ENFORCEABLE UNDERTAKING

Under s 33E of the *Privacy Act 1988 (Cth)*

This undertaking is offered to the Australian Information Commissioner by:

Business Service Brokers Pty Ltd (ACN 069 049 994) (trading as TeleChoice) of 74 Eastern Road, South Melbourne VIC 3205

1 Definitions and Interpretations

1.1 Definitions

In addition to terms defined elsewhere in this undertaking, the following definitions apply:

APP means Australian Privacy Principle.

BSB means Business Service Brokers Pty Ltd (ACN 069 049 994).

Information Commissioner means the person appointed as Australian Information Commissioner under subsection 14(1) of the AIC Act, or pursuant to subsection 21(1) of that Act.

Note: For rules that apply to acting appointments, section 33A of the Acts Interpretation Act 1901 also applies.

Enforceable Undertaking means a written undertaking under s 33E of the Privacy Act given by an entity that the entity will:

(a) in order to comply with the Privacy Act, take specified action

(b) in order to comply with the Privacy Act, refrain from taking specified action, or

(c) take specified action directed towards ensuring that the entity does not do an act, or engage in a practice, in the future that interferes with the privacy of an individual.

OAIC means the Office of the Australian Information Commissioner.

Privacy Act means the *Privacy Act 1988* (Cth).

1.2 Interpretation

Unless the contrary intention appears, terms defined in the Privacy Act have the same meaning in this Enforceable Undertaking as they have in the Privacy Act.

2 Background

2.1 BSB (trading as TeleChoice) is a body corporate incorporated in Australia, and an organisation within the meaning of s 6C of the Privacy Act. As such, it is an APP entity under the Privacy Act and is required to comply with the Privacy Act and the APPs. It provides telecommunications services to individuals and to organisations.

3 Commissioner initiated investigation

3.1 Under s 40(2) of the Privacy Act, the Commissioner may, on the Commissioner's own initiative, investigate an act or practice that may be an interference with the privacy of an individual or a breach of APP 1 if the Commissioner thinks it desirable that the act or practice be investigated.

3.2 On 18 May 2015, the Commissioner (who was then the Australian Privacy Commissioner) initiated an investigation into BSB in relation to the privacy incident outlined below (the '**Privacy Incident**').

3.3 ***Privacy Incident details***

3.3.1 On 23 April 2015, a news and current affairs television program broadcast footage that showed shipping containers that held documents belonging to BSB, open and apparently accessible to members of the public in Victorian bushland.

3.3.2 The documents contained personal information relating to former BSB customers. They included copies of telecommunication services contracts entered into by customers and copies of customer identification documents (such as drivers' licenses, passports, and other identification material).

3.3.3 On 24 April 2015, BSB provided the OAIC with a voluntary data breach notification to advise the OAIC of the privacy incident and the initial steps taken by BSB in response to the incident. On the same day, BSB destroyed the documents held in the containers.

3.3.4 In its subsequent investigations, BSB determined that the information had been stored within the shipping containers from approximately June 2013 to 23 April 2015 while awaiting destruction by a document destruction contractor. The shipping containers were initially stored on a fenced property in Bentleigh East, Victoria, before being moved to a location in Hastings in January 2015. The property in Hastings was private land, but was unfenced and physically accessible to members of the public.

3.3.5 The containers were locked and checked monthly by a BSB employee to ensure continuing security. However, the containers were broken into by an unknown person at some time after BSB's latest maintenance visit, which BSB states occurred approximately two weeks before 23 April 2015.

3.3.6 BSB is unable to determine which individuals had personal information stored in the containers. As such, the personal information may have related to any individual who was a BSB customer prior to 31 March 2013.

3.4 ***Issues under investigation***

3.4.1 APP 11.1 requires BSB to take reasonable steps to protect the personal information it holds from misuse, interference and unauthorised access and disclosure. APP 11.2 requires BSB to take reasonable steps to destroy, or de-identify, information when it is no longer required.

3.4.2 The Commissioner commenced the investigation on 18 May 2015 for the purpose of determining whether BSB had breached APP 11.1 and 11.2.

3.5 ***Acknowledgment of breach by BSB***

3.5.1 BSB have acknowledged to the Commissioner that the privacy incident constitutes a breach of APP 11.1. Some of the information held in the shipping containers was personal information. The shipping containers were locked, checked periodically and located on private land. However, the containers were not adequately secured from physical access. BSB did not take reasonable steps to prevent access to them by unauthorised persons.

