Social Security Act 1991 sets out the legislative requirements of the Newstart (NSA) and Youth Allowance (YAL) activity test[90] and penalties that can be imposed for breaches of the test. These penalties can be significant in terms of loss of payment.

4.8 The ANAO analysis focused on the application of activity test breaches as it is these types of breaches that are imposed where fraud or incorrect payment is detected through compliance activities.[91] An escalating scale of activity test breach penalties is intended to deter customers from re-offence. Table 4.1 shows the number of activity test breaches imposed by Centrelink over the last three years.

---

88 A high level of proof is necessary in order to establish that fraud has been committed by the customer. In many cases the cost of establishing fraud is prohibitive.

89 The ANAO found that where eligibility to receive a level of payment is found to be incorrect during the course of a review the amount of benefit received is adjusted immediately.

90 The activity test is a set of criteria and actions that applicants for Newstart and Youth Allowance need to meet in order to be eligible for payment. The activity test forms the basis of a welfare recipient's mutual obligation. Customers are provided with advice as to their rights and responsibilities the activity test at new claim stage and subsequent contacts.

91 For example, an activity test breach occurs when a person refuses to declare, or fails to correctly declare, earnings from employment.

Table 4.1

Number of breaches per financial year

Period	Newstart		Youth Allowance	
	Number	Percentage increase since previous period (%)	Number	Percentage increase since previous period (%)
July 1998–June 1999	54 241	n/a	15 941	n/a
July 1999–June 2000	136 020	150.8	40 294	152.8
July 2000–Apr 2001	155 564	37.2[1]	52 288	61.8[1]

1 This figure has been obtained by annualising the number of breaches applied between July 2000 and April 2001.

4.9 Based on Centrelink data, 24.3 per cent of all activity test breaches applied from 1 July 1999 to 31 May 2000 were imposed as a result of a failure to correctly declare earnings from employment.[92] These failures to declare earnings may or may not have been fraud.

4.10 Based on analysis of compliance reviews[93] the ANAO found that rules regarding date of effect for activity test breaches were not being consistently applied because of a lack of understanding among Centrelink staff as to what stage of the review process a breach should be imposed. While the majority of breaches were imposed on the same date a debt was raised for a particular offence, there were a number of cases reviewed where breaches were imposed on the date the review commenced and a number of breaches imposed some time after review finalisation. This suggests a gap in knowledge among some review staff and leads to inconsistent treatment of customers. Centrelink should identify the training requirements for staff who are unclear about the legislative requirements for imposing breaches. Centrelink advised that a broad training package would be delivered during 2001 across the network to address this issue.

92 Job Network Member recommendations comprised 41.7 per cent of all breaches imposed. These recommendations were made primarily for customers failing to attend job interviews.

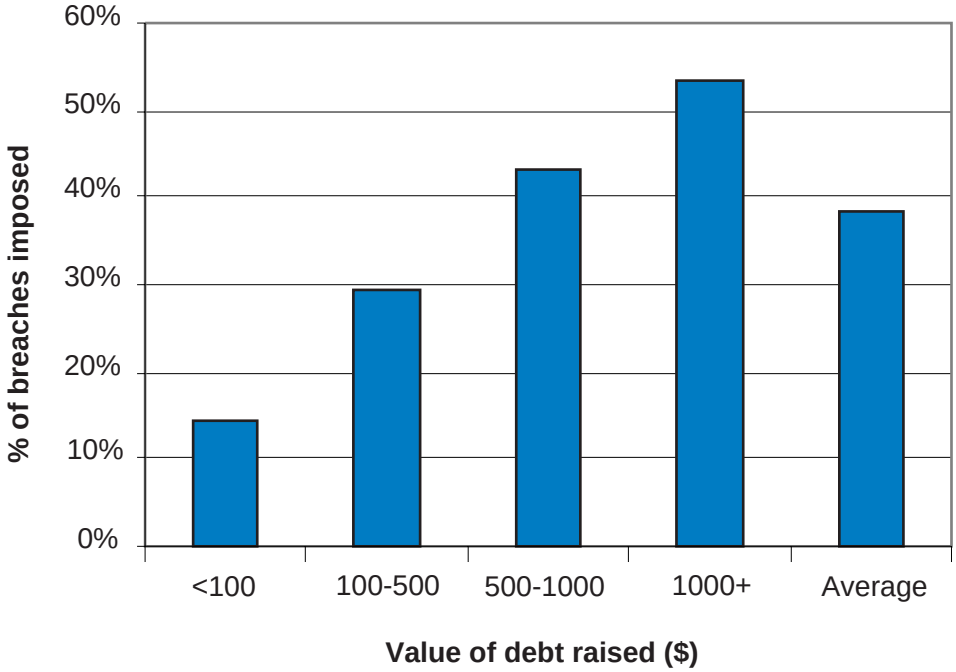
93 Based on the ANAO's examination of compliance reviews and tip-off investigations where an incorrect payment was identified and a debt raised as a result of a customer failing to declare, or incorrectly declaring, income and earnings.

4.11 For cases where debts had been raised under Section 1224 of the *Social Security Act 1991*, the application of activity test breaches ranged from about 10 per cent to over 40 per cent of benefit payments. Overall, activity test breaches were imposed in about 20 per cent of cases where a debt under Section 1224 of the Act had been raised. This reflects the scope available for Centrelink staff to determine whether customers have a 'reasonable excuse' for failing to comply with their obligations to provide information in relation to their income or whether the customer has knowingly or recklessly provided false or misleading information.[94]

4.12 Figure 4.1 illustrates that Centrelink staff were more likely to apply an activity test breach the higher the level of debt raised. For example, ANAO testing found that activity test breaches were imposed in approximately 14 per cent of cases where the value of the debt raised was below $100 and 53 per cent for debts over $1000 (approximately a fourfold increase). This is consistent with breach legislation as smaller debts are less likely than large debts to have been incurred knowingly or recklessly.

Figure 4.1

Percentage of breaches imposed to debts raised[1]



1 The results are taken from a review of 319 NSA/YAL files where a breachable offence, namely a s1224 debt, was detected. Of these files, 247 were compliance review cases, such as EDF match reviews, and 72 were tip-off investigations.

94 Sections 500A and 630AA, *Social Security Act 1991*.

4.13 While Centrelink was applying breaches in the case of higher level debts in line with the legislation, they were not being applied consistently in relation to the point-in-time at which they were applied to different customers.

Formal cautions

4.14 Centrelink has two standard compliance letters, warning letters and obligation letters. The warning letter is intended to be used generally where a Record of Interview has been taken and a formal caution given to the customer. The obligation letter is used to remind customers of their reporting obligations in cases where no interview has been taken or formal caution given.

4.15 The ANAO examined whether formal cautions were being used in a consistent manner. For the financial year to 30 June 2000, Centrelink issued 1770 warning letters and a further 197 were issued by the DPP. The ANAO found that these warning letters were not issued consistently across Centrelink's service delivery network. Staff interviewed during the audit suggested that the main reason cautions were not issued more frequently was that the message contained in the standard letter sent to customers may be too strong in relation to the nature of the offence in some cases.

4.16 The ANAO noted that in some Area Support Offices (ASO) visited that there had been a concerted effort by prosecution staff to increase the use of formal warning letters, particularly for cases relating to multiple offenders. This highlighted a growing appreciation across the network of the value of the formal caution letter as an effective means of encouraging voluntary compliance and identifying suspected higher risk customers and to ensure that the activities of these individuals is closely monitored in the event of subsequent non-compliance.

4.17 Customers that have previously received a formal caution, in the form of a warning letter, meet the case selection guidelines for prosecution referral in the event of any subsequent offence.

4.18 In July 2001, Centrelink also reviewed the content of its warning and obligation letters in conjunction with the DPP and made appropriate changes to assist consistent usage and Centrelink's ability to follow-up in relation to any subsequent failures on the part of customers to advise Centrelink of changes in circumstances.

Prosecutions

4.19 The most severe action available to Centrelink to deal with offenders is to prosecute. Prosecution sends a clear message that Centrelink is committed to protecting the integrity of the welfare system from fraudulent abuse. The maximum penalty available for each offence under the *Social Security (Administration) Act 1999* is 12 months imprisonment and / or fines of up to $6000.[95] However, more serious cases of social security fraud are normally prosecuted under the *Crimes Act 1914* or *Criminal Code Act* which carry more severe penalties.

4.20 During 1999–2000, there were 2935 convictions for welfare fraud involving over $27 million in debts. It should be noted that it is the Office of the Director of Public Prosecutions (DPP) that is responsible for prosecuting cases and not Centrelink. Centrelink is responsible for referring cases to the DPP.

4.21 To assess the effectiveness of Centrelink's prosecution function, the ANAO examined whether Centrelink had:

- procedures and guidelines for the referral of cases to the DPP and whether these were being adhered to;
- appropriate procedures for gathering, handling and storing evidence;
- an effective relationship with the DPP; and
- a management information system for recording and disseminating prosecution performance information to relevant officers.

4.22 Each of these is discussed under separate headings below.

Prosecution procedures and guidelines

4.23 Centrelink, in conjunction with the DPP, had developed an appropriate set of procedures and guidelines for all aspects of the prosecution process, and these are set out in the agency's Prosecutions Manual. The manual contains appropriate references to a number of other selected documents including the Prosecution Policy of the Commonwealth, the Fraud Control Policy of the Commonwealth and relevant legislation. The manual is available to all Centrelink officers via the agency's intranet.

---

95 *Social Security (Administration) Act 1999*, Div. 3, section 217.

4.24 Most cases falling within the guidelines are referred automatically through the Debt Management and Information System (DMIS) for registration by prosecution staff once a debt is raised. The accuracy of the information entered into DMIS is an important determinant of the integrity of the referral process. The ANAO found that information relating to cases referred for prosecution was generally recorded accurately on DMIS. Where cases were found to be incorrectly coded, prosecution staff provided feedback to the relevant officer. This quality feedback loop was an important aspect of ongoing training for staff and provided an important mechanism for ensuring high quality referrals. To reinforce the need for accurate information prosecution awareness sessions provided to staff emphasise the importance of correctly coding information on DMIS.

4.25 However, some cases that fall within the case selection guidelines do not meet the automatic system referral criteria and need to be manually referred to prosecution officers. Cases which fall into this category include:

- where alleged offenders have previously been convicted of social security offences;
- where alleged offenders have previously been issued a formal caution in respect of alleged social security offences; and
- where alleged offenders have previously incurred debts for the same reason.

