The Auditor-General
ANAO Report No.33 2015–16
Performance Audit

Defence's Management of Credit and other Transaction Cards

Department of Defence

Australian National Audit Office

ISSN 1036–7632 (Print)
ISSN 2203–0352 (Online)
ISBN 978-1-76033-141-2 (Print)
ISBN 978-1-76033-142-9 (Online)

Requests and inquiries concerning reproduction and rights should be addressed to:
Executive Director
Corporate Management Branch
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Or via email:
communication@anao.gov.au.

Australian National
Audit Office

Canberra ACT

5 May 2016

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Department of Defence titled *Defence's Management of Credit and other Transaction Cards.* The audit was conducted in accordance with the authority contained in the *Auditor-General Act 1997*. I present the report of this audit to the Parliament.

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

Yours sincerely

Grant Hehir
Auditor-General

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

AUDITING FOR AUSTRALIA

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

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

Phone: (02) 6203 7300
Fax: (02) 6203 7777
Email: ag1@anao.gov.au

ANAO audit reports and information about the ANAO are available on our website:
http://www.anao.gov.au

Audit Team

David Rowlands
Kim Murray
Franco Rosin
Dr Tom Clarke

Contents

Summary and recommendations 7
Background 7
Conclusion 7
Supporting findings 8
Recommendations 9
Summary of entity responses 10
Audit Findings 11
1. Background 13
Introduction 13
Audit approach 14
2. Controls on the Defence Travel Card and the Defence Purchasing Card 15
Has Defence identified risks and documented key elements of the control framework to guide its management of credit cards? 16
Has Defence implemented effective preventative controls on the use of credit cards? 18
Has Defence implemented effective detective controls on credit card use? 23
3. Defence's use of its Travel Card and Purchasing Card 32
How does Defence spending on the Travel Card compare with other entities? 32
How does Defence Purchasing Card expenditure vary over the financial year? 34
Has Defence actively monitored and analysed credit card expenditure? 36
4. Cabcharge Fastcards and eTickets 42
Has Defence managed the issuing of Fastcards effectively? 43
Has Defence managed the issuing of eTickets effectively? 44
Has Defence implemented adequate systems to support the monitoring and management of Fastcard and eTicket use? 45
How can analysis of eTicket data help Defence manage its risks? 48
5. Fuel cards for vehicles 52
Are there effective controls on the use of Defence fuel cards? 53
What have been the trends in fuel card usage? 56
Appendices 61
Appendix 1 Defence response to the proposed report 63
Appendix 2 Cabcharge response to an extract from the proposed report 64
Appendix 3 New arrangements for credit card governance in Defence 66
Appendix 4 Defence use of its Purchasing Card, October 2013 – June 2014 71
Appendix 5 Instances of Purchasing Card cash withdrawals not consistent with Defence policy 72
Appendix 6 Instances of practices in the use of the Travel Card that are difficult to reconcile with Defence policy 73
Appendix 7 Expenditure on Defence fuel cards 74
Appendix 8 Additional fuel card preventative/detective controls 75
Appendix 9 Glossary 77

Summary and recommendations

Background

1. Credit cards offer an efficient means to pay for goods and services purchased for official purposes, and their reporting arrangements provide a basis for managing risks of misuse and fraud.

2. In mid-2015, Defence had over 100 000 credit and other transaction cards on issue. The main official credit cards are:

- the Defence Travel Card, issued by Diners under a whole-of-government arrangement;
- the Defence Purchasing Card, a Visa card issued by the National Australia Bank; and
- Cabcharge 'eTickets' and Cabcharge cards ('Fastcards') to pay for taxi fares.

3. Defence also uses fuel cards for both its commercial vehicle fleet ('white fleet') and military vehicle fleet ('green fleet'); however, these are not credit cards.

Audit objective and criteria

4. The objective of the audit was to assess whether Defence is effectively managing and controlling the use of Commonwealth credit and other transaction cards for official purposes in accordance with legislative and policy requirements.

5. To form a conclusion against the audit objective, the ANAO adopted the following high-level criteria:

- Defence has effective arrangements to control the issue and return of credit cards;
- controls over individual purchases are sound and operating effectively; and
- Defence has a sound framework in place to provide evidence-based assurance that controls over relevant card issue, use and return are effective.

Conclusion

6. Defence does not have a complete and effective set of controls to manage the use of credit and other transaction cards. An active management process and use of IT-based analytical techniques would help Defence to develop its control framework and provide better assurance over the use of these cards to purchase goods and services.

7. In response to emerging audit findings, Defence introduced new governance arrangements for credit card management in January 2016 to improve its monitoring and control arrangements.[1] This work was under way at the conclusion of the audit and will require ongoing senior leadership attention to firmly establish it. Defence also advised the ANAO in April 2016 that it now undertakes a range of analytical activities to investigate expenditure on a regular basis, including forensic accounting work and a newly developed credit card work program.

1 See Appendix 3.

Supporting findings

Controls on the Defence Travel Card and Defence Purchasing Card

8. Defence has identified risks from the use of credit cards and incorporated these in its fraud control plans. It has also documented relevant controls in its fraud control plans.

9. The suite of preventative controls used by Defence to control spending on credit cards is not complete and has limited effectiveness: it has not used blocking in any substantial way; access to cash advances for purchasing was not properly authorised until after this audit commenced; a 2009 plan to lower default limits on available credit was not implemented until January 2016; and Defence has issued thousands of credit cards that have never been used.

10. Defence has implemented a range of detective controls, including cardholder verification, independent reviews and spot checks, but their effectiveness is undermined by, for example, a lack of rigour in the independent monthly review process. Defence's controls would benefit, in particular, from greater clarity and emphasis on the role of the CMS Supervisor, the person who regularly performs an independent review of a cardholder's credit card transactions.

Defence's use of its Travel Card and Purchasing Card

11. Defence was responsible for around 41 per cent of all Commonwealth travel card expenditure in 2014–15. Compared with other entities, Defence expenditure is proportionately greater for cash advances, car rental and taxis. Defence staff have spent between $10 million and $40 million a month using the Purchasing Card over the last three years. This expenditure exhibits a peak in May–June each year.

12. Defence has not been drawing upon management information in its extensive credit card records or those of credit card suppliers to monitor or analyse credit card activity. The audit identified transaction types where analysis by Defence of available data could have helped it to identify and manage risks such as those arising from payment of personal traffic infringement penalties on the Purchasing Card; non-compliance with AusTender requirements; and non-compliance with a range of Defence policies including those for cash withdrawal.

Cabcharge Fastcards and eTickets

13. Defence has not effectively managed the issuing of Cabcharge Fastcards to staff. Defence decided to terminate the use of Fastcards some years ago, but a number remained on issue at the time of this audit. At the commencement of the audit, Defence was not aware, centrally, of the Fastcards it had issued, to whom or when.

14. The ANAO identified records of 261 158 taxi trips paid by eTicket at a total cost of $16.28 million over the three years examined in the audit. Defence has not effectively managed the issuing of eTickets to its staff. At the commencement of the audit, Defence had no central awareness of how many eTicket accounts it held with Cabcharge. Some 303 accounts were opened without proper authority, reflecting a lapse in the control framework intended to ensure that only persons delegated by the Finance Minister may enter into borrowing arrangements on behalf of the Commonwealth. Defence has commenced taking corrective action to authorise its issuing of eTickets.

15. Defence has not systematically monitored or managed activity on Cabcharge accounts. Analysis done within Defence has shown that eTickets have frequently been used where the Travel Card could have been used, as expected by internal policy. However, Defence had no internal system to help it monitor or manage activity on Cabcharge accounts. Defence's internal analyses and risk assessments have pointed to a need to introduce better systems to monitor and manage eTicket use. Defence advised the ANAO that it has a plan to use the existing Cabcharge module in its Card Management System, which should enable it to satisfy this requirement.

16. Active analysis of eTicket data would help Defence manage the risks it has identified with eTicket use. The ANAO's analysis identified patterns of usage of potential interest in managing eTicket use, such as high use of particular taxis, multiple expensive fares and 'small hours' travel. In some cases, the ANAO has referred particular analyses to Defence's Fraud Control and Investigations Branch.

Fuel cards

17. There are new controls in place on the use of Defence fuel cards for vehicles, administered for Defence by a private company, SG Fleet, which provides Defence with useful exception reports listing irregularities in the operation of the vehicle fleet.

18. Defence has advised the Senate in June 2015 that an arm's length assurance framework has been in place since April 2015, and included compliance testing. However, that testing did not begin until September 2015 and Defence will not gain assurance as to the effectiveness of the framework until it has completed audits of the implementation of the framework at Defence bases. Defence expects this to occur between September 2015 and June 2016.

19. The number and volume of fuel overfills—where the fuel obtained and paid for exceeds the recorded capacity of the fuel tank—was substantial during 2014 and 2015, but declined over the last six months of available records. There is also evidence of ill-discipline in the provision of odometer readings by Defence personnel. However, the number of irregular odometer readings—where an odometer reading is not in sequence with previous readings held or otherwise appears incorrect—is also declining.

Recommendations

20. Recommendations Nos 1 and 2 are made in the context of Defence advice that it commenced implementation of a governance reform of credit cards in the course of this audit.

Recommendation No.1
Paragraph 2.71

To improve its management of credit cards, the ANAO recommends that Defence:

(a) identifies the risks associated with its credit cards and its current control framework;
(b) implements enterprise-wide control arrangements aligned to key risks; and
(c) implements arrangements to provide assurance that the control arrangements are working as intended.

Defence's response: *Agreed.*

Recommendation No.2
Paragraph 3.33

To provide assurance that credit card use is consistent with Defence policies, the ANAO recommends that Defence:

(a) undertakes periodic analysis of credit card transactions, targeting key areas of risk; and
(b) takes corrective action, where necessary.

Defence's response: *Agreed.*

Recommendation No.3
Paragraph 5.27

To help ensure that the new fuel management arrangements are operating satisfactorily and have addressed the risks identified in this performance audit report and in its 2012 internal audit on fuel cards and fuel management, the ANAO recommends that Defence conduct a follow-up review of progress in the 2016–17 financial year.

Defence's response: *Agreed.*

Summary of entity responses

21. The proposed audit report was provided to Defence, with extracts provided to Cabcharge and SG Fleet. Defence's letter of response is at Appendix 1 and its summary response is set out below. Cabcharge also provided a response which is at Appendix 2. SG Fleet provided comments but no formal response. Relevant comments received from Defence, Cabcharge and SG Fleet have been incorporated into the report.

Defence's summary response

Defence thanks the ANAO for their audit and acknowledges the findings contained in the audit report on the Management of Credit and Other Transaction Cards and agrees with the three recommendations.

Defence has made significant progress on improving its current and future management of credit and other transaction cards. The Chief Finance Officer has already revised the Department of Defence credit card governance arrangements to address issues identified by the ANAO, as well as implementing a suite of investigative analytics covering all aspects of credit cards within Defence.

Defence welcomes the acknowledgement of the improvement in fuel card management and the work that has been completed to support the new fuel card arrangements, particularly since the formation of the new Fuel Services Branch in early 2015.

Defence will aggressively continue the implementation and refinement of the new fuel card assurance framework across all Defence transport management units. Defence will continue to work closely with SG Fleet and commercial fuel card providers to streamline exception reporting, introduce appropriate innovative IT solutions and put in place additional preventative and detective controls as necessary.

Audit Findings

1. Background

Introduction

1.1 Credit cards offer a transparent, flexible and efficient way for Australian Government officials to obtain cash, goods or services to meet business needs.

1.2 In mid-2015, Defence had over 100 000 credit and other transaction cards on issue. The main official credit cards are:

- the Defence Travel Card, issued by Diners under a whole-of-government arrangement;
- the Defence Purchasing Card, a Visa card issued by the National Australia Bank; and
- Cabcharge 'eTickets' and Cabcharge cards ('Fastcards') to pay for taxi fares.

1.3 Defence also uses fuel cards for both its commercial vehicle fleet ('white fleet') and military vehicle fleet ('green fleet'); however, these are not credit cards for the purposes of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).[2]

1.4 Defence expenditure on each of these types of card is set out below for each of the last three financial years (Table 1.1).

Table 1.1: Defence's credit cards and fuel card: numbers of cards and expenditure

Card type	No. of cards on issue[a]	Purpose of card	Expenditure 2012–13	Expenditure 2013–14	Expenditure 2014–15
Credit cards					
Travel Card (Diners)[b]	70 016	Official travel expenses	$240 929 188	$263 650 607	$287 781 633
Purchasing Card (Visa)	7 378	Official purchases under $10 000	$243 451 575	$208 383 686	$247 122 431
Fastcards	34	Pay taxi fares	$232	$1 265	$2 908
ETickets	–	Pay taxi fares	$5 259 240	$5 279 388	$4 460 401
Fuel card					
Fuel card–vehicle[c]	23 262	Fuel for Defence vehicles	$9 995 102	$9 092 308	$9 107 350
Totals	**100 690**		**$499 635 337**	**$486 407 254**	**$548 474 723**

Note a: As at March 2015. The numbers of travel, purchasing and vehicle fuel cards fluctuate.

Note b: Where travel is expected to occur in locations where Diners Cards are not accepted, a companion Mastercard may be issued to the Defence cardholder.

Note c: Defence's fuel card arrangements are managed by Fuel Services Branch in Joint Logistics Command. A summary of Defence's fuel cards is included in Appendix 7.

Source: Data provided by Defence.

1.5 The Australian Defence Organisation (Defence) comprises the Department of Defence, the Australian Defence Force and, until 1 July 2015, the Defence Materiel Organisation (DMO).[3] It has a budget of $33 billion (2015–16) and employs some 19 000 civilian and 58 000 military personnel.

2 Defence also had 793 Telecards on issue during the early period covered by this audit. Telstra withdrew the Telecards from use in September 2013. They were not considered further in the audit.

Audit approach

1.6 The objective of the audit was to assess whether Defence is effectively managing and controlling the use of Commonwealth credit and other transaction cards for official purposes in accordance with legislative and policy requirements.

1.7 To form a conclusion against the audit objective, the ANAO adopted the following high-level audit criteria:

- Defence has effective arrangements to control the issue and return of credit cards;
- controls over individual purchases are sound and operating effectively; and
- Defence has a sound framework in place to provide evidence-based assurance that controls over relevant card issue, use and return are effective.

1.8 The audit focused on the Defence Travel Card, Defence Purchasing Card, vehicle fuel card, Fastcard, and Defence use of eTickets, over three financial years (2012–13 to 2014–15).

1.9 The ANAO extracted card transaction data from 1 July 2012 to 30 June 2015 from Defence's Credit Card Management System (CMS) to examine the records for the Travel Card and Purchasing Card using software tools. The audit also considered management arrangements for Defence's use of Fastcards, eTickets, and fuel cards and analysed detailed data obtained by Defence for our analysis from Cabcharge.

1.10 The audit reviewed Defence's controls on card use by reference to both those generally accepted as good or standard practice and those established by the *Financial Management and Accountability Act 1997* (FMA Act) and its successor, the PGPA Act, which came into effect on 1 July 2014.[4] This legislation and associated policies and guidance set out the legislative requirements and regulatory framework for the proper use and management of public resources by Commonwealth entities. This includes official use of credit and other transaction cards.

1.11 The audit was conducted in accordance with the ANAO auditing standards at a cost to the ANAO of approximately $677 000.

3 From 1 July 2015, the role of DMO—to purchase and maintain military equipment for Defence—was transferred to Defence's Capability Acquisition and Sustainment Group.

4 Research across multiple jurisdictions established that a core set of controls is applied consistently in reviewing and auditing credit control arrangements in public sector bodies. A similar set is advocated among non-government organisations. These formed a point of reference for the audit.

2. Controls on the Defence Travel Card and the Defence Purchasing Card

Areas examined

This chapter examines Defence's use of controls to manage expenditure on its Travel Cards and Purchasing Cards. The examination of Defence's controls considered whether Defence had identified risks of credit card misuse and put preventative and detective controls in place.

Conclusion

Defence has identified a range of controls for the use of its Travel and Purchasing cards, but implementation of these controls has been variable. This limits the assurance that Defence, at an enterprise-level, can take from its control framework. In particular:

- key preventative controls have either been inconsistently applied or have not been implemented at all; and
- key detective controls, such as reviews of transactions, have been implemented in a manner that limits their effectiveness.

The recent move to place responsibility for the management of all credit cards in Defence's Chief Finance Officer (CFO) Group presents Defence with an opportunity to develop and implement an enterprise-wide approach for the control of credit card use. In January 2016, the Chief Finance Officer revised the Defence credit card governance arrangements to address issues identified by the ANAO.[5]

Areas for improvement

To improve Defence's management of credit cards, the ANAO has recommended that Defence develops and implements enterprise-wide control arrangements for credit card use which reflect the risks associated with that use—including those it had already identified—and implements arrangements to provide assurance that the controls are working as intended.

The guidance provided by Defence for the independent review of each cardholder's transactions by their CMS Supervisor, would be improved by a more complete specification, with examples, of Defence's expectations of the CMS Supervisor's check of the transactions.

2.1 This audit considered whether Defence had identified the risks associated with widespread credit card use by staff and whether it had put controls in place to address these risks. Broadly, the risks fall into two categories: waste (using public resources uneconomically) and fraud (dishonestly obtaining a benefit, or causing a loss, by deception or other means). The ANAO drew on the Defence Chief Executive's Instructions and Accountable Authority Instructions under the FMA and PGPA Acts (each of which encompasses part of the period audited) and the subsidiary Defence internal policy. Within that context, Defence's controls were considered against a list of preventative and detective controls in widespread use in other organisations.

5 The new Defence credit card governance arrangements are set out at Appendix 3.

Has Defence identified risks and documented key elements of the control framework to guide its management of credit cards?

Defence has identified risks from the use of credit cards and incorporated these in its fraud control plans. It has also documented relevant controls in its fraud control plans.

Defence's Fraud Control Plan

2.2 The Defence Fraud Control Plan sets out the fraud control framework within which Defence seeks to prevent, detect and respond to fraud. *Defence Fraud Control Plan No.10*, first issued in June 2013, was in place for most of the period on which the audit focuses. It was updated several times, including to reflect replacement of the FMA Act with the PGPA Act. It was succeeded by *Defence Fraud Control Plan No.11* in June 2015.

2.3 *Defence Fraud Control Plan No.10* identifies 'fraudulent use of the Defence Travel Card by Defence personnel or third parties' in its summary of enterprise-wide fraud risks (no other specific credit card risks are identified at this level).[6] It identifies current key controls at a summary level and a 'risk steward'. The risk steward is expected to manage the risk and ensure that critical controls for each risk are identified, actively monitored and that their status is reported to the Defence Audit and Risk Committee.[7]

2.4 Sitting below the Defence Fraud Control Plan, each Defence Group[8] has been required to have a Group Fraud Control Plan to document how the respective Group will prevent, detect and respond to fraud. For example, the Chief Finance Officer (CFO) Group, which now manages credit cards in Defence, provided a relevant excerpt from its Group Fraud Control Plan, listing the risks, controls and proposed controls set out in Table 2.1.[9]

6 Defence advised the ANAO that Defence Fraud Control and Investigations Branch staff are working with Chief Finance Officer Group representatives to update the Defence Enterprise-wide fraud risk register to better reflect the fraud risks associated with the use and management of Defence credit and other transaction cards.

