KPMG

The Trustee for SAVELOSS UNIT TRUST Trading as Tasmanian Collection Services

Compliance with Part IIIA of the Privacy Act 1988, the Privacy Regulations 2013 and the Privacy (Credit Reporting) Code 2014

Report

Inherent Limitations

As set out in our Engagement Letter dated 6 July 2017 ("Engagement Letter"), KPMG has undertaken an independent review of compliance with Part IIIA of the Privacy Act 1988, the Privacy Regulations 2013 and the Privacy (Credit Reporting) Code 2014 (collectively "the Privacy Requirements"), for The Trustee for SAVELOSS UNIT TRUST Trading as Tasmanian Collection Services (TCS) as required in accordance with paragraph 24.2 of the Privacy (Credit Reporting) Code 2014, ("the Engagement").

Any reference to 'audit', 'review' and/or 'independence' throughout this Engagement have not be used in the context of their respective meanings under assurance and other standards issued by the Australian Auditing and Assurance Standards Board. The services provided in connection with the Engagement comprise an advisory engagement, which is not subject to assurance or other standards issued by the Australian Auditing and Assurance Standards Board and consequently no opinions or conclusions intended to convey such assurance have been expressed.

This Report ("Report") provides an overview of KPMG's key findings and observations in connection with the Engagement during the course of the work undertaken for Tasmanian Collection Services. No warranty of completeness accuracy or liability is given in relation to the statements and representations made by, and the information and documentation provided by TCS or TCS' management and personnel consulted as part of the process. KPMG is under no obligation in any circumstances to update this report, in either oral or written form, for events occurring after the report has been issues in final form.

Due to the inherent limitations of any internal control structure, it is possible that fraud, error or non-compliance with laws and regulations may occur and not be detected. Further, the internal control structure, within which the control procedures that have been subject to the procedures we have performed, has not been reviewed in its entirety, and therefore, no opinion or view is expressed as to the effectiveness of the greater internal control structure.

The procedures performed were not designed to detect all weaknesses in control procedures as they were not performed continuously throughout the period and the tests performed on the control procedures were performed on a sample basis. Any projection of the evaluation of control procedures to future periods are subject to the risk that the procedures may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

The findings and observations in this Report have been formed on the above basis.

Third Party Reliance

This Report has been prepared solely for the purpose set out in Section 2 and for TCS' information, and is not to be used for any other purpose or distributed to any other party without KPMG's prior written consent. This Report has been prepared at the request of TCS in accordance with the terms of KPMG's Engagement Letter dated 6 July 2017. Other than our responsibility to TCS, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this Report. Any reliance placed is that party's sole responsibility. In that regard, we consent to this Report being released to the OAIC on the basis set out in our Engagement Letter.

We disclaim any assumption of responsibility by KPMG to any person other than TCS, or for any use of this Report for any purpose other than that for which it was prepared.

The definitive version of this Report is the one bearing our original signature and Tasmanian Collection Services management is responsible for any errors or in accuracies appearing in any reproduction in any form or medium.

Public Release

KPMG permits TCS, at its discretion, to the public release of this Report on the TCS website.

Contents

1. Background

In accordance with paragraph 24.2 of the *Privacy (Credit Reporting) Code 2014 (Version 1.2)* ("CR Code"), every 3 years (or more frequently, if the Commissioner requests), The Trustee for SAVELOSS UNIT TRUST Trading as Tasmanian Collection Services ("TCS") as a Credit Reporting Body ("CRB") must commission an independent review of its operations and processes to assess compliance by the CRB with its obligations with the Privacy Requirements. In addition, the CRB must consult with the Commissioner as to the choice of reviewer and scope of the review. This Report and the CRB's response to this Report must be provided to the Commissioner and made publicly available.

As set out in our Engagement Letter dated 6 July 2017 ("Engagement Letter"), KPMG has undertaken a review of compliance with *Part IIIA of the Privacy Act 1988* ("the Privacy Act"), the *Privacy Regulations 2013* and the Privacy (Credit Reporting) Code 2014 ("CR Code") (collectively "the Privacy Requirements"), in accordance with paragraph 24.2 of the CR Code, ("the Engagement").

2. Scope and Approach

TCS engaged KPMG to undertake a review of the design and operating effectiveness of its Privacy Framework for compliance with the Privacy Requirements. This review is necessarily a point in time review focusing on the Privacy Framework of the TCS credit reporting business entity only.

The scope of the Engagement was agreed as follows:

- Conduct a governance and process review to gain an understanding of the Framework that was implemented by TCS to comply with the Privacy Requirements.
- Consider the policies and processes used to differentiate the different types of information held by the CRB (e.g. tenancy and rental debt information, credit information, public information).
- Consider the design, implementation and operating effectiveness of the key processes and controls contained in the framework.
- Preparation of a report to present findings and observations including any breaches in accordance with the obligations analysed (collectively, Scope).