4.26 The ANAO found that the process for referral of such cases could be improved. A number of ASOs visited during fieldwork had recognised weaknesses in the automatic referral parameters and had taken action to address the problem. For example, one ASO was requesting monthly computer selections from National Support Office (NSO) of all cases where debts in excess of $2000 had been raised to identify cases that did not meet the automatic referral criteria but satisifed the case selection guidelines for prosecution.[96] Centrelink could consider extending this process to all ASOs in order to assist prosecution units to identify all cases that should be considered for referral to the DPP. Alternatively, system enhancements could be implemented to include on-line prompts that assist staff identify those categories outlined in paragraph 4.24 for automatic referral. This would ensure all cases that meet Centrelink's Case Selection Guidelines are considered for referral to the DPP. Centrelink advised that such a facility was introduced in the September release.

---

[96] Another area advised that it conducted similar computer selections (SAS runs) on a more informal basis.

Evidence gathering and handling

4.27 Before a prosecution can be instituted there must be admissible, substantial and reliable evidence of a prima facie case against the person alleged by Centrelink to have committed an offence.

4.28 As much of the evidence gathered by investigators and prosecution officers relates to documentation obtained from, and signed by, Centrelink customers it is critical to the prosecution process that effective records management practices are in place across the agency. The ANAO therefore examined arrangements Centrelink had in place for the storage and retrieval of both physical and electronic records and documents to determine whether they supported the evidentiary requirements of the prosecution process. These are discussed separately below.

Arrangements for storage of physical documentation

4.29 Centrelink had developed a Customer Records Management Manual that provided guidance for the collection, storage and destruction of records and documentation. However, the ANAO found that there was a low level of awareness among staff in Customer Service Centres (CSCs) of the existence and contents of this manual, which resulted in significant variations in the quality of record management practices across Centrelink Areas.[97]

4.30 Compliance and prosecution staff indicated that deficiencies in records' management practices in CSCs often caused delays in retrieving important evidentiary documents and in some cases resulted in such documents not being found, thereby compromising Centrelink's ability to successfully prosecute offenders. The ANAO found that records management practices were of a higher standard in Areas where Records' Management Units (RMUs) had been established, with files and documents easier to locate and able to be located in a more timely manner than in areas where these units had not been established.[98]

---

97 The ANAO noted that records management is a minimum standard under the Getting it Right strategy. As well the strategy emphasises issues such as correct documentation.

98 In Areas where an RMU had been established, Centrelink was able to provide a larger proportion of the files requested as part of the ANAO's testing of adherence to POI procedures.

4.31 One aspect of records management where major inconsistencies between CSCs and RMUs was identified was in relation to staff not being able to differentiate between documents that should be batch-stored and those required to be maintained on a customer's permanent file.[99] The most common problem concerned documents being batch-stored that should have been maintained on a customer's permanent file. This means that insufficient documentation is located on a customer's file to support decision-making.[100] In addition, as batch-stored documents only need to be maintained for two years, it has resulted in documents being inappropriately destroyed with adverse consequences for downstream processes such as prosecutions.

4.32 Centrelink advised that it was developing separate prosecution files for matters that are referred to the DPP that will be disposed of according to separate criteria from normal customer records. This initiative should ensure the integrity of the prosecution process and high quality referrals to the DPP. As well as this the ANAO considered that Centrelink staff should be made aware of the need to appropriately store customer records so that they are not disposed of inappropriately.

Electronic records

4.33 Centrelink had recently taken steps towards improving the quality of information that is recorded electronically on its mainframe. This included:

- minimum standards for online document recording as well as recording reasons for all decisions as part of the Getting it Right strategy; and
- the use of scripts[101] to support a range of functions performed by both CSOs and compliance staff and facilitate greater consistency in information recorded for various activities. Centrelink has formalised script development through the implementation of the *Script Development Policy* implemented in 1999, which was endorsed by the Chief Information Officer.

---

99 Staff in CSCs were also generally not aware of Records Disposal Authority 1335 (RDA 1335), issued by the Australian Archives in January 1998 which establishes arrangements specifically for Centrelink regarding the disposal of records in accordance with the *Archives Act 1983.* This Authority sets out the period of time that certain types of documents should be held.

100 As part of the ANAOs compliance testing for adherence with POI procedures, 6.6 per cent of files reviewed did not have the appropriate claim form on the file.

101 A script is a series of simple computer programs that facilitates the recording of information onto various systems used by Centrelink.

4.34 However, the use of scripts is not yet consistent across Centrelink's network. As all staff use the national mainframe system for accessing customer records, it is important that better practice scripts are identified at an early stage and rolled out nationally. This will ensure consistency and assist the improvement of electronic document recording across the entire network.

4.35 One issue that is becoming increasingly important for Centrelink is the admissibility of electronic evidence to support prosecution action against a customer as opposed to physical evidence such as documents signed by customers. The *Electronic Transactions Act 1999*, which came into force on 1 July 2001, enables the acceptance of electronic information as a substitute for physical documentation in a number of cases.[102]

Relationship with the DPP

4.36 The ANAO found that Centrelink has taken appropriate steps towards establishing a good working relationship with the DPP to assist its prosecution process. Centrelink has a Memorandum of Understanding (MOU) in place with the DPP that sets out the roles and responsibilities of each party in relation to fraud investigation and prosecution. Prosecution team members in all Centrelink ASOs visited reported that excellent lines of communication existed with DPP regional offices and that referrals were dealt with in a timely manner.

4.37 Importantly, for cases that the DPP decided not to prosecute, feedback was given to the relevant prosecutions unit as to the reason for the decision. This feedback is important in assisting Centrelink to continue to achieve the high rate of acceptance of cases for prosecution with the DPP.

4.38 Apart from assistance provided to Centrelink's Area prosecution units, the DPP also liaises with NSO in relation to broader, national issues that are relevant to Centrelink's prosecution process. Centrelink, in consultation with the DPP, had developed a standard brief of evidence to be used nationally and was liaising with the DPP on the issue of separate prosecution files.

---

[102] The Act allows the following requirements imposed under a law of the Commonwealth to be met in electronic form: (a) the requirement to give information in writing; (b) the requirement to provide a signature; (c) the requirement to produce a document; (d) the requirement to record information; and (e) the requirement to retain a document.

Prosecution Management and Information System

4.39 Centrelink had established a computer based Prosecutions Management and Information System (PMIS) to assist management of prosecution cases. The system provides data storage for information relating to the progress of cases referred for prosecution, maintaining information such as current status of a case and the number of cases referred to the DPP.

4.40 The ANAO found that performance information was readily available from PMIS and that most staff considered it a useful tool for managing the prosecution process.

Prosecution performance information

4.41 Centrelink's 2000–2001 Business Partnership Agreement (BPA) with FaCS sets out the performance requirements for the prosecution function in Centrelink. Centrelink has also established a range of internal performance indicators and targets for its prosecution function to complement those contained in the BPA.

4.42 Performance indicators for 1999–2000 included quantity, quality and timeliness issues. During the fieldwork the ANAO identified a number of other, external factors that impact on the performance of the prosecutions function that are not fully accounted for under the current performance monitoring framework, such as:

- the time taken by an investigating officer to refer a case to prosecution —currently the prescribed timeframe is two days after a debt has been raised; and
- the quality of investigative work conducted prior to referral and the additional amount of evidence gathering and investigation required to be undertaken by the prosecution officer.

Assessing the deterrent effect of remedies

4.43 A recent report released by the OECD Working Party on Regulatory Management and Reform[103] argued that '*the threat of enforcement will not act as a deterrent if people do not believe non-compliance is likely to be discovered or punished*'.

---

[103] *'Reducing the risk of policy failure: Challenges for regulatory compliance'*, OECD Working Party on Regulatory Management and Reform, March 2000. Extract taken from *'Factors affecting voluntary compliance'*, Paper presented to the six countries benefit fraud conference, Department of Family and Community Services, September 2000, Ireland.

4.44 The report highlighted that maintaining the integrity of social security systems required effective deterrent mechanisms to promote voluntary compliance and discourage attempted fraud and other incorrect claims.

4.45 The ANAO found that the impact of penalties on compliance had not been assessed. As well, it was not possible to determine whether the value of penalties and the circumstances in which they were imposed provided an effective deterrent to non-compliance. Such analysis could assist Centrelink, and its client agency FaCS, to target compliance and education activities to individuals with higher risk characteristics. The lack of analysis of the impact of penalties on compliance meant that Centrelink and its client agencies could not be assured that the dollar value of different penalties and the circumstances in which they are imposed provides an effective deterrent to non-compliance. A review of the fraud deterrence framework was announced by FaCS in the 2001–02 Budget.

4.46 The ANAO conducted some preliminary analysis of the deterrent effect of Centrelink's various remedies. Examples from the analysis undertaken include:

- an examination of debts raised by Centrelink revealed over 22 000 recipients incurred three or more debts between July 1998 and June 2000. This may indicate that, in some cases, raising debts and making payment variations that reduces the amount of benefit paid does not provide sufficient deterrence for non-compliance. Further analysis would be required to identify the most common factors contributing to the incidence of multiple overpayments for customers; and
- a review of Centrelink breach data showed that 30 per cent of all Newstart activity test breaches raised during 1999–2000 were for second or third breaches indicating that for this group of Newstart customers, the initial breach was not an effective deterrent. However, Centrelink was unable to advise what proportion of these breaches were for the same reason as the first breach. This data would be valuable in assisting Centrelink and FaCS to measure the deterrent effect of breaches on particular offence types and the reasons that customers were incurring multiple breaches.

4.47 Analysis of various international current penalty systems could also be conducted to identify additional remedies that may be appropriate or more effective in dealing with fraud and non-compliance. Examples of the types of remedies available in other jurisdictions to deter

fraudulent activity include the United Kingdom, where the Department of Social Security is able to offer welfare recipients suspected of committed social security fraud the choice of paying an administrative penalty equal to 30 per cent of the amount of an overpayment.[104] Such an administrative charge would provide an additional penalty to be imposed as a result of continued non-compliance and recognise the costs associated with dealing with persistent non-compliance. An administrative penalty would also enable prosecution resources to be concentrated on cases more likely to be fraudulent.