7 Defence advice of 21 April 2016.

8 Defence comprises 11 groups, major organisational units headed by a band 3/three star officer.

9 Defence advised in April 2016 that, in accordance with Defence Fraud Control Plan No. 11, Group Fraud Control Plans were no longer required, as the Group prevention, detection and response actions were to be documented in the Group Fraud Risk Assessments.

Table 2.1: Risks, controls and proposed controls in the CFO Group Fraud Control Plan for 'Misuse of Defence Purchasing Card (DPC) Defence Travel Card (DTC) or Diners Master Card (DMC)'

Risks	Controls	Proposed controls
Used for unauthorised purchases: cardholder uses card to purchase items for personal use or sale. Collusion between CMS Supervisor and cardholder. Retaining entitlements when circumstances change. Withdrawing additional funds on DTC when not entitled. DPC/DTC/DMC cardholder disputes transaction to hide fraud. Inadequate understanding of DTC/DPC/DMC card use policy. Rushing processing and approvals. Credit card misuse by outsider fraud attack by a hacker.	• QA [*Quality Assurance*] check and data analysis. • Transactions are monitored by card providers, supervisors, resource and governance areas, cost centre managers, and the Inspector-General. • Periodic audit of DTC cardholder trans-actions by independent auditors, testing of internal financial controls. • DPC/DTC card limits maintained at minimum levels. • Staff undertake mandatory learning and awareness training relating to ethical behaviour. • CFO Group Business Rules and procedures. • Staff Awareness Training. • Annual audit of cardholders. • Regular review of card use. • Monthly reconciliation reports. • Testing of internal financial controls. • Credit limits. • Two-person approval process.	• Reduce credit limits to $10k. • Development of CMS [*Card Management System*] Travel module to work-flow travel approvals, automated matching of expenses to travel budget and automated compliance testing and reporting.

Note: There is no specific relationship between the order in which the risks are listed in the first column and the controls in the second.

Source: Extract from Defence CFO Group Fraud Risk Assessment, provided by Defence, May 2015.

Defence's advice to Parliament on controls

2.5 Defence has regularly received questions on notice about credit cards at Senate Estimates hearings in recent years. Senators have asked how Defence monitors credit card use and what action it takes to prevent credit card misuse. Defence has responded, in writing, each time in similar terms. Part of each answer has included the statement:

> Other mechanisms in place to guard against credit card misuse include:
>
> a. delegate approval and funds availability sign off prior to the commitment of Commonwealth monies;
>
> b. credit card limits, cash advance controls and card merchant blockings;
>
> c. a two-step process (involving both the card-holder and supervisor) for acquittal of expenditure that includes the provision of expenditure documentation to the supervisor.[10]

10 See, for example, Senate, Defence Supplementary Budget Estimates, November 2013, Answer to Question on Notice No. 100. <http://www.aph.gov.au/Parliamentary_Business/Senate_Estimates/fadtctte/estimates/sup1314/def/defenceqonsindex>. Viewed 10 March 2016.

Has Defence implemented effective preventative controls on the use of credit cards?

The suite of preventative controls used by Defence to control spending on credit cards is not complete and has limited effectiveness: it has not used blocking in any substantial way; access to cash advances for purchasing was not properly authorised until after this audit commenced; a 2009 plan to lower default limits on available credit was not implemented until January 2016; and Defence has issued thousands of credit cards that have never been used.

2.6 Preventative controls work by reducing the likelihood of inappropriate spending before a transaction has been completed. Preventative controls include: blocking certain categories of merchant; issuing cards only to those with an established business need; placing limits on available credit and regulating the availability of cash advances.

Merchant category code blocking

2.7 Credit card blocks prevent transactions with merchants identified by certain merchant category codes.[11] For example, an entity may prohibit access to merchant category codes such as 7273 (Dating and Escort Services) because such merchants are unlikely to be offering goods or services required for official purposes. Where an entity wishes to block a merchant category it must ask its credit card supplier to put the block in place.

2.8 If a cardholder tries to make a purchase—whether deliberately or by mistake—from a merchant in a blocked category, the transaction is automatically declined. If the cardholder needs to make a proper purchase from a blocked merchant, then specific pre-authorisation can be arranged.

2.9 At the time of the audit, Defence had no categories blocked on its Purchasing Card and only one on its Travel Card: 7997, *Clubs; Country Clubs, Membership (Athletic, Recreation, Sports), Private Golf Courses, Entertainment*. The ANAO's analysis shows that Defence's attempt to block this merchant category on the Travel Card has not worked. Review of Defence transactions over the last three years found 24 Travel Card transactions in the blocked category, with a total cost of over $15 000. Also, the audit identified over 1900 Purchasing Card transactions in that period in the same category, with a total cost of about $3.3 million.[12] Defence advised the ANAO that it cannot now retrieve from its records its rationale for blocking this merchant category on the Travel Card, which has been in place for at least eight years.

2.10 Defence also advised the ANAO that, generally, it had not blocked merchant categories because of 'the inconsistencies in the merchant categories when compared to the goods and services that are provided by the actual merchant'. This advice is inconsistent with the assurance Defence gave in its response to Senate Estimates questions that card merchant blockings are among the mechanisms in place to guard against card misuse (see paragraph 2.5).

11 The merchant category code is a four-digit number assigned to a merchant by major credit card companies when that merchant begins to accept one of these cards for payment. The merchant category code of each merchant or supplier reveals, broadly, the nature of the goods and services purchased with credit cards.

12 Defence informed the ANAO that a review of its fraud reporting records had not identified any records of allegations or investigations relating to 'Country Clubs'.

2.11 In response to the audit, Defence introduced new credit card governance arrangements (18 January 2016) and has now blocked two merchant categories—*gambling transactions* and *dating and escort agencies*—on both the Travel Card and Purchasing Card. Defence also advised that it would monitor over 50 merchant category codes for inappropriate transactions.[13]

Approving and reviewing the need to hold a credit card

2.12 Another well-established preventative control on misuse is to confine access to credit cards to those persons in the organisation with an established business need. Access must also be limited to those legally permitted to use a credit card and, where access to cash is needed, those who are authorised under Defence's Accountable Authority Instructions.

2.13 That many credit cards are not being used indicates a lack of a business need and the acceptance of an avoidable risk. A Defence internal audit in late 2006 found that 20 873 Travel Cards of the 56 840 that had then been issued (nearly 37 per cent) had never been used. The then Defence Management Audit Branch wrote to all Defence Groups to draw this to attention, and with a view to cards being cancelled where they would not be used.[14]

2.14 The current audit identified over 16 300 cards, issued before April 2015, that had not been used by the cardholder in the three years covered by this audit (July 2012 to June 2015):

- For the Travel Card, Defence assumes all personnel need to travel. The current audit found over 15 500 Travel Cards (over 20 per cent) had not been used in the period.
- For the Purchasing Card, Defence requires a line manager's authorisation as part of an application for the card. Some 830 Purchasing Cards (over 10 per cent) had not been used in the period.

2.15 On 20 January 2016, in response to this audit, Defence contacted some 12 500 cardholders whose cards had not been activated since issue (where more than 90 days had elapsed since issue), and informed them that if they did not activate their card within seven days, it would be cancelled. Defence advised the ANAO that 9217 cards were cancelled initially, followed by a second tranche of 814 cards being cancelled. A third tranche of 2070 inactivated cards had been identified and cardholders given 30 days to activate or the card would be cancelled. Further, Defence's new credit card governance arrangements, introduced in the course of this audit, include a new policy to cancel all credit cards that are not activated within 90 days of issue.

Restricting the issue of credit cards to Defence officials

2.16 Before July 2014, under the FMA Act and the Defence Chief Executive's Instructions (CEIs) then in force, contractors could be issued with a credit card, in particular, a Purchasing Card. From the commencement of the PGPA Act on 1 July 2014, the issue of credit cards to contractors has been prohibited as they can be provided only to officials. Under the transitional arrangements between the FMA Act and PGPA Act, Defence contractors who already held credit cards have been able to continue to hold and use them.

2.17 From 1 July 2015 contractors may be prescribed as officials, and therefore hold and use a Commonwealth credit card, provided they meet all the conditions set out in section 9(1)1A of the

13 See Appendix 3.

14 Defence was unable to advise what further action it took in response to the internal audit finding and communication from Audit Branch.

Public Governance, Performance and Accountability Rule 2014. ANAO testing identified 18 Defence credit cards currently issued to contractors. Contractors have spent $8 million using Defence credit cards over the last three years.

2.18 ANAO testing also identified some $942 700 spent by foreign exchange or foreign military personnel who are not permanent Defence employees (78 credit cards). Defence advised the ANAO as follows:

> Defence has had a number of foreign exchange and foreign military personnel that held Defence credit cards during the [*period*] 2012–15. These personnel have been treated as officials under the PGPA Act, as they are required to operate under the direction of the Accountable Authority. We are seeking to clarify this issue with the Department of Finance to amend the PGPA rule.

Review of ongoing business need

2.19 In addition to issuing a credit card only to those with a business need, a further control is to review from time to time whether that need continues. A business need may cease should the holder, for example, change position within the entity or leave the entity. The ANAO's review showed that:

- Defence had no procedure for the general review of a cardholder's business need for a Purchasing Card.[15],[16]
- Defence had a procedure for annual review and reconfirmation of the need for cash access through the Purchasing Card (see below).

2.20 When a credit card is no longer required, Defence places primary responsibility for card cancellation on the cardholder and their manager. Defence's Credit Card Support Centre has a procedure to carry out cancellation requests received as a result of staff members separating from Defence. Acknowledging that 'the risk associated with ex-employees retaining active cards is **high**' the Credit Card Support Centre also has a procedure intended to be run monthly 'to identify employee [*Card Management System*] users who may have left the Department and should have their DPC or DTC cancelled'. This approach should identify instances where a request for a card cancellation has not been made. Defence has provided copies of completed quality assurance reports for November and December 2015 indicating that the card cancellation work was done for those months. Defence has not provided evidence that the work was done during or for the remainder of the period covered by the audit.

Setting and reviewing expenditure limits

2.21 Credit card limits cap the expenditure that can be made on a credit card. Any transaction that requires credit to exceed a limit is declined. This controls the risk of financial loss to the organisation by ensuring that an individual with a credit card cannot spend more than the limit allows. Defence has referred to expenditure limits in its answers to Senate Estimates questions (paragraph 2.5) and, in its CFO Group Fraud Control Plan (see Table 2.1), to their being maintained at minimum levels.

15 Under Defence's business rules prevailing at the time of the audit, all personnel continued to need a Travel Card while engaged by Defence.

16 In April 2016, Defence advised the ANAO that it now 'has in place a procedure to ensure the cardholders are reviewed by Group CFOs to ensure a continued business requirement for having a DPC.'

Purchasing Card

2.22 The rules set out in Defence's Financial Manual require that the Defence Purchasing Card 'be used for low value, low risk purchases'.[17] At the point of original application for a Purchasing Card, a Credit Card Support Centre officer is required to approve a specific credit limit for the applicant. The credit limit is intended to 'reduce exposure towards potential fraud'. High limits (over $250 000) can be approved 'on the basis the request has come from a Defence manager of an appropriate level who is not the cardholder, and the case for the high limit is a reasonable one'. ANAO analysis showed that, among records examined for the Purchasing Card:

- the approved limits ranged from $500 (one card) up to $2 million (one card);
- three cards had approved limits of $1 million or more, and a further 107 had a limit of $250 000 or more; and
- over 900 had limits of $100 000 or more.

2.23 Defence advised the ANAO that:

> The Corporate Card Support Centre QA [*quality assurance*] report 2.1.10, which is conducted every 12 months, identifies cards which have a limit of over $250,000.01. All cardholders identified are contacted by email and requested to respond as to whether the high limit is still required.

2.24 Defence provided evidence of this review taking place in 2015.[18] It also provided evidence that, for a limit to be increased on the Purchasing Card, justification was required, as was the approval of the cardholder's supervisor.

Travel Card

2.25 A control on Travel Card expenditure is pre-travel approval by a delegate of a travel budget. The cardholder is expected to ensure their expenditure is within the approved limit.

2.26 A sub-plan to Defence's 2009 Fraud Control Plan (July 2009) for the Travel and Purchasing cards noted that the Travel Card had 'a series of standard limits which is currently under review and will be reduced in the future':

> The current default limit of $30 000 was identified when the program commenced as a limit that was not likely to impact on normal card use. Now that the program has been in place for several years we have a significant data set available which shows that a reduction in the base credit limit would not impact the majority of travellers. Accordingly, [*the former Defence Support Group*] intends to reduce default credit limits significantly and in doing so will further limit the amount of potential loss due to fraudulent activity. ... Regular travellers ... will be able to request an increase to their limit.

2.27 Notwithstanding the intention to reduce Travel Card limits, Defence's default spending limit for newly-issued Travel Cards remained at $30 000 (standard), $50 000 (overseas travel) and

17 FINMAN 5, version of 9 January 2015, item 5.2.9.2. The 100 highest-value Defence Purchasing Card transactions over the three years considered by the audit ranged from about $97 000 to $692 000. These would not ordinarily be considered low-value transactions. For example, the Commonwealth Procurement Rules establish an $80 000 (GST inclusive) procurement threshold which triggers the application of competitive requirements.

18 The documentation showed that in 25 of the 32 such cases, the limit was required to be maintained, five limits were reduced, one card was cancelled and one case was unresolved.

$100 000 (senior leadership group). Reducing credit limits to $10 000 remains a 'proposed control' in the CFO Group Fraud Control Plan (Table 2.1).

2.28 There have been other proposals to reduce Travel Card limits. The *Review of Defence Travel Services* for Defence Support and Reform Group in February 2014 recommended (among other things) that Defence 'Review Defence Travel Card limits to align with actual need'. This recommendation was to be implemented by December 2015. By March 2015, this had been given low priority and no action had been taken.

2.29 In January 2016 Defence informed the ANAO that, in response to this audit, Defence:

- is progressively reviewing existing credit card limits (including considering actual patterns of expenditure by the cardholder);
- has established default card limits to apply to new Travel Cards ($10 000) and Purchasing Cards ($30 000);
- has introduced a business rule requiring that business cases for increased card limits be provided to the appropriate Defence Group Chief Finance Officer for approval; and
- has introduced a business rule requiring Defence Group Chief Finance Officers to conduct annual reviews of credit card spending limits, credit card cash access, merchant categories, and unused credit cards.

Approving access to cash advances

2.30 Cash withdrawn using a Defence credit card, except for entitlements such as meals and incidentals allowances associated with travel, is an advance of relevant money.[19] To withdraw cash using a Defence credit card, officials must have the authority to operate that advance in accordance with Defence's Accountable Authority Instructions.

Purchasing Card

2.31 Purchasing Cards are issued without cash access being available at the outset. Defence's Accountable Authority Instructions require written approval from the First Assistant Secretary, Resource and Assurance Division, to permit access to a cash advance on the Purchasing Card.

2.32 CFO Group advised the ANAO in May 2015 that it had 'recently discovered that members were able to request cash access from the Defence Corporate Card Support Centre (CCSC) ... with no approval from the Group CFOs, Treasury & Banking and no delegate approval from [*the Acting First Assistant Secretary, Resource and Assurance Division*]'.

2.33 In July 2015, CFO Group formally sought nominations from Group CFOs for personnel who needed 'ongoing access' to cash advances, based on a list of cardholders who it knew held that access. No approvals had been in place until this time, though cash advances had long been made. In authorising access to cash on the Purchasing Card, CFO Group made no enquiries (for example, on a risk basis) to verify that those nominated had previously made proper use of their cash access privileges before authorising continued access.[20]

19 Section 8 of the PGPA Act defines 'relevant money' as money held by the Commonwealth or standing to the credit of any bank account of the Commonwealth.

20 In April 2016, Defence advised that 'this process will be strengthened for the next review.'

- As at July 2015, 125 Purchasing Card holders had cash withdrawal access approved with limits ranging from $5000 to $1 million. Collectively these cardholders could access about $13 million in cash.
- On 12 November 2015, following a review of cash access on the Purchasing Card, 115 Purchasing Card holders had cash withdrawal access with limits ranging from $5000 to $500 000. Through those 115 cards, the cardholders collectively could access about $10 million in cash.

2.34 In response to this audit, Defence stated in April 2016 that the CFO had removed access to cash from Purchasing Cards with the exception of cases approved by the relevant Group or ADF Service CFO.

Travel Card

2.35 The sub-plan to the July 2009 Defence Fraud Control plan stated that 'the single greatest risk to the [*Defence Travel Card*] program is the unauthorised use of cash'. Defence staff access cash using the Travel Card to withdraw allowances for meals and incidentals. Once the travel has been approved and, subject to it taking place as envisaged at approval, this withdrawal of cash requires no separate authorisation.

2.36 Defence personnel can access cash from the Travel Card greater than the amount provided as allowances. Withdrawal of cash amounts greater than the approved allowances represents a cash advance, in a similar fashion to the Purchasing Card (this is considered further in Chapter 3).

2.37 Defence's Card Management System (CMS) processes are not well suited to acquitting cash taken in advance. Cash advances are processed through CMS in the same manner as any other credit card expenditure. They are not identified as advances that need to be acquitted at a later stage through presentation of receipts, and Defence relies on the cardholder and the independent reviewer of their transactions (CMS Supervisor) to ensure the cash advance is appropriately acquitted. As discussed in Chapter 3, ANAO testing identified instances of cash advances that have not been adequately acquitted. This risk was not yet identified in Defence's risk plans.[21]

Has Defence implemented effective detective controls on credit card use?

Defence has implemented a range of detective controls, including cardholder verification, independent reviews and spot checks, but their effectiveness is undermined by, for example, a lack of rigour in the independent monthly review process. Defence's controls would benefit, in particular, from greater clarity and emphasis on the role of the CMS Supervisor, the person who regularly performs an independent review of a cardholder's credit card transactions.

2.38 Detective controls work after a transaction has occurred by identifying if there is a risk that it may have been inappropriate. Detective controls can include:

- *cardholder verification*—this is acceptance or rejection by the cardholder that each transaction attributed to them has actually been incurred by them. This mainly controls

21 In April 2016, Defence advised that its risk register had been updated to include this risk.

third-party fraud or error (such as card theft, vendor fraud or duplicate transactions). Defence refers to a rejected transaction as a 'dispute';

- *monthly review*—this is review of all the cardholder's transactions by a second person—either the cardholder's supervisor or someone at arm's length from the cardholder—to form a view on whether the cost and character of the transactions is proper. Defence refers to this as 'acceptance' of the transactions; and
- *spot-checking*—a further independent review of a proportion of transactions, selecting them either at random or by targeting high-risk areas. This can be done using IT techniques to detect suspicious practices such as transaction-splitting.[22]

Cardholder verification

2.39 In Defence, cardholder verification is a standard detective control on credit card misuse. Defence requires that when a cardholder detects a transaction they do not recognise as theirs, the cardholder must lodge a dispute within a defined period.[23] Where a dispute is raised within agreed timeframes, the matter may be settled at no cost to the Commonwealth. If, on the other hand, it is not raised within agreed timeframes, the Commonwealth will bear the cost of the transaction.

