SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 38

Senator Ludwig asked the following question at the hearing on 16 February 2004:

Has the OFPC asked for extra funding to deal with complaints handling or for doing credit audits? If so, when was the request made and how much was requested?

The answer to the honourable senator's question is as follows:

Since the commencement of the private sector provisions of the Privacy Act, 21 December 2001, the OFPC has sought additional funding to address its increasing workload.

In September 2002 as part of the 2003/2004 budget process the OFPC sought approximately $1.3million pa in additional funding.

The Office has sought additional funding through the budget process for the 2004/2005 financial year.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 39

Senator Ludwig asked the following question at the hearing on 16 February 2004:

a) Is the OFPC aware of the claims in CHOICE Magazine that 34% of their readers found mistakes in their credit reports?
b) In the OFPC's experience [ie conducting Credit Information Audits and from complaints received], would this be representative of the entire population?

The answer to the honourable senator's question is as follows:

The Office is aware of the claims in the CHOICE articles that of the 50 of its subscribers who obtained a copy of their credit report, 34% found one or more mistakes in the report.

We understand that the largest credit reporting agency in Australia, Baycorp Advantage Business Information Systems Limited, hold records on 13 million individuals and one and a half million commercial entities in Australia and New Zealand.[1] The Office received 1708 enquires about credit reporting and 208 credit reporting complaints in 2002-2003. Given the extremely large number of credit records held by Baycorp the Office is wary about drawing conclusions based only on number of complaints or enquiries to this Office.

The Office has conducted over 140 audits of the credit sector since the commencement of the credit reporting provisions of the Act – Part IIIA – commenced in 1991. The audits have considered the question of accuracy of personal information in credit reports. However, the focus has been on identifying systemic practices that may lead to inaccuracies. To date the Office has not taken the approach of checking the detail of individual records with the individuals concerned.

For these reasons the Office is not in a position to say if this experience would be representative of the population as a whole.

---

[1] *Liberating Potential* Baycorp Advantage Information Package or www.baycorpadvantage.com.au

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 40

Senator Ludwig asked the following question at the hearing on 16 February 2004:

Can you provide an estimate of the number of Australians who may have a mistake in their credit report?

The answer to the honourable senator's question is as follows:

As noted in the answer to Question 39 the Office is not in a position to provide this information.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 41

Senator Ludwig asked the following question at the hearing on 16 February 2004:

How many credit information audits have been done in the last 5 years? Please provide the information in the following way:

- Name of company
- Date of audit
- Reason for the audit
- The duration of the audit
- The number and classification levels of OFPC officers that carried out the audit
- The outcomes of the audit
- The recommended follow up action by the OFPC

The answer to the honourable senator's question is as follows:

The Office has conducted 25 credit reporting audits in the last five years. Attached to this response are the summaries of the audit outcomes and/or recommendations for each of the organisations audited in order of the date the audit was commenced.

It is important to note that since the commencement of the Commissioner's powers to conduct credit information audits each subsequent Commissioner has taken the decision not to report publicly the detailed results of audits undertaken on private sector organisations. This decision was based on a general concern that making such reports public might unfairly affect the audited organisation's business position if undue publicity were given to minor or arguable infractions of relevant standards. This was especially so where there has been a preparedness to remedy the difficulties identified. Consequently, the Commissioner's Annual Reports, while providing a list of the organisations that had been subject to a credit information audit, did not link those organisations to specific findings. Rather, a de-identified summary of the findings from all the credit information audits undertaken during the reporting period was provided within each Annual Report.

The answers to many of the specific issues covered by this question are very similar for each audit and in some cases can only be provided as an estimate. For these reasons we have provided general responses to these matters. These responses are as follows:

- Reason for the audits:
    - The Office makes its decisions about audit targets using a risk management framework. This includes deciding on a broad allocation of resources between jurisdictional areas (federal agencies in relation to the Information Privacy Principles, credit reporting, tax file number recipients and inspections under the *Telecommunications Act 1997* in relation to records of disclosures to law enforcement agencies), identifying a number of possible audit targets and then applying a more detailed risk management framework to these.[1] The risk management factors are reviewed each year but generally cover matters such as:

[1] Generally speaking the Office receives about the same number of complaints in relation to credit reporting and the information privacy principles and only a small number of complaints in relation to other jurisdictional areas where the Privacy Commissioner has an audit function. The Commissioner does not have any audit powers in

- Whether it is a new agency or organisation.
- Whether there is either new legislation or a new government program being implemented.
- The sensitivity of personal information held by an agency or organisation.
- The quantity of personal information held or dealt with by an agency or organisation.
- The number of complaints or enquiries received about a particular agency or organisation.
- Any substantial media coverage about the possible mishandling of personal information by an agency or organisation.
- If new technologies are changing the way personal information is handled by an agency or organisation.
- If new procedures are changing the way personal information is handled by an agency or organisation.
- The timeframe since any previous audit.
- Any other risks reported from other sources such as other government regulators.

o In relation to the credit sector, the risk analysis may only suggest the type of organisation we might target – for example medium sized credit union – we then randomly select an organisation within this category. We note here that the Office has cancelled its audit program for the 2003-2004 financial year with the exception of those required and funded by agreements. The Office therefore plans to conduct two-three audits this financial year, as required by its Memorandums of Understanding (MOUs) with the ACT Government and with the Australian Customs Service.

o The Office has aimed to audit each of the credit reporting agencies on a regular basis.

- Duration of the audit – A typical audits involves 3-5 days field work and 2-3 weeks to complete the analysis and prepare a draft report. Finalisation of the report can take up to a further week depending on whether or not an organisation accepts the Office's recommendations.

- The number of staff involved in the audit program for the period 1 July 2000 to 30 June 2003 is as follows:

	1 July 2000 to 30 June 2001	**1 July 2001 to 30 June 2002**	**1 July 2002 to 30 June 2003**
APS 6	2	2	.75
Executive Level 1	1	1	.5
Executive Level 2	.25	.25	.2
Total	3.25	3.25	1.45

- Following are the audited companies, dates of the audits and the summaries of the audit outcomes and/or recommendations.

relation to private sector organisations with respect to the National Privacy Principles. To date the Office has conducted approximately equal numbers of Information Privacy Principle and credit reporting audits.

1. **Harvey Norman Financial Services Pty Ltd, Sydney**
   Audit opened Feb 99/ Audit closed Nov 00

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 10 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That in any amendments to current contracts, or in drafting of new contracts, where contractors may have access to credit reports, either directly or incidentally, HN Financial Services include conditions regarding the security and confidentiality of information that take into account the provisions of the Privacy Act.

Recommendation 2

That all loan application forms used by HN Financial Services which contain a Privacy Authorisation should be reviewed and, where necessary, amended to more accurately reflect the requirements of the Privacy Act and Code of Conduct. Suggested wording for the required written consents is contained in the Explanatory Notes to the Code of Conduct.

Recommendation 3

That

- assessment procedures be implemented to enable a determination on whether an application is for consumer or commercial purposes. If HN Financial Services is unable to ascertain the nature of the credit being applied for, it should ask the applicant; and

- when individual customer account records are next accessed, HN Financial Services should identify any instances where a commercial loan has been recorded as a consumer application and advise the relevant CRA of any amendments required.

Recommendation 4

That all staff with access to a CRA be reminded of the need to record the correct details from the credit application when providing information to the CRA. If an error is made, HN Financial Services should notify the CRA that the information requires amendment.

Recommendation 5

That HN Financial Services ensure that all relevant staff are made aware of the individual's right of access to their credit report pursuant to section 18H of the Privacy Act and have adequate information and facilities available to advise individuals in accordance with paragraph 2.20 of the Code of Conduct.

Recommendation 6

That HN Financial Services include in its internal procedures, guidelines for action in respect of accounts which have been listed in default with a CRA and which the individual disputes. These procedures or guidelines should be communicated to all staff.

Recommendation 7

That HN Financial Services should ensure that there are adequate procedures in place to notify the relevant CRA in all cases where an individual has paid an overdue amount that has previously been listed as overdue on the individual's CRA credit information file.

Recommendation 8

That information be provided to all staff with CRA access so that they are aware of the action they are required to take in respect of incorrect entries made by HN Financial Services, including notifying the CRA, advising any other person given a copy of the report and destroying all copies of the incorrect credit report.

Recommendation 9

That HN Financial Services review its staff training material to ensure that information contained therein accurately reflects the provisions of the Privacy Act and the Code of Conduct.

Recommendation 10

That:

- when Franchisees or HN Financial Services receive documents that contain TFN information, staff effectively mask the TFN on receipt; and

- when current credit application files are next accessed, they should be checked to see if any TFN information is present. If so, it should be deleted or masked.

2. Credit Advantage / Credit Reference Ltd
Audit opened Sep 99/ Audit closed Jul 00

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 7 recommendations for the improvement of the credit reporting agency's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

CRL should ensure that personal information contained in credit information files disclosed to law enforcement agencies meet the requirements of the Privacy Act.

CRL should also ensure that any disclosures of credit information files made to enforcement agencies are correctly recorded on an individual's credit information file, unless this is specifically unauthorized by law.

Recommendation 2

That CRL review the identifying information content of the credit information files to ensure that only information permitted by s.18E(1) is included.

Recommendation 3

That CRL review all accesses by subscribers to ensure that only those that are permitted under the Privacy Act are able to access personal information held on an individual's credit information file.

Recommendation 4

In any amendments to current contracts, or in drafting of new contracts, where contractors may have access to personal information, either directly or indirectly, CRL should include conditions regarding the security and confidentiality of information taking into account the provisions of the Privacy Act.

Recommendation 5

That CRL should review its procedural manuals to ensure that information contained therein is in accordance with the Privacy Act and the Code of Conduct.

Recommendation 6

That CRL develop and implement a regular program to review the currency of users' access rights to the Pegasus system.

Recommendation 7

That CRL ensure that there are adequate procedures in place to ensure that information recorded on credit information files meets the requirements of the Privacy Act and the Code of Conduct. CRL should consider conducting regular sampling of information recorded by subscribers to determine whether the information is accurate, up-to-date and not misleading, and to identify any systemic issues.

CRL should also ensure that its dispute resolution procedures fully comply with the requirements of the Privacy Act and the Code of Conduct.

3. Telstra Corporation Ltd, Melbourne, Sydney and Perth
Audit opened October 99/ Audit closed Dec 99

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 9 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That appropriate assessment procedures be implemented to determination whether an application is for consumer or commercial purposes. If Telstra (or its agents/representatives) are unable to ascertain the nature of the credit being applied for, it should ask the applicant.