4.48 The analysis of the deterrent effect of different penalties could also assist to identify improvements to policy and program design. Centrelink and client agencies should determine responsibility for such analysis. The ANAO noted that FaCS had announced that a review would be undertaken of the fraud deterrence framework as part of the 2001–02 Budget. It is important that the points raised in this report are considered as part of the review.

Conclusion

4.49 The ANAO concluded that a number of remedies available to deal with fraud and error such as activity test breaches and warning and obligation letters, were used inconsistently across the Centrelink network. However, Centrelink advised the ANAO that a coordinated training package would be delivered during 2001 to assist staff who are unclear about the legislative requirements for imposing breaches to gain the understanding to use such mechanisms consistently. As well, in July 2001, Centrelink in conjunction with the DPP reviewed and made appropriate changes to the content of the warning and obligation letters.

4.50 Centrelink had developed an appropriate prosecution process for addressing both routine and serious cases of welfare fraud and, in 1999–2000, met the prosecution referral target specified in its BPA with FaCS. While this indicates the high quality of referrals that are provided by the agency to the DPP, improvement could be made to the automatic referral process to assist prosecution units to identify all cases that should be considered for referral to the DPP.

---

[104] United Kingdom, *Social Security Administration Act 1992* Section 115A.

4.51 While Centrelink had developed guidelines for the collection and storage of records and documentation, the ANAO concluded that there was a low level of awareness among staff of these guidelines and compliance with the guidelines required improvement. Since the audit fieldwork was completed, Centrelink released its Getting it Right initiative in November 2000, which included a mandatory minimum standard for on-line documentation of decisions, including details of information provided to customers and information received from customers.

4.52 The ANAO concluded that the impact of penalties on compliance had not been assessed. As well, it was not possible to determine whether the value of penalties and the circumstances in which they were imposed provided an effective deterrent to non-compliance. This reduced the effectiveness of the targeting of activities to encourage voluntary compliance and thereby improve fraud prevention. A review of the fraud deterrence framework was announced by FaCS as part of the 2001–02 Budget initiatives.

5. Performance Assessment Framework for Compliance Activities

This chapter reviews the performance assessment framework in place to monitor Centrelink's performance in managing fraud and incorrect payment, including whether business systems provide relevant and reliable performance information and whether key performance indicators have been developed against which compliance and fraud control activities are measured.

Introduction

5.1 Good performance information can help agencies to develop policy, manage their resources cost effectively, improve departmental and program effectiveness and report their performance to Parliament and the general public. This information promotes accountability for public resources. The ANAO, therefore, examined whether Centrelink had:

- key performance indicators against which compliance review activities can be assessed;
- management information systems to provide relevant and reliable information on the efficiency and effectiveness of its compliance review activity; and
- measures to assess the cost effectiveness of compliance review activities.

5.2 In undertaking the review the ANAO focused on the framework in place to monitor Centrelink's performance in relation to programs it delivers on behalf of FaCS. Each of these areas is discussed under separate headings below.

Key performance indicators for compliance reviews

5.3 For performance indicators to be useful, they should contain a balance of input, process, output and outcome measures which address both quantitative and qualitative aspects of performance. Centrelink has two sets of performance indicators to monitor its management of fraud:

- indicators specified in the Business Partnership Agreement (BPA) with FaCS; and
- internal indicators, which form part of Centrelink's Balanced Scorecard and are complementary to those specified in the BPA.

5.4 As well as discussing the suitability of these measures the ANAO examined the incentive for Centrelink to reduce the level of fraud and error including developing an estimate of the level of fraud and error.

5.5 As outlined in Table 5.1, the ANAO found that Centrelink had an appropriate balance of measures which address both quantity and quality to measure the performance of its fraud control and compliance activities.

Table 5.1

Compliance performance indicators

Performance indicators in BPA:	***Type***
The number of reviews to be conducted.	input, quantity
The percentage of compliance reviews in which incorrect payment is identified.	output, quality
The percentage of cases referred to the DPP that can be actioned.	output, outcome, quality
Internal Indicators:	
A dollar indicator on the level of savings to be achieved.	output, quantity
The value of debts raised from compliance review activity.	output, quantity
An indicator on the number of prosecution referrals to the DPP.	input, quantity, quality

5.6 The ANAO found that Centrelink's current performance indicators for compliance review activity were an improvement on previous indicators. In particular, the focus on encouraging targeting of compliance reviews so that at least 30 per cent of reviews identify incorrect payment should improve the quality of review selections. In partnership with FaCS, Centrelink was continuing to refine performance measures with more attention being given to identifying appropriate indicators that measure the achievement of desired outcomes rather than activities undertaken.

5.7 However, only limited analysis of the available compliance performance data was undertaken by Centrelink and provided as part of its performance reports. Such analysis would be beneficial in identifying trends and emerging risks. This was, in part, due to a lack of clarity in the BPA regarding responsibility for undertaking the analysis. This was being clarified by Centrelink and FaCS.

5.8 While an improvement on past performance assessment frameworks, the BPA and internal performance indicators continue to place too much emphasis on the number of reviews conducted and the level of savings generated, rather than offering an incentive for Centrelink to reduce fraud and error. The current performance indicators for compliance activities do not include a measure to indicate whether losses from fraud and error are increasing or decreasing.

5.9 As well, the focus on the number of reviews undertaken and savings achieved has resulted in some reviews being of low quality or being terminated at an early stage, especially if it was considered to be a difficult case with an expected low return.[105] However, the ANAO noted that Centrelink had established a number of specialist investigation areas dedicated to the investigation of complex cases of fraud and error, involving matters such as identity fraud and undisclosed assets. These specialist teams are subject to their own specific performance indicators.

5.10 The ANAO considers that there needs to be a greater emphasis on the quality of compliance activities and on the long-term outcomes achieved from such activities,[106] particularly if sophisticated and systematic abuses designed to avoid detection are to be appropriately investigated and treated. While it is important to ensure the broadest possible coverage of review activities, it is equally important that the investigation of more complex cases is of a sufficiently high standard to discourage fraudulent and systematic abuse. The challenge for Centrelink, in collaboration with its client agencies, is to effectively target available resources to ensure the achievement of high level outcomes.

5.11 The ANAO recently completed a complementary fraud control audit of FaCS in which the BPA arrangements between Centrelink and FaCS for compliance and fraud control activities were analysed. The audit concluded that:

> *deriving an estimate on the level of fraud and error by income support payment type could assist FaCS and Centrelink develop more meaningful indicators to demonstrate the impact of compliance activities and other factors on the level of losses from fraud and error.*[107]

5.12 That is, the focus should be on developing and measuring the effect of strategies for ensuring the long term integrity of the social security system rather than strategies that return a short term financial gain.

---

105 Centrelink advised that deciding to cease a complex investigation early allows resources to be allocated to reviews that are less time consuming and have a higher probability of identifying fraud or an incorrect payment. It also enables Centrelink to cover a larger portion of the customer population for the same resources. In this regard more customers become aware of Centrelink's compliance and enforcement activities and the ability of the organisation to detect fraud and error.

106 Long term outcomes could include increased voluntary compliance, reduction in the number of repeat offenders and reductions in the number of offenders who deliberately seek to defraud or abuse the system.

107 ANAO Audit Report No.45 2000–2001 *Management of Fraud Control,* Department of Family and Community Services.

5.13 Changes over time in the estimate of the level of fraud and error in income support payments could be useful in assessing whether compliance efforts (including debt prevention strategies and customer education strategies) are influencing customer behaviour and achieving the desired outcomes of improved compliance and reductions in fraud and incorrect payment.[108] This could provide the basis for a better long term measure of the effectiveness of compliance and fraud control activities and complement current indicators which are more short term in focus and aimed at promoting a visible and effective compliance presence.[109] An estimate of the level of fraud and error could also assist to quantify the costs to the Government and the community of fraud and incorrect payment.[110]

5.14 In 1998, FaCS began a program of random sample surveys to measure the level of incorrect payment.[111] The surveys, which are undertaken by Centrelink on behalf of FaCS, aim to derive a reasonable point-in-time measure of the percentage of incorrect payment for the selected programs that are reviewed. They also provide some information on reasons for incorrectness.

5.15 Ongoing work conducted through the random sample surveys will produce an estimate of Centrelink and customer error and, in turn, could provide useful information to allow FaCS to revise the current suite of performance indicators. For example, estimates of the percentage of benefits incorrectly paid that are derived from the random samples may allow meaningful targets to be developed on reductions in losses from fraud and error that should be achieved by Centrelink as a result of its compliance activities.

---

[108] The level of fraud and error can also be affected by other factors such as changes in legislation, program design and policy as a result of government initiatives, changes in the underlying customer demographics and changes in the macroeconomic environment. Another factor is public perceptions of the chances of fraudulent activity being detected and the penalties that are likely to be imposed, which is in turn influenced by the amount and type of media coverage devoted to this issue.

[109] An estimate of losses arising from fraud and error could also complement current risk assessment practices and help to guide resource allocation to areas of highest risk and is therefore important if a more strategic approach to improving compliance is to be achieved

[110] Similar conclusions have been made in relation to quantifying the extent and cost of identity fraud by the House of Representatives Standing Committee on Economics, Finance and Public Administration (2000), *Numbers on the Run*, Review of the ANAO Audit Report No.37 1998–99 on the *Management of Tax File Numbers*. The ATO has also sought to derive an estimate on the size of the cash economy; refer ATO Cash Economy Task Force report.

[111] Random sample surveys involve an in-depth review of entitlement to FaCS income support payments.

5.16 Another result of the random sample surveys is to detect incorrectness of payments that would not otherwise have been detected by Centrelink controls. This should assist to redirect review resources to those areas. This in turn should help to realign incentive structures and funding arrangements for Centrelink away from the number of reviews and towards the main goal of ensuring that only those people that are entitled to receive benefits actually receive benefits and also that they receive their correct entitlement.

5.17 The ANAO noted that random sampling is the primary mechanism used in the United Kingdom (UK) to determine the incidence and magnitude of fraud and error in its various social security programs. Results from the random samples are then used to measure the performance of the UK Department of Social Security (DSS) in reducing fraud and incorrectness over time[112] and are published on an annual basis by the UK DSS.[113]

5.18 Centrelink and FaCS are continuing to develop initiatives aimed at improving the quality of the assurance framework under the current Centrelink and FaCS BPA (2001–2004)[114]. These initiatives include changes to the assurance processes which are based on the following principles:

- the availability of a wider range of methodologies for different stages of the assurance process;
- a validation of the assurance process that is independent of Centrelink;
- there will be common agreed approaches to definition of error, cause of error, correctness and accuracy, sampling size and structure, and methodology; and
- results of this work will be publicly available.

