Loyalty program assessment: flybuys
Coles Supermarkets Australia Pty Ltd

Summary report
Australian Privacy Principles assessment
Section 33C(1)(a) Privacy Act 1988

Assessment undertaken: November 2015
Draft report issued: June 2016
Final report issued: July 2016
## Contents

Introduction ........................................................................................................................................ 1

Background ........................................................................................................................................ 1

Overview of flybuys ........................................................................................................................ 2

**Key findings — Open and transparent management of personal information** ......................... 2
  Implementing practices, procedures and systems to ensure APP compliance .......................... 2
  Privacy issues — practices, procedures and systems ................................................................. 3
  APP privacy policy ...................................................................................................................... 3
  Privacy issues — privacy policy ................................................................................................. 4
  Recommendation — privacy policy ............................................................................................ 4
  flybuys response ......................................................................................................................... 4

**Key findings — Notification of the collection of personal information (APP 5)** .................... 5
  flybuys registration process ....................................................................................................... 5
  Privacy issues — notification ..................................................................................................... 5

**Key findings — Data analytic activities** ..................................................................................... 5
  Privacy issues — data analytic activities ..................................................................................... 6
  Other findings — secondary cardholders .................................................................................... 7
  Privacy issues — secondary cardholders ..................................................................................... 7
Summary of OAIC’s assessment of flybuys loyalty program

Introduction

The Office of the Australian Information Commissioner (OAIC) undertook a privacy assessment of the Coles flybuys loyalty program (flybuys) to assess whether the program:

- managed personal information in an open and transparent way as required by Australian Privacy Principle (APP) 1
- notified individuals of the collection of personal information in accordance with its APP 5 obligations.

The assessment also considered whether flybuys was adequately describing its main uses and disclosures of information, particularly in relation to any analytical or ‘big data’ activities, in its privacy notices.

Background

Loyalty programs aim to encourage regular customer spending by ‘rewarding’ individuals for purchasing from a particular company or group of companies. In the process, the company operating the loyalty program can collect data about customers’ purchasing activities and, through the application of analytic techniques, use this data for a variety of purposes including targeted advertising and marketing. A study by First Point Research and Consulting found that 88% of Australian consumers over the age of 16 are members of a loyalty program.¹

Big data analytics involves amassing, aggregating and analysing large amounts of data.² International data protection authorities, including the OAIC, have signalled an intention through the Mauritius Resolution on Big Data to closely monitor developments relating to big data.³ Where big data analytics involves the processing of personal information, entities must ensure they are complying with the requirements of the Privacy Act 1988 (the Privacy Act).

The OAIC decided to undertake an assessment of flybuys as it is one of the largest loyalty programs in Australia with over 7.6 million active members (65% of Australian households). Further, given the popularity of loyalty programs amongst Australian consumers, the large amounts of data collected via these programs, and the use of data analytics to process this information, it is in the public interest to ensure that these programs are handling personal information in accordance with the requirements of the APPs.

---

Overview of flybuys

flybuys is jointly owned by Wesfarmers Limited (Wesfarmers) and Coles Supermarkets Australia Pty Ltd (Coles) and is operated by Coles. flybuys is a ‘coalition’ loyalty program where members are able to earn and redeem points and rewards across a wide range of partner entities, including organisations in the retail, financial services, travel, utility and health sectors.

Key findings — Open and transparent management of personal information

The object of APP 1 is ‘to ensure that APP entities manage personal information in an open and transparent way’ (APP 1.1). This enhances the accountability of APP entities for their personal information handling practices and can build community trust and confidence in those practices.

Implementing practices, procedures and systems to ensure APP compliance

APP 1.2 requires an entity to take reasonable steps to implement practices, procedures and systems that will:

- ensure that the entity complies with the APPs, and
- enable the entity to deal with privacy related enquiries or complaints from individuals.

The OAIC was guided by the Privacy management framework in its consideration of the reasonable steps flybuys has taken to address the requirements of APP 1.2.

