ENFORCEABLE UNDERTAKING

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

This undertaking is offered to the Australian Privacy Commissioner by:

Singtel Optus Pty Ltd ACN 052 833 208
1 Lyonpark Road, Macquarie Park NSW 2113

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.

ASAE 3100 means the Australian Standard on Assurance Engagements ASAE 3100 *Compliance Engagements*, issued by the Australian Auditing and Assurance Standards Board.

Commissioner means the Australian Privacy Commissioner.

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.

Optus means Singtel Optus Pty Ltd ACN 052 833 208.

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 Optus is a body corporate incorporated in Australia, and an organisation within the meaning of s 6C of the Privacy Act.

2.2 Optus engages in the business of providing communications services to customers, including to individuals, in Australia. Optus holds personal information provided to it by its customers, including the names, addresses and phone numbers of those customers, and is required by the Privacy Act and the APPs to take reasonable steps to protect the personal information it holds.

2.3 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.

2.4 On 28 July 2014, the Commissioner initiated an investigation into Optus in relation to the incidents outlined below, being acts or practices which may have interfered with the privacy of Optus customers (the '**Privacy Incidents**').

2.5 ***Privacy Incident Details***

'White Pages' incident

2.5.1 Optus maintains and operates a website at www.optus.com.au. In February 2013, Optus made a change to its website. Due to a coding error that occurred during this change, between February 2013 and April 2014, when Optus customers who had elected not to have their details listed in a telephone directory completed a rate plan change via Optus's website, Optus's systems erroneously changed the White Pages listing preferences for those customers from 'No' to 'Yes'. As a result, the names, addresses and mobile phone numbers of approximately 122,000 Optus customers were listed in the White Pages online directory without the consent of those customers. The information of the majority of those customers was also published in various print editions of the White Pages.

2.5.2 Optus was made aware of the issue through a customer complaint in April 2014, and notified the OAIC about the issue on 3 June 2014.

'*Modem*' incident

2.5.3 Optus made a change to its network in relation to particular Netgear and Cisco modems, which it began deploying in November 2008 and March 2009 respectively. As part of the change, Optus deliberately left the management ports for these models of modems open, incorrectly assuming they were only accessible for network management purposes. In addition, Optus issued 197,000 of the Netgear modems and 111,000 of the Cisco modems to its customers with factory default settings, including user default names and passwords in place. Optus also did not conduct connectivity testing. These two issues in combination meant that Optus customers

using the equipment who did not change the default user name and passwords were left vulnerable, potentially allowing a person to make and charge calls as though they were the Optus customer.

2.5.4 Optus became aware of the issue through the media in early April 2014,[1] and notified the OAIC about the issue on 17 April 2014. On or about 4 April 2014, Optus closed off the vulnerability by implementing access controls and modifying configuration files on all affected and newly dispatched modems to harden security on these modems by enforcing stronger password protection.

2.5.5 There is no evidence that this security vulnerability was exploited.

'*Voicemail*' incident

2.5.6 Between September 2013 and 13 May 2014, a flaw in Optus's security processes led to certain customers not being prompted for their password when attempting to retrieve voicemail information from outside the Optus network. Optus did not identify the issue during testing. Consequently, where customer voicemail accounts were not password protected, some Optus customers were vulnerable to 'spoofing' attacks, where an unauthorised party could potentially access and use customer voicemail accounts messages, including being able to listen to recorded messages and change settings and preferences.

2.5.7 Optus was made aware of the issue by a third party on 28 April 2014, and notified the OAIC about the issue on 14 May 2014.

2.6 ***Issues of concern to the Commissioner***

2.6.1 Information provided by Optus in relation to the Privacy Incidents suggests that Optus did not have reasonable steps in place to safeguard the personal information held in its systems at the time the incidents occurred, and as required by APP 11.

2.6.2 That information also raised the following issues of concern to the Commissioner:

(a) The security of personal information of a large number of individuals was compromised as a result of each of these incidents (over 100,000 in each incident).