---

112 Specific performance targets have been established for the DSS that require percentage decreases in the level of fraud and incorrectness each year.

113 Analytical Services Division, *Results of the Area benefit Review from April 1998 to March 1999* and *Measurement of the Public Service Agreement; Fraud and Error in Income Support* and *Jobseeker Allowance* (2000), United Kingdom Department of Social Security, Government Statistical Service, Leeds.

114 Business Partnership Agreement between Centrelink and FaCS 2001–2004.

Recommendation No.3

5.19 The ANAO recommends that Centrelink, in collaboration with FaCS as client agency, quickly conclude the current negotiations aimed at an improved business assurance framework, to provide an estimate of losses from fraud and error by income support payment type in order to better assess the impact of compliance activities on the level of losses from fraud and error. The estimates should distinguish between losses from Centrelink error and those resulting from customer error and fraud.

Centrelink response:

Agreed.

FaCS Response:

Agreed.

Recommendation No.4

5.20 To facilitate the effective targeting of compliance to areas of highest risk, the ANAO recommends that Centrelink request FaCS, as client agency, to develop performance indicators that provide more incentive for Centrelink to reduce losses from fraud and error as well as discovering fraud.

Centrelink response:

Agreed.

FaCS Response:

Agreed.

Analysis of performance information

5.21 As well as using performance measures which will encourage reductions in the loss from fraud and error Centrelink should also analyse the performance data it has to identify trends and emerging risks as discussed in paragraph 5.7.

5.22 FaCS had recently commissioned a survey on voluntary compliance among customers and announced that a review would be undertaken of the fraud deterrence framework as part of the 2001–02 Budget initiatives. Information obtained from this work could provide a basis for the development of an appropriate performance assessment framework for measuring the deterrent effect of debt prevention strategies and compliance activities. The research could also assist to improve the targeting of compliance strategies.

5.23 During the audit, the ANAO identified a number of performance indicators, in addition to those developed as part of debt prevention strategies, that could be applied to measure changes in the level of voluntary compliance among customers, including:

- the proportion of total debts raised and fortnightly savings identified through customers voluntarily advising Centrelink of changes as opposed to those achieved as a result of compliance reviews;
- increases in the level of earnings declared by customers and the number of customers declaring income; and
- the number of cases where customers voluntarily disclose changes in circumstances to Centrelink compared to the number detected through review activity.

5.24 The ANAO considered that the analysis of existing data and the use of additional performance indicators would assist Centrelink to gain better understanding of how well each of its compliance strategies was working in practice.

Management information system

5.25 Centrelink's main tool for delivering, controlling, measuring and reporting compliance review activity is the National Selective Review System (NSRS).[115] This system delivers review selections and contains comprehensive information on each review conducted, including adjustments and debts raised as a result of review activity and information regarding the source and nature of the review activity. Given that it is the central mechanism for measuring review activity directed at ensuring compliance, ongoing development work on NSRS to improve its efficiency and effectiveness as a tool to support Centrelink's compliance and fraud control framework has been a high priority.

5.26 The ANAO reviewed the:

- relevance of the information provided by NSRS regarding the efficiency and effectiveness of Centrelink review activity; and
- reliability of management information contained on NSRS.

[115] There are a number of other systems that have been developed to manage particular aspects of review activity, including the Tip-off Recording System and the Prosecution Management and Information System (PMIS) for managing Centrelink's prosecution activity. In September 2001, Centrelink introduced a tip-off recording facility available to the general public through the internet.

Relevance of information

5.27 The ANAO found that there are clear guidelines regarding the type of review activities to be recorded on NSRS and the type of information that should be entered and stored on the system. These guidelines are aimed at ensuring relevant information is stored on NSRS to enable Centrelink to effectively monitor and report outcomes from review activities.

5.28 Centrelink has developed a comprehensive set of codes associated with different review types to be used when entering review results on NSRS. This provides Centrelink with the capacity to assess the effectiveness of different review types and trends over time. NSRS also has the capacity to report the time taken to complete reviews. The process by which the Detection and Review Team (DART) in National Support Office (NSO) distributes review selections to the network ensures that the types of reviews are correctly coded.

5.29 Relevant data is stored on NSRS to enable Centrelink to report on outcomes from review activity and support both internal and external accountability requirements. The ANAO found that there was currently limited data available to determine whether adjustments and results recorded on NSRS were attributable to voluntary disclosures due to an impending review rather than as a result of the conduct of an actual review. To allow Centrelink to assess the effectiveness of reviews in encouraging voluntary compliance, improvements should be made in the availability of information for measuring changes in the level of voluntary compliance. This new information would provide information to Centrelink on the deterrent effect of the compliance activities over time and the impact of compliance and prevention activities on voluntary disclosures.

Recommendation No.5

5.30 The ANAO recommends that Centrelink, in collaboration with its client agencies, assess the cost-effectiveness of developing its business systems to record and report on the preventive effect of compliance activities and their impact on voluntary disclosures, initially assessing whether NSRS or its replacement system could record whether payment adjustments were attributable to voluntary disclosures due to an impending review.

Centrelink response:

Agreed.

FaCS response:

Agreed.

Reliability of information

5.31 Centrelink had developed clear rules regarding the entry of the level of savings and debts to be recorded on NSRS. However, limited direct links between Centrelink's review systems and payment systems meant that results recorded on NSRS had to be entered manually which created doubt about the integrity of reported results.[116]

5.32 To mitigate the risk of inaccuracy, the ANAO found that several Area Support Offices (ASO) visited had established quality assurance processes to test the integrity of results recorded on NSRS and to correct any errors that are detected.[117] This validation process is an important element for ensuring the accuracy of performance reports relating to compliance activities provided by Centrelink to FaCS, other client agencies and Parliament. The ANAO considers that there should be clear national guidelines for conducting quality assurance checks to ensure a systematic and comprehensive approach to data validation across the network.

5.33 The ANAO noted that a number of enhancements to Centrelink's review systems had been planned or implemented. These include the Review on Activity Management (ROAM) and the Compliance Systems Re-engineering Project. These upgrades are aimed at facilitating improved selection of customers for review and improving the extent of direct links between Centrelink's review and payment systems. Improved links between Centrelink review and payment systems should result in more accurate recording of review results. In turn, this should mean that Centrelink has more information available to assess the effectiveness of various compliance activities it undertakes.

Cost effectiveness of compliance activities

5.34 Centrelink, along with many other government agencies, has been required to reduce its costs while maintaining service delivery standards that are specified in its agreements with purchaser agencies. Within this environment, it is important that Centrelink has cost information that is accurate, timely and relevant, to assist managers to make informed decisions regarding resource allocation and strategic planning issues.

---

116 Testing conducted by the ANAO found a number of cases were savings from reviews had been incorrectly recorded on NSRS.

117 Integrity checks conducted in these ASOs indicated that the nature and level of error detected was comparable to ANAO findings. Area integrity checks also aim to identify better practices and training needs. These checks encompass program and compliance reviews, including tip-offs.

5.35 The ANAO examined how Centrelink uses management information to assess the cost effectiveness of its compliance activities. An important aspect of this assessment was to determine whether Centrelink had developed appropriate mechanisms for measuring the relative efficiencies of the different organisational structures they have in place to undertake the compliance functions across areas, as well as the relative efficiency of different fraud and control of incorrect payment approaches. These organisational structures include:

- clustering (grouping activities);
- retaining compliance activities at the Customer Service Centre (CSC) level; and
- undertaking compliance activities into an integrated one-to-one service delivery model.

5.36 An assessment of the different structures and results from completed reviews would need to be undertaken to determine their effectiveness.

5.37 The ANAO found that Centrelink Areas were seeking to develop approaches to meet cost pressures and improve efficiency and performance. In recent years Centrelink has been to trying to assess the efficiency of different organisational structures.

5.38 The most common approach being adopted across the Centrelink service delivery network has been to cluster the compliance functions in ASOs. The decision to cluster compliance activities has been made on the basis that it provides efficiency gains, improves performance and consistency of compliance work practices within Areas. One of the primary reasons given for efficiency gains achieved under this compliance cluster model is that compliance staff are not subject to the competing priorities to which they are exposed within CSCs.[118] However, only a small number of ASOs had conducted a post implementation review to assess efficiency gains with the move to compliance clusters. While these reviews showed efficiency gains, Centrelink was unable to provide cost data to enable any conclusions on the most efficient compliance structure to be drawn.

5.39 As well as not being able to assess the cost effectiveness of different structures there was a lack of available cost data to assess the cost effectiveness of different compliance strategies and techniques. Therefore, it was not possible to undertake a cost benefit analysis of

---

[118] Many compliance officers reported that they would be required to assist in customer service roles during peak demand periods when they were located in CSCs which meant that compliance targets were not always achieved.

different review types or assess whether savings generated from specific review types were being obtained in an economical manner.

5.40 The ANAO considers that there are three components that must be considered in undertaking a comprehensive comparative analysis of compliance structures and techniques, including prevention versus detection methodologies. These are:

- cost comparisons. These need to be undertaken using the actual costs incurred and number of staff required to achieve a particular level of review activity;
- review results; and
- indirect costs and benefits of review activity. This is the main argument used by non-clustered Areas to maintain their approach to managing compliance activities and suggests that there are a number of indirect benefits associated with maintaining a compliance presence within CSCs. These benefits include greater workforce flexibility, compliance functions being more visible to CSOs and the deterrent effect of different organisational structures.

5.41 When assessing the efficiency and effectiveness of compliance activities it is important to make sure that it does not focus solely on direct costs and benefits. A broad indirect cost that should be considered by Centrelink relates to the cost of compliance associated with collecting information from the community, and in particular from employers.[119] It would be important for Centrelink when evaluating the relative efficiency of prevention and detection strategies that this aspect be considered to minimise the impact on third parties, and in particular, employers.

5.42 To assess its costs Centrelink advised that it was progressively introducing Activity Based Costing (ABC) which has the potential to provide Centrelink with the ability to determine the total costs of outputs (including all direct and indirect costs associated with compliance activity). Such information would allow Centrelink to establish the costs of debt prevention strategies and current review activities (including duplication) and enable Centrelink to accurately cost any proposed changes to review activity. However, the design of Centrelink's ABC model did not identify compliance activity at a sufficient level of detail to allow the comparative costs of different review activities to be determined.

