COMMUNICATIONS
ALLIANCE LTD

ARCA CREDIT REPORTING CODE

COMMUNICATIONS ALLIANCE SUBMISSION

MAY 2013

TABLE OF CONTENTS

INTRODUCTION	**2**
SECTION 1 – GENERAL COMMENTS	**3**
SECTION 2 – CLAUSE SPECIFIC COMMENTS	**4**

INTRODUCTION

Communications Alliance welcomes the opportunity to provide this submission in response to the Australasian Retail Credit Association (ARCA) calls for public submissions on the draft Credit Reporting Code of Conduct (**the CR Code**).

About Communications Alliance

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

SECTION 1 –GENERAL COMMENTS

Communications Alliance is pleased to have the opportunity to provide this submission. In addition to the following general comments, Communications Alliance has provided detailed comments on the Code in the following section.

In general, Communications Alliance considers:

- the language of the CR Code is very legalistic, which will limit the useability of the Code by our members' business areas, other than legal teams. We encourage the drafters to adopt a plain English style of drafting. We understand that additional guidelines (Explanatory Notes) will be drafted to clarify the code obligations over the coming months. We encourage ARCA to prioritise this activity in order to allow CPs the maximum amount of time available to fully understand the new Code requirements, educate their staff on the new obligations and implement those within their organisations.
- the examples included in the Explanation section of the Code are in general not relevant to credit providers who are telecommunication providers, and as such do not assist in providing guidance as to how these providers are meant to apply the Code rules. See for example: clause 6.1.
- With the emergence of the digital economy, the Code should be drafted to ensure compliance can be achieved through channels other than traditional ones, such as written communication. We have highlighted specific examples of this issue in the following section.
- We support the approach taken by ARCA to ensure that all industry sectors to which the Code will apply have the opportunity to participate in the development of the Code, through participation in the Code Industry Council. We encourage ARCA to ensure that the next stages in the Code development, and ultimately its approval, continue to be overseen by this cross-industry committee.

Communications Alliance requests that the Code be amended to take into account our comments.

SECTION 2 – CLAUSE SPECIFIC COMMENTS

Clause 2.2

Obligation goes beyond the requirements of the Privacy Act. A CP must be able to cap its liability. The wording of the clause is such that the obligation may never reach an end.

The same outcome could be reached via contractual mechanisms that allow for CPs to update the information with a CRB following termination of the contract between the CP and CRB. That is "Survive the termination of the agreement".

We request that this clause be removed.

Clause 4.1

This clause is covered in the PA and should not be reproduced in the Code.
We request that this clause be removed.

Clause 5.3

The Code should refer to contemplation of requests by a CP from a CRB only after becoming aware of a specific data integrity issue.

The concept of a data integrity issue is still too vague and needs tightening.

Clause 6.2

Note that the example does not apply to telecommunication CPs.
We propose that the Explanation to cl 6.2(a) include:

- the day the CP approves the application

The concept of 'credit limit' is problematic for telecommunication providers as not all customers are on a fixed term contract. Also credit may be granted to a customer who may never use it, which raises the question of whether this would need to be reported. We request clarity for telecommunication CPs.

Suggest adding to cl 6.2(b)(i) "or telecommunications product" after "charge card contract".

Some of these requirements are very rigid in relation to the dates and amounts that must be reported. Because of provisioning systems of services, Billing Account creation approximate dates and amounts should be sufficient and the Code should include some tolerances that credit providers can rely on – for example, reasonable estimates based on a reasonable period.

For the Explanation for cl 6.2(c) we suggest include the date that an account is closed/terminated.

Clause 9.1

Clause 9.1 needs to reference that a request for payment terms is part of a financial hardship application, in the Code rule itself, not only in the Explanation.

Note that telecommunication customers request new payment terms for a number of reasons, not only due to financial hardship. For example, a one-off request to vary the payment date by a few days, to align with a customer's salary pay date. In such cases, clause 9.1 should not apply.

Comms Alliance requests that the CR Code acknowledge that telecommunications providers' obligations are as per the TCP Code. See clauses 6.14 and 8.2.1(v) of the TCP Code.

Note that the TCP Code is silent on the period after a request is refused before the CP can disclose a consumer credit overdue payment to a CRB. The Code is also silent on clause 9.1(b).

Clause 9.2

"National Consumer Code" – is this meant to be the National Credit Code?

We suggest that clauses 9.2 and 9.3 introduce obligations on CPs that go beyond what the CR Code can address.

We believe that this is overreach, and request that these clauses be removed.

Clause 13.1

We note that the wording of this clause has been improved, but might still exclude some fraudulent circumstances.

The issue for telecommunication providers is how to reasonably prove that the CP did not know a statement made to it was false.

Our issue relates to cl 13.1 (a)

"….the CP must be able to reasonably establish that:" ……"and the individual made a false statement"

A CP could never be in a position to reasonably establish that the individual made a false statement.

We request that the Explanation explain what would constitute reasonable steps and how a CP could reasonably prove that the individual is a proper person and what would satisfy the definition of 'reasonable effort'.

Clause 14.1

A discrepancy exists between Code rule 14.1 and the Explanation.

We propose that rule be changed from "both" to "either and that the Explanation clarify the obligation.

Clause 15.1

Issue of "written statement", as it is not always possible to provide. Code must recognise other channels. See our General Comments.

Clause 17.1

We believe this is already covered in the Act and therefore not required in the Code. The current wording is too broad and may restrict a CP from using internal data.