It is also recommended that when individual customer account records are next accessed, Telstra should identify any instances where a commercial loan has been recorded as a consumer application and advise the relevant CRA of any amendments required.

Recommendation 2

Telstra should ensure that United has adequate procedures in place to ensure that, where credit is refused based wholly or partly on information derived from a credit report, the individual is notified in writing, including the name and address of the credit reporting agency from which the report was obtained.

Recommendation 3

That procedures be implemented to ensure that when staff next access a particular customer's account details they should seek determine whether incorrect information has been given to a CRA and then take prompt remedial action.

Recommendation 4

That all application forms and scripts used by Telstra and United which contain privacy terms and conditions should be reviewed and, where necessary, amended to correctly reflect the requirements of the Privacy Act and the Code of Conduct in relation to notification and consent. Suggested wording for the required written consents is contained in the Explanatory Notes to the Code of Conduct.

Recommendation 5

That Telstra and its agent either keep a hard copy of the mobile telephone application or have a system in place where it is electronically confirmed that the customer has read and signed the privacy acknowledgment and consent. It is suggest that such records for declined applications should be retained for a minimum period of 12 months.

Recommendation 6

That when contacting customers by telephone in relation to overdue accounts staff should not identify themselves as being from the NCC but rather simply state that they are from Telstra.

Recommendation 7

United should ensure that all relevant staff are made aware of the individual's right of access to a credit report in possession or control of United and have adequate information and facilities available to respond to requests from individuals.

Recommendation 8

That in any amendments to current contracts or in drafting of new contracts, where contractors may have access to credit reports, either directly or incidentally, United should include conditions regarding the security and confidentiality of information taking into account the provisions of the Privacy Act.

Recommendation 9

Computer monitors should be placed in a position where the screen details are not easily observed by unauthorised individuals.

4. Vodafone Pty Ltd, Melbourne, Sydney and Canberra
Audit opened Nov 99/ Audit closed Nov 00

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 12 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That Vodafone develop and implement procedures to ensure that the purpose of the service sought by an individual is determined when the customer applies for the service.

It is also recommended that when client records are next accessed, Vodafone should identify any instances where a commercial application has obviously been recorded as an application for consumer credit and advise the CRA of any amendments required.

Recommendation 2

That:

(a) Vodafone ensure that, at the time of or before acquiring personal information, it informs the customer that information may be disclosed to a credit reporting agency and where relevant seek any necessary consents.

(b) All application forms used by Vodafone that contain privacy terms and conditions should be reviewed and, where necessary, amended to correctly reflect the requirements of the Privacy Act and the Code of Conduct. Suggested wording for the required written consents are contained in the Explanatory Notes included in the Code of Conduct.

Recommendation 3

Dealer application forms that contain privacy terms and conditions should be reviewed and, where necessary, amended to correctly reflect the requirements of the Privacy Act and the Code of Conduct.

Recommendation 4

That Vodafone ensures that only outstanding amounts that are 60 days overdue and for which steps have been taken to recover the amount outstanding are listed on individuals' credit information files.

Recommendation 5

That Vodafone only access and use credit reports for those purposes permitted under the Privacy Act.

Recommendation 6

In any amendments to current contracts, or in drafting of new contracts, where contractors may have access to personal information, either directly or incidentally, Vodafone include conditions regarding the security and confidentiality of information taking into account the provisions of the Privacy Act.

Recommendation 7

That Vodafone should compare the accesses recorded on the CRA invoice bill to the number of applications received and processed in relation to a specific period. Large unexpected variances should be fully investigated to ensure that explanations are obtained and reported to senior management where appropriate.

Recommendation 8

Vodafone should implement policies and procedures to ensure that credit worthiness information and credit reports held by its dealers on its behalf are adequately protected.

Recommendation 9

It is recommended that procedural instructions include guidance on all relevant matters required by the Privacy Act and the Code of Conduct. Since many of the issues identified in the audit may be rectified by training and education of the relevant personnel, it is recommended that Vodafone consider providing training for all staff that have exposure to credit information and credit reports.

Recommendation 10

If a customer provides a document containing TFN information and has not removed the TFN, then Vodafone, its dealers and/or agents should effectively mask the TFN on receipt of the document. It is also recommended that when customer files are next accessed, they should be checked to see if any TFN information is present. If so, it should be deleted or masked.

Recommendation 11

Vodafone should revise its procedures to ensure that the conditions set out in the Telecommunications Act are met before it discloses information about its customers to law enforcement agencies.

Recommendation 12

Vodafone should ensure that any disclosures of personal information are correctly recorded as required by s.306(5) of the Telecommunications Act.

5. Bank of Western Australia Ltd, Perth
Audit opened Dec 99/ Audit closed Sep 00

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 14 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That, where an applicant has been declined credit based wholly or partly on information in a credit report from a CRA, BankWest should ensure that the individual is informed in writing of the reason for declining the application.

Recommendation 2

Procedures should be implemented to ensure that staff are able to identify duplicate listings and then promptly inform the CRA of any inaccurate listing.

Recommendation 3

BankWest should develop and implement procedures to identify the purpose of credit applied for, before disclosing to and or obtaining information from a CRA.

Recommendation 4

It is recommended that BankWest should routinely compare the accesses recorded on the CRA invoice to the number of loan applications processed for a specific period. Large unexpected variances should be fully investigated and reported to senior management where appropriate.

Recommendation 5

BankWest should ensure that all relevant staff are made aware of the individual's right of access to credit reports pursuant to s.18H of the Privacy Act and paragraph 2.20 of the Code of Conduct.

Recommendation 6

BankWest should only obtain a credit report or disclose credit information to a CRA in relation to a cheque account that includes a credit facility and where the individual has specifically applied for credit and has been appropriately notified in accordance with s.18E(8)(c) of the Privacy Act.

Furthermore, BankWest should ensure that it meets all the requirements of the Privacy Act and Code of Conduct before listing individuals as having committed a serious credit infringement.

BankWest should also review all listings of overdrawn cheque accounts which have been reported to a CRA and where relevant inform the CRA of these incorrect entries.

Recommendation 7

That BankWest ensure that only amounts that are more than 60 days overdue and for which recovery steps have been taken are listed on an individual's credit information file.

Recommendation 8

That information be provided to all staff with CRA access so that they are aware of the action they are required to take in respect of incorrect entries made by BankWest, i.e. to notify the CRA, to advise other recipients of the incorrect credit reports, and to destroy the incorrect credit reports on hand.

Recommendation 9

BankWest should implement policies and procedures to ensure that credit worthiness information and credit reports held by its agents and representatives on its behalf are adequately protected.

Recommendation 10

That, after the approval of the customer's loan, BankWest not disclose to agents customer and ex-customer account details that has a bearing on the individual's credit worthiness, credit standing, credit history or credit capacity.

Recommendation 11

BankWest should review all physical storage facilities to ensure that they are adequately secured outside normal business hours. Doors that have keypad combination door locks should have the combinations changed periodically.

Recommendation 12

In any amendments to current contracts, or in drafting of new contracts, where agents, brokers or contractors may have access to personal information, either directly or incidentally, BankWest should include conditions regarding the security and confidentiality of information taking into account the provisions of the Privacy Act.

Recommendation 13

BankWest should provide training to all staff that have access to or use credit information and credit reports. In addition, procedural instructions that are under development should be finalised and issued to staff as a matter of urgency.

Recommendation 14

If the TFN has not been removed by the client or by the relevant credit provider, it is recommended that BankWest effectively mask the TFN on receipt of the document. It is also recommended that when current consumer credit files are next accessed, they should be checked to see if any TFN information is present. If so, it should be adequately masked or deleted.

6. Credit Corp Group, Sydney
Audit opened Dec 99/ Audit closed Oct 00

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 13 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That –

(a) when Credit Corp next purchases a loan portfolio that it negotiates with the vendor to ensure that it is provided with adequate information to distinguish between debtors with consumer or commercial credit respectively; and

if in the normal course of business, Credit Corp becomes aware that one of its debtors is a debtor in relation to commercial credit, that it observes the limitations the Privacy Act places on the use of credit reports in relation to commercial credit and on the information that may be disclosed to a CRA.

Recommendation 2

Credit Corp should ensure that debtors have been appropriately notified that a payment default or serious credit infringement may be listed with a credit reference agency prior to listing. Credit Corp should also obtain any required consents in writing from the debtor if that individual's consumer credit information is used for the purpose of collecting overdue payments in relation to commercial credit.

Recommendation 3

That Credit Corp:

- ensure that it does not relist overdue payments and serious credit infringements on an individual's credit information file which have previously been listed by the original credit provider;
- implement procedures to ensure that staff are able to identify a situation of duplicate access and then promptly inform the credit reporting agency of the duplicate access. A proforma is available from the CRA for this purpose; and
- ensure that steps are taken to inform the CRA of the assignment of debts that have been previously reported to the CRA as being in default by the original credit provider.

Recommendation 4

That Credit Corp not automatically on assignment list serious credit infringements ('clearouts') with a CRA if the assignee has made no recent attempts to recover the debt. Credit Corp could consider listing as a current credit provider with the CRA and as such would be able to receive updated address information under s.18K(1)(f).

Recommendation 5

That all staff with CRA access be made aware of the action they are required to take in respect of incorrect entries made by Credit Corp on an individual's credit information file including notifying the CRA and destroying the incorrect credit report.

Recommendation 6

In any amendments to current contracts, or in drafting new contracts, where contractors may have access to personal information, either directly or incidentally, Credit Corp should include provisions to ensure the security and confidentiality of personal information taking into account the provisions of the Privacy Act.

Recommendation 7

Credit Corp should take appropriate measures to ensure that staff do not re-use a credit report obtained in relation to an existing debt in relation to a second debt without ensuring that the credit report is accurate, up to date and complete. [*See Credit Corp's response to this recommendation and the auditors' comments in the body of the report.*]

Recommendation 8

Credit Corp should take appropriate steps to ensure that when it lists a payment default with a credit reference agency in relation to a joint debt, that the relationship between the borrowers is correctly listed.

Recommendation 9

That Credit Corp takes appropriate measures to ensure that files containing credit reports and reports are stored in locked filing cabinets or a compactus outside normal working hours.