---

[119] Centrelink does not estimate employer's compliance costs associated with providing information to Centrelink in order for Centrelink to verify income and employment details as part of its compliance review activity.

5.43 The ANAO considered that, overall, Centrelink was not collecting sufficient cost information to allow a comprehensive assessment of the cost effectiveness of its compliance activities to be undertaken or to undertake a comparative analysis of its various compliance structures. As a result, there are still significant deficiencies in the performance monitoring and assessment framework for compliance activity in Centrelink.

5.44 Similar issues were raised in a recent ANAO audit related to planning and monitoring for cost effective service delivery in Centrelink.[120] Centrelink should take action to develop appropriate cost data to allow the effectiveness of structures and strategies to be assessed.

5.45 Centrelink advised the ANAO that it is currently undertaking an Output Pricing Review and negotiating a new Funding Model. The Output Pricing Review provides an opportunity to improve the transparency of pricing as well as improving internal strategic cost management initiatives. The Output Pricing Review will support the development of the new Funding Model in relation to a better understanding of outputs in terms of price, quantity, quality and risk.

Conclusion

5.46 Centrelink had a range of performance indicators and targets, specified in BPAs, designed to allow Centrelink to provide regular management reports to its client agencies on the level and results of review activity.

5.47 Centrelink's National Selective Review System (NSRS) provided relevant data to enable Centrelink to monitor and report on outcomes from its review activity. However, there were questions about the reliability of adjustments to customer payments recorded on the system as a result of review activities and consequently the level of savings recorded and reported by Centrelink.[121] The ANAO therefore concluded that the implementation of a validation process (used by several ASOs visited during the fieldwork for this audit) would result in more accurate recording and reporting of review results.

5.48 Centrelink is contracted to implement fraud compliance strategies on behalf of FaCS and to achieve certain performance benchmarks. The performance indicators and targets in the BPA between FaCs and Centrelink should enable Centrelink to monitor and report on the level

---

[120] ANAO Audit Report No.43 1999–2000, *Planning and Monitoring for Cost Effective Service Delivery—Staffing and Funding Arrangements*, Centrelink.

[121] The ANAO sampled 17 program review cases to determine whether the results recorded on NSRS provided an accurate reflection of the outcome from the review. Of the cases sampled, three (18 per cent) were incorrectly recorded on NSRS.

and results of its fraud review activity. While the current performance indicators were an improvement on indicators contained in earlier BPAs, the ANAO concluded that the performance indicators continue to place too much emphasis on the number of compliance and fraud reviews conducted rather than on the results of reviews and the effect of review activity. As a consequence, the focus has been on discovering fraud and error rather than reducing them. As well, the new indicators have offered little incentive for Centrelink to reduce fraud and error through preventative measures and do not encourage the pursuit of more complex cases which are more time consuming and difficult to prove. Notwithstanding these deficiencies in the performance indicators, the ANAO noted that Centrelink has dedicated specialist teams in its National and Area Support Offices which deal with complex and serious frauds. These teams are subject to performance measures specific to their own work and their resources are not available to be diverted to routine and less serious fraud.

5.49 The ANAO concluded that, deriving an estimate on the level of fraud and error by income support payment type, could assist both FaCS and Centrelink, in conjunction with FaCS, to develop more meaningful indicators to demonstrate that they have been jointly successful in reducing consequent losses. Changes over time in this estimate may be useful in showing that Centrelink compliance efforts (encompassing debt prevention, customer education and review activity) are influencing customer behaviour.[122] The ANAO noted that other factors may also affect the level of losses from fraud and error. However, such an estimate could also assist to quantify the costs to the Government and the community of fraud and incorrect payment.

5.50 Centrelink did not have costing information available in a sufficient level of detail to enable the cost effectiveness of compliance activities to be assessed. Centrelink could not, therefore, make informed decisions regarding resource allocation for different review activities; determine the most effective compliance strategies for reducing the level of fraud and incorrect payment; or accurately price compliance strategies. Centrelink advised the ANAO that it is currently undertaking an Output Pricing Review and negotiating a new Funding Model. The Output Pricing Review provides an opportunity to improve the transparency of pricing as well as improving internal strategic cost management initiatives. The Output Pricing Review will support the development of the new Funding Model in relation to a better understanding of outputs in terms of price, quantity, quality and risk.

---

[122] The ANAO acknowledges that other factors, such as public perceptions on the likelihood of fraudulent activity being detected, may also affect the levels of losses from fraud and error.

6. Governance and Management Arrangements

This chapter discusses fraud control policy and planning, including risk assessment. The provision of appropriate training and awareness-raising for staff, administrative and information fraud are also considered.

Introduction

6.1 Sound governance and management arrangements are essential if the risks of fraud and incorrect payment are to be effectively managed by Centrelink.

6.2 To assess the overall fraud control framework established by Centrelink as part of sound corporate governance, the ANAO reviewed Centrelink's:

- policy for promoting an ethical workplace culture;
- planning regime, including associated risk assessment processes; and
- training and awareness-raising initiatives aimed at raising staff understanding of issues related to the effective control of fraud and incorrect payment.

6.3 The ANAO also reviewed Centrelink's arrangements for administrative and information fraud. Each of these is discussed under separate headings below.

Promoting an ethical workplace culture

6.4 The ANAO examined whether Centrelink had established and communicated widely the standards of conduct and/or ethics expected of its staff.

6.5 The Centrelink Board[123] and Chief Executive Officer have recognised the importance of Centrelink's ethical and control environment in maintaining community confidence in the programs that Centrelink delivers. The implementation of a number of measures, including audit and risk management processes, clearly show that they are committed to promoting an organisational culture of high ethical and professional standards.

[123] Centrelink is governed by a Board of Management (the Board) comprising a Chairman and six members—two departmental secretaries from purchaser agencies, the CEO of Centrelink and three members from the private sector.

6.6 The Board has implemented measures to address conflict of interest issues, among its members, in accordance with the requirements of Section 21 of the *Commonwealth Services Delivery Agency Act 1997* (CSDA Act). Board members are required to provide statements to the Chairman advising of their directorships of other companies and organisations and to disclose any direct or indirect pecuniary interest in a matter being considered at a meeting of the Board. These are important accountability arrangements and reflect accepted better practice in both the public and private sectors.

6.7 The ANAO also found that Centrelink had established a framework that aimed at demonstrating a commitment to creating and maintaining a high standard of conduct among all its officers. Initiatives that have been undertaken include:

- the release of an Expectations Statement by the CEO which includes the APS Values and Code of Conduct;
- widely communicating expected standards of conduct on the Centrelink intranet; and
- corporate documents such as the Fraud Control Plan that communicate to staff expectations regarding accountability and obligations concerning the prevention, detection deterrence of fraud.

6.8 An important signal in establishing an ethical culture is to have appropriate procedures for dealing with any identified breaches of codes of conduct. The ANAO found that Centrelink has established an appropriate set of procedures for determining breaches of the code of conduct for Centrelink employees.[124] The agency has also developed a more detailed guide to assist compliance with the endorsed procedures that outlines the APS Code of Conduct, sanctions available, delegations, legislation and other references.

6.9 The ANAO considers that Centrelink had taken appropriate steps to promote an ethical workplace culture.

Planning for effective fraud control

6.10 The Fraud Control Policy of the Commonwealth requires that the Fraud Control Plan be based on an assessment of the fraud risks to an organisation and include strategies and action plans for the treatment of identified risks. The Fraud Control Plan should be linked to the broader objectives of the organisation, as outlined in its corporate plan and the activities specified in the business and operational plans of the relevant work areas.

---

[124] The procedures were signed by the CEO on 5 December 1999.

6.11 The ANAO therefore examined whether Centrelink had:

- an appropriate risk management strategy, including the conduct of a fraud risk assessment, to address its major areas of fraud risk;
- a Fraud Control Plan; and
- established appropriate links between the Fraud Control Plan to other corporate planning processes.

6.12 Each of these is discussed under separate headings below. Where relevant, issues concerning administrative and information fraud are also discussed.

Risk management

6.13 The ANAO found that Centrelink had applied an appropriate risk assessment methodology in reviewing its fraud risk exposures for the major programs that it administers.[125] A rolling program of fraud risk assessments of all income support payments underpins its risk management framework, with major payment to be reassessed every three years.

6.14 As well, Centrelink was planning to include information gathered about the level of incorrect payment through the random sample surveys to feed into the risk assessment process. Such integration should provide Centrelink with additional information to identify and assess potential improvements to the effectiveness of the control framework currently in place and ensure effective allocation of available resources so as to minimise Centrelink's exposure to fraud and incorrect payment. Currently, Centrelink resource allocation and risk treatment decisions are assessed within individual programs rather than fully using a risk-based process for allocating resources and determinig risk treatments across programs.

6.15 In undertaking its audit of financial statements the ANAO found that Centrelink could improve its risk management strategy by developing an overarching assessment of the adequacy of existing mechanisms to maintain the risk of incorrect benefit payments at an acceptable level. This could identify areas where assurance processes require attention and identify any residual risk not controlled adequately or controlled excessively.

---

[125] Risk assessments are also an integral aspect of Centrelink's planning for the effective management of administrative and information fraud.

6.16 In relation to administrative fraud, Centrelink had recently updated its risk assessment framework to ensure greater consistency in approach across all areas dealing with these fraud risks. Centrelink will need to monitor the implementation of these new arrangements to ensure improved performance in relation to administrative fraud management is achieved.

Fraud Control Plan

6.17 A Fraud Control Plan is a specific requirement of both the Fraud Control Policy of the Commonwealth and the FMA Act. Centrelink has revised its Fraud Control Plan every two years in accordance with the requirements of the Fraud Control Policy of the Commonwealth. The current Fraud Control Plan is a useful document to raise staff awareness of Centrelink's fraud control responsibilities and provides a detailed overview of the fraud control environment in Centrelink. The plan reflects the key risks identified through the risk assessments and broadly describes strategies that are in place or will be implemented to rectify shortcomings.

6.18 In addition to the Fraud Control Plan, Centrelink develops specific Fraud Control Action Plans for program fraud for each of its major clients. These Action Plans, which complement the Fraud Control Plan, are based on the risk assessments and present the measures that have been deemed necessary to address the major control risks that have been identified. The action plans all included a timetable for implementation of risk mitigation strategies, identified priority areas for attention and nominated areas responsible for action.

