ACCC

AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

Telstra's Structural Separation Undertaking

Annual compliance report 2018–19

February 2020

ISBN 978 1 920702 05 2

Australian Competition and Consumer Commission
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 02/20_1648

www.accc.gov.au

AUSTRALIAN COMPETITION & CONSUMER COMMISSION

EXECUTIVE OFFICE

23 Marcus Clarke Street
Canberra ACT 2601

GPO Box 3131
Canberra ACT 2601

tel: (02) 6243 1111

www.accc.gov.au

10th December 2019

The Hon. Paul Fletcher
Minister for Communications, Cyber Safety and the Arts
Parliament House
CANBERRA, ACT, 2600

Dear Minister

ACCC report on Telstra's compliance with its Structural Separation Undertaking

The Australian Competition and Consumer Commission (ACCC) is required under the *Telecommunications Act 1997* (the Act) to monitor and report each financial year on breaches by Telstra of an undertaking in force under section 577A of the Act (Telstra's Structural Separation Undertaking).

Enclosed is the ACCC's report for the 2018-19 financial year. Please note that subsection 105C(3) of the Act requires you to table the report in each House of Parliament within 15 sitting days of that House after receiving the report.

Yours sincerely

Rod Sims
Chair

Contents

1. Introduction

The ACCC accepted a Structural Separation Undertaking (SSU) from Telstra on 27 February 2012. Telstra's migration plan, which forms part of the SSU, commenced operation on 7 March 2012.[1] The SSU and the migration plan together specify Telstra's commitments to progressively migrate its fixed line voice and broadband customers onto the NBN and promote equivalence and transparency during the migration period. These commitments are fundamental to promoting competitive outcomes during this period.

Section 105C of the Telecommunications Act 1997 (the Act) provides that each financial year, the ACCC must monitor and report to the Minister for Communications on any breaches by Telstra of its SSU.

This report outlines breaches of the SSU by Telstra between 1 July 2018 and 30 June 2019 and the steps Telstra has taken, or proposes to take, in order to remedy these breaches.

During the year, Telstra has reported four information security breaches and one network notification breach under the SSU. Chapter 2 provides more details in relation to these breaches.

During 2018–19, the ACCC approved one request from Telstra to vary its Migration Plan. The ACCC also provided regulatory forbearance on four occasions regarding proposed non-compliance by Telstra with its Migration Plan obligations, in order to promote service continuity and a better migration experience for end users. Chapter 3 provides more details in relation to the migration plan variations and regulatory forbearance regarding Migration Plan obligations.

This report is the ACCC's 8th SSU Annual Compliance report. Telstra's compliance with the SSU has improved relative to the early years of the undertaking. Over the initial four years the undertaking was in place (2011/12–2014/15), a total of 52 breaches were reported by Telstra. Over the past four years (2015/16–2018/19), Telstra has reported a total of 21 breaches, with an increase in 2018/19 (five breaches) compared to the previous year (three breaches in 2017/18).

The ACCC expects that the measures that have been implemented by Telstra to improve compliance with the SSU over the eight years it has operated, should by now have ensured breaches would not occur. With the NBN migration still underway, we emphasise the importance of Telstra eliminating SSU breaches and promoting equivalence and transparency during the remainder of the migration period.

1 Section 577BC of the Telecommunications Act 1997 requires Telstra to submit a migration plan to the ACCC once the SSU is in force.

2. Breaches of the SSU

This section details four information security matters and one network notification matter where the ACCC considers, on the balance of probabilities, that Telstra breached its SSU obligations.

2.1 Information Security

The SSU contains information security obligations designed to safeguard Protected Information obtained by Telstra in the course of supplying regulated services to wholesale customers. Because of Telstra's vertically integrated wholesale-retail structure, Protected Information could potentially be used to Telstra's advantage in downstream retail markets.

Telstra's information security obligations are contained in clause 10 of the SSU. These obligations include:

- a strict prohibition on the disclosure of Protected Information to retail business units unless the wholesale customer has authorised the disclosure
- a prohibition on Telstra using or disclosing Protected Information in a way that would be likely to enable its retail business units to gain or exploit an unfair commercial advantage over its wholesale customers
- further restrictions on disclosing other information to retail business units unless, with the approval of the ACCC, it makes the information available to wholesale customers at the same time.

Importantly, Telstra must protect any:

- confidential or commercially sensitive information obtained directly from wholesale customers for the purpose of, or in the course of, Telstra supplying regulated services such as the end user's name, address and service type
- confidential and commercially sensitive information derived from the above information (such as billing or service usage information) that would identify a wholesale customer or its end-users.

Item 1—Full National Number disclosed under ticketing system

Breach	Cause
In August 2018, Telstra identified four instances where a Wholesale Customers' Full National Number (FNN) was provided to Telstra retail staff. This information is protected under clause 10.1 of the SSU.	Telstra explained that this protected information was unintentionally provided to retail staff by Telstra Network Services Business Unit staff.

Remediation

Telstra advised that it has provided training on Telstra's SSU compliance responsibilities to the staff members involved in the disclosure of FNNs. Telstra also advised that it has continued to provide refresher training to staff on Telstra's obligations under the SSU and issued regular reminder notices to staff about their information security responsibilities.