3.5.2 BSB have also acknowledged to the Commissioner that the privacy incident constitutes a breach of APP 11.2. Whilst the personal information stored in the shipping containers was awaiting destruction, this could reasonably have occurred at some time between when the documents were no longer required, and the date on which they were destroyed, 24 April 2015. BSB did not take reasonable steps to destroy or de-identify that personal information once it was no longer required.

3.5.3 To address the privacy incident and to prevent similar incidents occurring in the future, BSB offers this enforceable undertaking under s 33E of the Privacy Act.

3.6 ***Regulatory outcome***

3.6.1 The Commissioner acknowledges that BSB has cooperated with the investigation, including acknowledging that it has breached APP 11.1 and APP 11.2, and agreeing to take steps to address the breach and prevent further breaches from reoccurring. BSB has also offered to take steps to address possible harm to affected individuals. Accordingly, the Commissioner formed the view that the acceptance of an enforceable undertaking offered by BSB would be an appropriate regulatory outcome of the Commissioner's investigation.

3.6.2 In summary, BSB undertakes to:

a) offer to reimburse the cost of a 12-month credit monitoring service for any individuals who were BSB customers prior to 31 March 2013, and are

concerned about the possibility of credit fraud as a consequence of the incident

b) conduct a review of the personal information BSB holds to ensure it is secure

c) establish written policies and procedures regarding storage and destruction of customer personal information

d) in consultation with the OAIC, engage a qualified third party to review certain aspects of BSB's handling of customer personal information and implement any subsequent recommendations

e) develop and conduct regular privacy training for staff

f) finalise and implement a data breach response plan.

3.6.3 At the time that BSB offered and the Commissioner accepted this enforceable undertaking, BSB had already commenced the actions outlined in paragraph 4.3.

3.7 ***Regard to objects of the Act***

3.7.1 Under s 29 of the Privacy Act, the Commissioner must have due regard to the objects of the Act (set out in s 2A of the Privacy Act) in performing the Commissioner's functions, and exercising the Commissioner's powers, conferred by that Act.

3.7.2 The OAIC has also published its Privacy regulatory action policy which explains the OAIC's powers and its approach to using its privacy regulatory powers and making related public communications.

3.7.3 The Commissioner has had regard to the objects of the Privacy Act and the Privacy regulatory action policy in commencing the investigation and accepting the enforceable undertaking.

3.8 ***Commencement date***

3.8.1 This undertaking comes into effect when:

a) the undertaking is executed by BSB; and

b) the executed undertaking is accepted by the Commissioner

(the '**Commencement date**').

4 Undertaking

4.1 ***Notifying potentially affected individuals***

4.1.1 BSB undertakes to, within two weeks of the commencement date provide a contact point for concerned individuals and list the contact point on BSB's website, together

with information informing individuals about how they can take up its offer to provide credit protection services as set out in clause 4.2.

4.2 ***Offer of credit protection to potentially affected individuals***

4.2.1 BSB is unable to identify precisely which individuals had personal information stored in the containers at the time of the incident. As such, for the purpose of this undertaking, '**potentially affected individual**' means any person who was a BSB customer or who signed up to a telecommunications service with the assistance of BSB prior to 31 March 2013.

4.2.2 BSB undertakes to reimburse the cost of a 12 month subscription to a credit protection service if any potentially affected individual is concerned about the possibility of credit or identity fraud as a consequence of the incident. The individual must be able to reasonably demonstrate to BSB that he or she was a customer of BSB prior to 31 March 2013 (for example, by providing copies of correspondence with BSB or other supporting material such as a statutory declaration).

4.3 ***General obligations when handling customer personal information***

4.3.1 BSB undertakes to handle customer personal information in accordance with BSB's obligations under the Privacy Act.

4.3.2 BSB undertakes to handle customer personal information in accordance with BSB's Customer Information Handling Policy and APP privacy policy.

4.4 ***Establish policies and procedures***

4.4.1 BSB undertakes to, within three months of the commencement date:

a) establish and finalise, written policies and procedures about the storage of customer personal information including the conduct of regular audits of BSB's records of customer personal information

b) establish and finalise, written policies and procedures about the destruction of customer personal information, including when and how paper based records are to be destroyed

c) finalise and implement a new data breach response plan in consultation with the OAIC.

4.5 ***Privacy training for staff***

4.5.1 BSB undertakes to:

a) develop and finalise, within three months of the commencement date, privacy training for BSB staff members about BSB's obligations under the Privacy Act, including:

(i) training on securing personal information and its destruction

(ii) training on how BSB's privacy obligations apply to staff member's roles, for example, by including scenario-based training, and

(iii) testing of staff members' understanding at the completion of the training

b) require all current BSB staff to complete the privacy training of subparagraph 4.5.1(a) within six months of the commencement date

c) require all new BSB staff to complete privacy training as a part of their induction training when they commence employment

d) require all BSB staff to complete refresher privacy training at least annually

e) retain appropriate records of the privacy training all BSB staff have completed or are required to complete.