Links to corporate plan and other business/operational plans

6.19 Preventing losses from fraud and error, especially of program funds, is an integral component of Centrelink operations and should have a high level of attention in all planning processes and documents. To ensure that its control framework is managed effectively as an integral part of the overall operating environment, Centrelink needs to promote a coordinated approach to planning at all levels of the organisation.

6.20 The ANAO found that fraud control planning was appropriately linked to higher level planning processes. In particular, there is a strong focus on fraud prevention and control at all planning levels, including the Centrelink Strategic Framework and in BPAs with client agencies.

6.21 The ANAO also found that the planning for the internal audit work program was linked to the fraud risk assessment process and the Fraud Control Plan. Detailed audits of internal controls in areas that have been identified through the fraud risk assessment process as high risk had been incorporated into the work program.

Staff training and awareness-raising

6.22 The ANAO reviewed Centrelink's approach to skill development of staff directly involved in compliance review activities including:

- the implementation of training initiatives that enable staff to develop the required expertise in relation to fraud control;
- providing appropriate support tools for staff to assist decision-making; and
- monitoring and reviewing the effectiveness of training strategies.

6.23 These issues were examined separately for compliance staff and Customer Service Officers (CSO). As well, the ANAO reviewed Centrelink's approach to promoting awareness of fraud and compliance related issues among CSOs.[126] The ANAO also noted some particular initiatives in regard to primary awareness were also noted during the audit and these are also discussed in this section.

Compliance staff have relevant expertise

6.24 The ANAO found that compliance teams in Area Support Offices (ASO) it visited had made a concerted effort to implement appropriate training programs, aimed at enabling compliance staff to develop the necessary skills to conduct their duties efficiently and effectively. At the time of the audit fieldwork Centrelink had issued a directive aimed at ensuring all specialist investigators had taken steps to achieve the new fraud control competency standards by 31 December 2000. The ANAO found that there was strong support for this directive in the network. In the Areas visited, staff identified as requiring the prescribed competency level had either completed or commenced appropriate training courses to achieve the required competency standards.[127] Similarly, Centrelink had met its responsibilities in providing adequate guidance and support in new and emerging areas of investigation and specialist compliance units.

---

[126] For a detailed examination of CSO training in Centrelink, refer to ANAO Audit Report No.9 2001-02, *Learning for Skills and Knowledge—Customer Service Officers,* Centrelink.

[127] Compliance staff also have access to the general training and support tools available to CSOs across the network including:

- the Centrelink Education Network (CEN) which is an interactive broadcast system developed by the People Management Team within NSO. It combines digital television with 'real time' interactivity to provide staff with an interactive distance learning facility; and
- Centrelink Reference Suite (CRS)—which contains a range of reference materials, including the *Social Security Act*, the *Guide to the Social Security Law* and a host of other relevant documentation.

6.25 Interviews with investigators and prosecution staff also acknowledged that the complex nature of investigations and prosecutions lends itself to on-the-job or mentor based training. Most investigators reported that this was their primary source of ongoing training. Using mentors was recognised across the network as an effective strategy to impart knowledge with experienced staff generally acting as mentors for inexperienced investigators and prosecution staff. While the ANAO acknowledges that the mentor approach could be an effective training delivery strategy, it could be improved by making available to both mentors and new staff, a prescribed checklist of minimum learning requirements and specific references to the wide range of support tools available to compliance staff. This could promote consistency in learning for staff.

6.26 A strategy to evaluate the effectiveness of all training provided to compliance staff had not been developed. Evaluating skills development programs is necessary to ensure they are timely, relevant and cost effective. Such evaluation should include the analysis of staff participation rates and can be based on staff feedback regarding programs that they have attended and analysing the effects of training on performance. A formal training evaluation process would be valuable to assist in providing an indication of the success of various training programs and strategies aimed at improving staff skill levels and performance.

Awareness-raising for Customer Service Officers

6.27 CSOs are the frontline for the delivery of Centrelink programs and have a key role in Centrelink's strategy to prevent fraud and incorrect payment as well as delivering the fraud control message to its customers.

6.28 The ANAO found that CSOs are provided with a range of information and reference material regarding their fraud control responsibilities. As well, most ASOs visited had recently undertaken their own training and awareness-raising programs covering a range of topics such as proof of identity policies, procedures and the effects of non-compliance, privacy issues and debt prevention.

6.29 In relation to Proof of Identity (POI), the ANAO found that, notwithstanding training and awareness-raising initiatives, there were a number of aspects where CSOs demonstrated a lack of knowledge in relation to fraud matters. For example, as highlighted by earlier ANAO audits[128] there appeared to be a general lack of awareness of the impact of processing errors at the new claim stage on downstream fraud detection systems, especially given the number of minor errors related to POI processing that were recurring throughout all CSCs visited.[129] As well, there was a perception in all the Areas visited by the ANAO that some CSOs were not concerned with processing claims which might contain errors as they considered that downstream compliance activities would detect any major errors. This suggests that the role of the compliance function may not be clearly understood by all CSOs.

6.30 The ANAO considers that the training and awareness-raising sessions regarding the importance of getting it right in the first instance delivered to CSOs could be improved by implementing a monitoring and review process to ensure that sessions are delivering the desired outcomes and making positive contributions to Centrelink's fraud control strategy.

Privacy awareness

6.31 A Privacy Awareness Strategy had been developed by Centrelink to keep staff continually aware of the importance of maintaining privacy. On commencing employment with Centrelink, staff are required to sign a Declaration of Confidentiality. A comprehensive privacy and confidentiality training package has also been developed and provided to new staff. All new staff receive privacy induction training and Centrelink makes available privacy manuals, training modules, videos and screen savers.

6.32 Centrelink had established Area Privacy Officers (APOs) in each ASO that are responsible for, among other things, conducting training sessions for new and existing staff, including specific modules for targeted training of various Centrelink teams. In the twelve months to 30 September 2000, over 3700 Centrelink staff members received privacy awareness training.

---

[128] ANAO Audit Report No.35 2000–2001, *Family and Community Services' Oversight of Centrelink's Assessment of New Claims for the Age Pension.*

[129] For example, many CSOs were not aware of the impact of poor recording of POI details on identity fraud data-matching techniques and for broader data-matching conducted by the organisation.

6.33 In addition to being responsible for conducting privacy and confidentiality training, APOs are also responsible for investigating alleged privacy breaches. All privacy officers nationally have either completed or are in the process of completing training to attain the Certificate IV competency level for fraud investigation. Customer Record Access Monitor (CRAM) reports are used by APOs to investigate allegations of privacy breaches. This mechanism allows APOs to identify cases where there has been unauthorised use of information, unauthorised access of information or unauthorised disclosure of information obtained from the mainframe.[130]

Administrative fraud

6.34 In relation to administrative fraud, for this audit, the ANAO relied on the review of controls undertaken as part of the annual financial statement audit of Centrelink. However, the ANAO examined whether Centrelink had developed relevant instructions, roles and responsibilities were clear and levels of administrative fraud were mentioned and reported appropriately.

Instructions

6.35 At the operational level the ANAO noted that to assist adherence with the FMA Act, Centrelink had developed Chief Executive Instructions (CEIs) which provide the policy and procedures for the agency's financial operations. In addition to this, there are number of other relevant guidelines issued by National Support Office (NSO) regarding financial and administrative processes such as asset management and financial delegations to assist in maintaining awareness of policy and procedural updates.

Roles and responsibilities

6.36 Centrelink's Fraud Control Plan allocates responsibility for administrative fraud to the Chief Financial Officer, Financial Systems and Development Team, People Management Team, and Area Managers.

[130] The ANAO acknowledges that where customer files are maintained on site in CSCs it is more difficult for an investigating officer to conclude with certainty that a particular officer has accessed information where all staff members have had access to the same information.

6.37 With responsibility for administrative fraud devolved across a number of different groups within the Centrelink organisational structure, it is important the roles and responsibilities are clearly defined and well understood and that effective planning processes are in place that ensure a coordinated approach to the function. In assessing the effectiveness of Centrelinks governance arrangements for managing administrative fraud in the agency, the ANAO found that:

- there was a diversity of approaches across the service delivery network for managing administrative fraud. For example, a number of ASOs had developed, or were developing, their own administrative fraud control action plans. However, these were of varying quality and effectiveness as planning tools and were not in all cases based on an appropriate risk assessment; and
- there could be greater clarity about the roles and responsibilities of the various areas with an administrative fraud control function in relation to quality assurance.

6.38 To address these issues, following discussions with the ANAO during the audit, Centrelink advised that it had:

- conducted an agency-wide administrative fraud risk assessment; and
- conducted a review of administrative fraud arrangements with particular attention paid to the risk assessment process for administrative fraud, the identification of better practices and standardisation of the quality assurance process.[131]

6.39 The ANAO considers that the successful implementation of these initiatives should result in significant benefits for the management of administrative fraud risks across Centrelink. Centrelink will need to monitor the effectiveness of implementation of the new arrangements to ensure that improved performance in relation to administrative fraud management is achieved.

Monitoring administrative fraud

6.40 The Financial Systems and Development Team provide quarterly reports to the Audit Committee of the Board on fraud control with details contained regarding program, administrative and information fraud. The Financial Services Team, through quarterly reports that are completed and returned by area offices, compiles reports relating to administrative fraud data. The level of reported administrative fraud over the past 18 months is contained in Table 6.1.

---

[131] This includes a larger role for National Support Office in establishing and improving processes for managing administrative fraud and the quality assurance framework.

Table 6.1

Administrative fraud detected and reported for 1999–2000 and 2000–01

Nature of offence	*1999–2000*		*2000–01 to 31 December 2000*	
	Number of cases	*Amount involved ($)*	*Number of cases*	*Amount involved ($)*
Theft or misuse of public money	2	2507	2	667
Inappropriate use of Commonwealth Credit Cards	1	7	0	0
Deliberate recording of incorrect overtime or other staff allowances, or unrecorded employee absences	2	2414	3	Nil
Theft of cheques or other public property (computers, mobile phones)	15	42 951	3	1663
Misuse/inappropriate use of public property (private phone calls on work/mobile phones, abuse of email facilities, etc)	43	290	13	1555
Total	**63**	**48 169**	**21**	**3885**

6.41 In reviewing the results contained in Table 6.1, the ANAO noted that the Audit Committee of the Board has previously questioned the relatively low incidence of internal fraud in Centrelink. During the audit the ANAO suggested that Centrelink could undertake a review of the operational arrangements for administrative fraud control to provide a high degree of assurance that the level of administrative fraud detected annually was a true reflection of the low incidence of this type of fraud in the agency.