Recommendation 10

Credit Corp should compare the accesses recorded on the CRA invoice to the number of accesses made for debt collection purposes. At present it is not possible to gain assurance that unauthorised or inappropriate accesses have not occurred. Large unexplained differences should be fully investigated to ensure that explanations are obtained and reported to senior management. Senior management should take appropriate action when unauthorised or inappropriate accesses have occurred.

Recommendation 11

That Credit Corp ensure that all staff dealing with individuals who have had consumer credit defaults reported to the CRA are aware that they are obliged to notify the CRA if the individual contends that he or she is not overdue in relation to the debt in question.

Recommendation 12

That Credit Corp should raise the awareness of staff regarding the contents of its security policy.

Recommendation 13

Given that many of the issues identified in the audit may be rectified by training and education of the relevant personnel, consideration should be given to providing staff training for all staff that have exposure to credit information and credit reports. Also procedural instructions that are under development should be finalised and issued to staff as a matter of urgency.

7. United Energy Ltd, Melbourne
Audit opened Feb 00/ Audit closed Jan 01

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 7 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

United and Ikon should ensure that Utili-Mode only discloses customer credit worthiness information in those circumstances permitted under the Privacy Act.

Recommendation 2

That Ikon and Utili-Mode;

- review the security of electronic transmission of information; and
- ensure that information given to mercantile agents does not include any information derived from a credit report.

Recommendation 3

That Ikon ensure that Utili-Mode introduces monitoring controls to ensure that all accesses made to the CRA database are made for purposes permitted under Part IIIA of the Privacy Act.

Recommendation 4

United and Ikon should ensure that all Utili-Mode staff are aware of their obligations to notify the relevant CRA where an individual is not overdue or contends that he or she is not overdue in making a payment that has been listed on the individual's consumer credit information file.

Recommendation 5

That United and Ikon ensure that Utili-Mode reports a customer as having committed a serious credit infringement only when it can demonstrate that the individual has clearly left their last recorded residential and mailing addresses.

Recommendation 6

That Ikon review the information Utili-Mode provides to the CRA and the manner of provision of that information to ensure that all customer information is accurate, up-to-date, complete and not misleading.

Recommendation 7

That United and Ikon

- ensure that Utili-Mode provide adequate training to staff whose responsibilities involve handling of credit worthiness information; and
- ensure that Utili-Mode reviews and updates training material in line with the requirements of the Privacy Act.

8. AAPT Sydney and Gold Coast
Audit opened Apr 00/ Audit closed Dec 01

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 9 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That AAPT:

- require all staff faxing application forms to send the terms and conditions, including the Privacy Act notification, as well as the front page; and
- review its application forms to ensure that each contains the notification required by s.18E(8)(c) of the Privacy Act

Recommendation 2

That AAPT ensure that all CRA enquiries are made using AAPT logon IDs.

Recommendation 3

That AAPT ensure that, where a debt is paid in full by the customer and that debt had previously been listed as a default with a CRA, it informs the CRA that the individual has ceased to be overdue.

That AAPT ensure that, where a customer *contends* that he or she does not owe the alleged outstanding amount, and that amount has previously been listed as a default with a CRA, it informs the CRA that the individual contends that he or she is not overdue.

Recommendation 4

That AAPT:

- limit CRA access to relevant staff;
- no longer allow the sharing of CRA logon IDs among employees; and
- ensure no staff member has more than one logon ID.

Recommendation 5

That AAPT develop and implement procedures to ensure that when a customer applies for credit, he or she is asked to identify whether the credit is sought for consumer or commercial purposes and that the codes used to enquire about the application with the CRA accurately reflect the purpose of the application.

That when client records are next accessed, AAPT identifies instances where an application for consumer credit has been recorded on the individual's commercial file and advise the CRA of any amendments required.

Recommendation 6

That AAPT institute procedures to ensure that staff identify the correct customer file held by the CRA and that, where a duplicate access occurs, staff are able to identify that duplication and inform the credit reporting agency.

Recommendation 7

That AAPT ensure that staff with access to the CRA database are required to change passwords on a regular basis and that those staff are aware of the requirement to protect those passwords from dissemination to others.

Recommendation 8

That AAPT compare the accesses recorded on the CRA invoice to the number of applications processed in the relevant period. Unexpected variations should be investigated and reported to senior management where appropriate.

Recommendation 9

That, where a customer supplies documentation which includes a Tax File Number, AAPT staff should remove the number and dispose of it securely or alternatively should mask the number before taking a copy of the document supplied.

9. Cellular One Communications Ltd, Sydney and Gold Coast
Audit opened Apr 00/ Audit closed Dec 01

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 10 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That Cellular One implement procedures to ensure that, where a payment default is listed with a credit reporting agency and the customer disputes that he or she is overdue in making the a payment, the relevant credit reporting agency is informed.

Recommendation 2

That, when Cellular One enters into an agreement with a dealer, the contract should specify what information is regarded by Cellular One to be of a confidential nature. That definition should include a reference to the requirements of the Privacy Act in relation to credit worthiness information.

Recommendation 3

That, when the Application for Personal Digital Service form is next reprinted, Cellular One review the privacy terms and conditions and, where necessary, amend them to accurately reflect the requirements of the Privacy Act and the Code of Conduct.

Recommendation 4

That, where credit is refused based wholly or partly on information derived from a credit report, Cellular One ensure that the individual is notified in writing and that the notification include the name and address of the relevant CRA.

Recommendation 5

That Cellular One develop and implement procedures to ensure that when a customer applies for credit, he or she is asked to identify whether the credit is sought for consumer or commercial purposes and that the codes used to enquire about the application with the CRA accurately reflect the purpose of the application.

That when client records are next accessed, Cellular One identifies instances where an application for commercial credit has been recorded on the individual's consumer file and advise the CRA of any amendments required.

Recommendation 6

That Cellular One institute procedures to ensure that staff identify the correct customer file held by the CRA and that, where a duplicate access occurs, staff are able to identify that duplication and inform the credit reporting agency.

Recommendation 7

That Cellular One ensure that staff with access to the CRA database are required to change passwords on a regular basis and that those staff are aware of the requirement to protect those passwords from dissemination to others.

Recommendation 8

That Cellular One compare the accesses recorded on the CRA invoice to the number of applications processed in the relevant period. Unexpected variations should be investigated and reported to senior management where appropriate.

Recommendation 9

That, where a customer supplies documentation which includes a Tax File Number, Cellular One staff should remove the number and dispose of it securely or alternatively should mask the number before taking a copy of the document supplied.

Recommendation 10

That Cellular One review its procedures to ensure that it does not disclose information to an enforcement agency unless the conditions of s.282 of the Telecommunications Act are met.

10. Tasmanian Collection Service, Tasmania
Audit opened Oct 00/ Audit closed Dec 01

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 15 recommendations for the improvement of the credit reporting agency's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

TCS must not charge individuals who request a copy of their Credit Information File a fee in circumstances where this is not permitted under the Privacy Act and the Code of Conduct.

Recommendation 2

TCS should implement changes to its recording systems to distinguish between enquiries and applications for credit.

Recommendation 3

TCS should review the telephone credit enquiry access controls including lengthening the credit provider access code and periodically changing this code.

Recommendation 4

Where TCS receives a request for consumer credit information from a law enforcement agency, it should ensure that the agency specify the legislative provisions that require or authorise the disclosure.

Where TCS receives a request for consumer credit information from a commercial credit provider, it should ensure that the commercial credit provider has:

- given notification to the customer under section 18E(8)(c) of the Act that information may be provided to a credit reporting agency; and
- obtained the relevant written permissions from the customer, under section 18K(1)(b) of the Act, to access that information.

Recommendation 5

Where a credit provider seeks access to an individual's Consumer Credit Information file to assess a commercial credit application, TCS staff should verify that the credit provider has the written permission of the individual.

Recommendation 6

TCS should take proactive steps to ensure that staff have a clear understanding of the distinction between consumer and commercial credit.

TCS should make changes to TCS Online to ensure that credit providers are prompted to determine whether the access relates to an application for consumer or commercial credit.

Recommendation 7

TCS must ensure that, if an individual disputes a default listing recorded on his or her Consumer Credit Information file, the file is updated to reflect the fact that the listing is disputed.

Recommendation 8

TCS should ensure that occupational information is not included on an individual's Credit Information file. TCS must ensure that only permitted information is included on an individual's Credit Information file.

Recommendation 9

TCS should take steps to ensure that collections staff do not have access to the credit reporting database, credit reports or personal information derived from a report.

Recommendation 10

That, at the next reprint of the Client Agreement, TCS revise it to more accurately reflect the requirements of the Privacy Act and the Code of Conduct.

Recommendation 11

TCS should cease including information about unpaid real property rent on individuals' Consumer Credit Information files.

TCS should undertake a review of all credit information files to determine if they include unpaid real property rental information and, if so, take action as soon as possible to have this information deleted.

Recommendation 12

That TCS modify the existing staff Confidentiality Agreement to specifically refer to unauthorised access to and modification of the credit reporting database.

Recommendation 13

TCS should implement adequate procedures to ensure that credit reports and other credit worthiness information are disposed of in a secure manner.

TCS should ensure that all staff are aware of the need to dispose of this information securely and that steps are taken to prevent staff from disposing of this information in the general waste bins.

Recommendation 14

TCS should enter into contracts that contain a confidentiality clause with all service providers who have access to credit information.

Recommendation 15

Given that many of the issues identified in the audit may be rectified by training and education of the relevant personnel, TCS should provide training to staff who handle credit information and credit reports on the requirements of the Privacy Act and the Code of Conduct.

11. ANZ Banking Group, Melbourne
Audit opened Nov 00/ Audit closed Feb 01

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 15 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That, where a credit applicant has been declined credit based wholly or partly on information in a CRA credit report, ANZ Bank should ensure that the individual is informed in writing of the reason for declining the application.

Recommendation 2

ANZ Bank should ensure that access to the CRA database is granted only to staff that require it to perform their duties.

Recommendation 3

That ANZ Bank ensure that all relevant staff are made aware of the individual's right of access to their credit report pursuant to section 18H of the Privacy Act and that it has adequate information and facilities available to advise individuals in accordance with paragraph 2.20 of the Code of Conduct.

Recommendation 4

ANZ Bank should take adequate steps to ensure that duplicate entries are not listed on an individual's credit information file. Where inaccurate or misleading information is provided to a CRA, ANZ Bank should also take remedial action to inform the CRA.