We present below a summary of the approach undertaken:

- We reviewed copies of documents provided by TCS and made further enquiries of TCS' management and personnel as required.
- We conducted interviews with members of TCS' management in order to understand the level of awareness and how TCS' Privacy Framework is applied in practice.
- We undertook on-site walk throughs and testing of key processes and controls.

Our findings and observations set out in this Report should be considered in this context.

3. Findings and Observations

We acknowledge the cooperation that has been provided by TCS in our preparation for this report and throughout the course of our review.

Our assessment of TCS's policies, processes and controls has been performed in accordance with the scope set out in our engagement letter dated 6 July 2017. Based on the work performed during the Engagement, we make the following key findings and observations:

Overview of Observations	
Governance	
1	In relation to Section 20B(5)(a) of the Privacy Act and Sections 3 and 3.1 of the CR Code, we considered TCS's Privacy Policy published on their website as at 3 July 2017. We note that the Privacy Policy is provided free of charge for the general public. However, we note that the Privacy Policy is not periodically reviewed and does not outline how TCS holds personal information.
2	Except for the Privacy Policy, TCS does not have any documented policies, procedures and controls ("Privacy Framework") in place to ensure compliance with their Privacy Requirements.
3	We note that formal Privacy training is conducted only on a high level basis on induction for TCS employees. We did not observe annual or refresher training requirements for TCS employees or any other mechanism deployed by TCS to ensure ongoing training and awareness of privacy requirements amongst its employees.
Monitoring	
4	TCS does not have a formal process to regularly assess the design and operational effectiveness of its privacy controls.
5	In relation to Section 6.1 of the CR Code, TCS has not developed and maintained common descriptors in conjunction with Credit Providers (CPs). These descriptors are then to be used by CPs when disclosing to TCS information about the type of consumer credit that they have provided to individuals.

6	Section 20N(3)(b) and 20N(3)(c) of the Privacy Act and Sections 23, 21.1 and 23.2 of the CR Code require specific actions in relation to agreements with CPs. We note the following in relation to those requirements: • TCS has not engaged an independent person to conduct regular audits over CPs to ensure that the credit information they disclose to TCS (under Section 21D of the Privacy Act) is accurate, up-to-date and complete; • TCS does not have a formal documented procedure to identify and deal with suspected breaches of the agreements with CPs; • TCS has not incorporated into its agreements with CPs a risk based program to monitor the CPs obligations under Part IIIA of the Privacy Act, namely: o the credit information the CP discloses to TCS is accurate, up-to-date and complete; o the credit reporting information that TCS discloses to the CP is protected by the CP from misuse, inference and loss and from unauthorised access, modification or disclosure; and o the CP takes the steps in relation to requests to correct credit-related personal information required by the Privacy Requirements; • TCS has not established a documented risk based monitoring program.
7	In relation to Sections 20K(4)(d) and 20K(4)(e) of the Privacy Act and Section 17.3 of the CR Code: • TCS does not end the ban period for credit reporting information about an individual 21 days after the day on which the request is made; • TCS does not give the individual written notification that the ban period for their credit reporting information has been extended past the ban period; • TCS does not notify the individual no less than 5 business days before the end of the ban period regarding: o the date the ban period is due to finish o the individual's rights under the Privacy Requirements o what, if any, information TCS requires to support the individual's allegation of fraud; • KPMG observed that the ban period placed on an individual's credit reporting information is held indefinitely.
Security	
8	In relation to Section 20V(2) of the Privacy Act and Section 22.3 of the CR Code, we observed that TCS has a robust control in place for the suppression and deletion of information held in the credit reporting system. However, we observed one instance where credit information dated 2014 was stored outside of the credit reporting system and was not subject to a suppression and deletion control.
9	In relation to Section 20Q of the Privacy Act and Section 15.1 of the CR Code, TCS has encryption software in place when transferring credit information between internal credit reporting systems. However, there is no encryption or password protection in place for the electronic transmission of credit reports directly to an individual and for storage of credit reporting information outside the credit reporting systems.
Reporting	
10	In relation to Section 23.11 of the CR Code, TCS has not published on its website a report for the financial years ending 30 June 2014, 2015 or 2016.

Whilst, we acknowledge the nature, size and complexity of TCS's Credit Reporting Business, the absence of effectively designed and documented policies, procedures and controls will impact the ability to promote compliant outcomes and behaviours. It may also limit TCS' ability to promptly and effectively respond to breaches or other compliance issues regarding its Privacy requirements. A commitment to continuous improvement is a key element in achieving effective and enduring compliance with the Privacy Requirements.

Tasmanian Collection Service
COLLECTION AND CREDIT REFERENCE SERVICES

Paragraph 24.2 of the CR code requires a credit reporting body (CRB) to conduct an Independent Compliance Review every 3 years, or as directed by the OAIC.

Tasmanian Collection Services engaged KPMG on 6 July 2017 to conduct the review. Below are the findings and responses.

Governance

Finding 1

In relation to Section 20B(5)(a) of the Privacy Act and Sections 3 and 3.1 of the CR Code, we considered TCS's Privacy Policy published on their website as at 3 July 2017.
We note that the Privacy Policy is provided free of charge for the general public. However, we note that the Privacy Policy is not periodically reviewed and does not outline how TCS holds personal information.