2.40 Defence requires cardholder verification for both Purchasing Card and Travel Card transactions. ANAO testing shows that this occurs and that timeliness of verification has improved slowly but continually in recent years: in 2012–13, cardholders verified some 96.1 per cent of transactions within two months, whereas in 2014–15 that figure had climbed to 98.1 per cent.[24]

Review of transactions

2.41 Review of credit card transactions is a strong detective control on credit card misuse, widely practised in organisations with corporate credit cards. Vigorous monthly review, if well publicised, may also have some deterrent benefit.

2.42 For review of credit card transactions to work effectively:

- it must be done by someone other than the cardholder so as to introduce a second party and a degree of independence into the process;
- it must be practicable for the reviewer to discharge the task. That is, it must be possible for the reviewer to examine each transaction—if only briefly—and form a judgement. In Defence, there are, overall, around 6000 transactions a day to be considered; and
- the reviewer must be in a position to exercise independent judgement;
  - this means that they cannot be in a position which would constrain unreasonably their capacity to question transactions that appear inappropriate; for example, this may be difficult for a person junior to the cardholder; and
  - reviewers need to be sufficiently familiar with the types and magnitude of expenditure the cardholder is likely to make.

22 Transaction splitting may undermine controls over expenditure and authorisation limits.

23 A dispute must be lodged within 60 days for the Travel Card and 90 days for the Purchasing Card.

24 Defence requires transactions in CMS to be processed within 60 days.

2.43 Each of these criteria has been recognised in Defence documentation. The degree to which they are met in practice is discussed below.

Guidance on the responsibilities of CMS Supervisors

2.44 Defence documentation recognises that 'To reduce the risk of misuse or abuse, a two person process is required for card purchase processes'. To be fully effective, this approach needs to be supported by a clear statement of the second person's (reviewer's) responsibilities in identifying potential misuse. Defence documentation is ambiguous about those responsibilities, which fall to the cardholder's CMS Supervisor.

2.45 Defence rules require that, after the cardholder verifies the transaction in CMS, the cardholder submits the transaction to their CMS Supervisor:

> The CMS Supervisor plays an important part in reducing the risk of credit card misuse by performing a 'check' on transactions verified by the cardholder. This check is not an approval of the transaction, as this has already taken place through pre-purchase delegations, but is a quality control measure. Ordinarily, this is done online using the CMS to 'accept' transactions.

2.46 To help the CMS Supervisor's check of Travel Card transactions, the CMS Manual requires that the cardholder provide the CMS Supervisor with a copy of the supporting documentation (approved travel budget and CMS expense summary report signed by the cardholder) for the travel. The guidance does not require Purchasing Card users to provide the CMS Supervisor with a copy of the supporting documentation for Purchasing Card transactions: it requires only that the documentation be available should the CMS Supervisor call for it.

2.47 Defence's rules for CMS Supervisors are formulated as 'Task Cards'. The documentation would be improved by a more complete specification, with examples, of Defence's expectations of the CMS Supervisor's check of the transactions.

Cardholders have reviewed and accepted their own transactions

2.48 ANAO testing identified instances where Defence cardholders had been able to review and accept their own transactions. Specifically, audit testing found:

- some 173 transactions made using physical cards where the cardholder had verified and reviewed their own transaction, including 14 cash withdrawals; and
- over 1300 transactions made using virtual cards where the individual responsible for the virtual card (the account holder) verified and reviewed the transactions.[25]

2.49 Self-acceptance of transactions undermines the effectiveness of this control and detracts from the integrity of Defence credit card processing.[26]

Cardholders can choose their reviewer

2.50 A new user of either a Travel or Purchasing card, when first set up on CMS, can select a CMS Supervisor. Defence does not require the CMS Supervisor to be the cardholder's line

25 Defence issues both physical cards and 'virtual' cards. Physical cards are generally issued to an individual. The purpose of virtual cards is to allow travel arrangers to pay travel costs associated with military exercises, deployment and training that generally involve the movement of a large number of people. Defence informed the ANAO that these accounts are generally set up with automatic acceptance.

26 Defence informed the ANAO that an error has been identified in CMS which allowed self-acceptance to occur and which Defence is working with the system vendor to resolve.

supervisor and leaves it to individual work areas to determine the most appropriate CMS Supervisor. Also, the cardholder can change CMS Supervisor by sending a request to the CCSC.

2.51 Having a cardholder choose their own supervisor, whether permanently or temporarily, introduces risks associated with collusion and fraud. Defence does not have a specific control in place to mitigate this risk even though the same risk was identified in a Defence internal audit in late 2007. That audit assessed the risk as a 'systemic control weakness' in relation to the 'critical function' performed by the CMS Supervisor.

2.52 Defence informed the ANAO that it has now implemented a system-based process that notifies incoming and outgoing supervisors when a change in supervisor occurs.

The auto-accept function limits independent review

2.53 CMS allows for automatic 'acceptance' of transactions under a predetermined dollar value. The rationale is that CMS Supervisors with large numbers of transactions to 'accept' may choose to request the auto-acceptance of transactions for their cardholders. Each CMS Supervisor who seeks auto-acceptance is expected to perform an off-line review of transactions at the end of the month using CMS reporting functionality. In practice, this means they are required to print a report of auto-accepted transactions and check 'a sample of, or all such transactions on a regular basis, which should be at least monthly'. The purpose is explicitly to ensure that two people are involved in processing the transaction.

2.54 This practice delays the review process or reduces the burden of acceptance duties to a sampling exercise. The former CMS Manual describes this approach as the 'the most efficient scenario for CMS Supervisors with a higher volume of transactions' but does not otherwise document a clear rationale for the existence of the function. There is also no evidence of a means to provide assurance that delayed or sample-based acceptance is done, or done satisfactorily.

2.55 Defence documentation is imprecise on the availability of this function, stating that it is an option for 'CMS Supervisors with a higher volume of transactions', without offering any view on what constitutes 'higher'. Defence documentation states that the function is available only for Purchasing Card transactions and ANAO testing found 484 physical Purchasing Cards with this facility. ANAO testing also showed that the function exists for 4686 physical Travel Cards and 405 virtual Travel Cards.

2.56 Earlier documentation (2008) shows that Defence intended auto-approval to be restricted to transactions under $5000 where the cardholder verifies their own transactions. However, ANAO testing showed that most cards have auto-approval transaction thresholds over $1 million.

Box 1 Analysis of auto-accept transactions

ANAO analysis of automatically accepted transactions identified some 67 747 such transactions (approximately $80 million in transaction value) on physical Purchasing Cards.

Some 14 517 of these transactions (over $22 million), were verified by the cardholder. Verification constitutes only acknowledgement that a transaction was actually incurred by the cardholder. Because the transactions are auto-accepted, there is no second-person check on the integrity of these transactions in normal processing. The only opportunity to identify any inappropriate use of the credit cards involved would lie with later spot-checking or audit.

In the case of the remainder of these transactions (about 75 per cent of them), the only persons directly involved in their processing were the cardholder, who initiated the transaction, and the account holder, who verified the transaction on behalf of the cardholder. This would include scrutiny to identify and preclude any third-party fraud. On the other hand, even though the account holder is a 'second person', there is no duty imposed on them by any Defence policy to provide an independent check of the integrity of the transactions.

Similar issues arise for Travel Card transactions that are automatically accepted:

- Of the 906 655 auto-accepted transactions (about $253 million in transaction value) made on virtual Travel Cards, 279 491 transactions (over $59 million) were verified by the individual responsible for the virtual card (the account holder).
- Of the 319 435 auto-accepted transactions ($64 million) on physical Travel Cards, some 4646 (about $775 000 in transaction value) were verified by the cardholder.

These processes precluded the involvement of a second person in the transaction.

2.57 In response to this audit, Defence informed the ANAO that:

> in accordance with Defence's new credit card governance document of 18 January 2016, all credit cards are to be validated by a CMS supervisor. The Group CFOs are required to determine CMS supervisor and once this task has been completed the auto approve function [is] to be switched off in [CMS].

Reviewer sometimes junior to the cardholder

2.58 The ANAO analysed CMS records to determine how often a reviewer of transactions is junior in rank to the cardholder. That analysis shows that the reviewer is junior in over one-third of transactions. Moreover, that proportion has been rising slowly in recent years (Table 2.2).

Table 2.2: How many transactions are approved by a person junior to the cardholder?

Calendar Year	No. of approved transactions	No. approved by a junior person	Proportion approved by a junior person
2012 (last six months)	780 858	254 207	32.6%
2013	1 578 753	545 864	34.6%
2014	1 641 724	592 238	36.1%
2015 (first six months)	759 974	287 399	37.8%
Total	4 761 309	1 679 708	35.3%

Source: ANAO analysis of Defence records.

2.59 The review process is the only opportunity built in to the workflow which enables arm's length review of transactions. The arrangements observed by the ANAO—involving review by personnel more junior to the cardholder—are inconsistent with Defence's answer to Senate Estimates questions, discussed in paragraph 2.5, that acquittal of expenditure involves both a cardholder and their supervisor. A person without a detailed understanding of the CMS Supervisor arrangements would reasonably read 'supervisor' to mean a 'superior' or more senior person. A 2007 Defence internal audit also identified risks where 'supervisors' were subordinate or junior to those they were reviewing:

> Where the nominated CMS Supervisor is a junior member, there is the potential for the CMS Supervisor to feel constrained in the degree to which they are able to perform their functions in relation to verifying the transactions of more senior members. Controls are further weakened when the CMS Supervisor is remote from the cardholder and does not have easy access to source documentation.

Wide span of control limits capacity for reviewers to discharge their duties

2.60 Some of the guidance formerly available in Defence recognised that the CMS Supervisor 'does need to have an understanding of the work being performed by the cardholder in order to identify any "unusual transactions"'. However, the span of control for independent review in Defence can be too large for that to be practicable. Defence's Fraud Control and Investigations Branch pointed out at the commencement of this audit, for example, that there are at least three ADF units where one reviewer has to process the transactions generated by 600 to 750 cardholders.[27] Similarly, the 2014 Review of Defence Travel Services concluded that 'CMS Supervisor acquittals can be 'Tick and flick' given large volumes and late timing'. The ANAO found that, on over 1100 occasions in three years, individual CMS Supervisors had reviewed over 100 transactions in a day, with over 300 being approved in a day on 32 separate occasions.

Spot checks on the use of credit cards

2.61 Individual transactions and trends can be monitored by an independent party after the event to detect misuse. For example, within Defence, the CIO Group's taskcard on fraud tells credit card users:

> Your use of the CMS and the use of corporate cards in general is closely monitored, particularly in relation to potentially fraudulent use. When the transactions are loaded to the CMS from Diners and NAB each work day, all transactions are reviewed for suspected fraudulent activity.

2.62 Defence generates a large number of transactions—around 30 000 transactions a week on the Purchasing and Travel Cards combined, or about 6000 each working day. To address transaction loads of this size, checking can involve random and targeted sampling, data mining or other more sophisticated IT techniques. These processes, if well publicised, can also deter card misuse. The audit examined Defence's current mechanisms for spot-checking transactions.

The Corporate Card Support Centre undertakes only limited checking

2.63 The Defence Factsheet 'Use of the DTC and Cabcharge eTickets issued by DSO Customer Service Centres' states, under the heading 'Fraud': 'It should be noted that the Corporate Card

27 A 2007 Defence internal audit of the implementation of the Travel Card had noted concerns at the number of cardholders being assigned to CMS Supervisors because they 'may not be able to clear CMS transactions in a timely manner and provide appropriate attention to ensure transaction validity'.

Centre has a formal process for monitoring and reviewing expenditure on DTC'. In response to enquiries as to the nature of this formal process, Defence advised the ANAO that:

> The Corporate Card Support Centre [*CCSC*] in Hobart through regular QA [*quality assurance*] checks monitor[s] the administration of the DTC and DPC.

2.64 Defence has also advised Parliament that:

> Corporate credit card transactions are monitored by ... Corporate Card Support Centre staff ... The Corporate Card Support Centre also reviews a percentage of daily transactions to identify any unusual trends.[28]

2.65 A 2007 Defence internal audit found that 'ongoing QA and fraud detection work has been recognised as an important internal control' and recommended that the fraud detection function undertaken by the CCSC be formalised. This was agreed by management. However, the current audit found that the procedures prescribed for quality control checks in the CCSC address only card management operations (such as the issue of new cards and reviewing whether a person has an ongoing requirement to hold a card at their current cash limit). None of the procedures concerns monitoring or reviewing credit card transactions or trends. Moreover, the CCSC Quality Assurance Manual (p. 18) explicitly states that:

> The CCSC is not responsible for proactively scanning or looking for potentially fraudulent transactions. ... Individual cardholders and CMS account holders are responsible for identifying suspicious, unusual or unauthorised transactions.

Other mechanisms for detecting and reporting misuse

2.66 Other internal mechanisms with the potential to detect credit card misuse are managed by the CFO Group, the Fraud Control and Investigations Branch, and the Audit Branch. The ANAO found:

- *There has been no systematic spot checking by management to date.* During the audit, CFO Group stated that it is introducing 'Business Intelligence' arrangements to review all Defence credit card transactions to detect unauthorised or fraudulent use.
- *There is limited spot-checking by the Fraud Control and Investigations Branch (FCIB).* Defence advised the ANAO that FCIB has only a limited capacity to detect suspicious credit card transactions, particularly given the high volume generated.[29]
- *No recent checking by auditors.* The audit found no recent record of any 'periodic audit of DTC cardholder transactions by independent auditors', a control identified in the CFO Group Fraud Control Plan (Table 2.1). The last relevant internal audit identified was that by Defence's (then) Management Audit Branch in late 2007.

28 See, for example, Senate, Defence Supplementary Budget Estimates, November 2013, Answer to Question on Notice No. 100. <http://www.aph.gov.au/Parliamentary_Business/Senate_Estimates/fadtctte/estimates/sup1314/def/defenceqonsindex>. Viewed 10 March 2016.

29 Defence advised that it 'has three data analysts responsible for fraud detection across the agency. Due to the high number of programs, projects, systems and functions within Defence, FCIB [*Fraud Control and Investigations Branch*] adopts a risk-based approach when allocating resources to monitoring CMS. Monitoring is focused on specific fraudulent behaviours that have, in the past, been realised and which have a high probability of occurring (for example, regular monitoring of cash withdrawals on Defence Travel Cards during the Christmas and New Year periods)'.

2.67 Since the Certificate of Compliance process was introduced, the Department of Finance's annual Certificate of Compliance reports to the Parliament show that Defence has reported an average of only 117 instances a year of non-compliance against financial framework requirements relating to credit cards (Table 2.3).[30] Given that, in the case of the Travel Card, Defence accounts for over 40 per cent of expenditure across the Commonwealth (see Chapter 3), Defence's share of reported non-compliance is lower than might be expected.

Table 2.3: Certificate of Compliance report, Category 3: non-compliance with the proper use of financial resources, Defence portfolio group

Year	No. of reported instances of Defence non-compliance	Defence's share of the non-compliance reported across all portfolios
2008–09	126	16.8%
2009–10	107	15.6%
2010–11	155	25.5%
2011–12	99	15.1%
2012–13	125	13.8%
2013–14	88	13.4%

Note: Category 3—the proper use of financial resources—included reported instances of non-compliance with section 60 of the FMA Act (which provided that an official must not use a Commonwealth credit card to obtain cash, goods or services otherwise than for the Commonwealth) and FMA Regulation 21 (which regulated the use of a Commonwealth credit card to pay for coincidental private expenditure).

Source: Department of Finance, http://www.finance.gov.au/publications/certificate-of-compliance-report/

2.68 Defence has provided information to the Parliament from time to time in response to specific questions about Defence credit card management, including fraud and breaches of departmental guidelines. For example, an answer to a question about fraud in Defence identified five cases in 2014–15 which were attributed to the Defence Travel Card.[31]

Strengthening Defence's credit card controls

2.69 Defence's CFO Group has had responsibility for managing the Purchasing Card since July 2012. It took responsibility for Defence's Travel Card management framework in May 2015, and Defence advised the ANAO in January 2016 that, in response to emerging audit findings, it was implementing revised operational governance arrangements aimed at strengthening controls around the use of its credit cards. Consolidation of management arrangements within CFO Group in May 2015, and the reform agenda, present Defence with an opportunity to develop and implement a consistent, enterprise-wide approach to the control of credit card use. Such an approach should be aligned to assessed risks and should include arrangements to provide reasonable assurance that credit card controls are complete and working as intended.

30 The Certificate of Compliance process involved agency Chief Executives preparing a self-assessment of their agency's compliance with the Commonwealth financial framework. The Department of Finance prepared a public report providing aggregate analysis of agency results annually, covering 2008–09 to 2013–14.

31 House of Representatives, Questions in Writing, Department of Defence: Instances of fraud or theft (Question No. 1771), 2 February 2016.

2.70 In addition, Defence internal audit and the Defence Audit and Risk Committee could give attention to implementation of the new governance arrangements and Defence's credit card control framework, to provide additional assurance to the Secretary.[32]

Recommendation No.1

2.71 To improve its management of credit cards, the ANAO recommends that Defence:

(a) identifies the risks associated with its credit cards and its current control framework;
(b) implements enterprise-wide control arrangements aligned to key risks; and
(c) implements arrangements to provide assurance that the control arrangements are working as intended.

Defence's response: *Agreed.*

32 The Compliance Reporting process under the PGPA Act (like the Certificate of Compliance process under the former FMA Act) requires the accountable authority of a Commonwealth entity to certify, having regard to advice provided by the agency's internal control mechanisms, management and the audit committee, the agency's compliance during the previous financial year with the PGPA framework requirements.

3. Defence's use of its Travel Card and Purchasing Card

Areas examined
This chapter considers how Defence uses its Travel Card and Purchasing Card and examines trends and areas of higher-risk use, such as cash withdrawals.

Conclusion
Defence's use of its Travel Card and Purchasing Card reflects the fact that it is a very large Commonwealth entity with a dispersed and mobile workforce. Patterns of expenditure, particularly for the Purchasing Card, show distinct seasonality, and warrant close management oversight to ensure the proper use of public monies.

Defence has not analysed the available data on credit card expenditure to identify trends or areas of non-compliance with Defence policies and instructions. Such analysis would have assisted Defence to identify areas of risk and inappropriate spending, such as the failure of individuals to take responsibility for the payment of their traffic fines, and to take appropriate corrective action.

Areas for improvement
The ANAO has recommended that Defence use credit card analytics to obtain greater assurance that its policies for credit card use are being complied with.