(b) The incidents created a risk of harm for affected individuals. In particular, the White Pages incident resulted in the disclosure of the contact information of silent line customers, which the Commissioner has previously found can

[1] As reported in the Sydney Morning Herald, 4 April 2014, *www.smh.com.au/it-pro/security-it/default-password-leaves-tens-of-thousands-of-optus-cable-subscribers-at-risk-20140403-zqprz.html*

create significant risks for affected individuals.[2] The White Pages incident was also the subject of individual privacy complaints to the OAIC.

(c) The security measures in place were not reasonable to protect the personal information that Optus held, particularly in relation to the White Pages incident.

(d) In each case, there was a failure by Optus to detect the incidents; the incidents were brought to Optus's attention by third parties. This resulted in Optus experiencing substantial delays in taking action to contain each incident, which also prolonged the duration of the risk to affected individuals.

2.6.3 The Commissioner is concerned to ensure that Optus adequately addresses the general issue set out in paragraph 2.6.1, and the specific issues set out in paragraph 2.6.2.

2.6.4 Optus acknowledges the Commissioner's concerns, and offers this enforceable undertaking under s 33E of the Privacy Act to address those concerns.

2.7 ***Regulatory outcome***

2.7.1 The Commissioner acknowledges that Optus has cooperated with the investigation, including taking steps to respond to the Commissioner's concerns. Accordingly, the Commissioner formed the view that the acceptance of an enforceable undertaking offered by Optus would be an appropriate regulatory outcome of the Commissioner's investigation.

2.7.2 At the time that Optus offered and the Commissioner accepted this enforceable undertaking, Optus had already commenced the actions outlined in paragraphs 3.1.3(c)(i)—(iv) below. This undertaking includes the additional actions in paragraphs 3.1.3 (a)—(b) to address the Commissioner's particular concerns.

2.7.3 This undertaking requires Optus to:

(a) complete the reviews and certifications as set out in paragraph 3 (some of which have already commenced);

(b) provide copies of those reviews and certifications to the OAIC;

(c) implement any recommendations and rectify deficiencies identified in those reviews and certifications; and

(d) provide a report by an independent third party to the OAIC certifying that the specified actions have been completed.

---

[2] See, e.g., Office of the Australian Information Commissioner, *Telstra Corporation Limited: Own motion investigation report*, http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-omi-march-2014.

2.8 ***Regard to objects of the Act***

2.8.1 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.

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

2.8.3 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.

2.9 ***Commencement date***

2.9.1 This undertaking comes into effect when:

(a) the undertaking is executed by Optus; and

(b) the executed undertaking is accepted by the Commissioner

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

3 Undertaking

3.1 ***Independent* reviews *and recommendations***

3.1.1 Optus undertakes, within 14 days of the Commencement date, to engage, in consultation with the OAIC, an appropriately experienced and qualified independent third party (the '**Auditor**') to conduct the reviews and certifications listed in paragraph 3.1.3. Optus will engage the Auditor to conduct the reviews and certifications in accordance with ASAE 3100, and in accordance with the reporting timeframes provided for in paragraph 3.2.

3.1.2 Optus undertakes to engage the Auditor, for each of the reviews and certifications listed in paragraph 3.1.3, to:

(a) express a conclusion as to whether Optus's practices, procedures and systems are reasonable to protect the personal information Optus holds from misuse, interference or loss, or unauthorised access, modification or disclosure; and

(b) where compliance deficiencies with the Privacy Act are identified:

(i) make recommendations to improve Optus' practices and procedures to achieve compliance ('**Recommendations**'); and

(ii) make recommendations as to the time it would reasonably take for Optus to implement those recommendations set out above in sub-

paragraph (i), having regard to matters including, the risk posed by the potential vulnerability and the complexity of systems and network infrastructure.

3.1.3 The Auditor will conduct the following reviews and certifications:

(a) a review of the additional security measures Optus adopted in response to the Privacy Incidents ('**Review A**'). These additional security measures include:

(i) Enhancing Optus's monitoring program of change management that has the potential to affect the security of its customers' personal and sensitive information;

(ii) Enhancing Optus's penetration testing: for fixed and mobile services; on all major IT projects as part of Optus's Security Risk Assessment process; and as part of its annual monitoring program.