ACCC view

The ACCC is satisfied that the actions taken by Telstra were appropriate in minimising the risk of recurrence of the SSU breach.

Items 2 and 3—Disclosure of wholesale customers' end user information

Items 2 and 3 concern two incidents regarding disclosure of wholesale customers' protected information (WCPI) that occurred during 2018–19, relating to the NBN migration process for two of Telstra's 'special services',[2] ISDN2[3] and CustomNet.[4]

Both incidents occurred in part due to a failure in one of Telstra's computer systems which led to WCPI being made accessible to Telstra retail staff. The ACCC used information provided by Telstra as well as information from affected wholesale customers to assess these incidents.

Item 2—Disclosure of WCPI – ISDN2

Breach	Cause
In January 2019, Telstra received a complaint through the Accelerated Investigations Process (AIP)[5] about wholesale customer end user information for ISDN2 products being made available to Telstra retail staff. As part of its investigation of this complaint Telstra examined its computer system[6] records and found that Telstra's wholesale customer end user information for ISDN2 products had been available to Telstra retail staff between August 2018 and February 2019, in breach of clauses 10.3 and 10.4 of the SSU. Telstra's retail staff had accessed the information during this period and used this information to contact end users of the wholesale customers. In total, 470 end users of a total of 29 wholesale customers were contacted by Telstra retail staff. Of the 470 end users, Telstra identified six wholesale ISDN2 end users who subsequently changed from their existing wholesale provider to Telstra.	According to Telstra this issue arose because ISDN2 service information was not being filtered out of reports generated from its computer system which are used by its retail staff. Telstra also stated that the retail staff who made contact with wholesale customers' end users were not aware that the data contained wholesale customers' protected information under the SSU.

Item 3—Disclosure of WCPI – CustomNet

Breach	Cause
On 31 January 2019, Telstra identified that WCPI for 15 wholesale customers' end users' CustomNet product was accessible to Telstra retail staff between 9 December 2018 and 4 February 2019. Four of the 15 wholesale customers' end users were subsequently contacted by Telstra retail staff. No wholesale customers' end users of CustomNet products changed their services to Telstra following this contact. The unauthorised contact was in breach of clauses 10.3 and 10.4 of the SSU.	According to Telstra this issue also arose because CustomNet service information was not being filtered out of reports generated from its computer system which were used by its retail staff. Telstra also stated that the retail staff who made contact with wholesale customers' end users were not aware that the data contained wholesale customers' protected information under the SSU.

2 Special Services are typically business-grade services used for critical purposes other than standard landline phone or internet service.

3 ISDN2 is an ISDN (Integrated Services Digital Network) service that enables businesses to conduct 2 concurrent telephone calls at the same time over one PSTN line. It's referred to as a 'special service' in relation to the NBN product migration.

4 CustomNet is a business communication service that provides advanced call handling features and in particular is used by a number of emergency services. It's referred to as a "special service" in relation to the NBN product migration.

5 The AIP is a 'fast-track' dispute resolution process for wholesale customers to raise equivalence complaints.

6 This system is used to manage the transition of retail customers from Telstra services to NBN and also interfaces with other Telstra systems which extract data to provide pipeline management notification, service verification, reconciliation, prioritisation, sales order submission and service order tracking and management across the enterprise NBN transition program.

Remediation

Telstra has taken the following steps to prevent future disclosure of wholesale customers' end user information:

- Implemented strategic fixes to prevent wholesale data being put into Telstra's systems accessed by retail staff.
- Undertook quarterly reviews of the effected business system to ensure that no wholesale customer end user information is included in this system.
- Conducted regular refresher training for all Telstra staff to make them aware of their information security obligations.
- Undertook investigations to assess any non-compliance by Telstra staff in completing training on information security obligations.
- Ongoing monitoring of access to computer systems to prevent inappropriate access to wholesale customer information.
- Conducted regular validation of systems containing wholesale data. During this process, any potential SSU considerations are identified and controls implemented to protect wholesale data.

At ACCC's request, Telstra published an acknowledgment of these information security breaches on its website[7] and also wrote to all impacted wholesale customers advising them of the details of the breach and Telstra's remediation actions.

ACCC's view

The ACCC requested information about the corrective measures Telstra had implemented in response to the breaches discussed above and contacted the major wholesale customer affected by the breach.

On 17 July 2019 the ACCC wrote to Telstra accepting Telstra's rectification measures and requested that Telstra publish an explanation of these matters on its website and contact the wholesale customers affected.

The ACCC is satisfied that the actions taken by Telstra were appropriate in minimising the risk of recurrence of the SSU breaches.

Item 4—Disclosure of wholesale customers' end user information

Breach	Cause
In March 2019, Telstra identified that a screenshot containing service details of a single wholesale customer end user was sent to a Telstra retail employee by a Telstra wholesale employee in response to an email. This was in breach of clause 10.4.	Telstra explained that the issue was as a result of a Telstra wholesale employee not performing the necessary checks to confirm the identity of the retail employee prior to sending the wholesale customer end user information.