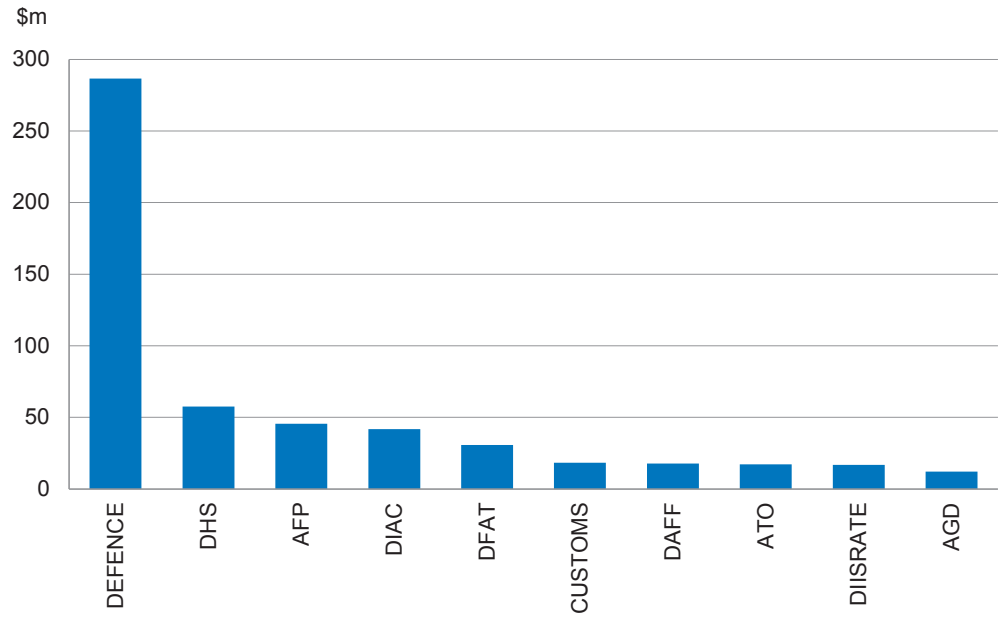
3.1 The ANAO examined available data on the use of credit cards across Commonwealth entities and within Defence to gain a perspective on Defence's use of its Travel and Purchasing Cards. The ANAO also undertook some more detailed transaction testing in areas of suspected high risk to analyse actual use.

How does Defence spending on the Travel Card compare with other entities?

Defence was responsible for around 41 per cent of all Commonwealth travel card expenditure in 2014–15. Compared with other entities, Defence expenditure is proportionately greater for cash advances, car rental and taxis.

3.2 Among entities using the whole-of-Australian Government Travel Card, Defence is by far the biggest user. In 2014–15 Defence accounted for 41 per cent of expenditure through this arrangement (some $286.7 million) whereas the second and third-largest spending entities accounted for around 8.2 per cent and 6.5 per cent of expenditure respectively (Figure 3.1).

Figure 3.1: Expenditure on the Travel Card, 2014–15: top ten entities by expenditure



Note: Entity names/abbreviations are as in the source document: DHS—Department of Human Services; AFP—Australian Federal Police; DIAC—Department of Immigration and Citizenship; DFAT—Department of Foreign Affairs and Trade; DAFF—Department of Agriculture, Fisheries and Food; ATO—Australian Taxation Office; DIISRATE—Department of Industry, Innovation, Science, Research and Tertiary Education; AGD—Attorney-General's Department. A number of entity names have since changed.

Source: Department of Finance.

3.3 Data supplied to the Department of Finance by the credit card company enables a comparison to be made across entities. The company has aggregated data from individual merchant category codes into simpler categories, such as 'airlines', 'hotels' and so on. Because this data is based on merchant category codes, aggregated and reported by the credit card company, caution is needed with its interpretation.

3.4 Over three-quarters of expenditure across all entities through the whole-of-Australian Government Travel Card is on airlines and hotels. Car rental, taxis and fuel together account for a further 6.1 per cent. The most substantial of the remaining items are cash advances (7.5 per cent), other (5.4 per cent) and retail (2.3 per cent) (Table 3.1).

3.5 Two categories of Travel Card expenditure stand out where Defence spending is proportionally higher than other entities' spending:

- *Car Rental and taxis*—Defence accounts for a high proportion of all taxi travel expenditure (51.5 per cent) and car rental expenditure (71.3 per cent) purchased through the Travel Card.
- *Cash Advances*—The third highest category in the table comprises cash advances to travellers, $52 million, comprising 7.5 per cent of all entities' travel card expenditure in the period. Defence accounts for almost all this amount—comprising 97 per cent of all cash advances across government using the Travel Card.

Table 3.1: Travel Card expenditure, 1 July 2014 to 30 June 2015

Category	Whole-of-government travel card expenditure	Defence travel card expenditure	Percentage of all Commonwealth travel card spending in this category attributable to Defence	Percentage of all Defence's travel card spending that is in this category
Airlines	$393 505 101	$152 016 269	38.6%	53.0%
Hotels	$149 220 278	$53 442 892	35.8%	18.6%
Cash Advance	$52 354 809	$50 761 587	97.0%	17.7%
Other	$37 814 637	$3 424 284	9.1%	1.2%
Car Rental	$23 720 301	$16 901 481	71.3%	5.9%
Taxis	$18 712 769	$9 645 838	51.5%	3.4%
Retail	$16 154 053	$158 758	1.0%	0.055%
Restaurant	$4 685 697	$101 336	2.2%	0.035%
Telephone Services	$1 033 890	$4 291	0.4%	0.0015%
Fuel	$536 092	$142 930	26.7%	0.050%
Mail Order	$532 400	$15 602	2.9%	0.0054%
Rail	$470 891	$67 957	14.4%	0.024%
Total	**$698 740 919**	**$286 683 224**	**41.0%**	**100%**

Note: The data in this table has been aggregated based on merchant category codes. This gives a sound general picture of the expenditure pattern but may not always represent the individual transactions accurately.

Source: Data provided by the Department of Finance.

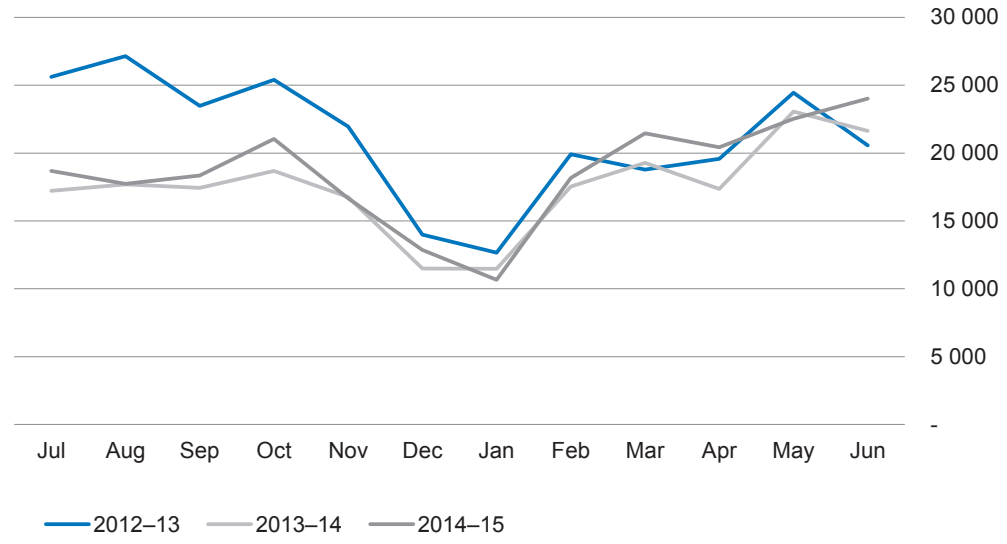
How does Defence Purchasing Card expenditure vary over the financial year?

Defence staff have spent between $10 million and $40 million a month using the Purchasing Card over the last three years. This expenditure exhibits a peak in May–June each year.

3.6 Analysis of Defence records shows that Defence's use of its Purchasing Card is uneven through the year and that there are seasonal trends. Purchasing activity was more intense in the period from July to November 2012 than in the corresponding periods in the two later years. Analysis of the records shows that this was due to greater use of the Purchasing Card to purchase health-related services than in subsequent periods (Figure 3.2).

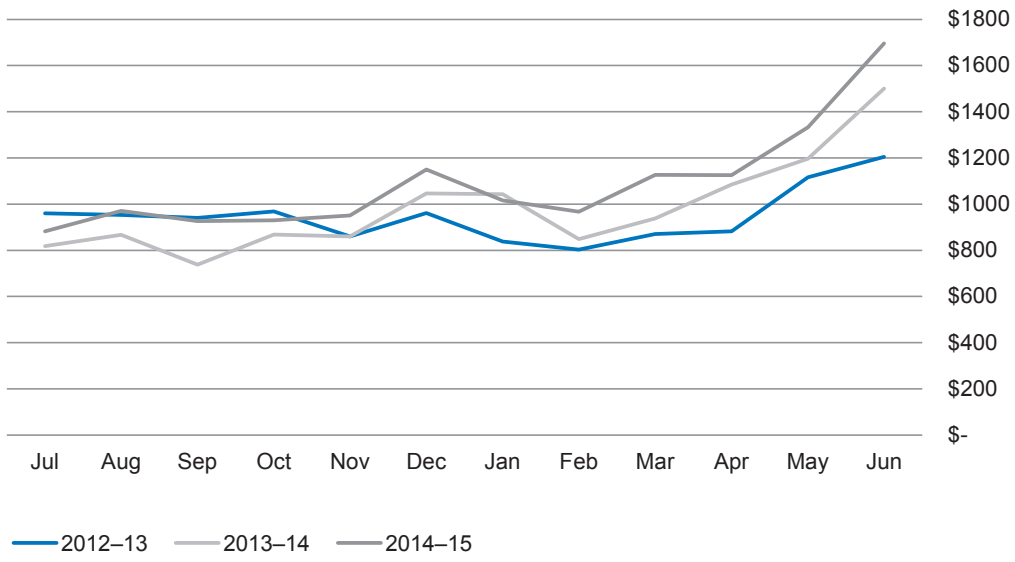
3.7 The average value of transactions shows high consistency across all years, with a tendency for values to increase, year-on-year (Figure 3.3). The most prominent feature is a rise in the average value of transactions in May–June each year. The analysis shows that Defence buys more items with the Purchasing Card towards the end of the financial year and it makes more expensive purchases during that period each year.

Figure 3.2: Number of Defence Purchasing Card transactions, by month, over three financial years, 2012–13 to 2014–15



Source: ANAO analysis of Defence CMS data.

Figure 3.3: Mean value of Defence Purchasing Card transactions, by month, over three financial years, 2012–13 to 2014–15



Source: ANAO analysis of Defence CMS data.

3.8 A possible explanation for the peak in spending at the end of the financial year is that certain regular accounts must be settled at that time. Another explanation may be that some parts of Defence are seeking to consume funds remaining in their annual allocation. As discussed in Box 2, below, there is also some evidence of parts of Defence seeking to artificially increase credit card expenditure towards the end of the financial year. This is a matter which would

warrant close examination by Defence management, as such practices risk inefficient or unnecessary spending on items of marginal value. Defence has indicated that it will be undertaking a detailed review.

Box 2 Request to increase Purchasing Card credit limit to facilitate end of year spend

An application made by a Defence official in April 2015 for a temporary increase in their Purchasing Card expenditure limit stated:

> This request for the increase to my DPC limit is to enable [*Defence Support Group*] to make the necessary payments for ***the end of financial year spend*** and is required until 03 July 2015.
>
> I work in the [*Defence Support Group*] Regional Resources Team and the purchasing/payment activities that I undertake include (but are not limited to) the following:
>
> 1. Stationery and office requisites for the Region;
>
> 2. Gas and Utilities (i.e. Water, Sewerage, Trade Waste) for all Defence Sites in [*a particular state*].
>
> 3. Low value assets and furniture for the Region.
>
> 4. Gymnasium support for the Region.
>
> The current limit on my DPC will not allow me to fully support these activities for the remainder of the FY [*financial year*]. As mentioned, this limit is only required until 03 July 2015 when the DPC limit can be re-adjusted back to $200 000 [***emphasis added***].

The nature of the items described as being purchased provides no indication of great urgency that the expenditure must be made at the end of the financial year, rather than as needed. The application was supported by the applicant's supervisor. The request was acted upon by the Defence Corporate Card Support Centre on the same day without further enquiry.

Has Defence actively monitored and analysed credit card expenditure?

Defence has not been drawing upon management information in its extensive credit card records or those of credit card suppliers to monitor or analyse credit card activity. The audit identified transaction types where analysis by Defence of available data could have helped it to identify and manage risks such as those arising from payment of traffic infringement penalties on the Purchasing Card; non-compliance with AusTender requirements; and non-compliance with a range of Defence policies including those for cash withdrawal.

Defence has not systematically analysed available data on credit card expenditure for management assurance purposes

3.9 There is an emerging practice among large public sector entities to have an active process that systematically analyses data on credit card usage. Such processes, sometimes called 'credit card analytics', can be tailored to provide assurance that key controls are working as intended and to identify individual or systemic patterns of card usage that may not meet Australian Government requirements or entity policies. Defence has the necessary data and the systems to do so but has not been using them in any systematic way to provide assurance that credit card controls are working satisfactorily.

3.10 Defence produces annual statistical overviews of credit card use and receives regular reports from the companies providing the Travel Card and the Purchasing Card. An example of a significant table from one of the latter reports for the Purchasing Card is reproduced at Appendix 4. The transaction data is aggregated based on the merchant category codes into larger categories and the total spend against each category is set out in the table. The table shows:

- There is no single dominant merchant category among those in this table: rather, Purchasing Card transactions are distributed widely across the categories displayed.
- There are three aggregated merchant categories each with more than 10 per cent of the business by value (highlighted in the table): 'Non-essential/luxury purchases'; 'Business Services' and 'Other'. These categories are so general in name that this conveys little useful information about the constituent Purchasing Card transactions. Defence has not sought to modify these categories so as to provide more useful information.

3.11 As discussed, data aggregated by merchant category code has limitations and requires care in interpretation. This limits the usefulness of the reports provided by the companies, but there is no evidence that Defence has used these reports or the data they contain as part of any active monitoring, analysis or review process for either credit card. On the other hand, Defence has not specified to the companies what form of report it would like to receive or find useful in monitoring its credit card activities.

3.12 All Travel Card and Purchasing Card transactions are conveyed electronically by the provider companies to Defence and kept on Defence's Card Management System, CMS. Consequently, Defence could generate its own reports and perform its own analyses and checks on credit card transactions should it wish, but Defence has not done so in any systematic way.

3.13 In response to this audit, Defence advised the ANAO that it now monitors credit card transactions monthly, with a focus on merchant categories that Defence has identified as high risk. It has also advised that it now produces a monthly report to support its 'forensic [analysis] function'.

Analysis of credit card expenditure data would yield important management information for Defence

3.14 To illustrate the value of an active and risk-based approach to analysing credit card expenditure, the ANAO identified a number of transaction types where Defence has established policies and procedures and where analytics would have provided Defence with insight into the implementation of these policies. These policies cover: the payment of traffic infringement fines; AusTender reporting requirements; and cash withdrawals on the Purchasing and Travel Cards.

Traffic infringements

3.15 Defence policy is that drivers are personally liable for all fines or penalties for traffic and driving infringements and offences imposed by civilian police and State and Territory authorities arising out of the use of a Defence vehicle.

3.16 ANAO testing of Defence Purchasing Card transactions identified about 50 transactions (totalling over $35 000) in which Defence has paid fines to State or Territory authorities for traffic infringements incurred in the three years examined by this audit. A case study arising from ANAO sampling of Defence Purchasing Card transactions is set out in Case Study 1, below.

Case Study 1. Traffic infringements by ADF members, based at Richmond, NSW

A Defence-plated vehicle was detected speeding in a school zone in Western Sydney on 29 June 2012. A penalty of $278 was imposed by the NSW state authorities on 28 July 2012, payable by 25 August 2012 and requiring the organisation to which the vehicle belonged—Defence—to nominate the driver.

Defence paid the penalty with a Defence Purchasing Card on 9 October 2012. A representative of 22 Squadron wrote to the NSW authorities stating that 22 Squadron was unable to identify the driver but procedures had been tightened to ensure such an incident could not recur.

The NSW State Debt Recovery office then (27 October 2012) imposed a penalty of $1258 for failure to nominate the driver. The penalty was paid by Defence credit card on 2 November 2012.

Any consequential change to procedures was not of wide or enduring effect at Defence's Richmond base. A 35 Squadron vehicle incurred nine infringements in two days, 10 and 12 December 2013, for driving on a 'T-way' lane. The NSW authorities imposed one penalty for each day ($1520 each) and issued cautions for the other seven infringements. Again, Defence was required to nominate the driver(s), by 14 January and 16 January 2014. In January, Defence received a penalty reminder notice.

A representative of 35 Squadron would not nominate the drivers when requested by another Defence official and stated that Defence would be paying the bill.

The NSW authorities then issued two enforcement orders of $1585 each for not paying the penalties and not nominating the driver(s). Defence paid these by Defence credit card.[33] On 18 March 2014, Defence received two corporate penalties of $1282 each for failing to nominate the driver(s).

3.17 The ANAO has drawn these payments to the attention of Defence's Fraud Control Branch. Defence enquiries have subsequently determined that at least $75 138 was paid on Purchasing Cards for 119 traffic infringements from 1 July 2012 to 9 November 2015. Defence's First Assistant Secretary Audit and Fraud Control wrote to the Deputy Chiefs of Navy, Army and Air Force in January 2016 seeking an assessment of the effectiveness of the management of traffic fines within the ADF, noting the anomalies detected by the ANAO. The letter drew their attention to cases in which individuals had been identified as vehicle operators yet their identities had not been passed to the traffic authority, as required by state law. Stakeholders were due to report back to FAS Audit and Fraud Control on the results of their review of their business practices in relation to payment of traffic fines by late April 2016.

3.18 Internally, senior Defence officials have expressed concern about 'what appears to be a cultural attitude within some ADF units towards protecting members from the statutory and pecuniary consequences of committing traffic offences while driving Commonwealth-plated vehicles'.[34] In its assessment report prepared in response to ANAO referrals made during this

33 These penalties of $1585 each were reduced to $1520 each in light of the timely payment.

34 Minute from the First Assistant Secretary, Audit and Fraud Control, to Deputy Chief of Navy, Deputy Chief of Army and Deputy Chief of Air Force, dated 12 January 2016.

audit, Defence's Fraud Control Directorate reported the following rationales provided for the Commonwealth to pay the relevant fines:

> Command decision that due to fines occurring during a charity exercise it would be unfair to burden the [ADF] members with fines. Supporting documentation also suggested the members should not pay fines because the local base driving instructions did not provide sufficient direction for members not to drive in a T-way;

and

> CPL [*name*] parked vehicle outside [*a named*] Hospital ... to visit one of his members injured on a ... course. The vehicle was parked in a metered area with no ticket displayed. CPL [*name*] claimed he parked the vehicle but did not believe he should pay the fine as he was attending to one of his injured soldiers. ... MAJ [*name*] stated he was sympathetic to CPL [*name*] as his situation was a serious medical issue.

3.19 As discussed in paragraphs 5.9 to 5.11 of this audit, where individuals are protected or do not take responsibility for their infringements, Defence must absorb penalties at a higher institutional rate, and individuals avoid personal sanctions such as payment of fines and driver demerit points. Issues of ethical conduct may also arise.

3.20 Defence informed the ANAO that it proposes to monitor the relevant merchant categories more closely in future. This should enable it to identify any fine payments made in future on Defence credit cards and take any necessary follow-up action.