This is already covered – so far as it relates to CPs - by the blanket prohibition in section 21(G) of the Act. See the definition of CP derived information (which is part of credit eligibility information) and the statements in the EM that make it clear that CP derived information is something that a CP has developed using source information from a CRB.
Hence it is unnecessary repetition to have it in the Code.

Clause 17.2

We do not agree that change of address is a valid indicator of a significant default risk.

Clause 18.4

The Act does not give authority to the Code for CRBs to seek credit reporting information. We request ARCA to articulate what authority allows this rule to be included.

CPs require relief for any repercussions that could result in a breach of the PA.

We agree that the customer has the right to a ban period if they believe they are the victim of identity fraud.

Our issue lies with the level of information that a CRB could request to establish whether the individual has been a victim of fraud.

We request that the Code includes an obligation on the CRB to provide a waiver to the CP from the individual giving their consent for the CP to release the information to the CRB.

Clause 20.1

Again, see general comments re means of communication with customers.

Clause 20.5

We have concerns that "accessible means" may be unlimited. We request the Code be amended to articulate that a CP need only take "reasonable steps" and that reasonable costs can be charged, to allow for cost recovery. See TCP Code clause 8.1.1(a)(ii).

Clause 21.1

If the correction request is in relation to credit reporting data of another CP, then the CP contacted should not have to manage that correction request, rather refer the individual to the CP concerned.

Clause 21.3

Suggest that the Explanation be expanded to address the issue of when an individual unreasonably refuses to give consent.

Clause 22.4

As per clause 21.3 - Suggest that the Explanation be expanded to address the issue of when an individual unreasonably refuses to give consent.

Clause 23.1

The record keeping obligations in the Code are particularly onerous for larger telecommunication providers. They go far beyond the requirements of the PA. We request that the Code obligations are aligned with the Act.

This is potentially a very onerous record keeping obligation for CP's, both in terms of the range of information it must retain (which goes significantly beyond what is contemplated in the Privacy Act) and also in terms of the level and quality of that information (a full audit trail).

We propose that:

- (record keeping should be confined to what the Act contemplates) the range of information that must be retained should be limited as much as possible to what is expressly contemplated in the Act or absolutely necessary for compliance. The Act expressly contemplates making a written record of disclosures of credit information to a CRB (section 21D(6)) and uses and disclosures to third parties of credit eligibility information (Section 21G(6)). However, the records proposed in clause 23.1 go far beyond this (and beyond what is required under the current Code) such as recording in a full audit trail all consents, all Data Integrity and destruction steps, all notifications, all other requests etc;

- (other matters should be covered by evidence of compliant systems and processes) Such an obligation is also not consistent with other laws relating to consumer protection, which tend to require only documented systems and processes. For a credit provider to show they are taking adequate steps to comply with the various obligations under Part IIIA and the New CR Code, it should not be necessary for them to be obliged to record every type of handling of regulated information. It should be sufficient if they adequately document (as well as implement) adequate compliance systems and processes.

This requirement is likely to impose substantial IT related costs to comply.

Note that individual consent is not normally retained for 5 years, rather for 2 years. This requirement is excessive.

Clause 24

Clause 24 imposes on CRBs not only extensive obligations in relation to auditing of credit providers but also extensive discretion and rights they can exercise when doing so.

Given the potential impacts and power imbalance that could affect CP's commercial arrangements with CRBs, the following points need to be addressing:

- if a credit provider deals with multiple CRBs, the CRBs should, as far as practicable, use the same auditor/audit process at the same time;
- there should be a common audit standard/manual issued by the Information Commissioner so that as far as practicable CRBs and their auditors will adhere to the same practices;
- CPs should have greater rights to propose and reject auditors on reasonable grounds and to challenge aspects of audits;
- paragraph 24.8, which would require a credit provider to take reasonable steps to rectify issues identified by an audit, should make it clear that such issues would be confined to compliance matters relating to credit reporting data;
- paragraph 24.10, which gives a CRB a wide discretion to take action against a credit provider that fails to comply with the Part IIIA of the Act or the Code, should be subject to an effective process that protects a credit provider from inappropriate/disproportionate action. This could include rights of the credit provider to:

  - be consulted by the CRB;
  - be given opportunities to rectify issues; and
  - be able to escalate proposed decisions to another body which should ideally be, or be endorsed by, the Information Commissioner;
  - have the CRB stop taking action while it is subject to dispute resolution;

The Commissioner should also provide detailed guidance regarding how a CRB should exercise this responsibility.
For completeness, it is not clear that clause 24.10 is subject to clause 24.12, (which provides for a general obligation to resolve disputes) but even if this is the case, it is too general and does not provide sufficient protection to a credit provider.

We suggest the Code requires CRBs to take a practical/reasonable approach in their requests for audits.

Clause 24.9

Data breach notification is part of proposed legislation - Privacy Amendment (Privacy Alerts) Bill – currently under consideration by the Govt as to whether to introduce a mandatory data breach notification scheme.

Regardless of this Bill being passed, this clause should be removed as it is covered by the OAIC Data Breach Notification Guide.

In addition, we have concerns that "serious harm" is not defined.

Clause 25

Acknowledging that credit providers will not be identified to the OAIC, we request changes to the draft such that a CP should be informed by a CRB if any of their alleged material breaches will be reported, as the Commissioner may determine their identity on further inquiries and the CP will then need to be prepared to respond.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 9
32 Walker Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507