Recommendation 5

ANZ Bank should develop and implement procedures to identify the purpose loans applied for before disclosing information to a CRA.

It is also recommended that, when loan files are next accessed, ANZ Bank should review them to identify any cases where a commercial loan application has been recorded as a consumer application and advise the CRA of any amendments required.

Recommendation 6

ANZ Bank should include in its internal procedures, guidelines for action in respect of accounts which have been listed in default with a CRA and which the individual disputes. These procedures or guidelines should be communicated to all staff.

Recommendation 7

ANZ Bank should ensure that, before listing an overdue payment against a guarantor's consumer credit information file, the guarantor has been advised in writing that the borrower is overdue by more than 60 days.

Recommendation 8

ANZ Bank should ensure that when providing personal information to a CRA it accurately reports their status as co-borrowers or joint borrowers.

Recommendation 9

ANZ Bank should ensure that where an individual applies for credit and this information is disclosed to a CRA, the amount reported is included where it is known and that this information is accurate and up to date.

Recommendation 10

It is recommended that ANZ Bank should compare the accesses recorded on the CRA invoice bill to the number of loan applications processed in relation to a specific period. Large unexpected variances should be fully investigated to ensure that explanations are obtained and reported to senior management where appropriate.

ANZ Bank should also limit access to the CRA database to those staff that require it to perform their duties

Recommendation 11

The auditors suggest that ANZ Bank review its relationship with mortgage insurance staff to ensure that the disclosure of credit worthiness information complies with the requirements of the Privacy Act and that credit worthiness information held by ANZ Bank is protected against unauthorised access, use, modification and against other misuse.

Recommendation 12

That, after the approval of the customer's loan, ANZ Bank not disclose to agents customer account details that have a bearing on an individual's credit worthiness, credit standing, credit history or credit capacity.

NB. As ANZ has since provided the relevant documentation that indicates that the customer's consent is obtained in relation to this type of disclosure, this finding is no longer applicable.

Recommendation 13

That - in any amendments to current contracts, or in drafting new contracts, where contractors may have access to personal information, either directly or incidentally - ANZ include conditions regarding the security and confidentiality of information taking into account the provisions of the Privacy Act.

Recommendation 14

It is recommended that ANZ Bank institute a process whereby staff are regularly reminded of their obligations under the Privacy Act and the Code of Conduct.

Recommendation 15

If the TFN has not been removed previously, it is recommended that ANZ Bank effectively mask the TFN on receipt of the document. It is also recommended that when current loan files are next accessed, they should be checked to see if any TFN information is present. If so, it should be adequately masked or deleted.

12. Receivables Management Group, Melbourne,
Audit opened Jan 01/ Audit closed Nov 01

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 11 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That:

(a) when RMG next purchases a loan portfolio, it negotiate with the vendor to ensure that it is provided with enough information to distinguish between debtors with consumer or commercial credit respectively; and

(b) if RMG discovers that in relation to existing accounts it has improperly reported commercial credit information as consumer credit information, it notify the credit reporting agency.

Recommendation 2

Before listing, RMG should check that debtors have been notified that a payment default or serious credit infringement may be listed with a credit reporting agency.

RMG should also make sure it has consent in writing from the debtor if his or her consumer credit information is to be used to collect overdue payments in relation to commercial credit.

Recommendation 3

That RMG not automatically list serious credit infringements ('clearouts') with a CRA if the assignee has not attempted to contact the individual for a period of years. (RMG could consider listing as a current credit provider with the CRA, where it has not done so, and as such would be able to receive updated address information under s.18K(1)(f).)

That staff be trained accordingly.

Recommendation 4

That RMG:

- cease disclosing creditworthiness information of individuals to ANZ Bank;
- contact the credit reporting agency directly to update default entries; and
- consider listing itself as a current credit provider with the CRA.

Recommendation 5

That RMG:

- should refrain from accessing creditworthiness information (including address updates) addressed to Ford Credit from the terminal which contains CAL's electronic message mailbox. (It is permissible under ss. 18N(1)(c) and (ca) of the Act for Ford Credit, as the credit provider, to directly access such updated information and then pass it to RMG); and

- ensure that only staff in the Acquisitions Section have access to the terminal used to access the CRA.

Recommendation 6

That - in any amendments to current contracts, or in drafting new contracts, where contractors or staff may have access to personal information, either directly or incidentally - RMG include conditions regarding the security and confidentiality of information taking into account the provisions of the Privacy Act.

Recommendation 7

That RMG:

- install password protected screen savers on terminals used to access databases containing creditworthiness information;

- preclude staff performing debt recovery work for third parties from accessing RMG databases containing creditworthiness information;

- preclude staff performing debt recovery work for third parties from accessing creditworthiness information from the terminal which contains CAL's electronic message mailbox; and

- ensure that only staff in the Acquisitions Section have access to RMG databases containing creditworthiness information and to the terminal used to access CAL.

Recommendation 8

It is recommended that RMG should compare the accesses recorded on the CRA invoice bill to the number of loan applications processed in relation to a specific period. Large variances should be fully investigated to ensure that explanations are obtained and reported to senior management where appropriate.

RMG should also limit access to the CRA database to those staff in the Acquisitions Section that require it.

Recommendation 9

That RMG:

- takes appropriate measures to ensure that files containing credit reports and reports are stored in locked filing cabinets or a secured compactus or store room;

- keeps creditworthiness information secure and physically separate from records belonging to other divisions of the organisation performing non-credit provider functions (such as debt collection for third parties);

- provides secure waste bins or shredders for staff in the Acquisitions Section for the disposal of creditworthiness information; and

- takes steps to ensure that, if password access codes to credit reports held by Credit Advantage Limited are recorded in an exercise book, only the manager of staff performing credit provider functions (Acquisitions Section) should have access to it.

Recommendation 10

RMG should provide appropriate training to all staff who are exposed to credit information and credit reports. In addition, the procedural instructions that are now under development should be finalised and issued to staff as a matter of priority.

Recommendation 11

That RMG put in place a dispute settling procedure to deal with complaints in relation to credit reporting and disseminate its contents to relevant staff.

13. Debt Purchase Australia, Melbourne
Audit opened Mar 01/ Audit closed Dec 01

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 8 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

When entering into contracts to purchase debt ledgers, DPA should establish whether the debt for sale relates to consumer or commercial credit so as to ensure any entries made by DPA on an individual's credit report are accurate.

Recommendation 2

DPA should ensure that files containing credit worthiness information are stored securely. Measures warranting consideration include: lockable storage cabinets, storing files separately from the mercantile agent's files and reinforcing to staff the need to for good security.

DPA should ensure that correspondence sent to or received by DPA is not opened or actioned by the staff of Repcol or Austwide Investigations.

DPA should have its own facsimile machine and number for the sending and receipt of correspondence.

Recommendation 3

When a CRA has been notified that a debtor is overdue in relation to a payment, and the debtor *contends* that they are not overdue in making the payment, DPA must notify the relevant CRA of the dispute.

Recommendation 4

DPA should allow debtors to complain directly to DPA about credit reporting matters for which it is responsible. A particular officer should be nominated as the first point of contact.

Recommendation 5

When DPA checks CRA records in relation to fuzzy matches and accesses a credit information file that turns out not to be that of the DPA client, DPA must advise the CRA to remove the entry.

Recommendation 6

That DPA cease the practice of providing information about any subsequent files listed with the CRA to a mercantile agent.

Recommendation 7

That DPA discuss the issue of service provider access with the building owners and establish that the contractors are bound by contracts that include conditions regarding the security and confidentiality of information sufficient to meet the requirements of the Privacy Act.

That DPA revise its procedures to ensure that information derived from a credit report (other than that permitted by s.18N(1)(c)(ii)) is not available to the mercantile agent and is securely disposed of.

Recommendation 8

That in training current and future staff, DPA ensure the distinction is made between the accepted industry meaning of 'skip' and the meaning of serious credit infringement as defined under the Privacy act.

14. Westpac Banking Corporation, Sydney and Adelaide
Audit opened Apr 01/ Audit closed Jan 02

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 4 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That Westpac review its storage and security arrangements for credit worthiness information to ensure that information is not disclosed in breach of s.18N of the Privacy Act. Measures warranting consideration include: lockable storage cabinets, avoiding keeping hard copies of credit reports on customer files, and reinforcing to staff the need for good security.

That Westpac ensure credit reports and files containing credit worthiness information are stored securely, particularly those files that are used outside the bank branches, for example, by mobile lending officers.

Westpac should institute procedures to prevent credit worthiness information remaining unattended within the office.

Recommendation 2

That Westpac ensure that all relevant staff are made aware of the individual's right of access to their credit report pursuant to section 18H of the Privacy Act and that it has adequate information and facilities available to advise individuals in accordance with paragraph 2.20 of the Code of Conduct.

Recommendation 3

That Westpac ensure that staff and supervisors are aware of the IT security policy and how to access it and also ensure that access to the CRA and other databases is granted only to staff who require it to perform their duties.

Recommendation 4

That - in any amendments to current contracts, or in drafting new contracts, where contractors may have access to personal information, either directly or incidentally - Westpac include conditions regarding the security and confidentiality of information taking into account the provisions of the Privacy Act.

15. Australian Guarantee Corporations, Sydney and Brisbane
Audit opened Feb 02/ Audit closed Sep 02

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 9 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That:

- when AGC process applications for credit it ensure that it is provided with enough information to distinguish between applications for consumer or commercial credit; and

- if AGC discovers that in relation to existing accounts it has improperly reported commercial credit information as consumer credit information, it notify the credit reporting agency.

Recommendation 2

AGC must ensure before it uses a credit report from a CRA in relation to an application for commercial credit that the individual's written consent has been obtained.

Recommendation 3

That AGC not automatically list 'clear-outs' with a CRA where the debtor has not made a payment to AGC. In such circumstances, AGC is only permitted to report the amount as overdue and not as 'clear-out'.

Recommendation 4

AGC must take appropriate action to ensure that it:

- furnishes a notice to an individual under s.18E(8)(c) of the Act; and

- obtain any consents required under s.18K(1)(b) of the Act.

Recommendation 5

It is recommended that AGC periodically compare the accesses recorded on the CRA invoice to the number of loan applications processed in the relevant period. Large variances should be investigated to ensure that explanations are obtained. Discrepancies should be reported to senior management where appropriate.