Transactions valued at $10 000 or above that should be reported on AusTender

3.21 Since September 2007, non-corporate Commonwealth entities (such as departments) have been required to publish on AusTender[35] details of all procurement contracts and entity agreements entered into valued at $10 000 or more. Further, entities must report contracts and amendments on AusTender within 42 days of entering into (or amending) a contract.

3.22 ANAO analysis of Defence's largest 100 payments (from over $97 700 to over $691 700) on the Purchasing Card identified that:

- some contract values reported on AusTender are incorrect;
- reporting sometimes occurs outside the required timeframe;
- payments are being incorrectly blocked from AusTender by CMS users;
- payments are not reported on AusTender, but the reasons for this are not clear; and
- some payments have been incorrectly reported on AusTender by being recorded under the wrong supplier.[36]

35 AusTender is the Australian Government's web-based procurement information system for the centralised publication of business opportunities, annual procurement plans, multi-use lists, contracts and entity agreements. See: <https://www.tenders.gov.au> [accessed October 2015].

36 ANAO testing identified instances where a bank or foreign currency provider was wrongly identified on AusTender as the supplier of goods. For example, a $68 000 payment for arms and ammunition accessories was listed with a bank as the supplier. This occurred because the cardholder withdrew cash using the Purchasing Card to pay the actual supplier of the goods. After the matter was drawn to Defence's attention during this audit, some correction of the AusTender records took place.

3.23 ANAO testing also identified over 1000 pairs of Purchasing Card payments that, on face value, should have been reported on AusTender but were not because the payments were split into amounts of less than $10 000, contrary to Defence policy.[37]

3.24 In response to this audit, Defence informed the ANAO that it is reviewing its AusTender information and making corrections as necessary.

Cash withdrawals on the Purchasing Card

3.25 Defence allows Purchasing Card holders access to cash using the Purchasing Card on a case-by-case basis. Defence policy is that such cash withdrawals are only to be used as a last resort. Where cash is withdrawn, appropriate records, such as receipts and purchase approval forms, must be retained.

3.26 ANAO testing of a small sample[38] of cash withdrawals using Purchasing Cards identified:

- multiple withdrawals of substantial amounts of cash, with a transaction description indicating that the cash was to be used to pay merchants for goods and services. In one case, audit analysis identified three cash withdrawals of $99 999 by the same Defence official on the same day, on the face of it, to pay the same supplier. These were part of a succession of cash withdrawals over a period of ten days from the Defence Purchasing Card by the same official totalling over $879 000. In October 2015, Defence informed the ANAO that it was examining the cardholder's purchasing activities and that the CFO Group 'will be developing clear policy around the payment of Defence suppliers and the appropriate use of Defence credit cards'. Further enquiries by Defence revealed that the cardholder withdrew over $1.147 million to pay suppliers. Defence subsequently informed the ANAO that these transactions were, in fact, electronic funds transfers rather than physical cash withdrawals. Nevertheless, the transactions are identified and treated as cash withdrawals by the bank and in reports received by Defence.
  - These cash advances attracted interest payments of $18 278, paid by Defence.
- In January 2016, Defence advised the cardholder that their access to cash on the Purchasing Card had been removed, and their credit limit had been reduced to $50 000. Defence also advised the ANAO that Defence's Audit and Fraud Control Division had examined the documents relating to these procurements and referred the case to the Directorate of Investigations and Recovery where the matter is under formal investigation.

3.27 Appendix 5 lists other examples of cash withdrawals not consistent with Defence policy. In response to this audit, Defence informed the ANAO, in January 2016, that the CFO intended to remove cash access from Purchasing Cards and that cash access would be reinstated only where a case could be made, subject to approval by the relevant Group or ADF Service CFO.

37 The transactions were made on the same day to the same merchant on the same card. Each transaction was under $10 000 but they had a collective value of more than $10 000. Transaction splitting may also undermine controls over expenditure and authorisation limits.

38 The ANAO selected a sample of 52 transactions and requested supporting documentation from Defence on 15 September 2015. As at 3 February 2016, Defence had been unable to provide any supporting documentation for 14 of the selected transactions.

Cash withdrawals on the Travel Card

3.28 In practice, Defence allows its personnel to access their travel allowances (meals and incidentals) as cash drawn against their Travel Card. However, Defence financial policy encourages use of the DTC to pay direct to the supplier for the expenses these entitlements are intended to meet.[39]

3.29 Cash withdrawals carry a charge, in most cases, of 1.75 per cent of the value of the withdrawal. In 2014–15 Defence personnel withdrew $50 761 587 using the Defence Travel Card, at an approximate further cost to Defence of $888 328.

3.30 Defence personnel can withdraw cash to the total value of their approved meals and incidentals allowances in advance of travel. They often do so from Travelex outlets.[40] For longer trips, these allowances can amount to tens of thousands of dollars: for example, the top 30 individual Travel Card cash withdrawals between January 2015 and June 2015 ranged from just under $8500 to $42 384.

3.31 Some Defence personnel withdraw in cash not only the value of their meals and incidentals allowances but also a further part of their approved travel budget (that is, funds approved for expenditure as part of the trip on hotel accommodation, training course fees, bank and ATM fees, parking, taxi fares, medical supplies and so on). In a sample of 43 large cash withdrawals on the Defence Travel Card (ranging from $6182 to $42 384), 37 per cent either: exceeded the approved amount for meals and incidentals allowances, and no receipts or other supporting documentation was provided to show that any actual expenditure was incurred (up to $15 560 in one case); or insufficient documentation was provided to determine the value of approved meals and incidentals. ANAO testing also identified practices in the use of the Travel Card that are difficult to reconcile with Defence policy (see Appendix 6).

3.32 In the context of the Defence reform agenda launched in January 2016, instituting a program of credit card analytics that draws upon already available data and targets key areas of risk would provide Defence with greater assurance that its policies for credit card use are being complied with. Defence advised the ANAO in April 2016 that it has strengthened its analytics function and examines cash withdrawals monthly and traffic fines regularly.

Recommendation No.2

3.33 To provide assurance that credit card use is consistent with Defence policies, the ANAO recommends that Defence:

(a) undertakes periodic analysis of credit card transactions, targeting key areas of risk; and

(b) takes corrective action, where necessary.

Defence's response: *Agreed.*

39 FINMAN 5, version of 9 January 2015, note following item 5.2.11.3.

40 Obtaining cash advances from Travelex outlets enables Defence personnel to withdraw larger amounts than would be available from an ATM.

4. Cabcharge Fastcards and eTickets

Areas examined

This chapter examines Defence's arrangements for issuing and managing Cabcharge Fastcards and Cabcharge eTickets. These are both credit cards.

Conclusion

Defence has not exercised adequate central control over the issuing or use of Fastcards or eTickets.

Defence has no system in place and little capacity to routinely monitor and manage the risks it has identified in its use of Cabcharge eTickets. Defence could have used an available IT system to help it manage risks but did not do so. Defence has expressed concern internally at both the number of high-cost fares incurred with eTickets and the lack of justification for some of them. The ANAO found that, using eTickets over the last three years, Defence's 100 most expensive taxi fares incurred costs to the taxpayer ranging from $425 to $840 for single taxi trips, and a dozen taxis each took 500 or more trips for Defence. One taxi took over 2000 trips.

Defence advised the ANAO that it proposes to begin using an appropriate system. In doing so, it will need to consider the triggers for closer consideration of transactions, as this is the starting point for an effective risk-based approach to monitoring and follow-up.

Areas for improvement

The ANAO has made recommendations in Chapters 2 and 3 that should assist Defence to better manage its risks with respect to future use of Cabcharge eTickets.

4.1 Defence personnel travel extensively and make regular use of commercial ground-based transport services such as taxis and hire cars with drivers.[41] Generally, the Travel Card (discussed in Chapters 2 and 3) is Defence's preferred method of paying for official car trips as it provides greater accountability to Defence. Defence also allows Cabcharge eTickets to be used in defined and limited circumstances to pay for official car trips and has also allowed the use of Cabcharge Fastcards in the past.

4.2 Cabcharge Fastcards (formerly 'Cabcharge Cards', see Figure 4.1) are credit cards that enable the Defence user to pay for taxi travel for official purposes, with the cost billed to Defence. Cabcharge eTickets are single-use paper-based vouchers which also allow the holder to pay for a taxi with the cost billed to Defence. Defence's Accountable Authority Instructions recognise eTickets as credit cards.

41 Both taxis and hire cars with drivers (sometimes self-described as 'limousines') are encompassed by the term 'taxis' through the rest of this chapter.

Figure 4.1: What Cabcharge Fastcards and eTickets look like

Source: https://www.cabcharge.com.au.

Has Defence managed the issuing of Fastcards effectively?

Defence has not effectively managed the issuing of Cabcharge Fastcards to staff. Defence decided to terminate the use of Fastcards some years ago, but a number remained on issue at the time of this audit. At the commencement of the audit, Defence was not aware, centrally, of the Fastcards it had issued, to whom or when.

4.3 At the commencement of this performance audit, Defence stated that it had sought to terminate the use of Fastcards some years ago. Expenditure using these Fastcards has been limited over the last three years (Table 4.1).

Table 4.1: Defence Fastcard expenditure over 2012–13 to 2014–15

	2012–13	2013–14	2014–15
Number of transactions	–	63	66
Total cost	$232.03	$1 264.69	$2 907.95
Mean cost per trip	–	$20.07	$44.06

Source: Defence advice.

4.4 In response to ANAO enquiries, Defence found 34 individuals still held active and current Fastcards across 19 active Cabcharge accounts. With no systematic records, Defence had no central awareness of these cards or their status and had to rely on the card provider, Cabcharge, to provide details of the cards.[42]

4.5 According to Cabcharge, some of the Fastcards had never been used or had not been used in several years. Some cards had expired and been re-issued to the cardholder for a further period, even where the card had not been used. The ANAO was advised that this is common practice in the industry. In some cases, Defence stated that, because of the age of the accounts, it had no records as to who had authorised the issue of the Fastcards.

4.6 On 9 July 2015, in the course of the audit, Defence cancelled 31 of the 34 Fastcards mentioned above but left active each of those it had provided to the then Minister for Defence, Assistant Minister for Defence and Parliamentary Secretary to the Minister for Defence. Defence had previously advised Parliament in February 2015 that it 'does not issue corporate credit cards

42 The ANAO did not examine Defence's Cabcharge Card transactions as part of this performance audit.

to the Minister or ministerial office staff'.[43] Defence informed the ANAO that it was in the process of correcting this statement.

Has Defence managed the issuing of eTickets effectively?

The ANAO identified records of 261 158 taxi trips paid by eTicket at a total cost of over $16.28 million over the three years examined in the audit. Defence has not effectively managed the issuing of eTickets to its staff. At the commencement of the audit, Defence had no central awareness of how many eTicket accounts it held with Cabcharge. Some 303 accounts were opened without proper authority, reflecting a lapse in the control framework intended to ensure that only persons delegated by the Finance Minister may enter into borrowing arrangements on behalf of the Commonwealth. Defence has commenced taking corrective action to authorise its issuing of eTickets.

Cabcharge accounts were opened without proper authority

4.7 When this audit commenced, Defence had no central awareness of how many eTicket accounts it held as an entity with the Cabcharge company. Opening a credit card account on behalf of the Commonwealth requires proper authority, including the authority to enter into a borrowing arrangement.[44] Defence has two authorised delegates for such purposes. However, there is no evidence that any of the arrangements Defence has entered into with the Cabcharge company for the use of Fastcards and eTickets were made with the approval of either authorised delegate.[45] Nevertheless, some 303 accounts had been established and resulting invoices were paid by Defence. A total of 261 158 trips, at a cost of $16.28 million, were paid for using eTickets since January 2012 (usage of eTickets is discussed further below).

4.8 An August 2015 Defence fraud risk assessment in this area found that 'Any person who has a Defence email [*address*] can open a Cabcharge account and charge the account to Defence'.[46] During this audit, Defence received confirmation from the Cabcharge company as to how Defence personnel could set up Cabcharge accounts without the appropriate authority:

> We currently have no restrictions for who can open a Defence account. They need to be able to supply all of the information on the application and be a defence employee for us to process.

43 Senate, Defence Supplementary Budget Estimates, October 2014, Answer to Question on Notice No. 158—Credit cards. <http://www.aph.gov.au/Parliamentary_Business/Senate_Estimates/fadtctte/estimates/sup1415/def/defencegonsindex>. Viewed 10 March 2016.

44 Obtaining credit by way of credit card or credit voucher is a borrowing arrangement for the purposes of the PGPA Act (and its predecessor, the FMA Act). Only the Finance Minister or persons delegated by the Finance Minister may enter into an agreement for borrowing money on behalf of the Commonwealth.

45 The annual Certificate of Compliance process required all instances of non-compliance with the financial management framework to be reported to the responsible minister and the Finance Minister.

46 This could also include contractors and other external agents as they can have a Defence email address.

Corrective action taken by Defence

4.9 In July 2015, the Inspector-General of Defence[47] drew concerns about eTicket management to the attention of Defence's CFO Group. Defence advised that it had sought and agreed the following arrangements with Cabcharge, encompassing both Fastcards and eTickets:

- all requests received from Defence to open a new account with Cabcharge will be referred to its Directorate of Financial Operations (DFO);
- no Cabcharge Fastcards will be issued to any existing Defence accounts;
- from 16 July 2015, DFO is the main point of contact for all correspondence between Cabcharge and Defence, with the exception of the issuing of monthly account statements and invoices; and
- Cabcharge will provide a summary of the monthly statements, including the Defence contact at the end of every month.

4.10 Defence did not respond to a request for advice on whether it had (i) sought to identify and inform those who opened accounts in the past of the rules that apply to such actions; (ii) issued any internal directive to prohibit Defence members from seeking to establish new accounts without authorisation; or (iii) taken disciplinary action against anyone who has failed to exercise the care and diligence reasonably required and who, as a result, had set up the irregular accounts. It has advised that the new arrangement with the provider will be communicated.

Has Defence implemented adequate systems to support the monitoring and management of Fastcard and eTicket use?

Defence has not systematically monitored or managed activity on Cabcharge accounts. Analysis done within Defence has shown that eTickets have frequently been used where the Travel Card could have been used, as expected by internal policy. However, Defence had no internal system to help it monitor or manage activity on Cabcharge accounts. Defence's internal analyses and risk assessments have pointed to a need to introduce better systems to monitor and manage eTicket use. Defence advised the ANAO that it has a plan to use the existing Cabcharge module in its Card Management System, which should enable it to satisfy this requirement.

4.11 Each official incurring taxi costs should ensure that they are making proper use of public money. For example, this means using taxis at public expense only for an official purpose and only where it is the most cost-effective means of travel (a choice which may take account of security, reliability and so on). To provide this assurance at an enterprise level requires that Defence has the capacity to analyse information such as the eTicket data collected for this audit.

Defence has had little capacity to monitor the use of Fastcards or eTickets

4.12 Defence has had no internal system to help it manage or monitor the activity on Cabcharge accounts. For Fastcards, because it had no central awareness of their continuing use, it had undertaken no monitoring. Further, Defence did not have central visibility of eTicket accounts or usage. To obtain management information, Defence has relied on manual collection and

47 Under an internal reorganisation within Defence, the Inspector-General of Defence is now the 'Assistant Secretary, Fraud Control and Investigations'.

collation of eTicket data from across Defence or special data extractions from its Finance system. More recently, Defence has relied on Cabcharge to advise the details of the active accounts paid for by Defence. Consequently, Defence has had no system in place and little capacity to routinely monitor and analyse eTicket use, or to detect potential misuse.

4.13 All the credit card transactions generated by the Travel Card and Purchasing Card flow through Defence's CMS, an off-the-shelf software system. Defence was aware that a module for managing Cabcharge transactions was available for this system.[48] Defence had not acquired this module because it expected eTicket use to decline substantially and planned to replace CMS with another system. In practice, eTicket use has declined only gradually (discussed below).

Internal analyses have highlighted risks in Defence's management of eTickets

4.14 Defence's policy on the use of eTickets is that:

> To maximise efficiencies for Defence, the issue of Cabcharge eTickets **must be limited** to recruits, trainees, students, and members under 18 years of age. Noting the exceptions, it is expected that all Defence personnel use the DTC for taxi fares. The benefit of correctly using the DTC is that there is NO administrative surcharge fee.[49]

4.15 Service fees are payable by the vendor to the payment system provider and may not always be itemised and made transparent to the individual purchaser of the taxi services. For example, Cabcharge has advised that:

> virtually all Australian providers of taxi payment systems charge a service fee on top of the fare of 10 per cent (in the ACT, Tasmania, Northern Territory, Queensland and South Australia) and 5 per cent (in New South Wales, Victoria and Western Australia). Unlike other methods such as credit card and DTC, Cabcharge products do not consolidate this service fee at the point-of-sale, rather it is separated from the transaction and itemised on the invoice presented to Defence.

4.16 The ANAO considers that Defence's statement about administrative surcharge fees in its policy advice to staff on use of taxi payment methods may warrant reconsideration.

4.17 Defence's Directorate of Customer Access Management (DCAM) reviewed eTicket use in 2014. From the subset of about 54 accounts (among over 300) for which DCAM had visibility, it identified 22 141 Cabcharge eTickets issued between January and July 2014. For this subset, it found that:

- most were used where the Travel Card could have been used;
- some 456 eTicket journeys incurred fares above $100, the highest being $480.70; and
- for 45 of the fares above $100, including the fare for $480.70, insufficient detail was available to justify the fare.

4.18 DCAM estimated that more than half these taxi trips could have been paid for using Defence's preferred method, the Travel Card: 'Research also revealed that ADF members who have a [Defence Travel Card], and could use it ... are choosing to use the eTicket as it's perceived to be easier for the member'. This was of concern because (according to DCAM) 'It costs, on average, $10 000 a month in salary costs to manage the issue, receipt, reconciliation and payment

48 Cabcharge has also advised that it provides complimentary software to manage the issuance of eTickets and is 'happy to investigate options for interfacing the Cabcharge module with [CMS].'

49 Defence, 'Ethics Matters', 29 June 2015. Emphasis in the original.

of eTickets and Cabcharge Invoices'. Further, it was 'much more difficult to detect instances of fraud using the current manual Cabcharge eTicket system'.

4.19 In 2015, the Inspector-General of Defence undertook a risk assessment of Defence's use of eTickets. The risk assessment concluded that there was:

- uncontrolled fraud risk with multiple Cabcharge accounts and cards operating across the organisation;
- no single point of delegation or control;
- a lack of oversight and/or reconciliation process; and
- use of eTickets was inconsistent with Commonwealth value-for-money principles.