Information fraud

6.42 Centrelink collects, processes and stores large volumes of personal information relating to millions of Australians every year. The effective protection of this personal and sensitive information requires Centrelink to have effective controls in place to ensure the security and integrity of the data.

6.43 In 1999, the ANAO tabled a performance audit of data privacy management in Centrelink.[132] The audit concluded that Centrelink had at that time established key elements of a sound framework to meet the Information Privacy Principles and confidentiality provisions in other legislation. However, the audit also found that there were a number of areas requiring improvement[133] and made 11 recommendations aimed at improving administrative arrangements and information technology systems associated with Centrelink customer privacy.

6.44 In reviewing progress made by Centrelink in addressing the recommendations contained in the report, the ANAO found that Centrelink had either resolved and/or made satisfactory progress with all the recommendations.

6.45 In particular, the ANAO noted that Centrelink had implemented a number of measures to prevent unauthorised access to information. This included the erection of firewalls to protect information from access by outside users[134] as well as the use of passwords for controlling access to computer mainframes and systems. Furthermore, position-based access allows Centrelink to restrict access to different types of information on a need-to-know basis subject to the requirements of the position being occupied.

6.46 The phased introduction of Accesslink[135] from March 1999 to May 2000 has had a major impact on Centrelink's ability to manage and control its information technology environment. Accesslink controls access to Centrelink's computer mainframes and network. It provides a 'single sign-on' environment through which access to Centrelink computers is made.

6.47 Accesslink enables Centrelink to monitor every computer access made by staff to customer information through records or logs of access which form the basis of audit trails. Where necessary, Centrelink is able to identify privacy breaches, whether deliberate or inadvertent, through a report facility known as the Customer Records Access Monitor (CRAM).[136] CRAM reports are used to assist investigations of alleged privacy breaches. The ANAO found that Centrelink was making

---

132 ANAO Audit Report No.8 1999–2000, *Managing Data Privacy in Centrelink*, Centrelink.

133 Areas requiring improvement included performance information for privacy breaches, there was no agency wide assessment of risks to data privacy undertaken and information technology control enhancements relating to secondary data stores and staff access rights.

134 These controls are tested periodically by independent external bodies to ensure they can withstand attempts to break into them from the outside, including from the Internet.

135 Accesslink is the Smart Card Token system that allows all staff to access Centrelink computer systems.

136 Only authorised employees can request CRAM reports.

satisfactory progress in developing its use of (CRAM) report information to actively identify suspected cases of privacy and confidentiality breaches.

6.48 In addition to monitoring arrangements, Centrelink employs a Security Access Management System (SAMS), which provides an online request and approval system for position based access to Centrelink's computing resources. Positional access (including existing, outstanding and historical access) can be monitored by employees with SAMS access. A link with Centrelink's human resource system also enables new employees to be automatically added to the system and separated employees to be deleted.

6.49 The high degree of information security in Centrelink was acknowledged by the Senate Select Committee in its report on information technologies where it commended Centrelink on the '*measures that it has instituted to protect the personal records of millions of Australians*'.[137]

6.50 One particular risk Centrelink faces relates to the use by FaCS staff of Centrelink systems and data for the purposes of audit and quality assurance. The nature of access by FaCS staff to Centrelink systems is specified in the BPA between the two agencies. During the audit Centrelink advised that 117 FaCS staff had SAMS access privileges.[138] It is important to the integrity of data privacy in Centrelink that FaCS staff who do have such access are subject to the same privacy obligations, monitoring arrangements and penalties for breach as Centrelink staff. At the time of the audit fieldwork, Centrelink could not advise whether FaCS staff with SAMS access had signed a Declaration of Confidentiality or received any privacy awareness training. Centrelink advised that it has recently reviewed all FaCS access to Centrelink systems and new profromas combined with tighter controls have been implemented.

Conclusion

6.51 The ANAO concluded that Centrelink had generally taken appropriate action to promote a fraud control culture among its staff. However, there were still a number of aspects where CSOs demonstrated a lack of knowledge in relation to fraud matters. These should be addressed by implementing an evaluation process to ensure that awareness —raising and training sessions are delivering the desired outcomes.

---

[137] Report by the Senate Select Committee on Information Technologies, *Cookie Monsters? Privacy in the information society*, Commonwealth of Australia, November 2000.

[138] The majority of these staff have retained the access since the initial split into purchaser/provider arrangements.

6.52 Centrelink had undertaken detailed fraud risk assessments of the major programs that it administers for client agencies. Recently introduced risk management guidelines should improve this process by promoting a holistic approach to risk management across all segments of the agency. As well, the fraud risk assessment framework for administrative fraud has been updated to ensure greater consistency in approach across areas dealing with these fraud risks.

6.53 A Fraud Control Plan, as required by the Fraud Control Policy of the Commonwealth, had been developed and was supported by lower level action plans that contain specific details regarding actions to be taken to address risks.

6.54 Centrelink had increased its focus on ensuring investigation staff had achieved, or are working towards attaining, the fraud investigation competency level prescribed in the latest draft on the new Commonwealth Fraud Control Policy and has specifically provided information for staff on privacy awareness.

6.55 The ANAO concluded that Centrelink had established appropriate procedures to prevent and detect administrative fraud but there was a diversity of approaches being used across its service delivery network. As well, the roles and responsibilities of the various Areas with an administrative fraud control function in relation to quality assurance were not clearly understood. However, Centrelink was undertaking a range of initiatives to address these problems.

6.56 Centrelink had taken action on all recommendations in the recent ANAO audit *Managing Data Privacy in Centrelink* and had implemented a number of technological measures to prevent unauthorised access to information stored electronically, particularly confidential customer information. In addition, processes, such as records or logs of access, have also been implemented to monitor staff access to systems which enables Centrelink to investigate and report on alleged privacy breaches, whether inadvertent or deliberate.

Canberra ACT
14 December 2001

P. J. Barrett
Auditor-General

Appendices

Appendix 1

Previous ANAO Performance Audits on Agency Fraud Control Arrangements

- Audit Report No.25, 1990–91, *Efficiency and Effectiveness of Fraud Investigations*, Australian Federal Police
- Audit Report No.15, 1991–92, *Procedures for Dealing with Fraud on the Commonwealth*, Department of Defence
- Audit Report No.40, 1991–92, *Systems for the Detection of Overpayments and the Investigation of Fraud*, Department of Social Security
- Audit Report No.11, 1992–93, *Procedures for Dealing with Fraud on the Commonwealth*, Department of Administrative Services
- Auditor General's Report No.4, 1999–2000, *Fraud Control Arrangements in the Department of Education, Training and Youth Affairs*
- Auditor General's Report No.47, 1999–2000, *Survey of Fraud Control Arrangements in APS Agencies*
- Auditor General's Report No.5, 2000–01, *Fraud Control Arrangements in the Department of Industry, Science and Resources*
- Auditor General's Report No.6, 2000–01, *Fraud Control Arrangements in the Department of Health and Aged Care*
- Auditor General's Report No.16, 2000–01, *Australian Taxation Office Internal Fraud Control Arrangements*, Australian Taxation Office
- Auditor General's Report No.22, 2000–01, *Fraud Control in Defence*, Department of Defence
- Auditor General's Report No.45, 2000–01, *Management of Fraud Control*, Department of Family and Community Services

Appendix 2

Area Support Offices and Customer Service Centres (CSCs) Visited

Area Support Offices (ASO)	*Customer Service Centres (CSC)*
East Coast—NSW	Wollongong Darlinghurst Bondi Junction
South Metro—NSW	Cabramatta Campbelltown Lakemba Liverpool
Hunter—NSW	Gosford Charlestown Port Macquarie Tamworth
Pacific Central—Queensland	No CSCs visited
Brisbane—Queensland	Mt Gravatt Caboolture Fortitude Valley
Central North Queensland—Queensland	Townsville Cairns Charters Towers Bowen
North Central—Victoria	Wangaratta South Melbourne Richmond Broadmeadows
South East—Victoria	Springvale Camberwell Dandenong Morwell
South Australia	Mildura Berri Modbury Elizabeth
West Australia	Mandurah Victoria Park Fremantle

Appendix 3

Sample Design

Sampling methodology

1. The audit examined the following three populations:

- a random sample of new benefit claims, for selected payment types[139], that were granted between 1 January 2000 and 31 August 2000 in the CSCs visited, to assess CSC compliance and adherence with current Proof of Identity (POI) policies and procedures;
- a random sample of tip-off reviews conducted between 1 July 1999 and 31 August 2000 in each ASO visited to assess, among other things, the timeliness of investigations, the rate of breaches being applied (where applicable) and data relating to the types of tip-offs received and outcomes from tip-off investigations; and
- a random sample of compliance reviews between 1 July 1999 and 31 August 2000 in each ASO visited to determine timeliness, imposition of breaches as well as to obtain information regarding prosecution referrals and multiple offenders.

2. The ANAO's examination was aimed at identifying, within the relevant populations, the extent of compliance with Centrelink policies and procedures. Specifically:

- for new benefit claims tested, the aim was to measure the extent of error in POI processing; and
- for tip-off and compliance reviews, the aim was to measure the extent of compliance with legislation and Centrelink review guidelines and to identify better practices.

[139] The payment types reviewed were clustered into 3 categories:
- Newstart (NSA) and Youth Allowance (YAL);
- Disabilities Support Pension (DSP); and
- Parenting Payment Single (PPS) and Parenting Payment Partnered (PPP).

Sample size

3. Sample sizes for each of the categories tested are presented in Table A.

Table A

Sample size for each category tested

Category tested	*Location of testing*	*Number of sites visited*	*Files requested*	*Files intended for review*	*Total files reviewed*
New Benefit claims					
—Newstart/Youth Allowance	*CSC*	*33*	*30*	*15*	*546*
—Disability Support Pension	*CSC*	*33*	*30*	*15*	*389*
Parenting Payment Single/ Parenting Payment Partnered	*CSC*	*33*	*30*	*15*	*440*
Tip-off reviews	*ASO*	*10*	*45*	*30*	*287*
Compliance reviews	*ASO*	*10*	*45*	*30*	*299*

4. Table A indicates that the ANAO sought to review 15 new benefit claims for each of the payment groupings and 30 files relating to compliance and tip-off reviews. However, the ANAO estimated that some selected files would be unable to be audited due to, for example, failure to locate the file or the file not being available within the required timeframe. Consequently the ANAO requested a larger sample be produced from which files would be reviewed.