Recommendation 6

AGC should ensure that staff are made aware that, if a second credit report is obtained from a credit reporting agency in relation to the one credit application, steps are taken to remove the duplicate entry from the individual's credit information file.

Recommendation 7

That all staff with access to a CRA be reminded of the need to record the correct details from the credit application when providing information to the CRA. If an error is made, AGC should notify the CRA that the information requires amendment.

Recommendation 8

AGC should cease the practice of obtaining more than one credit report from the CRA in relation to the same credit application. AGC may like to contact Credit Advantage Limited to determine what other methods may be available to it to obtain this information.

Recommendation 9

If the TFN has not been removed by the client, it is recommended that AGC effectively mask or delete the TFN on receipt of the document. It is also recommended that when current consumer credit files are next accessed, they should be checked to see if any TFN information is present. If so, it should be adequately masked or deleted.

16. Commonwealth Bank of Australia, Melbourne and Sydney
Audit opened Nov 01/ Audit closed Jun 02

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 18 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

The Bank should ensure that all parties to a credit application where a credit check may be required are notified that their information may be disclosed to a credit reporting agency. The Bank would not be meeting its obligations under s.18E(8)(c) by relying on a credit applicant who has been issued with this notice to notify other applicants.

Recommendation 2

At the time each application is made, the Bank should identify what the purpose of the application is, i.e. to seek either consumer or commercial credit. The outcome of this assessment will affect what information the bank is able to obtain from, and provided to, a credit reporting agency and what consent or notification the Bank is required to obtain from the customer.

If the Bank becomes aware that it has provided inaccurate information to a credit reporting agency, it is legally obliged to immediately advise the credit reporting agency of the inaccuracy.

Recommendation 3

That the Bank review the procedures in place in Personal Loans (Melbourne) to ensure that only permitted and accurate information is included in an individual's credit information file and steps are taken to advise the credit reporting agency of inaccuracies or the existence of prohibited information.

Recommendation 4

The Bank should implement procedures and or inform staff that loan applications for the purposes of purchasing shares are not applications for consumer credit in terms of the Privacy Act.

Recommendation 5

The Bank must ensure that the individual's written consent has been obtained before it uses a credit report from a CRA in relation to an application for commercial credit.

Recommendation 6

The Bank must take steps to ensure that it does not use any credit report obtained from a credit reporting agency except for a purpose set out in s.18L(1) of the Act. It should be noted that a

credit provider that intentionally contravenes s.18L(1) is guilty of an offence punishable by a fine of up to $150,000.

Recommendation 7

That CRA credit reports retained by the Bank be marked to indicate that they are obsolete and they should not be re-used unless reasonable steps are taken to ensure that they are accurate, up to date and complete. Consideration should also be given to destruction of obsolete reports if the Bank feels that the information they contain does not warrant storage.

Recommendation 8

That the Bank ensures that co-applicants in joint applications are reported to CAL as such. That the Bank advise staff that where the amount of credit is known in relation to a credit application, this should be recorded on the individual's credit information file.

Recommendation 9

That the Bank ensure that staff made aware of their obligations to notify the credit reporting agency in circumstances where they include incorrect information in an individual's credit information file.

Recommendation 10

That the Bank implement procedures to ensure that, if a credit application has been declined partly or wholly on the basis of an adverse credit report, the applicant is always notified in writing.

Recommendation 11

That the Bank immediately cease the practice of combining all debts owed by an individual and reporting a single overdue amount on the individual's credit information file. In instances where the Bank is aware that it has combined debts as a single overdue payment which has been reported to a credit reporting agency, it should advise the credit reporting agency of this inaccurate information.

Recommendation 12

That the Bank put in place systems and controls to ensure that it notifies the relevant CRA when an individual contends that he or she is not overdue in making a payment.

Recommendation 13

That the Bank introduce adequate security controls over staff access to the CAL database so that only staff whose duties require it have access to the database.

Recommendation 14

That the Bank ensure that all relevant staff are made aware of the individual's right of access to the credit information pursuant to Section 18H of the Privacy Act and have adequate information and facilities available to respond to the requests in accordance with paragraph 2.20 of the Code of Conduct.

Recommendation 15

It is recommended that the Bank periodically compare the accesses recorded on the CRA invoice to the number of loan applications processed for a specific period. Unexpected variances should be fully investigated and reported to senior management where appropriate.

Recommendation 16

That the Bank reviews its storage and security arrangements for the disposal of credit worthiness information to ensure that information is not disclosed in breach of s.18N of the Privacy Act.

Recommendation 17

That - in any amendments to current contracts, or in drafting new contracts, where contractors or staff may have access to personal information, either directly or incidentally – the Bank include conditions regarding the security and confidentiality of information taking into account the provisions of the Privacy Act.

Recommendation 18

The Bank should provide appropriate training to all staff who are exposed to credit information and credit reports. In addition, the procedural instructions that are now under development should be finalised and issued to staff as a matter of priority.

17. Debt Default Register
Audit opened Dec 01/ Audit closed Sep 02

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 3 recommendations for the improvement of the credit reporting agency's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That procedures are developed to ensure that the DDR database only contains consumer credit information.

Recommendation 2

That procedures are developed to ensure that accesses by credit providers to the DDR database are recorded against the individual's credit information file.

Recommendation 3

That DDR develop consistent procedures for updating credit information files relating to accounts that are under dispute.

18. Island State Credit Union, Tasmania
Audit opened Feb 02/ Audit closed Sep 02

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 7 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That ISCU develop and implement procedures to identify the purpose of credit applied for (i.e. consumer or commercial), before disclosing information to, or obtaining information from, a credit reporting agency.

Recommendation 2

That ISCU review the privacy notice in its online application form and amend it to reflect the notification requirements under the Privacy Act.

Recommendation 3

ISCU should ensure that it changes the relevant form so that the consent in writing of the prospective guarantor is obtained before it accesses his or her consumer credit file to assess an application for commercial credit.

Recommendation 4

ISCU should ensure that access to the CARS database is granted only to staff that require it to perform their duties.

Recommendation 5

That ISCU should notify the credit reporting agency of duplicate accesses and other errors as soon as practicable.

That procedures should be implemented to ensure that ISCU does not make unauthorised duplicate accesses to consumer credit reports.

Recommendation 6

That ISCU ensure that all relevant staff are made aware of the individual's right of access to the credit information pursuant to section 18H of the Privacy Act and have adequate information and facilities available to respond to the requests in accordance with paragraph 2.20 of the Code of Conduct.

(

Recommendation 7

That - in any amendments to current contracts, or in drafting new contracts, where contractors may have access to personal information, either directly or incidentally - ISCU include conditions regarding the security and confidentiality of information that take into account the provisions of the Privacy Act..

19. The Australian Gas Light Company
Audit opened Feb 02/ Audit closed Sep 02

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 15 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That AGL and its franchisees develop and implement procedures to identify the purpose of credit applied for (i.e. whether it is for consumer or commercial purposes), before disclosing information to, or obtaining information from, a credit reporting agency.

Recommendation 2

That AGL review the application forms used by its franchisees that contain privacy terms and conditions, and, where necessary, amend them to meet the notification requirements in the Privacy Act.

Recommendation 3

That a nominated person, other than in the Collections Section, should compare the accesses recorded on the Baycorp invoice bill to the number of accesses made to Baycorp in relation to a specific period. Large unexpected variances should be fully investigated to ensure that explanations are obtained and reported to senior management where appropriate.

Recommendation 4

AGL should notify Baycorp Advantage Ltd of these duplicate accesses and other errors as soon as practicable so that Baycorp can corrects its records.

Recommendation 5

That - in any amendments to current contracts, or in drafting new contracts, where contractors may have access to personal information, either directly or incidentally - AGL include conditions regarding the security and confidentiality of information taking into account the provisions of the Privacy Act.

Recommendation 6

That AGL communicates to staff the circumstances under which old credit reports may be legitimately used.

Recommendation 7

That procedures should be implemented to ensure that AGL does not make duplicate accesses to consumer credit reports.

Recommendation 8

That procedures be implemented to ensure that staff are able to identify a situation of duplicate access and then promptly inform the CRA.

That the file amendment form (issued as a standard form) be used for this purpose, completed by the staff member who has made the access and sent directly to the CRA.

Recommendation 9

That AGL ensure that terminals with access to credit information at Baycorp are protected by adequate security safeguards including password protected screen savers and regularly review staff access privileges to credit information with Baycorp.

Recommendation 10

That a periodic review of access rights be undertaken to assess whether access to customers' billing history is necessary for staff of AGL and its agents and franchisees to perform their respective roles.

Recommendation 11

AGL should ensure that customer credit worthiness information is only disclosed under s.18N(1)(g) in circumstances where it can be sure that the disclosure is required or authorised by or under law. Such a request should be made in writing stating the appropriate legislation and signed by an authorising officer of the appropriate level.

AGL should establish a register of contact officers from within the police service and government departments including telephone numbers and a copy of their signatures to ensure that, where a request is received by facsimile or telephone, call back procedures are available to check the validity of the request. All requests should be retained within a central register.

Recommendation 12

The auditors recommend that AGL should take immediate steps to notify Baycorp:

- that access by IPS to credit information under the ostensible authority of AGL should cease forthwith and access codes be withdrawn; and

- to correct the information recorded on all relevant credit files of individuals to indicate that access was made by IPS.

Recommendation 13

That AGL include in its internal procedures, guidelines of what staff are required to do under the Privacy Act in respect of amendments of, or the inclusion of a statement, or in relation to a disputed matter on a member's CRA credit information file. These procedures or guidelines should be communicated to all relevant staff.

Recommendation 14

That relevant staff are made aware of an individual's right of access to a credit report held by AGL.

That AGL has adequate information and facilities available to respond to the requests in accordance with Paragraph 2.20 of the Code of Conduct.

Recommendation 15

That dispute settling procedures in relation to credit reporting should be established.

20. Australian National Credit Union
Audit opened Apr 02/ Audit closed Jan 03

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 11 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That ANCU immediately allocate individual user IDs and passwords to all staff who require access to Baycorp.

Recommendation 2

That ANCU periodically compare the accesses recorded on the Baycorp invoice to the number of credit applications processed in the relevant period. Unexpected variations should be investigated and reported to senior management where appropriate.

Recommendation 3

That ANCU inform all staff that they are not to record their user IDs or passwords.

Recommendation 4

That ANCU install mandatory password protected screensaver software on all systems that contain credit information.

Recommendation 5

That ANCU take immediate action to ensure that its security policy is finalized, promulgated and implemented.