(b) a review of Optus's vulnerability detection processes across the organisation concerning the security of personal information ('**Review B**').

(c) certifications of the following reviews and assessments that Optus has carried out or arranged for an appropriately qualified independent third party to carry out:

(i) A privacy incident review for the 'Modem' incident, 'Voicemail' incident and 'White Pages' incident ('**Certification A**'), and

(ii) A service level security posture assessment as set out in Confidential Schedule A ('**Certification B**');

(iii) An architecture review of Optus's principal IT systems (top 20 applying a risk based approach) involved in storing and handling personal information ('**Certification C**'); and

(iv) A review of Optus' new voicemail platform as set out in Confidential Schedule B ('**Certification D**').

3.1.4 Optus undertakes to provide to the OAIC, within 14 days of the Commencement date, a copy of the terms of engagement pursuant to which the Auditor is engaged to conduct the reviews and certifications.

3.2 ***Provision of reviews and certifications to the OAIC***

3.2.1 Optus undertakes to provide a copy to the OAIC of the Auditor's reports concerning Review A, Review B, Certification A and Certification D within 14 days of receiving each report from the Auditor, and not later than 3 months from the Commencement date.

3.2.2 Optus undertakes to provide a copy to the OAIC of the Auditor's reports concerning Certification B and Certification C within 14 days of receiving each of those reports from the Auditor, and not later than 6 months from the Commencement date.

3.3 ***Implementation* of *Recommendations***

3.3.1 Optus undertakes to provide to the OAIC a project plan to implement the Recommendations made in the Auditor's reports set out above in paragraph 3.2.1 within 5 months from the Commencement date, such project plan to accord with the recommendations as to implementation timeframes made by the Auditor under paragraph 3.1.2(b)(ii).

3.3.2 Optus undertakes to provide to the OAIC a project plan to implement the Recommendations made in the Auditor's reports set out above in paragraph 3.2.2 within 8 months from the Commencement date, such project plan to accord with the recommendations as to implementation timeframes made by the Auditor under paragraph 3.1.2(b)(ii).

3.3.3 Optus undertakes to:

(a) Implement the project plans referred to in paragraphs 3.3.1 and 3.3.2; and

(b) Engage the Auditor:

(i) within 18 months of the Commencement date, to certify that Optus has implemented the Recommendations and rectified deficiencies identified in accordance with the timetable set out in the project plans; or

(ii) in the event that the timetable set out in the project plans requires longer than 18 months for implementation and rectification, to provide an interim report at 18 months and every six months thereafter as to the state of Optus' compliance, until the above certification can be provided;

(c) Provide to OAIC a copy of each report or certification referred to in paragraph 3.3.3(b) within 14 days of receiving that report or certification.

3.4 ***Other matters***

3.4.1 Optus will pay the costs of its compliance with this enforceable undertaking.

3.4.2 Optus 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.

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

3.4.4 Optus nominates David Epstein, VP, Corporate & Regulatory Affairs, Optus as the person tasked with ensuring the establishment and operation of Optus's Privacy Compliance Monitoring and Reporting Framework. Optus has provided the OAIC with this person's contact details.

4 Acknowledgments

4.1 Optus acknowledges that the Commissioner:

(a) may issue a media release, media interview or 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 Optus; and

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

4.2 Optus 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.

4.3 Optus acknowledges that the Commissioner had a reasonable basis to be concerned that the conduct of Optus described in the background section to this undertaking may have interfered with the privacy of individuals.

Confidentiality of information received

4.4 The Commissioner and OAIC acknowledge that audit scopes, reports, reviews, audits and assessments that are provided by Optus in accordance with this undertaking are likely to contain sensitive commercial information and security protocols ('**commercial-in-confidence information**'), which if publicly disclosed, have the potential to undermine the security of Optus's network and systems and consequently its customers' personal information.

4.5 The Commissioner and OAIC acknowledge that this commercial-in-confidence information is provided by Optus in confidence.

4.6 The Commissioner and OAIC:

(a) will only publish or otherwise disclose the commercial-in-confidence information with Optus's written agreement; and

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

Signed by:

Allen Lew, CEO Optus

Date

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

Timothy Pilgrim

Date