5. The ANAO did not seek to produce estimates with associated confidence intervals for each category tested. However, to derive indicative results of the populations tested the sample sizes were selected in such a way to ensure that there were sufficient files reviewed to allow comparisons across categories as well as CSCs in relation to new benefit claims and to allow comparison across ASOs for tip-off and compliance reviews.

Sample Selection

6. The sample was selected in a systematic fashion as follows:

- for each category, all claims were sorted by Area and CSC;
- a skip, k, equal to the total number of files in each category divided by the number of files to be selected from each category and then rounded to the nearest integer was calculated;
- a random number, r, between 0 and the skip was chosen; and
- claim numbers r, r+k, r+2k,...up to r + (n-1) x k, where n is the number of claims allocated to that category, were then selected.

7. This selection technique was adopted to ensure that the resulting sample selection was representative of the populations examined.

Appendix 4

Main Data-matching Projects Conducted

Table 4.2

Main data-matching projects conducted

Data-matching project	*Payment risks addressed*	*Matching agencies*
Tax File Declaration Form (TDF)	Customers who have not notified or incorrectly notified Centrelink of income from employment.	Australian Taxation Office (ATO)
Data-matching program (DMP) [1]	Customers who incorrectly receive two payments from different agencies. Customers who have provided inaccurate information about their or their partner's or parental income.	Department of Veterans Affairs (DVA), ATO
Immigration	Customers who depart Australia without notifying Centrelink.[2]	Department of Immigration and Multicultural Affairs (DIMA)
Corrective services	People who receive payment after imprisonment or who assume imprisoned person's identity.	State and Territory Departments of Corrective Services.
Enrolment checking	Verify that students are still enrolled and doing a full time workload as well as verifying attendance at the institution named at the time of application.	Educational institutions including secondary schools, TAFEs and Universities.
Accelerated Claimant Matching (ACM) rent assistance	Detect customers residing at the same address who may have misrepresented their circumstances.	Centrelink's own address data
DEWRSB Job Network Placement matching	Identifies customers who have been placed in employment (by a Job Network member) and have failed to declare or incorrectly declared income from the employment to Centrelink.	Department of Employment Workplace Relations and Small Business (DEWRSB) and Job Network Members
Other	Aimed at addressing risks associated with undisclosed assets, investments, compensation pay-outs etc.	Comsuper, Australian Securities and Investment Commission (ASIC), and ATO

1 Matching under the *Data-matching Program (Assistance and Tax) Act 1990* (the DMP Act).

2 Centrelink has been conducting a pilot exercise with DIMA visa class and arrivals records to detect people receiving family assistance payment but who are not residentially qualified.

Appendix 5

Recent Developments in Fraud Control in Centrelink

Background

1. Centrelink was established in July 1997 and took over the legacy systems of the Department of Social Security (DSS)in relation to fraud control of social security payments and of the Department of Employment, Education, Training and Youth Affairs (DETYA) in relation to fraud control of student assistance payments. Since that time, Centrelink has carried out many significant improvements to these legacy systems.

Summary of Developments since 1997

2. The major improvements in Centrelink's fraud control systems and practices in recent years fall into the following main categories:

- integration of the former DSS and DEETYA compliance and fraud control regimes into a single Centrelink fraud control regime;
- introduction of new technology to fraud control activities, particularly in detection of fraud and incorrect payment, and enhanced systems support for fraud control staff;
- cost-effectiveness gains through a major shift in the use of resources away from field activity into data-matching
- cost-effectiveness gains through consolidating fraud control staff at an Area level and consolidating some activities at a National level
- increasing the scope and depth of data-matching and targeted compliance activities, especially to address new areas of risk and tapping into new data sources to better address existing risks;
- improving methods of detecting identity fraud through the use of sophisticated matching systems and tools;
- improving methods of measuring incorrect payment and targeting risk-based activities;
- strengthening fraud prevention measures; and
- using opportunities presented by Government reforms to enhance fraud control activities.

Appendix 6

Bibliography

Audit Office of New South Wales, *Fraud Control: Developing an Effective Strategy*, Sydney, c. 1994.

Commonwealth Law Enforcement Board (CLEB), *Fraud Control Policy of the Commonwealth* in *Best Practice for Fraud Control*, Australian Government Publishing Service (AGPS), Canberra, 1994.

Commonwealth Law Enforcement Board, *Fraud Control Policy of the Commonwealth Consultation Draft No.1*, Canberra, 21 June 1999.

Director of Public Prosecutions, *The Prosecution Policy of the Commonwealth*, Australia, [Online], available at http://www.nla.gov.au/dpp/prospol.html

Graycar, Adam, Fraud Prevention and Control in Australia, Paper presented at the Fraud Prevention Conference, Gold Coast, 24 August 2000.

House of Representatives Standing Committee on Banking, Finance and Public Administration, *Focussing on Fraud: Report on the Inquiry into Fraud on the Commonwealth*, Canberra November 1993.

Institute of Chartered Accountants in Australia, *Taking Fraud Seriously: Issues and Strategies for Reform*, November 1998.

Smith, RG, Identity-related Economic crime: Risks and Countermeasures, Australian Institute of Criminology, Canberra, 1999.

Smith, RG, Defrauding Governments in the Twenty-first Century, Australian Institute of Criminology, Canberra, 1999.

Smith, RG, Measuring the Extent of Fraud in Australia, Australian Institute of Criminology, Canberra, 1997.

Special Minister for State, *Review of systems for dealing with fraud on the Commonwealth*, March 1987.

Standards Association of Australia, *Guidelines for Managing Risk in the Australian and New Zealand Public Sector* (AS/NZS 4360:1999) Strathfield, 1999.

Other publications

Australian Federal Police, Comfraud Bulletin, published quarterly.

Fraud Prevention Services, Fraud Prevention Review, published quarterly.

Index

Series Titles

Titles published during the financial year 2001–02

Audit Report No.25 Assurance and Control Assessment Audit
Accounts Receivable

Audit Report No.24 Performance Audit
Status Reporting of Major Defence Acquisition Projects
Department of Defence

Audit Report No.23 Performance Audit
Broadcasting Planning and Licensing
The Australian Broadcasting Authority

Audit Report No.22 Protective Security Audit
Personnel Security—Management of Security Clearances

Audit Report No.21 Performance Audit
Developing Policy Advice
Department of Education, Training and Youth Affairs, Department of Employment, Workplace Relations and Small Business, Department of Family and Community Services

Audit Report No.20 Performance Audit
Fraud Control Arrangements in the Department of Agriculture, Fisheries and Forestry—Australia (AFFA)
Department of Agriculture, Fisheries and Forestry—Australia

Audit Report No.19 Assurance and Control Assessment Audit
Payroll Management

Audit Report No.18 Performance Audit
Performance Information in Portfolio Budget Statements

Audit Report No.17 Performance Audit
Administration of Petroleum Excise Collections
Australian Taxation Office

Audit Report No.16 Performance Audit
Defence Reform Program Management and Outcomes
Department of Defence

Audit Report No.15 Performance Audit
Agencies' Oversight of Works Australia Client Advances

Audit Report No.14 Performance Audit
Client Service Initiatives Follow-up Audit
Australian Trade Commission (Austrade)

Audit Report No.13 Performance Audit
Internet Security within Commonwealth Government Agencies

Audit Report No.12 Financial Control and Administration Audit
Selection, Implementation and Management of Financial Management Information Systems in Commonwealth Agencies

Audit Report No.11 Performance Audit
Administration of the Federation Fund Programme

Audit Report No.10 Assurance and Control Assessment Audit
Management of Bank Accounts by Agencies

Audit Report No.9 Performance Audit
Learning for Skills and Knowledge—Customer Service Officers
Centrelink

Audit Report No.8 Assurance and Control Assessment Audit
Disposal of Infrastructure, Plant and Equipment

Audit Report No.7 Audit Activity Report
Audit Activity Report: January to June 2001
Summary of Outcomes

Audit Report No.6 Performance Audit
Commonwealth Fisheries Management: Follow-up Audit
Australian Fisheries Management Authority

Audit Report No.5 Performance Audit
Parliamentarians' Entitlements: 1999–2000

Audit Report No.4 Performance Audit
Commonwealth Estate Property Sales
Department of Finance and Administration

Audit Report No.3 Performance Audit
The Australian Taxation Office's Administration of Taxation Rulings
Australian Taxation Office

Audit Report No.2 Performance Audit
Examination of Allegations Relating to Sales Tax Fraud
Australian Taxation Office

Audit Report No.1 Financial Statement Audit
Control Structures as part of the Audits of the Financial Statements of Major Commonwealth Entities for the Year Ended 30 June 2001

Better Practice Guides

Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	Jun 2001
Internet Delivery Decisions	Apr 2001
Planning for the Workforce of the Future	Mar 2001
Contract Management	Feb 2001
AMODEL Illustrative Financial Statements 2001	May 2001
Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Managing APS Staff Reductions (in Audit Report No.47 1998–99)	Jun 1999
Commonwealth Agency Energy Management	Jun 1999
Corporate Governance in Commonwealth Authorities and Companies–Principles and Better Practices	Jun 1999
Managing Parliamentary Workflow	Jun 1999
Cash Management	Mar 1999
Management of Occupational Stress in Commonwealth Agencies	Dec 1998
Security and Control for SAP R/3	Oct 1998
Selecting Suppliers: Managing the Risk	Oct 1998
New Directions in Internal Audit	Jul 1998
Life-cycle Costing (in Audit Report No.43 1997–98)	May 1998
Controlling Performance and Outcomes	Dec 1997
Management of Accounts Receivable	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997
Public Sector Travel	Dec 1997
Audit Committees	Jul 1997
Core Public Sector Corporate Governance (includes Applying Principles and Practice of Corporate Governance in Budget Funded Agencies)	Jun 1997
Administration of Grants	May 1997

Management of Corporate Sponsorship	Apr 1997
Telephone Call Centres	Dec 1996
Telephone Call Centres Handbook	Dec 1996
Paying Accounts	Nov 1996
Performance Information Principles	Nov 1996
Asset Management	Jun 1996
Asset Management Handbook	Jun 1996
Managing APS Staff Reductions	Jun 1996