Annual Customer Proprietary Network Information Certification
for Calendar Year 2017

Pursuant to 47 C.F.R. § 64.2009(e)
EB Docket No. 06-36

February 2018

Name of Company: Telstra Incorporated
Form 499 Filer ID: 819740
Name of Signatory: Amy G. Rosen
Title of Signatory: General Counsel

I, Amy G. Rosen, certify that I am an officer of Telstra Incorporated ("Company"), and acting as an agent of Company, that I have personal knowledge that Company has established operating procedures that are adequate to ensure compliance with the Federal Communications Commission's ("FCC") CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how Company's procedures ensure Company is in compliance with the requirements set forth in sections 64.2001 *et seq.* of the FCC 's rules.

Company has not taken any actions (instituted proceedings or filed petitions at either state commissions, courts, or at the FCC) against data brokers in 2017. Company has no information outside of FCC Docket No. 96-115, or that is not otherwise publicly available (*e.g.*, through news media), regarding the processes pretexters are using to attempt to access CPNI. The steps Company has taken to protect CPNI include regularly monitoring its CPNI practices and procedures and conducting training designed to ensure compliance with FCC's CPNI rules.

Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Amy G. Rosen
General Counsel
Telstra Incorporated

Date: 2-28-18

Customer Proprietary Network Information Certification
Attachment A

Company has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("FCC") rules pertaining to customer proprietary network information ("CPNI") set forth in sections 64.2001 – 64.2011 of the FCC's rules. This attachment summarizes those practices and procedures, which have been updated so that they are adequate to ensure compliance with the FCC's CPNI rules.

Safeguarding against pretexting

- Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, including the authentication of customers in accordance with FCC rules prior to disclosing CPNI based on customer-initiated contacts. Company is committed to notify the FCC of any novel or new methods of pretexting it discovers and of any actions it takes against pretexters and data brokers.

Training and discipline

- Company trains its supervisory and non-supervisory personnel in an effort to ensure that its employees, in accordance with FCC regulations: (a) understand what CPNI is, (b) join in and carry-out Company's obligation to protect CPNI, (c) understand when they are and when they are not authorized to use or disclose CPNI, and (d) keep records regarding customer complaints regarding CPNI and the use of CPNI for marketing campaigns.

- Company employees are required to review Company's CPNI practices and procedures and to acknowledge their comprehension thereof.

- Company has an express disciplinary process in place for violation of the company's CPNI practices and procedures. The careless or intentional failure to comply with these practices and procedures may result in disciplinary action, up to and including discharge.

Company's use of CPNI

- Company may use CPNI for the following purposes:

  - To initiate, render, maintain, repair, bill and collect for services;
  - To protect its property rights; or to protect its subscribers or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services;
  - To provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent.
  - To market additional services to customers that are within the same categories of service to which the customer already subscribes;
  - To market services formerly known as adjunct-to-basic services; and
  - To market additional services to customers *with the receipt of informed consent via the use of opt-in or out-out, as applicable.*

- Company does not disclose or permit access to CPNI to track customers that call competing service providers.

- Company will disclose and permit access to CPNI where required by law (*e.g.*, under a lawfully issued subpoena).

Customer approval and informed consent

- Company currently does not use CPNI for marketing communications-related services outside the basket of service to which the customer subscribes. Prior to using CPNI in instances where approval is required, Company will implement a system to obtain approval and informed consent from its customers in accordance with FCC rules. This system also will allow for the status of a customer's CPNI approval to be clearly established prior to the use of CPNI. Records of approval will be maintained for at least one year.

- **One time use.** After authentication, Company may use oral notice to obtain limited, one-time approval for use of CPNI for the duration of a call. The contents of such notice will comport with FCC rule 64.2008(f).

Additional safeguards

- Company will maintain for at least one year records of all marketing campaigns that use its customers' CPNI, including a description of each campaign and the CPNI used, the products offered as part of the campaign, and instances where CPNI was disclosed to third parties or where third parties were allowed access to CPNI. Such campaigns are subject to a supervisory approval and compliance review process, the records of which also are maintained for a minimum of one year.

- Company has established a supervisory review process designed to ensure compliance with the FCC's CPNI rules for outbound marketing situations and maintenance of records.

- Company designates one or more officers, as an agent or agents of the company, to sign and file a CPNI compliance certificate on an annual basis. The certificate conforms to the requirements set forth in FCC rule 64.2009(e).

- Company will provide written notice to the FCC in accordance with the requirements of FCC rule 64.2009(f) if ever its opt-out mechanisms malfunction in the manner described therein.

- For customers with a contract that specifically addresses Company's protection of CPNI, a dedicated account team authenticates the customer's Authorized Representative without the use of readily available biographical or account information with respect to customer-initiated telephone inquiries regarding or requiring access to CPNI.

- For customers without a contract that specifically addresses Company's protection of CPNI, Company only provides CPNI during a customer initiated telephone call if the customer provides a customer-specific password.

- If the dedicated account team is unable to verify the Authorized Representative or the customer is unable to provide the password, then Company only discloses call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record.

- For online customer access to CPNI, Company only provides CPNI if a customer provides the correct customer-specific password. To the extent Company provides such access, Company establishes passwords and has employed back-up authentication for lost or forgotten passwords consistent with the requirements of FCC rule 64.2010(e).

- Company does not have any retail locations where customers may access CPNI.

- For common carrier services, Company notifies customers immediately of any account changes, including address of record, authentication, online account and password related changes.

- In the event of a breach of CPNI, Company will notify law enforcement as soon as practicable and no later than seven (7) business days from discovering the breach. Customers will be notified after the seven (7) day period, unless the relevant investigatory party directs Company to delay notification, or Company and the investigatory party agree to an earlier notification. Company will maintain a record of all CPNI security breaches, including a description of the breach and the CPNI involved, along with notifications sent to law enforcement and affected customers.