Recommendation 6

That ANCU only list that portion of the debt that is at least 60 days overdue.

Recommendation 7

That ANCU ensure that it record credit information on the correct file held by the credit reporting agency.

Recommendation 8

That ANCU revise its 'Oral Consent and Notification' statement to make it easier for staff to follow.

Recommendation 9

That ANCU ensure that all relevant staff are made aware of the individual's right of access to their credit report pursuant to section 18H of the Privacy Act and that it has adequate information and facilities available to advise individuals in accordance with paragraph 2.20 of the Code of Conduct.

Recommendation 10

That ANCU implement procedures to ensure that, where a payment default is listed with a credit reporting agency and the customer disputes that he or she is overdue in making the a payment, the relevant credit reporting agency is informed.

Recommendation 11

That ANCU provide staff with regular training on Part IIIA of the Privacy Act.

21. Virgin Mobile (Australia) Pty Ltd
Audit opened May 02/ Audit closed Jan 03

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 13 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That Virgin Mobile develop and implement procedures to identify the purpose of credit applied for (i.e. whether it is for consumer or commercial purposes), before disclosing information to, or obtaining information from, a credit reporting agency.

Recommendation 2

That a nominated senior person should compare the accesses recorded on the Baycorp invoice bill to the number of accesses made to Baycorp in relation to a specific period. Large unexpected variances should be fully investigated to ensure that explanations are obtained and reported to senior management where appropriate.

Recommendation 3

Virgin Mobile should:

- consider reporting the actual amount of credit that an individual has applied for, or if that is not the case, that the individual has applied for an unspecified amount as credit rather than arbitrarily reporting an amount of $500 in all cases;
- implement procedures to ensure that it does not make duplicate accesses to consumer credit reports; and
- notify Baycorp Advantage Ltd of duplicate accesses and other errors as soon as practicable so that Baycorp can correct its records.

Recommendation 4

That - in any amendments to current contracts, or in drafting new contracts, where contractors may have access to personal information, either directly or incidentally – Virgin Mobile include conditions regarding the security and confidentiality of information that take into account the provisions of the Privacy Act.

Recommendation 5

That Virgin Mobile implements procedures to ensure that staff are aware of the circumstances under which old credit reports may legitimately be used.

Recommendation 6

That procedures be implemented to ensure that staff are able to identify a situation of duplicate access and then promptly inform the credit reporting agency.

That the file amendment form (issued as a standard form) be used for this purpose, completed by the staff member who has made the access and sent directly to the credit reporting agency.

Recommendation 7

That Virgin Mobile:

- review its access controls and instruct staff not to share passwords;
- ensure that staff log out of a session when not active or that the system logs them out of the session after a short period of inactivity;
- review and, if required, make representations to the TIO so that the insecure email link with the TIO is made secure and/ or emails containing credit worthiness information are encrypted;

ensure that terminals in Virgin's shop front retail stores which have access to credit worthiness information of customers are placed away from areas in which customers or the general public can view the monitor screens.

Recommendation 8

That Virgin Mobile include in its internal procedures, guidelines on its obligations under the Privacy Act in relation to requests for amendments to, the inclusion of statements in, and disputes about the accuracy of, a member's credit information file. These procedures or guidelines should be communicated to all relevant staff.

Recommendation 9

That relevant staff are made aware of an individual's right of access to a credit report held by Virgin Mobile.

That Virgin Mobile has adequate information and facilities available to respond to requests in accordance with paragraph 2.20 of the Code of Conduct.

Recommendation 10

That, where an agency has provided a legislative basis for a request under s.282(1) or (2) of the Telecommunications Act, Virgin Mobile satisfy itself that that legislative provision cited does relate to the enforcement of the criminal law, a law imposing a pecuniary penalty or the protection of the public revenue.

Recommendation 11

Virgin Mobile should review its procedures to ensure that requests received from enforcement agencies comply with the requirements of section 282(3), (4) or (5). In particular, it should take steps to satisfy it that an officer issuing a certificate under section 282(3), (4) or (5) has been authorised in writing by the Head of the agency to do so. It should do this by sighting such authority before disclosing subscriber information.

Virgin Mobile should satisfy itself that any certificates being furnished by the NSW Police Service under sections 282(3) (4) or (5) are in fact being issued by an authorised officer (i.e. a 'commissioned officer') before disclosing subscriber information.

Recommendation 12

Virgin Mobile should take steps to ensure that the Fraud Section maintains records of disclosures made to enforcement agencies in accordance with s.306(2) and (5) of the Telecommunications Act. In particular, the Fraud Section must ensure that the record of a disclosure made under s.306(2) or (3) lists: the name of the Virgin Mobile employee disclosing the information; the date of the disclosure; the grounds for the disclosure; and, if the disclosure is made on the grounds of a certificate under s.282(3), (4) or (5), the name of the person who issued the certificate and the date of the issue of the certificate. The requirements of sub-section 5(e) and (f) should also be followed where applicable.

Recommendation 13

Virgin Mobile should submit to the ACA an annual written report about the disclosures it has made to enforcement agencies within two months of the end of the financial year on 30 June.

22. Collection House Limited (Lion Finance)
Audit opened Jul 02/ Audit closed Jan 03

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 9 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That Lion Finance implement procedures to ensure that, where a payment default is listed with a credit reporting agency and the customer disputes that he or she is overdue in making the a payment, the relevant credit reporting agency is informed as soon as practicable.

Recommendation 2

That Lion Finance review its complaints handling system to identify options to ensure that Lion Finance has appropriate mechanisms to deal with any Privacy Act compliance obligations that may arise as a result of a complaint.

That Lion Finance implements the changes to their complaints handling system in accordance with the outcome of their review.

Recommendation 3

That Lion Finance regularly compare the accesses recorded on the Baycorp invoice with the number of listed debts processed in the relevant period. Unexpected variations should be investigated and reported to senior management where appropriate.

Recommendation 4

That, when Lion Finance is considering purchasing a debt portfolio, it take reasonable steps to assure itself that debts which have been listed with a credit reporting agency have been listed in accordance with Part IIIA of the Privacy Act. This could include examining the systems used by the original credit provider to list overdue debts.

That, where the requirements have not been met, Lion Finance amend or delete the listing as appropriate.

Recommendation 5

That Lion Finance ensure that all relevant staff are made aware of the individual's right of access to their credit report pursuant to section 18H of the Privacy Act and that it has adequate information and facilities available to advise individuals in accordance with paragraphs 2.20 and 2.21 of the Code of Conduct.

Recommendation 6

That Lion Finance install mandatory password protected screensaver software on all systems that contain consumer credit information.

Recommendation 7

That Lion Finance and Collection House review its procedures for identifying individuals, taking into account the high volume environment in which Collection Officers work.

Recommendation 8

That Lion Finance delete TFNs that it is not permitted to maintain, use or disclose in accordance with TFN Guideline 2.2.

Recommendation 9

That - when amending or drafting new contracts for service providers who may have either indirect or direct access to personal information - Collection House include in its contracts conditions regarding the security and confidentiality of information that take into account the provisions of the Privacy Act,.

23. Baycorp Advantage (Business Information Services) Pty Ltd
Audit opened Sep 02/ Audit closed Dec 03

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 24 recommendations for the improvement of the credit reporting agency's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

Baycorp incorporate into its terms and conditions the requirement that subscribers notify Baycorp when operators should no longer have access and their IDs should no longer be accepted. Baycorp implement a system of automatic termination of Operator IDs for the dial-in and direct access connections after a set period of time and advise subscribers accordingly, or Baycorp implements a process to check that operator IDs should still be active.

Recommendation 2

Baycorp implement procedures and audits to check periodically that its subscribers comply with its terms and conditions.

Recommendation 3

Baycorp should decline access to the Child Support Agency and Centrelink where it does not receive a properly exercised authority seeking access to the information. Baycorp should check the accesses that have already been made by the Child Support Agency and Centrelink and ensure that no unauthorised disclosures have been made. The most effective way in which to ensure that only authorised accesses are made is by Baycorp controlling directly the release of that information, which would likely require termination of the direct access that Centrelink and the Child Support Agency have currently.

Baycorp list the name of the law enforcement agency in file access records, where the anonymity of the law enforcement agency is not required.

Recommendation 4

Baycorp ensures that any advertisements for the superior service also carries a notice about the right of free access or that individuals are notified at the time they request the superior service that the free service is also available.

Recommendation 5

Baycorp use secure transmission on all websites used to disclose credit information.

Recommendation 6

A higher level of security would exist if the operator IDs and passwords were sent separately. Baycorp could send the operator IDs in the first letter to be distributed by the subscriber to the

individual operators and then the password could be sent in a separate letter directly to the operator concerned.

Recommendation 7

That Baycorp advise its subscribers that operators' passwords should not be stored by their browsers. Additionally, Baycorp assess the extra security measures that may be required to reduce the risk of unauthorised access through the web interface.

Recommendation 8

That Baycorp requires its subscribers to provide further information to ascertain whether there is an existing file or to create a new one, such as a date of birth, and possibly, a drivers' licence number, in addition to the name and address.

Recommendation 9

When Baycorp contacts a subscriber to confirm a disputed entry, the subscriber should be asked to fax the relevant documentation that the subscriber is relying upon to provide the verbal confirmation. If the subscriber maintains that the entry is valid and is unable to provide any supporting evidence or refuses to do so, Baycorp should mark the entry as being in dispute and advise the individual to complain directly to the credit provider concerned. Baycorp should also advise the individual that he or she may seek to have the Federal Privacy Commissioner investigate the complaint, although that the Federal Privacy Commissioner would only investigate before the credit provider has had a reasonable opportunity to deal with the complaint, in exceptional circumstances.

Recommendation 10

Baycorp develop and implement a policy which dictates the circumstances under which files may be linked and preferably have particular staff who are responsible for making the decision.

Recommendation 11

Baycorp run a report for all enquiries listed on its individual consumer credit information files that have '$0' as the amount of credit applied for and change these to 'unspecified' to be consistent and avoid inaccuracy or being misleading. Baycorp should change the programming of its database so that it does not allow a subscriber to enter '$0' where an individual's consumer credit information file is accessed for an enquiry.

Recommendation 12

Baycorp check every subscriber's name that can be used for enquiries and defaults and ensure that all of them sufficiently identify the credit provider to consumers. Listings on individual consumer credit information files of names which currently do not completely identify the credit provider should be replaced with the new versions that sufficiently identify the subscriber.