4.20 Defence policy mandates that, other than in specific circumstances, its Travel Card should be used for approved travel in taxis, not eTickets. This is for two reasons:

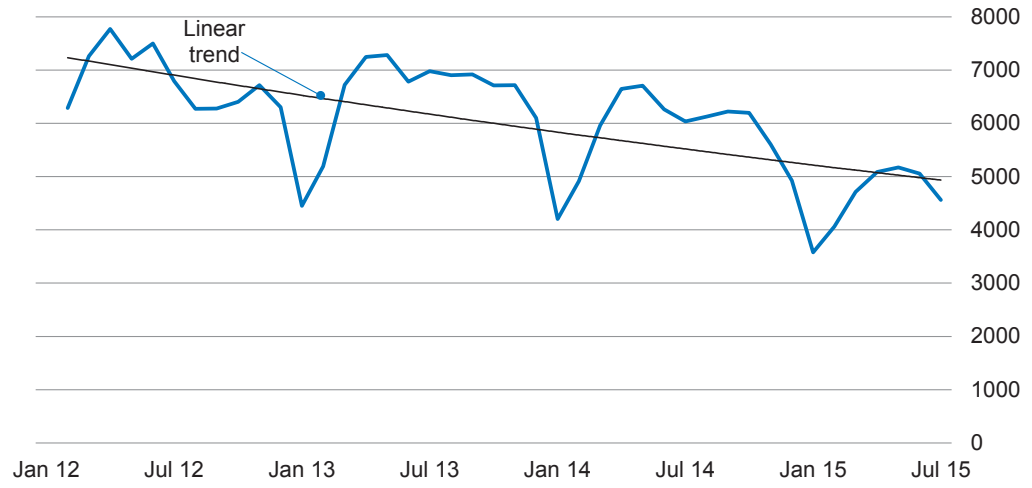
- Defence was aware that—because of weaknesses in its controls over eTickets—where eTickets are used rather than the Travel Card there is a greater risk to Defence of fraud or misuse;[50] and
- Defence has found that its use of eTickets incurs additional administrative costs which are avoided by using a Travel Card.

4.21 The Inspector-General of Defence has re-emphasised management concern that personnel continue to use eTickets when policy requires them to use their Travel Card. There has also been extensive publicity within Defence emphasising that the Travel Card is preferred for taxi trips.

4.22 ANAO analysis (Figure 4.2) shows that Defence has reduced eTicket usage, with a decline from around 7000 trips/month in January 2012 to 5000 trips/month by July 2015. For comparison, taxi trips by Defence personnel charged to the Travel Card are estimated to number between 12 000 and 13 000/month over the last three years.

50 The Cabcharge company considers that: 'Etickets do not inherently carry a higher fraud risk. Incorrect issuance and management of eTickets increase the risk of misuse'. They also state that 'Cabcharge products are very often procured by organisations for employees instead of typical credit cards due to the minimised fraud exposure that arises from usage restriction to one product type: on-demand passenger travel'.

Figure 4.2: Numbers of eTickets used by Defence per month, January 2012 – July 2015



Source: ANAO analysis of data supplied by Defence.

How can analysis of eTicket data help Defence manage its risks?

Active analysis of eTicket data would help Defence manage the risks it has identified with eTicket use. The ANAO's analysis identified patterns of usage of potential interest in managing eTicket use, such as high use of particular taxis, multiple expensive fares and 'small hours' travel. In some cases, the ANAO has referred particular analyses to Defence's Fraud Control and Investigations Branch.

4.23 As discussed, Defence has no system in place and little capacity to routinely monitor and manage the risks it has identified in the use of Cabcharge eTickets. Defence has advised the ANAO that it is proposing to make use of the Cabcharge module in CMS. In doing so, Defence will need to consider the parameters and patterns of usage that could trigger closer consideration.

4.24 By way of example, the ANAO analysed a large selection of eTicket usage data obtained from Cabcharge, focusing on outlier transactions, such as large fares and unusual usage patterns. In comparison with the analysis conducted by Defence's Directorate of Customer Access Management (DCAM, see paragraph 4.15), the ANAO's analysis encompassed data over a longer period and from Defence eTicket accounts of which, centrally, Defence was not previously aware. This yielded ten times as much data as was available to DCAM for its analysis.

Fourteen per cent of fares exceed $100

4.25 Over 80 individual taxi fares were higher than the fare of $480.70, the highest observed by Defence's DCAM. The most expensive 100 fares, including service charges, were all greater than $425. Further, whereas DCAM had observed 456 fares that exceeded $100 (some 2 per cent of its sample), the ANAO observed around 36 500 fares that exceeded $100 (some 14 per cent of the records examined). The highest fare observed was $840, a trip described as 'airport to Mollymook' (Table 4.2).

Table 4.2: The twenty most costly eTicket fares identified in ANAO analysis of Defence records, January 2012 – July 2015

Fare	Service Fee	From	To
$800.00	$40.00	Airport	Mollymook
$800.00	$40.00	Airport	Home
$750.00	$75.00	Airport	Nowra Hill
$715.00	$71.50	Suburbs	Airport
$680.00	$68.00	Airport	Wamuran
$680.00	$34.00	Syd Int Arpt	Williamtown
$680.00	$68.00	Office	Syd Dom Arpt
$670.00	$67.00	Airport	Bomaderry
$666.00	$66.60	City	Whittingham
$660.40	$66.04	City	Syd Dom Arpt
$654.20	$65.42	Westdale	Coonabarabran
$650.00	$32.50	Airport	Suburbs
$650.00	$65.00	Airport	Goonengerry
$650.00	$65.00	Airport	Nudgee
$622.70	$62.27	Reedy Creek	Reedy Creek
$622.00	$31.10	Airport	Syd Dom Arpt
$620.00	$62.00	Home	Brisbane Arpt
$620.00	$62.00	Hospital	Williamtown
$600.00	$60.00	Home	Chermside
$585.00	$58.50	City	Pinkenba

Notes: The cost of each trip is the sum of the fare (which includes GST) and the service fee. The departure point and destination for each trip are as specified in the information held by the Cabcharge company and provided to Defence.

Source: ANAO analysis of data supplied by Defence. Defence obtained the data from the Cabcharge company.

4.26 Routine analysis of high taxi fares may be a useful trigger for closer examination by Defence to ascertain whether personnel are making appropriate judgements in using taxis rather than options such as a self-drive hire car for official travel. However, this type of analysis and monitoring is only possible where, as in the case of eTickets, the payment mechanism automatically collects data such as that set out in Table 4.2. Similar analysis and monitoring is not possible with precision for individual taxi trips paid for using the Travel Card.

Patterns of use of specific taxis

4.27 Some 17 905 different taxis (by recorded taxi number) were involved in making 261 158 trips over the period January 2012 to July 2015, a mean of just under 15 trips per taxi (Table 4.3).

4.28 Some taxis were much more fortunate than others in winning Defence eTicket business. Whereas 16 800 taxis each undertook 50 or fewer of these trips for Defence, some 12 taxis each took 500 or more such trips, with three of these taxis each taking more than 1000 trips. One

particular taxi took 2160 trips using eTickets, an average of over 4.5 trips a day, at a total cost of $174 621. On its busiest day, it did 15 trips, costing $1162 in fares. The same taxi earned fares of over $1000 on each of seven separate days. Three taxis each earned over $100 000 in fares (exclusive of service fees) in the period.

4.29 In some areas, where there may be fewer taxis available, it may be reasonable to expect a higher-than-average use of particular taxis. Nevertheless, some of the most successful taxis in winning Defence business operate in major urban areas where competition exists. The data suggests the possibility of special arrangements or inappropriate activity in some cases. This analysis does not include taxi trips taken and paid for by the Travel Card.

Table 4.3: Number of Defence eTicket trips taken by separate taxis, grouped by range of number of trips (January 2012 – July 2015)

Number of trips (range)	Number of taxis whose number of trips lies in this range	Total number of trips taken by taxis whose total trips lie in this range
1–10	13 439	55 543
11–50	3 339	69 022
51–100	722	50 066
101–200	244	34 561
201–500	149	41 892
501–1000	9	5 298
1001–2000	2	2 616
>2000	1	2 160
	Total number of taxis: 17 905	**Total number of trips: 261 158**

Note: The table shows, for example, that 13 439 separate taxis each took between one and ten trips each for Defence in the period January 2012 to July 2015 and were paid using eTickets. Those taxis accounted for a total of 55 543 trips. Similarly, nine separate taxis each took between 501 and 1000 trips, accounting for 5298 separate trips in total.

Source: ANAO analysis of data supplied by Defence.

'Small hours' travel by eTicket

4.30 ANAO analysis also identified taxi trips paid for by eTicket and timed between 1.00am and 4.00am. This is a period when little work-related travel might be expected to take place, with the possible exception of trips to or from an airport or shift work. After excluding airport-related trips, the analysis indicated there had been 1263 such taxi trips by eTicket during this period.

Use of hire cars with drivers

4.31 ANAO analysis also indicated the extensive use of eTickets to pay for hire cars with drivers.[51] Defence advised the ANAO that it has no policy on Defence personnel using hire cars with drivers:

> The [*PGPA Act*] Section 23 Commitment Approver of the travel is responsible for the expenditure decision to hire a car with driver. The Section 23 Commitment Approver may consider use of hire car with driver provides Value For Money being an efficient, effective, economical and ethical

51 This is more difficult to discern reliably with other means of payment, such as the Travel Card, as less data is captured and provided to Defence with each transaction.

> use of resources. Factors that could be considered include cost comparison to taxi, distance travelled, [*and*] number of personnel requiring transport and personnel security.[52]

4.32 The ten such hire cars used most frequently in the period under review had each been used between 130 and 683 times, in several cases almost twice a day and, in one case, more often. The two most frequently used hire cars had each been paid over $100 000 by Defence for their services. It would be of value to Defence management to monitor hire-car-with-driver use to gain assurance that the responsibility to secure proper use and value for money is being met.

4.33 During the course of the audit, the ANAO referred certain analyses to Defence's Fraud Control Branch to consider whether there are matters that warrant investigation. Defence's First Assistant Secretary, Audit and Fraud Control wrote to the Navy, Army and Air Force, Joint Health Command, Joint Operations Command and the Chief Finance Officer Group in January 2016 seeking a review of Cabcharge eTicket business processes and the promotion of a 'cost-consciousness' culture for taxi travel. The letter specifically identified a number of the anomalies detected in this audit. Defence advised that all stakeholders were due to report back to FAS Audit and Fraud Control on their respective review activity by late April 2016.[53]

4.34 Implementation of risk-based controls and post-transaction analyses as recommended in Chapters 2 and 3 should also assist Defence to better manage its risks with respect to future Cabcharge eTicket use.

52 Defence advice of 29 October 2015.

53 Defence advice of 13 April 2016.

5. Fuel cards for vehicles

Areas examined

This chapter examines Defence's use and management of fuel cards for vehicles, with a particular focus on the arrangements to manage the risk of fraud.

Conclusion

The new whole-of-Australian Government motor vehicle fleet supply contract has allowed Defence to implement a new fuel card arrangement with improved controls.

Defence's performance, as measured by 'overfill' of fuel tanks and the frequency of questionable odometer readings, has reflected an ill-disciplined approach. There was an improvement from November 2015 to January 2016, but this may partly reflect a seasonal low-point in activity.

Defence has advised the Senate that its assurance framework has been in place since April 2015. However, Defence will not gain assurance as to the effectiveness of the framework until it has substantially completed audits of the implementation of the framework at Defence bases. Defence expects this to occur between September 2015 and June 2016.

Area for improvement

The ANAO has made a recommendation aimed at providing assurance that Defence's new fuel management arrangements are operating satisfactorily and have addressed the risks raised in this performance audit report and previous Defence internal audit work.

5.1 Defence experienced a major instance of vehicle fuel card fraud between April and June 2011.[54] A subsequent Defence internal audit (completed in 2012) found that the controls for the management of Defence fuel cards were ineffective and that Defence could have no confidence in the accuracy of fuel card transaction data. It also found that over $35 million of expenditure a year on fuel card purchases was acquitted without any verification process and the potential for misuse was significant.

5.2 During 2013–14, in line with the mandatory whole-of-Australian Government arrangements, Defence entered into an agreement with SG Fleet Pty Ltd (SG Fleet) to outsource the provision of vehicle fleet management services and commercial fuel cards (non-aviation). The contract commenced on 1 February 2013 with an initial term of six and a half years. The roll-out of fuel cards for Defence's 'white' fleet (cars and ordinary commercial vehicles) began in July 2013. This was followed by the roll-out of fuel cards for the 'green' fleet (Defence-owned four-wheel drives and trucks) in May 2014. Defence stated that the process to issue new fuel cards to Defence vehicle fleets was completed in May 2015. Before June 2015, Defence had been operating two fuel card systems in parallel. From July 2015, a single fuel management system has been operating for all vehicle fuel management across Defence. Most Defence vehicles have been

54 This instance of fraud was estimated to have cost the Commonwealth $585 000. Two fuel cards had been left in a Defence vehicle which was sent for repair and subsequently sold. Multiple purchases of diesel were made at service stations in various states over the period 9 April to 18 July 2011. On 18 July 2011, Defence became aware of the suspicious transactions and cancelled the cards.

issued with one (Caltex) fuel card per vehicle, though additional cards can be obtained with a business case.[55]

5.3 Defence's arrangement with SG Fleet differs from those of other government entities under this contract. Specifically, Defence pays directly to the fuel supply companies rather than having SG Fleet pay for the fuel and invoice Defence later.[56] Consequently, Defence has not entered into a borrowing arrangement to implement the Fuel Card and the card is not, under the PGPA Act, a credit card.

Are there effective controls on the use of Defence fuel cards?

There are new controls in place on the use of Defence fuel cards for vehicles, administered for Defence by a private company, SG Fleet, which provides Defence with useful exception reports, which list irregularities in the operation of the vehicle fleet.

Defence advised the Senate in June 2015 that an arm's length assurance framework had been in place since April 2015, and included compliance testing. However, that testing did not begin until September 2015 and Defence will not gain assurance as to the effectiveness of the framework until it has completed audits of the implementation of the framework at Defence bases. Defence expects this to occur between September 2015 and June 2016.

5.4 Defence bases its controls for fuel cards on the following principles:

- Defence provides each new fuel card for a specific vehicle identified by its registration number or equipment number;
- the fuel card is linked to a specific fuel type and tank capacity for the vehicle identified;
- the Defence user must use the fuel card supplied for the vehicle to purchase fuel and, at the time of purchase, provide the vehicle's then current odometer reading;
- each fuel card is issued with a transaction limit of $1000;[57]
- the user can purchase no other goods or services with the card (blocking); and
- the user must enter a PIN to use each card.

SG Fleet provides Defence with useful exception reports

5.5 To give effect to these controls, Defence has relied on action taken by SG Fleet. As part of the fleet management arrangement, SG Fleet produces exception reports showing irregularities which call for management attention. Three regular exception reports address:

- *overfills*—where:
  - the volume of fuel paid for using a fuel card allocated for that vehicle exceeds the recorded capacity of its fuel tank by more than three per cent; or
  - the same vehicle is filled more than three times within 24 hours;

55 Defence advises that 2666 vehicles have a second fuel card and 2211 have a third card.

56 This difference flows from the capacity of Defence as a major fuel user, including for naval and aviation assets, to negotiate a better price direct with the fuel supplier than through the third party.

57 Defence stated that it has increased this limit on about 400 cards associated with trucks, buses and tankers.

- *irregular odometer readings*—where an odometer reading is not in sequence with previous readings held or otherwise appears incorrect or anomalous; and
- *infringements*—a list of road or traffic offences committed by the driver of the vehicle. In the case of Defence's white fleet, SG Fleet receives notice of these in the first instance and refers them to the relevant unit in Defence for identification of and personal payment by the driver.

Overfills and irregular odometer readings

5.6 SG Fleet's 'Fleet Intelligence' computer system obtains information from the fuel supply companies on a weekly basis. When an overfill or irregular odometer reading occurs, the system generates a 'ticket' that requires SG Fleet to contact the relevant area of Defence for explanation and resolution.[58] Thus, were a fuel card to be persistently misused in a way similar to the 2011 incident, it should come to attention within about one week. In July 2015, Defence described SG Fleet's follow-up process to the ANAO as follows:

> SG Fleet actions the exception by contacting the relevant unit transport manager and seek[ing] an explanation for the exception identified. Unit Points of Contact and/or Unit Transport Managers with access to Fleet Intelligence have the obligation to remediate exceptions when a representative from SG Fleet contacts them. If no response is received or [an] inadequate response [is] provided, SG Fleet escalates the exception to the next level in the chain of command/responsibility, which is usually CGVSPO [*Commercial and General Vehicle System Program Office*].

5.7 Defence provided the ANAO with a sample of four cases to show how the company followed up overfills. These indicated that the company contacted the relevant officer at the Defence base where the vehicle was kept and obtained an explanation for each. Defence has no process for assessing the adequacy of such explanations.

5.8 SG Fleet's fuel exception escalation procedure shows that, at each stage of escalation, the matter is terminated by 'response received and stored for audit purposes'. As discussed below, Defence is yet to establish a systematic audit and assurance process for vehicle fuel.

Traffic Infringements

5.9 Over the period 2 November 2013 to 23 May 2015, vehicles leased to Defence incurred some 340 known infringements. These were recorded and reported to Defence by SG Fleet in an 'exception report'. These mainly comprised speeding fines (about 286), but there were also 27 instances of 'running red lights', 10 of driving in a bus lane and a few instances of illegal parking, disobeying traffic signs and other breaches. The report also shows:

- HMAS *Kuttabul*/Sydney Pool was the unit whose drivers attracted the largest number of fines (30), closely followed by HMAS *Cerberus* with 26;
- the vehicle numbered D1202W (at HMAS *Cerberus*) was the single vehicle attracting the largest number of fines (5); and
- the largest single fine was $3952 imposed in March 2015 for a speeding vehicle from Joint Logistics Unit (Victoria) Bandiana.

58 From July 2015, Defence's Electronic Supply Chain Manual places an onus on Unit Transport Managers to act upon invalid odometer readings, fuel overfill reports and infringement reports and to email relevant information to SG Fleet.

5.10 Where a vehicle belongs to an organisation, the state authority imposing a penalty will require the organisation to nominate the driver, who may have attracted both a financial penalty and demerit points. Where the organisation does not nominate the driver, a further penalty may be imposed on the entity, which may be over $1000. This may explain the presence on the SG Fleet infringement list of about 80 instances of penalties of around $3000 each.

5.11 The sum of the fines listed in the SG Fleet report provided to Defence is about $440 000, including penalties charged at the institutional rate. Where the driver has been identified, the relevant state or territory authority will not proceed with the institutional penalty but will impose an individual penalty (at a lower rate) on that driver. However, Defence has no easily accessible record of how each infringement has been resolved and, therefore, cannot state in which cases it could not identify the driver involved.[59]

Testing of Defence's assurance framework not yet complete

5.12 In November 2014, in the context of auditing Defence's financial statements, the ANAO noted that fuel consumption information within the Fleet Intelligence system was incomplete, reducing the effectiveness of exception reports. There was no acquittal or exception reporting process over fuel consumed during the 2013–14 financial year. The ANAO recommended that Defence establish monitoring policies and procedures to action the exceptions identified in Fleet Intelligence reports related to the quantity and type of fuel purchased.[60] In response, Defence informed the ANAO that work was continuing on an improved assurance framework which will include 'utilisation of business intelligence provided through the SG Fleet contract and business process testing (BPT). The framework was expected to be in place by 31 March 2015'.[61]

5.13 Defence advised the Parliament, in response to a question on notice from a Senate Estimates hearing in June 2015, that: 'Since April 2015, Defence's Fuel Services Branch is providing independent oversight of fuel card management and independently tests for compliance with the new fuel card arrangements'. Fuel Services Branch is responsible for enforcing Defence's fuel policy.