During the assessment, the OAIC observed that flybuys:

- has appointed key roles and responsibilities for privacy management, including a Privacy Officer and staff responsible for handling privacy enquiries, complaints and access and correction requests
- has a dedicated team that handles internal privacy enquiries, advises project managers on privacy aspects of new project proposals and handles more complex external privacy enquiries, privacy complaints and access and correction requests
- has established a Privacy Council consisting of senior staff drawn from various business units across the Coles Group. The Privacy Council is responsible for setting privacy related policies and procedures, reviewing proposals for offshoring and outsourcing of data, discussing key privacy matters (including external privacy matters reported in the media), changes to privacy legislation and new guidance material issued by the OAIC
- has a range of appropriate reporting mechanisms which are used to routinely inform senior management about key privacy matters
- demonstrates a commitment to privacy by design by requiring new projects involving personal information, including projects involving flybuys data, to receive approval from the Privacy Compliance Manager after consultation with the IT Security area
• has a number of policy and procedural documents that address the handling of information during the information lifecycle and outline how staff are expected to handle personal information in their everyday duties

• requires all new staff to complete an induction program (containing privacy component) and complete mandatory annual privacy training

• has processes for responding to privacy enquiries and complaints about the loyalty program, and responding to access and correction requests from individuals

• has a number of risk management, audit and assurance processes, including an annual risk assessment that sets Coles internal audit and assurance activities

• has a comprehensive privacy breach management procedure which sets out key steps to undertake when responding to a privacy breach or suspected privacy breach

• regularly reviews its privacy practices, procedures and systems. This includes regular review of the flybuys privacy policy, monitoring and reviewing global best practice through the Privacy Council, creating channels for staff to provide feedback about various issues and conducting a simulation exercise to test the effectiveness of Coles’ procedure for responding to a data breach.

Privacy issues — practices, procedures and systems

The assessment indicated that Coles fosters a privacy aware culture and treats personal information as a valuable business asset. In particular, assessors noted the creation of the Privacy Council, which performs a number of key governance functions to ensure Coles and flybuys is meeting its obligations under APP 1.2.

Assessors also note Coles’ efforts to be proactive and to anticipate future challenges as demonstrated by the conduct of a simulation data breach exercise to ensure staff readiness in the event of a data breach and to test that its data breach response procedure was effective.

Assessors did not identify any particular risks regarding the requirements of APP 1.2 and has not made any recommendations in relation to this aspect of the assessment.

APP privacy policy

APP 1 requires entities to have an APP privacy policy explaining how personal information will be managed by the entity. The specific requirements for an APP privacy policy are set out in APPs 1.3, 1.4, 1.5 and 1.6.

Generally, assessors consider that flybuys privacy policy is easy to understand with minimal use of overly complex or technical language. It appears to only include information that is relevant to flybuys’ handling of personal information.

Coles advised that the flybuys privacy policy is reviewed regularly to ensure it is up-to-date and accurately reflects flybuys current information handling practices. The flybuys privacy policy is easily accessible from the flybuys website, is mailed to new members and the sign-up forms also include the flybuys privacy policy.
Privacy issues — privacy policy

APP 1.4(e) requires an APP entity to include in its privacy policy information about how an individual may complain about a privacy breach and how the entity will deal with such a complaint. Where applicable, the privacy policy could also include the procedure for complaining to an external complaint body. flybuys privacy policy does not explicitly outline how an individual may make a privacy complaint and how flybuys will deal with the complaint. The privacy policy does not include information about other complaint avenues (such as the OAIC) that are available to an individual if a complaint is not resolved with flybuys in the first instance.

flybuys could consider improving the navigability of its privacy policy by using a layered approach to assist an individual’s understanding of the information in the policy. A layered approach means providing a condensed version of the full policy to outline key information, with direct links to the more detailed information in the full policy. flybuys could also provide links to the respective privacy policies of its partner entities.

Assessors consider that the privacy policy is generally clearly expressed, however, flybuys could consider providing greater detail around the meaning of some broad terms such as ‘identification information’, ‘household details’, ‘information service providers’ and the circumstances in which it ‘exchanges’ and ‘combines’ personal information with partner entities.

Under APP 1.4(b), a privacy policy must describe an APP entity’s usual approach to holding personal information. This should include how the entity stores and secures personal information. flybuys could consider including further information, in broad terms, around the measures it has in place to protect the security of personal information.