Recommendation 13

Baycorp should ensure that its subscribers and individuals clearly understand the meaning of the term *current* or instead use the term *paid* in all cases where the debt has been paid in full.

Recommendation 14

As Baycorp has a responsibility to ensure that its subscribers know that information cannot be accessed when it is unauthorised by the Privacy Act, training should be compulsory for all new subscribers and could be incorporated into the new subscriber contract pricing structure, unless the subscriber can demonstrate that it has a satisfactory training program from another source.

Recommendation 15

Processes should be put in place to automatically update subscribers, for example through a blind subscriber email list to circulate information to all subscribers when changes are made or to inform them that a notice about a change has been posted on Baycorp's website.

Recommendation 16

That Baycorp analyses complaints received from individuals to ascertain any systemic problem in the way the information is collected or entered into individual consumer credit information files, and obtains updated information directly from the source where possible.

Recommendation 17

Baycorp cease disclosing credit reports or information derived from them to Baycorp NZ until the latter becomes a 'credit reporting agency' within the meaning of the Privacy Act.

Recommendation 18

Baycorp remove all enquiries and defaults listed by foreign credit providers and credit reporting agencies and ensure that this type of information is not recorded in individual consumer credit information files.

Recommendation 19

Baycorp ensures that binding contractual arrangements setting out the privacy obligations be entered into between it and its courier. If possible, Baycorp ensures that the building managers take steps to include appropriate confidentiality provisions and restrictions in the contract with the cleaners when the contract is next renewed.

Recommendation 20

Baycorp separate the current report format into two separate reports: one containing the consumer credit report and the other containing the unregulated information.

Recommendation 21

Baycorp ensures it finalises and implements an appropriate IT Security Policy.

Recommendation 22

Baycorp appoints a specific officer to hold the responsibility of being the IT Security Manager.

Recommendation 23

Baycorp develop and implement IT security training for staff as part of its IT Security Policy.

Recommendation 24

That Baycorp incorporates the requirement that users must make an election each day when logging on to the system to accept the restrictions and responsibilities upon them and that users will automatically be denied access if such acceptance is not elected.

24. Mobile Innovations
Audit opened Sep 02/ Audit closed Feb 03

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 18 recommendations for the improvement of the credit provider's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That Mobile Innovations develop and implement procedures to identify the purpose of credit applied for (i.e. whether it is for consumer or commercial purposes), before disclosing information to, or obtaining information from, a credit reporting agency.

That where Mobile Innovations becomes aware that it has incorrectly reported information against an individual's consumer file that Mobile Innovations amend the record accordingly.

Recommendation 2

That Mobile Innovations either seeks consent to disclose credit worthiness information to other credit providers or does not disclose such information and removes the reference to such disclosures from its privacy notices.

Recommendation 3

That Mobile Innovations take steps to identify instances where they may have listed a debt that was not 60 days overdue and arrange with Baycorp to have the listing deleted.

Recommendation 4

That Mobile Innovations implement procedures to ensure that, where a payment default is listed with a credit reporting agency, and the customer disputes that he or she is overdue in making the a payment, the relevant credit reporting agency is informed as soon as practicable.

Recommendation 5

That Mobile Innovations regularly compare the accesses recorded on the Baycorp invoice with the number of phone applications ("sell ons") and the number of bad debts processed in the relevant period. Unexpected variations should be investigated and reported to senior management where appropriate.

Recommendation 6

That Mobile Innovations implement policies and procedures to ensure that only authorized staff are able to access Baycorp.

Recommendation 7

That Mobile Innovations immediately allocate individual user IDs and passwords to all staff who require access to Baycorp, and ensure that these staff use their own user IDs and do not share their passwords.

Recommendation 8

That Mobile Innovations ensure that their staff do not record their user IDs or passwords in a manner such that they are readily available to any other person.

Recommendation 9

That Mobile Innovations ensure that access to its offices is secure, and that creditworthiness information is secured overnight.

Recommendation 10

That Mobile Innovations review its logical security and implement any recommendations resulting from the review.

That regardless of the outcome of the review Mobile Innovations at a minimum:

install mandatory password protected screensaver software on all systems that contain credit information.

ensure that staff change their passwords and do not disclose their password to others.

use passwords that are at least eight characters long with some alpha numeric combination

Recommendation 11

[This recommendation appeared in draft report but has been deleted from final report. See the body of this report for more detail.]

Recommendation 12

That Mobile Innovations ensure that Look Mobile staff are only able to access the personal credit information of those Look Mobile customers to which Look Mobile staff may need access in order to provide services to those customers and manage their accounts.

Recommendation 13

That - in any amendments to current contracts, or in drafting new contracts, where contractors may have access to personal credit information, either directly or incidentally – Mobile Innovations include conditions regarding the security and confidentiality of information that take into account the provisions of the Privacy Act.

Recommendation 14

Mobile Innovations should review its procedures to ensure that it can satisfy itself that any organisation requesting information under sections 282(3) to (5) of the Telecommunications Act is an enforcement agency as defined by section 282(10) of the Telecommunications Act.

Recommendation 15

That Mobile Innovations review its procedures to ensure that it can satisfy itself that an officer issuing a certificate under section 282 of the Telecommunications Act is a senior officer that has been authorised in writing by the Head of the agency to do so.

Recommendation 16

That Mobile Innovations does not disclose subscriber information where the agency has failed to identify the provision in the Telecommunications Act that is being relied upon when it is requesting the information.

That, where an agency has provided a legislative basis for a request under s.282(1) or (2) of the Telecommunications Act, Mobile Innovations satisfy itself that that legislative provision cited does relate to the enforcement of the criminal law, a law imposing a pecuniary penalty or the protection of the public revenue.

Recommendation 17

That Mobile Innovations maintains records of disclosures made to enforcement agencies in accordance with s.306(2) and (5) of the Telecommunications Act.

Recommendation 18

That Mobile Innovations implement procedures to ensure that it does not disclose information to an enforcement agency where a certificate had not been given to Mobile Innovations within 5 days of being issued.

25. Dun & Bradstreet Australia Pty Ltd
Audit opened Jun 03/ Dec 03

OUTCOME OF THE AUDIT

The outcome of the audit was the making of 17 recommendations for the improvement of the credit reporting agency's handling of personal information.

RECOMMENDED FOLLOW -UP ACTION

Recommendation 1

That D&B enhance the protection of the CCB database and decrease the potential risk of unauthorised access, use and disclosure of personal information by restricting the dissemination of the Subscriber numbers, User IDs and Passwords to those internal staff with an operational need to know that information.

That D&B enhance the protection of the CCB database and decrease the potential risk of unauthorised access, use and disclosure of personal information by having the Sales Administrator provide Subscriber numbers, User IDs and Passwords directly to the Subscriber and the Subscriber's authorised operators. This can be done by the Sales Administrator telephoning the Subscriber and the individual operator(s) directly or sending the information direct by letter.

Recommendation 2

That D&B ensure that all passwords for staff and Subscribers meet the current industry minimum standard of a randomly generated eight character alpha numeric value.

That D&B ensure that there is a mandatory change of passwords for all staff and Subscribers at the end of a 90 day period.

That D&B allow Subscribers the option of generating their own random configuration eight character alpha numeric passwords at the end of the 90 day period.

That D&B ensure that all passwords for staff and Subscribers are retained by its system to ensure that there is no reuse of old or deactivated passwords.

That D&B ensure that deactivated passwords are not reallocated to new Subscribers.

Recommendation 3

That D&B include contractual obligations on all Subscribers to advise D&B immediately when a staff member no longer requires access to the D&B database.

That D&B ensure that, when a Subscriber advises that a staff member access should be deactivated, D&B take action to deactivate that access and that the system retain a record of the date the access is deactivated.

Recommendation 4

That D&B ensure that staff do not use the autosave facility to retain passwords on the system.

Recommendation 5

That D&B include contractual obligations on all Subscribers to ensure the CCB is protected by security measures which are reasonable in the circumstances including the use of auto lock out on computers with access to the CCB.

Recommendation 6

That D&B ensure that when the manager's office is locked at close of business, the key to the filing cabinet is kept in a secure location outside the office.

Recommendation 7

That, where multiple files are held for one individual, D&B establish consistent criteria for linking the files to ensure that reasonable steps are in place that enables personal information contained in the reports and linked together to be accurate, up to date, complete and not misleading.

Recommendation 8

That D&B define the terms and abbreviations of status definitions used and make them available in the in reports.

That D&B ensure that, where a debt is not collected and the matter returned to the client organisation, the status field in the reports provides an accurate description of the actions taken and the status of the debt.

That D&B ensure that, where a debt is listed as a serious credit infringement, the debt fits the criteria in section 6 of the Privacy Act and that a serious credit infringement is not a subset of an existing default and defined by the status of the debt.

That D&B investigate the possibility of accessing updated information about judgement debts and bankruptcies from the courts and ITSA as and when changes to the status of judgement debts and bankruptcies occurs.

Recommendation 9

That D&B investigate the possibility of accessing updated information about judgement debts and bankruptcies from the courts and ITSA as and when changes to the status of judgement debts and bankruptcies occurs.

That D&B analyses complaints received from individuals to determine whether there is any systemic problem in the way the information is collected or entered into individual consumer credit information files, and obtains updated information directly from the source where possible.

Recommendation 10

That D&B clearly separate consumer and commercial credit information and public information into separate sections of the report

That D&B clearly mark the start and finish of each section of the report by implementing separate pagination within each section of the report.

Recommendation 11

That D&B insert confidentiality clauses into contracts with third parties who have physical access to D&B premises, for examples cleaning and maintenance staff. I note that D&B has committed to doing this when tenancy agreement is signed.

Recommendation 12

That D&B remove all enquiries and defaults listed by foreign credit providers and credit reporting agencies and ensure that this type of information is not recorded in individual consumer credit information files.

Recommendation 13

That D&B ensures that any accesses to the CCB by New Zealand based staff are for credit providers that meet the requirements and definitions of credit provider and corporation within sections 6 and 11B of the privacy Act.

Recommendation 14

That, when D&B receive a request for information from the CCB by a state, commonwealth or law enforcement agency, it ensure that its staff are aware that the request must be in writing, signed by an appropriate senior officer and should cite the relevant section of the relevant legislation that requests the information or authorises the disclosure by D&B.