5.14 In fact, this testing did not begin until September 2015. Examining the SG Fleet exception reports—which began in April 2015—was seen by Defence as an important step towards implementing an assurance framework. In July 2015, Defence advised the ANAO that:

> until the formation of [*Fuel Services Branch (FSB)*] in Feb 2015, there was no central fuel card assurance role. [*FSB*] has now taken up that role and the first time [*FSB*] looked at the reporting available through SG Fleet *Fleet Intelligence* system was Apr 2015 following the completion of the main fuel card rollout across the B [*vehicle*] fleet.
>
> Part of the assurance framework [*FSB*] is developing is to review exception reports at intervals ... Clearly, the exception reports may assist in targeting units for compliance checks.

5.15 By September 2015, Defence had developed a test program to use as a 'pilot assurance activity' over 12 Defence sites from 21 September to 31 March 2016. Defence will not gain

59 Instances where Defence has paid a traffic infringement fine with public funds are discussed in Chapter 3, (paragraphs 3.15 to 3.20).

60 ANAO, Department of Defence, Financial Statements Audit 2013–14, Final Closing Audit Report, Nov. 2014.

61 ibid., p. 23.

assurance as to the effectiveness of the framework it has designed until it has substantially completed this testing. Defence now expects this to take until June 2016.

Defence uses the same PIN on all fuel cards

5.16 In implementing the new arrangements, Defence announced to all staff that the same PIN would be used on all the new fuel cards. The main purpose of the PIN is to inhibit misuse of the fuel card by parties external to Defence. Nevertheless, using the same PIN on all cards introduces a weakness in controls against potential internal misuse.

5.17 SG fleet has confirmed that using a common PIN is standard commercial practice where there are pool vehicles. However, the number of Defence pool vehicles is atypically large. Defence's view is that the current fuel card system does not provide an effective method of managing PINs for green fleet and loan pool vehicles. In February 2016, in response to this audit, Defence advised the ANAO that, as an interim measure, it will require each business area to change the PIN for each fuel card in circulation and to reset the PINs for new cards within seven days of issue. Further, Defence advised that: it will work with the fuel service providers and SG Fleet to improve the PIN management system, which may include a technological solution; and a number of additional preventative/detective controls were identified at a meeting between Defence and SG Fleet on 29 January 2016.[62]

What have been the trends in fuel card usage?

The number and volume of fuel overfills—where the fuel obtained and paid for exceeds the recorded capacity of the fuel tank—was substantial during 2014 and 2015, but declined over the last six months of available records. There is also evidence of ill-discipline in the provision of odometer readings by Defence personnel. However, the number of irregular odometer readings—where an odometer reading is not in sequence with previous readings held or otherwise appears incorrect—is also declining.

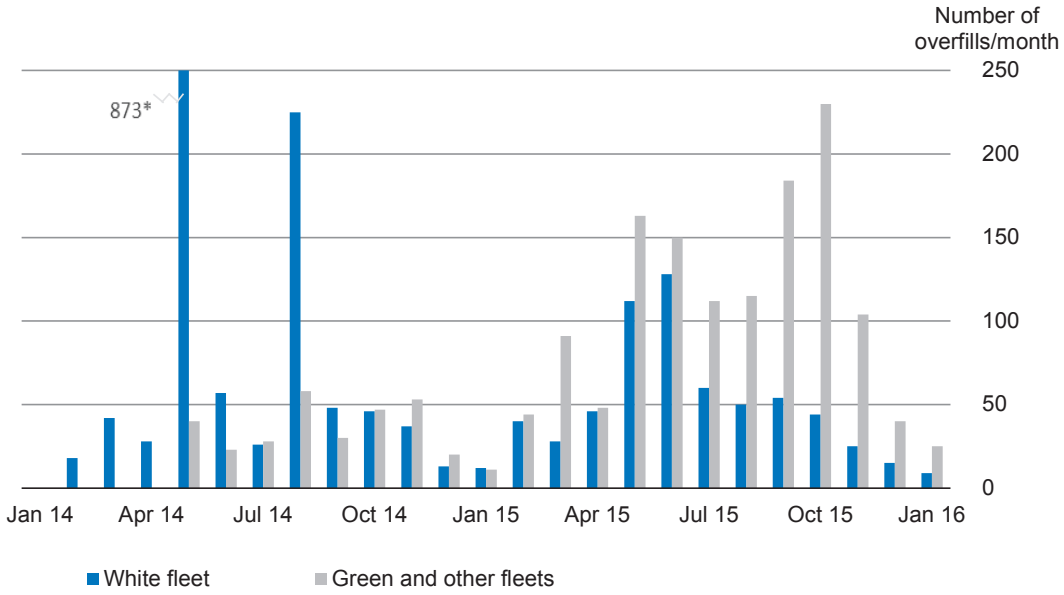
5.18 SG Fleet reports that over the last three financial years there have been 682 175 fuel transactions, with a mean of about 623 fuel transactions a day. It had facilitated management of the supply of 46.9 megalitres of fuel to Defence over the three financial years (at about 42 900 litres/day and 68.8 litres/transaction).

Overfills

5.19 SG Fleet's exception reports to January 2016 show both the number of overfills and the volume of fuel consumed in these overfills (reaching a peak of over 56 000 litres in May 2015). Both the number and the volume of overfills has been erratic over much of the period shown, with a downwards trend over the months leading to January 2016 (Figure 5.1).

62 Defence's advice on these additional controls is set out at Appendix 8.

Figure 5.1: Number of vehicle fuel overfills/month, February 2014 to January 2016



*Note: In May 2014, early in the current fuel card arrangement, Defence's white fleet recorded a peak of 873 overfills/month, off the scale of this graph. The scale has been selected to make more recent trends clear.

Source: ANAO analysis of Defence data, sourced from SG Fleet.

5.20 These figures must be regarded with caution because of several factors:

- further fleets of Defence vehicles have been introduced into the arrangement with SG Fleet over the period, and relevant Defence personnel may take time to learn the required practices. On the other hand, fuel card rollout data shows that the bulk of Defence fleets were subject to the new arrangement by the end of 2014; and
- SG Fleet questioned the integrity of data provided to it at the commencement of the contract, on the size of fuel tanks and presence of long-range tanks. In January 2016, SG Fleet reviewed 1353 overfills identified since March 2015, and advised Defence that:
  - 61 per cent (822) of overfills were the result of SG Fleet not receiving the correct tank capacity for the vehicles concerned;
  - 34 per cent (463) were the result of drivers not using the fuel card allocated to that vehicle to fill that vehicle (and only that vehicle);[63]
  - 5 per cent (68) relate to fuel cards for support equipment (such as generators, lawn mowers, and tow motors), for which SG Fleet have recorded a nominal tank capacity though, in practice, one card is used for many pieces of equipment.

5.21 The discipline introduced by the external management arrangement with SG Fleet may reduce the reported overfills in future: this should be closely monitored by Defence.

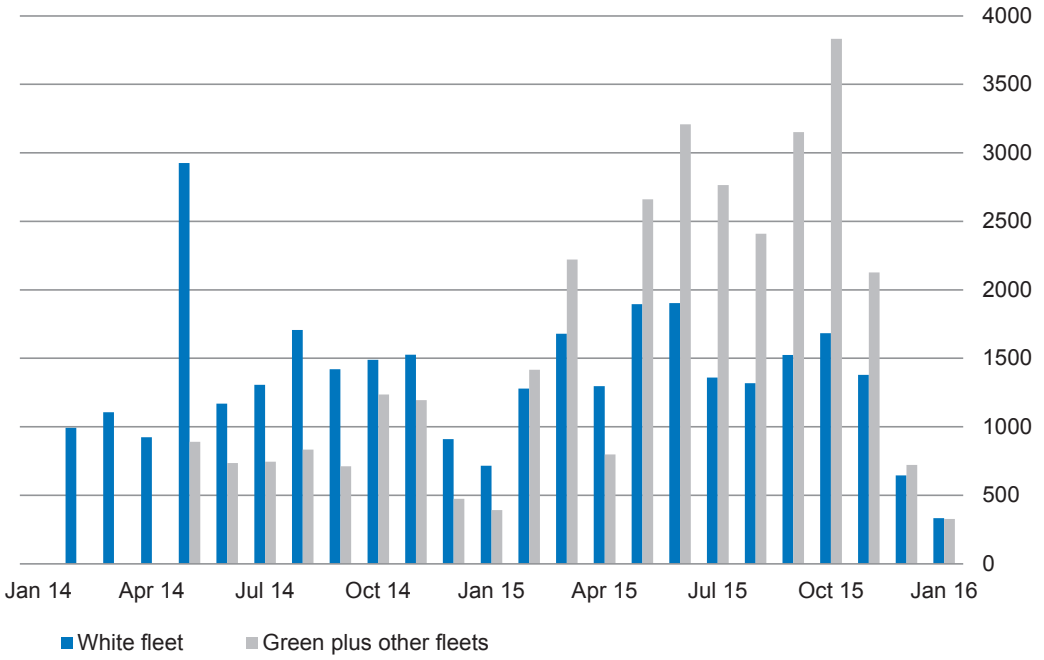
63 Of these, 162 instances were a result of a vehicle's fuel card being used to fill many vehicles in a convoy. Defence has stated that 'The practice of a single fuel card being used to fill a number of vehicles of a convoy remains acceptable, noting that an Overfill Exception Report will be automatically generated by SG Fleet Pty Ltd and which subsequently must be acquitted by the unit' (DEFGRAM 29/2016, 1 February 2016).

Irregular odometer readings

5.22 SG Fleet also produces a regular report listing 'rejected' odometer readings. SG Fleet advised that: 244 048 readings were supplied by Defence users and recorded in SG Fleet's Fleet Intelligence system from February 2014 to January 2016; and over 65 000 (some 26.6 per cent) were rejected as implausible by the company. The frequency of rejected odometer readings has been erratic but the trend over about fifteen months has been for it to rise substantially, with a mean of about 183 questionable readings a day being taken in October 2015.

5.23 The number of rejected readings (see Figure 5.2) rose as more fleets of Defence vehicles were brought into the system, with an associated need for the Defence personnel who use those vehicles to become accustomed to a more rigorous management regime. Most of the rejected readings through 2015 are attributable to the green fleet.[64] The numbers of rejected readings for both the white and green fleets declined in the period November 2015 – January 2016, but this is a seasonal low point of activity, and further data will be required into 2016 to gauge whether better discipline is being applied. The base readings held by SG Fleet may also require correction, though this should improve over time. As mentioned earlier, the company has advised the ANAO that it has recently made specific efforts to collect better data on Defence's vehicles.

Figure 5.2: Rejected odometer readings/month, February 2014 – January 2016, by fleet



Source: ANAO analysis of Defence data, sourced from SG Fleet.

64 Defence advised the ANAO that 'due to system limitations, Army has chosen not to maintain odometer readings in [SG Fleet's] *Fleet intelligence* [system] for the Green Fleet'. It has not explained the 'system limitations' or what action is being taken to address them.

5.24 Human error will lead to a small proportion of faulty odometer readings being provided when refuelling; however, the data suggests the existence of an ill-disciplined approach to supplying odometer readings. Among the 65 000 rejected readings:

- on over 8500 occasions Defence users have supplied an implausible 'zero' or 'one' as the odometer reading;
  - the unit for whose vehicles a zero odometer reading has been recorded most frequently (over 300 times) is the SAS Regiment;
  - the vehicle that attracted the most rejected odometer readings (over 200) was a Land Engineering Agency white fleet four-wheel drive based at Monegeeta;
- some 1097 values were the value of the PIN for the fuel card (as discussed above, Defence has used the same PIN on all fuel cards). This was most frequent among vehicles based at HMAS *Cerberus* (83 occasions) and HMAS *Kuttabul* (58 occasions); and
- the number '777' has been offered with particular frequency, on over 2095 occasions. SG Fleet advised that this is because the Caltex system defaults to 777 when a driver fails to enter an odometer when prompted. The driver is responsible for this error appearing on the report.

5.25 Two risks associated with this poor record of supplying odometer readings are: first, that it may conceal some misuse or fraud, such as the improper purchase of fuel for a non-Defence vehicle or purpose; second, it detracts from the capacity of both the company supplying the white fleet to manage the vehicles and Defence to manage the green fleet. In turn, this may have safety implications for drivers, passengers and other road users. The data collected through odometer readings is used to schedule maintenance and, ultimately, replacement of the vehicles. Therefore both Defence and the company have an interest in ensuring that Defence drivers provide accurate, current odometer readings when refuelling.

5.26 In response to this audit, Defence has acknowledged previous 'poor management and record-keeping practices across Defence with white and green vehicle fleets'. It has advised the ANAO that it is developing an online training package to inform Defence staff of expectations, to change culture and encourage compliance.

Recommendation No.3

5.27 To help ensure that the new fuel management arrangements are operating satisfactorily and have addressed the risks identified in this performance audit report and in its 2012 internal audit on fuel cards and fuel management, the ANAO recommends that Defence conduct a follow-up review of progress in the 2016–17 financial year.

Defence's response: *Agreed*

Grant Hehir
Auditor-General

Canberra ACT
5 May 2016

Appendices

Appendix 1 Defence response to the proposed report

Australian Government
Department of Defence

Mr Dennis Richardson
Secretary

Air Chief Marshal MD Binskin, AC
Chief of the Defence Force

SEC/OUT/2016/92
CDF/OUT/2016/297

Dr Thomas Clarke
Executive Director
Australian National Audit Office
PO Box 707
Canberra ACT 6203

Dear Dr Clarke,

AUSTRALIAN NATIONAL AUDIT OFFICE PERFORMANCE AUDIT ON DEFENCE'S MANAGEMENT OF CREDIT AND OTHER TRANSACTION CARDS

1. Thank you for your correspondence, which contained the Section 19 Proposed Report for the subject audit.

2. Attached to this letter are Defence's Proposed Amendments, Editorials and Comments (Attachment A), Responses to Requests for Information (Attachment B), the Agency Response (Attachment C) and the Response to Recommendations (Attachment D). These enclosures represent Defence's formal response to the Proposed Report.

3. We would like to take this opportunity to formally thank the ANAO for the time and resources they have allocated to the audit. The report's finding and recommendations will benefit Defence's current and future management of its credit and other transaction cards.

Yours sincerely,

Dennis Richardson
Secretary

13 April 2016

MD Binskin, AC
Air Chief Marshal
Chief of the Defence Force

14 April 2016

Enclosures:
A. Proposed Amendments and Editorials
B. Responses to Requests for Information
C. Agency Response
D. Response to Recommendations

PO Box 7900 Canberra BC ACT 2610 Telephone 02 626 52851 - Facsimile 02 6265 2375

***Defending Australia** and its National Interests*

Appendix 2 Cabcharge response to an extract from the proposed report

Cabcharge[65] thanks the Australian National Audit Office for the opportunity to provide comments on the proposed Audit report on Defence's management of credit and other transaction cards. Much of the discussion in the report focuses on the issuing of eTickets, as well as their monitoring, management and associated risk.

Our response clarifies some factual inaccuracies as well as questioning some of the methodology used to examine and categorise eTickets and FastCards as higher risk products.

- Cabcharge provides a range of tools to assist account holders in managing and tracking spend. Cabcharge's complimentary eTicket management tool (CTMS) provides solutions for the effective management and monitoring of eTickets. Cabcharge is able to work with Defence to explore integration with the existing CMS being used.
- A service fee exists with the use of non-cash payment methods in taxis, and is not exclusive to Cabcharge products.
- A few transaction amounts have been highlighted. For example, the headline figure of '$1467' was the result of a driver keying error—the driver having contacted the network immediately after, with the transaction corrected in the following period (the actual final amount charged to defence was $147.10).[66]
- The alleged excessive nature of these eTicket transactions lacks weight in the absence of due comparison with taxi transactions paid for using the Defence Travel Card (DTC). It is the very features of Cabcharge products that allow ANAO's analysis, namely effective reporting, otherwise unavailable with other credit products when used in taxis. In the absence of such a comparison, it remains unclear whether the transaction amounts are larger due to eTicket-specific factors, or rather, due to the operations and use case of Defence.

Cabcharge on the basis of industry experience believes that FastCards and eTickets provide an unparalleled level of control, due to their features: namely one-time use for eTickets and confinement to usage in a single industry channel (hire cars & taxis).

In fact, a new customisable eTicket (FLEXeTICKET) is being introduced which allows the account holder to set the maximum allowable fare, as well as set time and day restrictions, addressing inter alia the issues of 'small hours' travel and weekend use. This enhancement is aimed at preventing out-of-policy usage, rather than just detecting it.

These features are not available with other methods of Card payment.

The DTC, in comparison, can be used in a range of circumstances, in a potentially less restricted manner.

65 Cabcharge provided the ANAO with a detailed response addressing a range of technical issues covered in the report. The executive summary is reproduced here.

66 ANAO note: The erroneous transaction has been removed from the analysis.

Cabcharge notes recent delegation of Cabcharge product management to a centralised authority within Defence and is optimistic as to the productivity gains, increased clarity, monitoring ability as well as management of credit products provided by Cabcharge to Defence.

Appendix 3 New arrangements for credit card governance in Defence

The following document, with its four attachments, was distributed by the Chief Finance Officer, Department of Defence, to Defence's CFO Leadership group on 21 January 2016, with the advice that 'these new credit card governance arrangements [*were*] effective for all new credit cards as of 18 January 2016'.

Department of Defence
Credit Card Governance
January 2016

Credit Cards are an important and commercially sensible method of transferring funds to Defence's Vendors.

Credit Cards sit within a matrix of payment mechanisms, some of which are available to line managers and some are only available to the Treasury and Banking Branch within the CFOG. The full suite of payment mechanisms and their relevance are contained in Attachment 1.

It is Government policy that all payments to vendors less than $10 000 should be by Credit Card unless a vendor does not accept a Credit Card (Department of Finance, Resource Management Guide No. 416, *Facilitating Supplier Payment through Payment Card*).

Each payment mechanism has their particular inherent risks, efficiencies, effectiveness and cost profiles. The use of a particular mechanism is therefore considered in light of their profile. A summary of factors to be considered using a Credit Card are listed in Attachment 2.

The key governance elements of Credit Card management are as follows:

1. Travel Card spending limits are set at $10 000 on a default basis. Business cases for increased limits are to be provided to Group CFOs (or their delegate) for approval. Credit Card limits may be reduced depending on usage patterns.
2. Purchase Card spending limits are set at $30 000 on a default basis. Business cases for increased limits are to be provided to Group CFOs (or their delegate) for approval. Purchase Card limits may be reduced depending on usage patterns.
3. Virtual Card spending limits are set at $500 000 on a default basis. Business cases for increased limits are to be provided to Group CFOs (or their delegate) for approval. Virtual Card limits may be reduced depending on usage patterns. Virtual Travel Cards are to be used only when transaction volumes demand or as determined by the Group CFO.
4. The Group CFOs (or their delegate) will annually (first quarter of each financial year) review the following to determine whether to retain or alter:
   - Individual Credit Card spending limits;
   - Individual Credit Card cash transferral limits;
   - Virtual Credit Card limits;
   - Merchant Categories;
   - Unused Credit Cards.