Under APP 1.5, an APP entity is generally expected to make its privacy policy available by publishing it on its website. As a better privacy practice, flybuys could consider providing information either in its privacy policy, or on its website, about how individuals can request or access the privacy policy in other formats.

Recommendation — privacy policy

flybuys should update its privacy policy to include information about how it will deal with a privacy complaint as required by APP 1.4(e). For example, the policy could inform individuals of the different stages in the complaint handling process, that flybuys will respond in a reasonable time (usually 30 days) and that the complaint may then be taken to an external complaint body if the individual is not satisfied with flybuys’ handling of the complaint.

flybuys response

flybuys sincerely appreciates the guidance provided by the OAIC in regard to best practice complaints handling information within a privacy policy and will promptly update our privacy policy to include information about how flybuys will deal with a privacy complaint.

---

4 For an example of a layered approach, see OAIC, Summary of the OAIC’s APP Privacy Policy, OAIC website <www.oaic.gov.au>
Key findings — Notification of the collection of personal information (APP 5)

APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters (listed in APP 5.2) or to ensure the individual is aware of those matters.

flybuys registration process

Individuals are able to join flybuys via a number of channels, including: online; obtaining a hard copy form in-store; obtaining a ‘mini’ in-store sign up (ISU) card and activating the card online; calling the flybuys service centre or when purchasing Coles Financial Services products, such as insurance, credit cards or prepaid cards.

During online registration, the flybuys terms and conditions and flybuys privacy policy are displayed at the bottom of the registration page. An individual is required to check a box to indicate that they accept the flybuys terms and conditions including the flybuys privacy policy.

A condensed version of the flybuys privacy policy is included on hard copy forms. For phone registration, call centre staff are instructed to direct new members to the flybuys privacy policy online and also advise that they will receive a copy of the privacy policy in their flybuys welcome pack. When purchasing Coles Financial Services products, individuals are also provided with a link to the flybuys privacy policy prior to completing their registration.

Privacy issues — notification

Individuals are provided with flybuys terms and conditions and privacy policy at the various points of entry into the program. The purpose of an APP 5 collection notice is to provide an individual with enough information to make an informed decision about whether to provide their personal information to an entity. A privacy policy is generally not sufficient for this purpose because it is more general in nature about the entity’s information handling practices.

Assessors note that flybuys privacy policy provided to individuals at the point of collection describes the information handling practices that are specific to flybuys, rather than the broader information handling practices of Coles. Assessors also note that the specific flybuys privacy policy addresses all of the relevant APP 5.2 content matters.

Generally, the OAIC considers that APP privacy policies should not be used as a substitute for the notice requirements under APP 5. However, for the reasons outlined above, assessors consider that flybuys current notification practices appear reasonable in the circumstances.

Key findings — Data analytic activities

Assessors also considered whether flybuys is adequately explaining its uses and disclosures of personal information, particularly in relation to any analytical or big data activities, in its privacy notices.

Assessors made the following observations about flybuys data analytic activities:
• Access to flybuys data is limited to the flybuys division within Coles. Access is further restricted within this division, with only one team having access to identifiable personal information for the purpose of delivering marketing communications to particular individuals.

• Data analytic activities are conducted internally by a separate analytic area. This area has a restricted view into the flybuys systems and only sees member numbers, transactional data and points balance.

• flybuys collects transaction data from partners in the program only at a level which is necessary to operate the program. Partner organisations do not have access to flybuys data.

• Data is used primarily to conduct targeted marketing campaigns. flybuys analyses the data to identify purchasing patterns and deliver relevant campaigns to members.

• Marketing to members is done through a number of personalised channels, which include emails, website, direct mail, flybuys statements and docket deals. Customer responses to marketing campaigns are also monitored to assist better targeting in future campaigns.

• Analytics may be conducted on behalf of partner entities. Partner entities can request flybuys to conduct certain promotions to members meeting specified criteria appropriate to the partner entity promotion.

• Coles advised that they do not attempt to build profiles about individual customers. At the individual level, they keep a record of the campaigns that have been sent to each customer to avoid repetition or duplication.

• flybuys outsources some functions to overseas operators located in South Africa, the Philippines and the United States of America.