That D&B maintain a register of file of the requests as evidence that the disclosure was made by or under law and that the legislation requires or authorises that disclosure.

Recommendation 15

That D&B restrict the access that Melbourne staff have on CCB to the Australian partition only to ensure that the information in the credit report meets the requirements of section 18E.

That D&B ensure that when a credit report is disclosed to an individual, a credit provider or another credit reporting agency it contains only information that is permitted content under section 18E and that D&B is able to disclose that content under section 18K of the Act.

That D&B restrict access to the New Zealand partition to those staff that have an operational need to access the partition.

Recommendation 17

That D&B amend all company training and instructional policy to ensure that staff are aware that that D&B's obligations to protect personal information come under the Privacy Act 1988 and in particular Part IIIA and Schedule 3.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 42

Senator Ludwig asked the following question at the hearing on 16 February 2004:

What kind of issues or problems are usually picked up in credit information audits?

The answer to the honourable senator's question is as follows:

- A number of credit providers do not establish whether loans are for a domestic or commercial purpose. This can result in inaccurate information being placed on a consumer's file.

- A number of credit providers did not have in place policy or procedural manuals to inform staff of the credit provider's obligations under the Privacy Act and the Credit Reporting Code of Conduct, and staff were not provided with training to ensure an appropriate level of awareness of matters relevant to their duties.

- Most credit providers include in their application forms clauses to notify applicants that personal information may be disclosed to a credit reporting agency and, when relevant, to obtain any necessary agreements as required by the Privacy Act. In a number of instances the auditors found that these clauses did not notify the individual adequately of all relevant matters and did not seek all necessary agreements.

- Many Credit Providers were not protecting individuals' credit reports and credit worthiness information sufficiently from unauthorised use, or against loss, modification or disclosure, or other misuse. In some cases, these records were left unsecured outside normal working hours, and there was a lack of logical security controls over access to computer systems containing credit reports and credit worthiness information. Further, service provider contracts did not, in all cases, include provisions regarding the security and confidentiality of credit information.

- A number of credit providers were found not to meet their obligations to inform applicants in writing when an application for credit is declined wholly or partly on the basis of an adverse credit report.

- A number of credit providers were not aware of their obligations under the Privacy Act to notify the credit reporting agency when an individual contends that an overdue payment has been incorrectly listed on his or her credit information file.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 43

Senator Bolkus asked the following question at the hearing on 16 February 2004:

OFPC Resourcing

a) According to the annual report, complaints are queued for around six months before being allocated to a complaints officer, but Mr Crompton has said that it sometimes takes longer. How often does it take longer, and what time lengths are we talking about here?
b) After a complaint is allocated to a complaints officer, how much longer does it take for a complaint to be resolved?
c) What kinds of complaints take longest to resolve?
d) Please provide all the raw figures for these complaints for the last several years
e) And these delays are due to the OFPC's insufficient resources?

The answer to the honourable senator's question is as follows:

a) The average time in the complaints queue at June 2003 was approximately six months. At present a complaint that is assessed as needing a non-urgent investigation will be queued for ten to twelve months before it can be allocated to a case officer for investigation.

b) The Office's Complaint's management system does not currently allow for the calculation of duration of investigation excluding time in the queue. We can provide an estimate of this based on a sample of 67 complaints recently closed following preliminary enquiries or a formal investigation. We found in this sample that excluding time spent in the queue the average duration of an investigation was 192 days. We closed:

- 49% of the cases in less than 90 days
- 72% of the cases in less than 180 days
- 82% of the cases in less than 270 days
- 88% of the cases in less than 365 days
- 91% of the cases in less than 450 days
- 94% of the cases n less than 540 days

The OFPC is currently assessing options to modify the Complaints Management System to provide these statistics.

c) There is no particular type of complaint that will inherently take longer to resolve. The length of an investigation depends to some extent on the complexity of the issue and to some extent on how willing the parties are to resolve the matter. Factors which may mean a complaint investigation becomes protracted include:

- there are points of law on which legal advice is needed;

- new evidence or new issues are introduced as the investigation proceeds;
- one or both parties have entrenched positions about what they will agree to by way of resolution.

d) As noted in answer to question c) there is no particular type of complaint that will take longer to resolve.

e) The complaint queue is due to the significant increase in the number of complaints received following the introduction of the private sector provisions which has significantly exceeded the number anticipated and for which additional funding was provided.

The OFPC has attempted to limit the growth of the Complaints queue within its existing resources by reallocating positions from the Policy section to the Compliance section and ensuring more efficiency.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 44

Senator Ludwig asked the following question at the hearing on 16 February 2004:

Could you provide a list of all administered programmes in the OFPC, including:

- A description of the programme;
- number of people directly receiving funds/assistance under the programme;
- a breakdown on those receiving funds/assistance under the programme by electorate;
- the policy objective of the programme;
- whether the programme is ongoing;
- the funding in each financial year of the forward estimates for the programme (with a breakdown of administered and departmental expenses), including:
    - how much funding was allocated for the programme;
    - how much is committed to the programme; and
    - how much is unspent.
- indication of whether an evaluation of the programme effectiveness has been conducted:
    - if so, when that evaluation occurred; and
    - if so, the conclusion of that evaluation.

The answer to the honourable senator's question is as follows:

The Office does not have any administered programmes.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 45

Senator Ludwig asked the following question at the hearing on 16 February 2004:

How many Senior Executive Officers (or equivalent) were employed in the OFPC in 1996-97, 1997-98, 1998-99, 1999-00, 2000-01, 2001-02, 2002-03, 2003-04.

The answer to the honourable senator's question is as follows:

The Office of the Federal Privacy Commissioner was established on 1 July 2000. Prior to this date staff working for the Privacy Commissioner were employed by the Human Rights and Equal Opportunity Commission. The following table sets out the number of Senior Executive Officers (or equivalent) from 1 July 2000.

Financial Year	Response
2000-01	1 x SES Band 1
2001-02	1 x SES Band 1
2002-03	1 x SES Band 1
2003-04	1 x SES Band 1

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 46

Senator Ludwig asked the following question at the hearing on 16 February 2004:

What was the base and top (including performance pay) wages of APS 1, 2, 3, 4, 5, 6 (or equivalent), Executive Level 1 and 2 (or equivalent), and SES band 1, band 2 and band 3 (or equivalent)in the OFPC in 1996-97, 1997-98, 1998-99, 1999-00, 2000-01, 2001-02, 2002-03, 2003-04.

The answer to the honourable senator's question is as follows:

The Office of the Federal Privacy Commissioner was established on 1 July 2000. Prior to this date staff working for the Privacy Commissioner were employed by the Human Rights and Equal Opportunity Commission. The following table sets out the base and top (including performance pay) wages from 1 July 2000.

Classification	2000-01 (as at 30 June 2001)	2001-02 (as at 30 June 2002)	2002-03 (as at 30 June 2003)	2003-2004 (as at 30 June 2004)
APS1	$25,777 $28,489	$26,550 $29,344	$28,303 $31,280	$29,435 $32,532
APS2	$29,171 $32,350	$30,047 $33,320	$32,913 $35,519	$34,229 $36,940
APS3	$33,228 $35,862	$34,224 $36,938	$36,483 $39,376	$37,943 $40,951
APS4	$37,032 $40,210	$38,143 $41,416	$40,661 $44,149	$42,287 $45,915
APS5	$41,305 $43,799	$42,544 $45,113	$45,352 $48,984	$47,167 $50,943
APS6	$44,613 $51,247	$45,951 $52,784	$50,202 $56,268	$52,210 $58,519
EL1	$57,192 $62,718	$58,908 $64,600	$62,796 $68,863	$65,308 $71,618
EL2	$65,962 $75,968	$67,941 $83,247	$72,425 $88,412	$75,322 $86,748
SES Band 1	$107,468	$111,363	$116,996	$108,160

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 47

Senator Ludwig asked the following question at the hearing on 16 February 2004:

What was the average salary for an SES (or equivalent) in the OFPC in 1996-97, 1997-98, 1998-99, 1999-00, 2000-01, 2001-02, 2002-03, 2003-04.

The answer to the honourable senator's question is as follows:

The Office of the Federal Privacy Commissioner was established on 1 July 2000. Prior to this date staff working for the Privacy Commissioner were employed by the Human Rights and Equal Opportunity Commission. The following table sets out the average salary for an SES (or equivalent) from 1 July 2000.

Financial Year	Response
2000-01	$95,000
2001-02	$95,000
2002-03	$104,000
2003-04	$108,160

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 48

Senator Ludwig asked the following question at the hearing on 16 February 2004:

How many staff had mobile phones issued by the OFPC in 1996-97, 1997-98, 1998-99, 1999-00, 2000-01, 2001-02, 2002-03, 2003-04 to date.

The answer to the honourable senator's question is as follows:

The OFPC was established as an Executive Agency with effect from 1 July 2000. The following table sets out how many staff had mobile phones issued since 1 July 2000.

Financial year	No. of staff issued with mobile phones
2000-01	7
2001-02	7
2002-03	7
2003-04 to date	8

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 49

Senator Ludwig asked the following question at the hearing on 16 February 2004:

How many SES (or equivalent) were issued with cars in the OFPC in 1996-97, 1997-98, 1998-99, 1999-00, 2000-01, 2001-02, 2002-03, 2003-04

The answer to the honourable senator's question is as follows:

The OFPC was established as an Executive Agency with effect from 1 July 2000. The following table sets out how many SES (or equivalent) were issued with cars since 1 July 2000.

Financial year	SES or equivalent issued with cars
2000-01	1
2001-02	1
2002-03	1
2003-04 to date	1

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

Question No. 50

Senator Ludwig asked the following question at the hearing on 16 February 2004:

Could you please list all 'management retreats/training' conducted by the OFPC which were attended by employees during 2000-01, 2001-02, 2002-03, 2003-04 to date. For such meetings held off-site (from the OFPC), could you please indicate:

- where (location and hotel) and when they were held;
- how much was spent in total;
- how much was spent on accommodation;
- how much was spent on food;
- how much was spent alcohol/drinks; and
- how much was spent on transport.

The answer to the honourable senator's question is as follows:

The Office of the Federal Privacy Commissioner was established as an Executive Agency under the Public Service Act with effect from 1 July 2000. The following table sets out the 'management retreats/training' conducted by the OFPC from 1 July 2000.

Financial Year	Response
2000-01	Nil
2001-02	Nil
2002-03	Nil
2003-04 to date	Nil