4.6 ***Reviews and recommendations***

4.6.1 BSB undertakes to conduct and complete a review and prepare a report within three months of the commencement date that will identify all records of customer personal information it holds (including hardcopy records) and confirming that the personal information is held in accordance with BSB's obligations in APP 11.

4.6.2 BSB undertakes to engage, in consultation with the OAIC, an appropriately experienced, qualified and independent third party (**'the Reviewer'**) to review BSB's practices and procedures as specified in paragraph 4.6.3.

4.6.3 BSB undertakes to engage the Reviewer to:

a) review BSB's practices and procedures (including collection, record keeping, security and record destruction practices and procedures) to assess whether BSB is holding customer personal information in accordance with APP 11.1, and to identify possible areas for improvement

b) review BSB's record keeping and record destruction practices and procedures to assess whether BSB is holding customer personal information in accordance with APP 11.2, and to identify possible areas for improvement

c) where areas for improvement are identified:

(i) make recommendations for how BSB could implement those improvements (**Recommendations**)

(ii) make recommendations as to the time it would reasonably take for BSB to implement the recommendations.

d) finalise a report of the review set out in paragraph 4.6.2 within six months of the commencement date.

4.7 ***Provision of review information to the OAIC***

4.7.1 BSB undertakes to provide the OAIC with a copy of the report referred to in paragraph 4.6.1 within two weeks of its completion, and not later than four months from the commencement date.

4.7.2 BSB undertakes to provide the OAIC with a copy of the Reviewer's report referred to in sub-paragraph 4.6.3(d), including recommendations, within two weeks of receiving it, and not later than seven months from the commencement date.

4.8 ***Implementation of recommendations***

4.8.1 With regard to the Recommendations the Reviewer makes, referred to in sub-paragraph 4.6.3(c)(i), BSB undertakes to:

a) provide the OAIC with a project plan ('the **project plan**') to implement the Recommendations in accordance with the time recommendations referred to in sub-paragraph 4.6.3(c)(ii)

b) implement the project plan to address the Recommendations in accordance with the dates set out in the project plan

c) provide confirmation to the OAIC that the project plan has been completed.

4.9 ***Other matters***

4.9.1 BSB will pay the costs of its compliance with this enforceable undertaking.

4.9.2 BSB and its officers, employees or agents, will not make any statement, orally, in writing, or otherwise, which conveys or implies anything inconsistent with the content of this enforceable undertaking.

4.9.3 BSB will provide all documents and information requested by the OAIC from time to time for the purpose of assessing BSB's compliance with the terms of this enforceable undertaking.

5 Acknowledgments

5.1 BSB acknowledges that the Commissioner:

(a) may issue a media release, conduct interviews or publish social media posts on execution of this undertaking referring to its terms and to the circumstances which led to the Commissioner's acceptance of the undertaking;

(b) may from time to time publicly refer to this undertaking, including any breach of this undertaking by BSB; and

(c) will publish this undertaking as well as a summary of the undertaking, on the OAIC website.

5.2 BSB acknowledges that:

(a) the Commissioner's acceptance of this undertaking does not affect the OAIC's power to investigate, or pursue other enforcement options available to the Commissioner in relation to any contravention not the subject of the background section of this enforceable undertaking, or arising from future conduct;

(b) this undertaking in no way derogates from the rights and remedies available under the Privacy Act to any other person, arising from any conduct described in this undertaking or arising from future conduct.

5.3 ***Confidentiality of information received***

5.3.1 The Commissioner and OAIC acknowledge that information provided by BSB in accordance with this undertaking may contain sensitive commercial information ('commercial-in-confidence information').

5.3.2 The Commissioner and OAIC acknowledge that any such commercial-in-confidence information is provided by BSB in confidence.

5.3.3 The Commissioner and OAIC:

(d) will only publish or otherwise disclose any commercial-in-confidence information with BSB's written agreement; and

(e) will only use any commercial-in-confidence information for the Commissioner's privacy regulatory activities.

Signed by:

Ehab Abdou
Chief Executive Officer
Business Service Brokers Pty Ltd
trading as TeleChoice

Date

Accepted by Timothy Pilgrim, Acting Australian Information Commissioner, under s 33E of the Privacy Act:

Timothy Pilgrim

Date