Privacy issues — data analytic activities

Assessors note that flybuys conducts its data analytic activities with de-identified information, and that access to flybuys data is segregated amongst the various areas within the flybuys division.

flybuys privacy policy states that ‘Using personal information, we endeavour to improve our understanding of your interests, suitability, and behaviour in relation to products, services, and offers...’ The privacy policy also specifically states that flybuys may provide marketing communications and targeted advertising which may relate to products and services of interest to the individual. The policy provides information about how an individual can opt out of these direct marketing services.

The policy also describes, in general terms, how flybuys may share information with flybuys partners and other Wesfarmers companies. The policy specifically states that information may be shared with Wesfarmers group companies for ‘data processing’ and ‘data analysis’.

5 Transactional data is essentially what appears on an individual’s receipt when completing a purchase.
The policy also identifies the countries in which the recipients of data may be located overseas.

Based on information provided by staff from the Loyalty Operations and Analytics areas, flybuys uses and disclosures of personal information are consistent with the information provided to individuals in the privacy policy.

**Other findings — secondary cardholders**

Assessors also considered the issue of a primary applicant to flybuys providing the personal information of secondary cardholder(s) during the primary applicant’s registration process against the requirements of APP 3.2 and APP 3.6.

When an individual registers with flybuys they may also register a number of secondary cardholders by providing the secondary cardholder’s personal information to flybuys. The primary applicant (or primary cardholder when the registration is complete) has the ability to provide the secondary cardholder’s name, date of birth, gender and email address.

The flybuys terms and conditions, which the primary cardholder is required to agree to before the registration can proceed, also requires them to confirm that they have obtained the secondary cardholder’s consent to provide their personal information.

The secondary cardholder will then receive an email from flybuys containing an ‘activation link’ and links to the privacy policy and terms and conditions. The individual must click on the activation link to verify their email address to receive electronic direct mail. They will also be sent a welcome pack containing a membership card and the flybuys privacy policy.

**Privacy issues — secondary cardholders**

flybuys privacy policy indicates that the primary purpose of collection is to provide, administer, improve and personalise the flybuys program. The information collected about a secondary cardholder at registration is limited to name, date of birth, gender and email address. flybuys advised that each category of personal information is collected for a specific purpose in order to administer the flybuys program. This includes for security check purposes so flybuys can confirm a member’s identity in the event the member contacts flybuys about their membership, to personalise an individual’s flybuys card and marketing communications, to ensure that age appropriate marketing materials are sent to an individual and to improve the relevance of information and offers sent to members.

In these circumstances, it appears that the categories of information collected about a secondary cardholder are reasonably necessary for flybuys functions and activities in accordance with APP 3.2.

APP 3.6 requires organisations to only collect personal information about an individual only from the individual unless it is unreasonable or impracticable to do so.

flybuys operates on a ‘household’ model and the secondary cardholder function enables individuals to earn and redeem points as a household, rather than as individuals. This enables flybuys to link individuals by household to maximise the points that may be accumulated. In these circumstances, it may not be reasonable or practical for flybuys to
prevent the collection of information about secondary cardholders without an alternative means of linking individuals by household.

Additionally, Coles submitted that it is accepted industry practice and known to consumers that indirect collection of personal information may occur including for travel bookings, health insurance, event registrations and joining clubs/galleries (family membership).

Assessors note that flybuys will not collect any further information about the individual (such as transaction history) unless the secondary cardholder uses the membership card. The secondary cardholder also receives an activation email, alerting the individual to the fact that they have been registered as a flybuys member and providing links to flybuys privacy policy and terms and conditions.

There is a risk that that the secondary cardholder may not receive the activation email in circumstances where the secondary cardholder shares an email address with the primary cardholder or where the primary cardholder enters their own email address as an email contact for the secondary cardholder. However, assessors were advised that individuals are able to contact flybuys and deregister independently of the primary cardholder.

In these circumstances, the OAIC considers that flybuys is meeting the requirements of APP 3.6. flybuys could consider further measures to ensure the secondary cardholder’s active participation in the sign up process. This could include requiring the primary cardholder to enter a separate email address for each secondary cardholder in the household.