Response

We have reviewed and updated our Privacy Policy to include how we hold personal information.

We will amend our procedures to review the TCS Privacy Policy on a scheduled basis, or as required.

Finding 2

Except for the Privacy Policy, TCS does not have any documented policies, procedures and controls ("Privacy Framework") in place to ensure compliance with their Privacy requirements.

Response

TCS acknowledges the lack of structured policy framework and have commenced a project to rectify this. We anticipate this will be completed by the end of 2017.

Finding 3

We note that formal Privacy training is conducted only on a high level basis on induction for TCS employees. We did not observe annual or refresher training requirements for TCS employees or any other mechanism deployed by TCS to ensure ongoing training and awareness of privacy requirements amongst its employees.

Response

TCS acknowledges this. In addition to the induction training, we have implemented an annual refresher training program for existing employees.

Monitoring

Finding 4

TCS does not have a formal process to regularly assess the design and operational effectiveness of its privacy controls.

Response

TCS has commenced a project to develop a Privacy Policy Framework (as per response 2). This will incorporate control testing process design and implementation.

Finding 5

In relation to Section 6.1 of the CR Code, TCS has not developed and maintained common descriptors in conjunction with Credit Providers (CPs). These descriptors are then to be used by CPs when disclosing to TCS information about the type of consumer credit that they have provided to individuals.

Response

TCS records Default Information (Section 9 of the CR Code) and Information Requests (Section 7 of the CR Code). TCS does not record Consumer Credit Liability Information to which section 6.1 of the CR code relates. As such we do not believe the development of common descriptors is warranted.

Finding 6

Section 20N(3)(b) and 20N(3)(c) of the Privacy Act and Sections 23, 21.1 and 23.2 of the CR Code require specific actions in relation to agreements with CPs. We note the following in relation to those requirements.

- *TCS has not engaged an independent person to conduct regular audits over CPs to ensure that the credit information they disclose to TCS (under Section 21D) of the Privacy Act) is accurate, up-to-date and complete;*
- *TCS does not have a formal documented procedure to identify and deal with suspected breaches of the agreements with CPs;*
- *TCS has not incorporated into its agreements with CPs a risk based program to monitor the CPs obligations under Part IIIA of the Privacy Act, namely:*
    - *the credit information the CP discloses to TCS is accurate, up-to-date and complete;*
    - *the credit reporting information that TCS discloses to the CP is protected by the CP from misuse, inference and loss and from unauthorised access, modification or disclosure; and*
    - *the CP takes the steps in relation to requests to correct credit-related personal information required by the Privacy requirements;*
- *TCS has not established a documented risk based monitoring program.*

Response

TCS acknowledges this. These requirements will be further addressed in our Privacy Policy Framework development project. Refer to response 2.

Whilst we recognise our responsibilities in this area, and will be taking steps to meet our obligations, TCS have robust dispute management processes and are proactive when handling any issues that

might arise. It should be noted that to date, there have not been any matters referred to our external dispute resolution scheme.

Finding 7

In relation to Sections 20K(4)(d) and 20K(4)(e) of the Privacy Act and Section 17.3 of the CR Code:

- *TCS does not end the ban period for credit reporting information about an individual 21 days after the day on which the request is made;*
- *TCS does not give the individual written notification that the ban period for their credit reporting information has been extended past the ban period;*
- *TCS does not notify the individual no less than 5 business days before the end of the ban period regarding:*
    - *the date the ban period is due to finish*
    - *the individual's rights under the Privacy requirements*
    - *what, if any, information TCS requires to support the individual's allegation of fraud;*
- *KPMG observed that the ban period placed on an individual's credit reporting information is held indefinitely.*

Response

TCS acknowledges this and have amended our processes to end the ban period at 21 days and to include written notification to the individual not less than 5 days prior to the expiration of the ban, along with information regarding the individual's rights under the Act.

Security

Finding 8

In relation to Section 20V(2) of the Privacy Act and Section 22.3 of the CR Code, we observed that TCS has a robust control in place for the suppression and deletion of information held in the credit reporting system. However, we observed one instance where credit information dated 2014 was stored outside of the credit reporting system and was not subject to a suppression and deletion control.

Response 8

TCS notes this matter was in relation to an operator's email. TCS will develop controls over these ancillary systems in our Privacy Policy Framework development project. See response 2.

Finding 9

In relation to Section 20Q of the Privacy Act and Section 15.1 of the CR Code, TCS has encryption software in place when transferring credit information between internal credit reporting systems. However, there is no encryption or password protection in place for the electronic transmission of credit reports directly to an individual and for storage of credit reporting information outside the credit reporting systems.

Response

TCS is currently implementing PDF document encryption of credit information reports delivered via email.

Reporting

Finding 10

In relation to Section 23.11 of the CR Code, TCS has not published on its website a report for the financial years ending 30 June 2014, 2015 or 2016.

Response

The TCS website has now been updated to include this information and our procedures will be amended to report this annually.