Remediation

Telstra advised that the Telstra wholesale employee who had inappropriately sent wholesale customer end user information to a Telstra retail employee had been counselled about the need to prevent future inappropriate disclosure of wholesale customer information.

Telstra's retail employee confirmed that the email was deleted and the content had not been disclosed or sent to anyone else. The retail employee also confirmed that the protected information contained in the email had not been used for any purpose.

7 See https://www.telstrawholesale.com.au/wholesaleconnect/category/news/ssu-breach---closure-notification.html.

ACCC's view

The ACCC is satisfied that the actions taken by Telstra were appropriate in minimising the risk of recurrence of the SSU breach.

2.2 Network Notification

Schedule 4 of the SSU contains network notification obligations for Telstra.

Section 7 of this Schedule requires Telstra to provide reasonable information to affected wholesale customers in circumstance where the provision of an eligible service is affected by network incidents.

Section 11.2 of this Schedule requires Telstra to provide a written coordinated capital works program (CCWP) schedule to the relevant wholesale customer by giving them at least 12 months' notice of the anticipated commencement date of the CCWP.

Item 5—Adequate notification on major work not provided

Breach	Cause
In November 2018, Telstra identified that in breach of schedule 4 paragraphs 10 and 11 of the SSU, it did not provide: ▪ a notice of a major network modernisation and upgrade (MNMU) to its wholesale customers for an exchange service area (ESA) which effected two end users of a wholesale customer ▪ MNMU and CCWP forecasts and schedule notification within the required timeframes for 3 ESAs.	Telstra advised that due to a change in personnel, it had inadvertently failed to notify wholesale customers of some capital works activity it was undertaking.

Remediation

Telstra communicated with the relevant personnel to ensure clarity of obligations to prevent recurrence of this issue. Telstra also notified its wholesale ADSL customers of the MNMUs and CCWP forecast and schedule within a week of identifying the issue.

ACCC view

The ACCC is satisfied that the actions taken by Telstra were appropriate in minimising the risk of recurrence of the SSU breach.

3. Variation to Migration Plan

The Migration Plan sets out the steps that Telstra will take to progressively migrate voice and broadband services from its copper and hybrid-fibre coaxial (HFC) network to the NBN as it is rolled out across Australia.

Since the Migration Plan was approved by the ACCC in 2012, the ACCC has considered and approved a number of variations, including to:

- incorporate the shift to a multi-technology mix (MTM)
- facilitate the use of fibre-to-the-curb as an access technology for the MTM NBN.

During 2018–19, the ACCC approved one request from Telstra to vary its Migration Plan. On 26 October 2018, the ACCC approved Telstra's proposed variation to its migration plan after determining that it complied with the migration plan principles. The proposed variation included changes to migration arrangements for Special Services together with a number of other changes for which Telstra had previously received regulatory forbearance from the ACCC.

3.1 Regulatory forbearance

During 2018–19, the ACCC provided regulatory forbearance on four occasions regarding proposed non-compliance by Telstra with its Migration Plan obligations, in order to promote service continuity and a better migration experience for end users.

In May 2018, the ACCC agreed to Telstra's request for regulatory forbearance from its Migration Plan obligations for premises in HFC regions with disconnection dates between February and May 2018 and existing disconnection requirements for some premises that remained NBN non-serviceable. The ACCC agreed to the following related regulatory forbearance requests from Telstra in 2018–19, further extending the time period for disconnection of premises in HFC regions:

- on 12 April 2019, the ACCC agreed to Telstra's request for an extension of regulatory forbearance by 150 business days in response to NBN Co advising Telstra that there were approximately 2000 premises subject to the previous forbearance that were not NBN-serviceable at the time
- on 26 June 2019, the ACCC agreed to Telstra's request for a further extension of regulatory forbearance by 150 business days in response to NBN Co advising Telstra that there were approximately 300 premises subject to the previous forbearance that were not NBN-serviceable at the time.

The ACCC also agreed to the following regulatory forbearance requests from Telstra in 2018–19:

- on 9 January 2019, in relation to Telstra's disconnection obligations for Special Services at Commonwealth Government High Security sites
- on 16 May 2019, in relation to disconnection of critical infrastructure Special Services dependent on Telstra's atomic clock.

3.2 Continuity of Service Industry Standard 2018

On 15 October 2018, Telstra advised the ACCC that where there is an apparent conflict with its obligations under the ACMA *Telecommunications (Continuity of Service) Industry Standard 2018* (the Standard), Telstra will be complying with the Standard instead of the Migration Plan.[8]

Telstra advised that this accords with the Force Majeure exception in the Migration Plan and will provide additional assurance of service continuity for consumers who encounter difficulties with their NBN connections during the switchover period.

For example, the Standard requires Telstra to reconnect a legacy service to ensure a consumer is not left without a working service where an NBN service cannot be connected during the switchover period. However, legacy services will still be subject to the Migration Plan managed disconnection process at the end of the NBN switchover period.

8 For more information see https://www.acma.gov.au/theACMA/service-continuity-standard-your-obligations.


ACCC
AUSTRALIAN COMPETITION
& CONSUMER COMMISSION