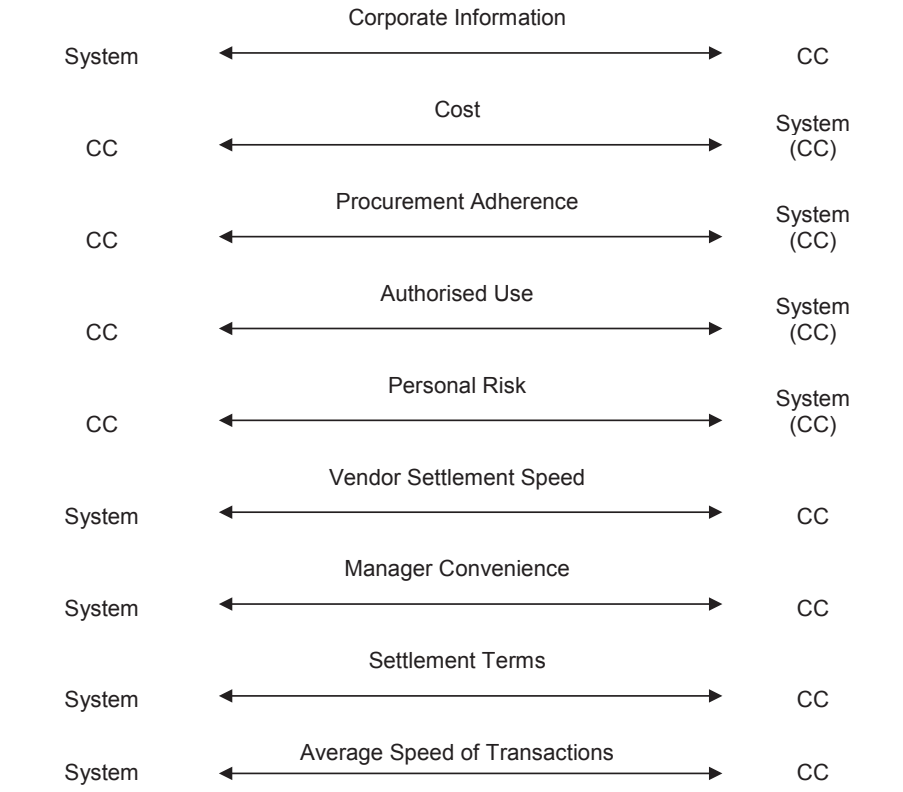
5. Purchasing card cash transfer limits are set at $0 on a default basis and business cases for increased limits are to be provided to Group CFOs for approval.
6. Credit Card transactions will be monitored monthly with particular focus on the merchant categories listed at Attachment 3.
7. Merchant categories barred from use and that have been disabled are at Attachment 4.
8. All Credit Cards are to be validated by a CMS Supervisor.
9. CMS Supervisors are determined by the Group CFOs (or their delegate).
10. All Credit Cards that are not activated within 90 days will be cancelled. Reapplication can be made through the usual process.
11. All physical Credit Cards are to be subjected to unique pin codes. Non-Aviation Fuel Cards are to be reset from the default pin on issue to either a unique pin code or a unit specific code within 7 days of issue.
12. These arrangements will be written into relevant policy documents, and are effective from 18/01/2016.
13. Any Credit Card transactions which are not supported by adequate explanation will be referred to the Audit & Fraud Control Division.

Attachment 1

Payment Method	System Used	Valid Currencies
Direct Entry (EFT)	ROMAN	Local & Foreign Currencies
Cheque	ROMAN	Local & Foreign Currencies
Manual Direct Entry	RBANet—Treasury & Banking use only	Local & Foreign Currencies
Manual (Collect) Cheque	Treasury & Banking use only	Local & Foreign Currencies
Credit Card—Credit Payment	Credit Card	Local & Foreign Currencies
Credit Card—EFT Payment	Credit Card	Local & Foreign Currencies
Credit Card—Cash Withdrawal	Credit Card	Local & Foreign Currencies
Urgent/Immediate Manual Direct Entry	Treasury & Banking use only	AUD only

Attachment 2

Credit Card Vs System Payments



Attachment 3

Defence Credit Cards

CATEGORIES TO BE MONITORED (54)	
Merchant Number	**Description**
1600	Real Estate Agent
1830	Traffic and Parking Fines
2110	Theatres & Ticket Services
3050	Liquid/Wines & Spirits
3200	Jewellery/Watches/Clocks
3320	Furs
3500	Duty Free
3835	Duty Free
3844	Messenger Services
3856	In-flight Sales
3882	Cheque Cashing
4400	Messenger Services
4722	Travel Agencies and Tour Operations
4723	Package Tour Operations (Germany Only)
5094	Precious stones, metals, watches & jewellery
5193	Florist Supplies, Nursery Stock and Flowers
5271	Mobile Homes Dealers
5300	Wholesale Clubs
5309	Duty Free Shops
5592	Motor Home Dealers
5598	Snowmobile Dealers
5600	In-flight sales
5681	Furriers and Fur Shops
5931	Used Merchandise and Second-hand Stores
5932	Antique Stores
5933	Pawn Shops
5937	Antique Reproductions
5944	Clock, Jewellery, Watch and Silverware Stores
5948	Leather Goods and Luggage Stores
5960	Direct marketing insurance services
5962	Direct marketing—Travel Related Arrangement Services
5963	Door-to-door sales
5964	Direct Marketing—Catalogue Merchants
5965	Direct Marketing—Combination catalogue and retail merchants
5966	Direct Marketing—Outbound telemarketing
5967	Direct Marketing—Inbound telemarketing
5968	Direct Marketing—Continuity subscription merchants

CATEGORIES TO BE MONITORED (54)	
Merchant Number	**Description**
5969	Direct Marketing—Other Direct Marketers
5972	Stamp & coin stores
5993	Cigar stores & stands
6010	Manual Cash Disbursement **formerly Tours/Holiday/Vacations
6220	On-Board Sales
7012	Timeshares
7276	Tax Preparation Services
7297	Massage parlours
7542	Car washes
7631	Watch, Clock and Jewellery Repair Shops
7832	Motion picture cinemas
7932	Billiard & pool establishments
7933	Bowling alleys
7993	Video amusement game supplies
7994	Video game arcades and establishments
7996	Amusement Parks, Circuses, Carnivals and Fortune Tellers
8003	Movie Tickets

Attachment 4

BLOCKED CATEGORIES (4)	
Merchant Number	**Description**
7273	Dating and Escort Services
7995	Gambling Transactions Entertainment

Appendix 4 Defence use of its Purchasing Card, October 2013 – June 2014

See discussion at paragraph 3.10.

Table A.1: Defence use of its Purchasing Card, October 2013 – June 2014

Merchant Category	Domestic	International	Total	%
Airlines	71.8%	28.2%	$1 229 133	0.79%
Associations/charities	99.0%	1.0%	$8 882 257	5.73%
Bank	79.2%	20.8%	$28 672	0.02%
Boat/car sales/repairs	98.6%	1.4%	$6 518 028	4.21%
Business services	96.5%	3.5%	$23 027 759	14.86%
Car rental	53.7%	46.3%	$1 618 843	1.04%
Department stores	98.3%	1.7%	$584 799	0.38%
Education	91.5%	8.5%	$13 630 421	8.80%
Entertainment	96.0%	4.0%	$3 072 079	1.98%
General merchandising	94.4%	5.6%	$3 680 928	2.38%
Hotels/accommodation	47.4%	52.6%	$7 288 000	4.70%
Legal	98.0%	2.0%	$6 141 667	3.96%
Medical	96.5%	3.5%	$2 002 557	1.29%
Other	95.6%	4.4%	$22 456 437	14.49%
Other rental	99.7%	0.3%	$189 534	0.12%
Petrol/service stations	69.1%	30.9%	$343 271	0.22%
Restaurants/fast food	92.6%	7.4%	$1 035 087	0.67%
Service to house/tradesmen	98.7%	1.3%	$13 122 317	8.47%
Telecommunications	95.3%	4.7%	$4 094 557	2.64%
Transport	97.7%	2.3%	$529 908	0.34%
Travel/holidays	83.2%	16.8%	$2 143 599	1.38%
Undefined	32.9%	67.1%	$7 149	0.0046%
Utilities	98.5%	1.5%	$837 539	0.54%
Non-essential/luxury purchases	95.9%	4.1%	$25 670 407	16.57%
Supermarket/food/general store	98.5%	1.5%	$6 561 534	4.23%
Insurance/tax	98.7%	1.3%	$246 317	0.16%
Total	**93.1%**	**6.9%**	**$154 942 798**	**100.00%**

Source: 'Quarterly Report (April–June 2014)', report provided to Defence by its credit card provider for the Defence Purchasing Card. This was the latest such set of data available in mid-2015.

Appendix 5 Instances of Purchasing Card cash withdrawals not consistent with Defence policy

Cash withdrawals on the Purchasing Card not consistent with Defence policy
• Cash withdrawals totalling $1059 without evidence of prior approval. Defence was unable to locate receipts to support the associated expenditure.
• A cash withdrawal of $332. No receipts to support actual expenditure.
• A cash withdrawal of $300 made without evidence of prior approval of the expenditure and the amount was repaid by the cardholder after ANAO requested supporting documentation.
• Travel allowances withdrawn on the Purchasing Card.
• Cash withdrawn and invoices paid before delegate approval was obtained.
• CMS expense summary report not signed by the cardholder or CMS Supervisor.
The ANAO's analysis also identified instances which highlight risks associated with cash withdrawals: • In one instance, the Cardholder's Defence credit cards and PINs were stored together. The cards and PINs were stolen and $1000 was withdrawn using the Purchasing Card.[67] • In another case, a total of $4839.57 was withdrawn and all receipts stolen. The receipts were allegedly in a bag that was stolen from a car in Lae, PNG.

Source: ANAO analysis of Defence documentation.

67 Defence's Financial Management Manual requires cards and PINs to be stored in a safe place, including ensuring that if recorded, the PIN is not located in such a way as to be associated or available on or near the card.

Appendix 6 Instances of practices in the use of the Travel Card that are difficult to reconcile with Defence policy

- Overseas travel allowances approved for a period during which the traveller returned to Australia, at Commonwealth expense, for leave.[68]
- Cash for meals and incidentals withdrawn in currencies other than the currency in which it was approved.[69]
- Cash withdrawn earlier than three working days prior to travel.[70]
- No clear documentation of actual travel dates compared with planned travel dates, which is important for ensuring that the correct allowances are paid.
- Travel budgets not signed by travellers and/or approvers.[71]
- After-travel declarations not signed by travellers.[72]
- Cash withdrawn on Travel Cards on behalf of other travellers.
- Travel delegates' approval for overseas travel costs on Overseas Visit Authority differs from the amounts calculated on the Defence Travel Budget calculator. It is not clear what the authoritative approved amounts are.

Source: Transactions, identified by the ANAO analysis, for which documentation was supplied by Defence.

68 The approval of leave as part of overseas travel is not permitted under Defence rules even when there is not apparent additional cost to the Department. In this case, leave was approved and the return flights to Australia were paid for by the Department.

69 Travel allowances should be withdrawn in the currency in which they were approved.

70 Defence's policy is that personal entitlement claims, when paid as advances, are normally paid not more than three working days before the commencement of the entitlement period.

71 Signing of the travel budget is evidence of the delegate's approval of the travel budget and the traveller's acknowledgement of understanding of the travel budget.

72 The failure of travellers to complete after-travel certification was one of the most common process failures identified by a 2008 Defence internal audit on the management of the Defence Purchasing and Travel cards.

Appendix 7 Expenditure on Defence fuel cards

Defence fuel card: type and purpose	Card managed by	Approx. no. of cards on issue[a]	2012–13	2013–14	2014–15
Vehicle / Ground *(Fuel for Defence vehicles at commercial fuel outlets)*	SG Fleet	23 262	$9 995 102	$9 092 308	$9 107 350
Aviation *(Fuel for Defence aircraft at commercial aviation fuel outlets)*	Varec	1 290	$32 528 526	$39 817 578	$24 454 287
Marine *(Fuel for Defence marine craft at commercial fuel outlets—Navy and Army)*	SG Fleet	177	*Not available. This class of fuel cards only existed with effect from 2015.*		NIL
Marine *(Local accounts established for refuelling of smaller watercraft at commercial fuel outlets. Accounts are operated via use of a vendor issued card. Accounts and cards are managed locally.)*	Defence—locally managed	Unknown	$630 211	$315 698	$48 424
Other assets *(See Note b)*	Defence	920	See Note b	See Note b	See Note b
'White' or 'On-Base' fuel cards *(See Note c)*	Defence	731	See Note c	See Note c	See Note c

Note a: The number of cards is a point-in-time figure that has fluctuated throughout the period for which expenditure is reported.

Note b: Defence informed the ANAO that the majority, if not all, of the Defence Fuel Cards Asset class cards are issued to assets which will not be refuelled at commercial premises (for example, ground support equipment, generators, tow motors, hydraulic rigs, and bomb loaders). Fuel is drawn from Defence owned bulk holdings therefore, the 'expenditure' will be the volume of fuel used multiplied by the weighted average cost of the fuel at the relevant Defence bulk fuel site. In July 2015, Defence informed the ANAO it was reviewing some of these cards to establish if they should be incorporated into the fuel card management and administration arrangements with SG Fleet.

Note c: Can be used to refuel any Defence vehicle or other asset 'on base' from fuel which has been purchased in bulk by Defence into bulk fuel tanks. As such the 'expenditure' will be consumption of fuel which has been purchased in bulk by Defence into bulk fuel tanks. Defence informed the ANAO that it intends to phase out these types of cards.

Source: Department of Defence.

Appendix 8 Additional fuel card preventative/detective controls

Defence advised the ANAO in April 2016 that the following additional preventative/detective controls were identified at meetings between Defence and SG Fleet.

From the meeting held on 29 January 2016, the primary control change implemented was via DEFGRAM 29/2016. The DEFGRAM was issued as interim policy by Commander Joint Logistics, as Head of the Defence Fuel Supply Chain, on 1 February 2016, to direct changes to the PIN arrangements for commercial ground fuel cards. The changes were implemented on 1 March 2016 and completed across all fuel card providers by 31 March 2016. At the meeting it was resolved to meet again with SG Fleet and Caltex to examine more closely potential IT solutions that could assist Defence to better manage vehicle and fuel card usage beyond the interim policy directed by Commander Joint Logistics.

A subsequent meeting was held on 23 March 2016 with SG Fleet and Caltex and several action items were identified that are being progressively actioned with SG Fleet and Caltex. Those action items are as follows:

- Caltex, as advised by SG Fleet, put in place in late February 2016 smart daily hard card limits which immediately reduced the ability to defraud Defence of high value purchases. Caltex advised that Defence could also impose smart monthly limits. Caltex has average fuel card monthly spend but need SG Fleet and Defence to look at actual asset categories to ensure asset use is not hindered by a low monthly limit.

  Action #1: SG Fleet and Caltex to liaise and recommend to Defence potential smart monthly hard limits.

  Action #2: Defence to establish protocol to inform SG Fleet if there is a large scale exercise to increase limits for a period of time if required.

- Monthly limits can be altered online by SG Fleet and Caltex at time of the transaction in the worst case. The Caltex system takes 15–20 minutes to update—same as a PIN reset request.

  Action #3: Caltex will issue an exception report to SG Fleet if the monthly card limit reaches 80%.

- The Caltex fuel card system already asks for the odometer reading and PIN number. The option was examined as to the ability of the fuel card system to have a third data check, being an Order Number. The idea was to capture the Employee ID number to further minimise the potential for fuel card misuse. While an invalid odometer reading and/or Employee ID number will not stop the transaction, the additional data field captured could be linked to SG Fleet's booking intelligence system and enable a data check against who was driving the car to who used the fuel card. The challenge is that Defence would need to cover the cost of reissuing 18 500 fuel cards to enable this information to be captured.

  Action #4: Defence to consider the value of the additional control check and advise SG Fleet. It is expected that once the data is captured at the time of the transaction, Defence can audit against PMKeys [*Defence personnel system*] data.

- Question was raised how these changes would integrate with the on-base POL system to capture the Employee ID number.

  Action #5: Defence to liaise with on-base POL system provider about the feasibility, cost and timeframe to capture the Employee ID number for on-base transactions.

- Discussion around availability of summarised fuel card exception reporting and visibility for CO level and Group and Service level to ensure improved compliance.

  Action #6: Defence to work with SG Fleet to develop summarised fuel card exception reporting to inform Defence managers of exceptions occurring, trends and close out of exceptions reported.

  Action #7: FSB to draft a DEFGRAM for CJLOG's release once the new summarised reporting is available.

- Defence sought IT options to remove the AD049 paper-based recording in favour of a more efficient electronic system. SG Fleet presented its Book intelligence system, which is a vehicle/asset booking system that is performed on line and can be tailored by Defence to suit the requirement. The system can be built around the Defence vehicle policy and Electronic Supply Chain Manual requirements. The user can book a vehicle on line and then the Defence transport manager completes the transaction and hands the keys over to the driver. The system can be altered to require key information to be collected, such as the driver's licence number and staff number.

  Action #8: Director-General Fuel Services Branch recognised in principle the potential value of the Book intelligence system. DGFS advised that he will recommend to CJLOG that a pilot be conducted and be promulgated by CJLOG. Defence is looking for suitable locations for the pilot.

Appendix 9 Glossary

CMS	Card Management System. The Defence computer system used to manage the processing of credit card transactions for both the Defence Travel Card and the Defence Purchasing Card. CMS is based on the commercial *Promaster* software system.
CFOG	Chief Finance Officer Group, Defence.
CMS Supervisor	The person appointed to perform a regular, independent review of a cardholder's transactions, usually at the end of each month.
Corporate Card Support Centre	Defence's Corporate Card Support Centre (CCSC), based in Hobart, manages the operation of Defence's Card Management System.
Defence Purchasing Card (DPC)	A credit card (Visa) provided to Defence staff to facilitate purchasing of goods and services for official purchases.
Defence Travel Card (DTC)	A credit card (Diners) provided to Defence staff to facilitate their official travel.
eTicket	A credit card (Cabcharge) in the form of a voucher allowing the holder to pay for one taxi trip.
Fastcard	A credit card (Cabcharge) used to pay taxi fares.
FMA Act	The *Financial Management and Accountability Act 1997* provided the framework for the management of public money and public property by government departments and other Commonwealth agencies until 30 June 2014, when it was succeeded by the PGPA Act.
FSB	Fuel Services Branch, Defence. This branch has responsibility within Defence for the administration of the Fuel Card.
Fuel Card	A transaction card used to purchase fuel for Defence vehicles and certain machinery (generators, lawn mowers, etc). Not strictly a credit card.
Green fleet	Defence's fleet of trucks and four-wheel drive vehicles (owned by Defence).
PGPA Act	The *Public Governance, Performance and Accountability Act 2013* establishes a coherent system of governance and accountability for public resources, with an emphasis on planning, performance and reporting. The Act applies to all Commonwealth entities and Commonwealth companies.
White fleet	Defence's fleet of commercial motor vehicles obtained under a whole-of-government contract from the SG Fleet company.