



Australian  
Competition &  
Consumer  
Commission

ACCC Report

# Telstra's Structural Separation Undertaking

Annual Compliance Report  
2013–14

Report to the Minister for Communications



Australian  
Competition &  
Consumer  
Commission

# Telstra's Structural Separation Undertaking Annual Compliance Report 2013–14

Report to the Minister for Communications

ISBN 978 1 922145 47 5

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

© Commonwealth of Australia 2015

This work is copyright. In addition to any use permitted under the *Copyright Act 1968*, all material contained within this work is provided under a Creative Commons Attribution 3.0 Australia licence, with the exception of:

- the Commonwealth Coat of Arms
- the ACCC and AER logos
- any illustration, diagram, photograph or graphic over which the Australian Competition and Consumer Commission does not hold copyright, but which may be part of or contained within this publication.

The details of the relevant licence conditions are available on the Creative Commons website, as is the full legal code for the CC BY 3.0 AU licence.

Requests and inquiries concerning reproduction and rights should be addressed to the Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601, or [publishing.unit@acc.gov.au](mailto:publishing.unit@acc.gov.au).

#### **Important notice**

The information in this publication is for general guidance only. It does not constitute legal or other professional advice, and should not be relied on as a statement of the law in any jurisdiction. Because it is intended only as a general guide, it may contain generalisations. You should obtain professional advice if you have any specific concern.

The ACCC has made every reasonable effort to provide current and accurate information, but it does not make any guarantees regarding the accuracy, currency or completeness of that information.

Parties who wish to re-publish or otherwise use the information in this publication must check this information for currency and accuracy prior to publication. This should be done prior to each publication edition, as ACCC guidance and relevant transitional legislation frequently change. Any queries parties have should be addressed to the Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601, or [publishing.unit@acc.gov.au](mailto:publishing.unit@acc.gov.au).

ACCC 02/15\_960

[www.accc.gov.au](http://www.accc.gov.au)

EXECUTIVE OFFICE



Australian  
Competition &  
Consumer  
Commission

23 Marcus Clarke Street  
Canberra ACT 2601

GPO Box 3131  
Canberra ACT 2601

tel: (02) 6243 1111  
fax: (02) 6243 1199

[www.accc.gov.au](http://www.accc.gov.au)

26 February 2015

The Hon Malcolm Turnbull MP  
Minister for Communications  
PO Box 6022  
House of Representatives  
Parliament House  
Canberra ACT 2600

**Sent electronically:** [Malcolm.Turnbull.MP@aph.gov.au](mailto:Malcolm.Turnbull.MP@aph.gov.au)

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 2013–14 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.

Please do not hesitate to contact me on 02 6243 1131 should you wish to discuss the report.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Rod Sims'.

Rod Sims  
Chairman



# Contents

<b>Executive summary</b>	<b>1</b>
<b>Introduction</b>	<b>2</b>
<b>Telstra's Structural Separation Undertaking</b>	<b>3</b>
Interim equivalence and transparency	4
Compliance reporting	5
Matters reported in Telstra's Annual Compliance Report	5
<b>The ACCC's approach to compliance and enforcement</b>	<b>6</b>
<b>Breaches of the SSU</b>	<b>7</b>
Information security	7
Breaches reported by Telstra	9
Matters identified after the end of the reporting period	14
Continuing information security breaches	17
Equivalence in the supply of regulated services	20
Breaches reported by Telstra	22
Other Rectification Proposals submitted during the reporting period	24
<b>Breaches of the Migration Plan</b>	<b>26</b>
Cease sale	26
Disconnection obligations	27
Reconnection of premises previously Permanently Disconnected	27
Communication with Retail Customers about Disconnection Dates	28
<b>ACCC action</b>	<b>29</b>
<b>Further information</b>	<b>30</b>
<b>ACCC contacts</b>	<b>30</b>



## Executive summary

In 2013-14, Telstra continued to demonstrate a commitment to increasing its level of compliance with its Structural Separation Undertaking (SSU) and respond to breaches in a positive manner.

The most common SSU compliance issue during the period remained Telstra's failure to prevent unauthorised disclosure of the confidential or commercially sensitive information that it receives from wholesale customers in the course of supplying regulated services (Protected Information).

During 2013-14, Telstra employees from Retail Business Units could continue to access up to 30 shared IT systems which disclosed wholesale customer Protected Information in breach of the SSU. Protected Information was also disclosed to Retail Business Unit staff by other Telstra employees on a small number of occasions, either through inadvertently sending the information to the recipient in error or not appreciating that the disclosure was not permitted under the SSU.

Telstra is continuing to take steps to remediate its IT systems and reduce the incidence of unauthorised use or disclosure of Protected Information, and has advised the ACCC that it is on track to remediate the majority of its IT systems by March 2015.

Telstra also breached its SSU obligations that promote equivalence in service delivery to retail and wholesale customers in two ways during the 2013-14 reporting period. The first breach concerned the processes used to test basic telephone service (BTS) faults which require technician assistance. These processes made it more likely that wholesale faults would be closed without action than was the case for retail faults.

The second breach concerned the process used to conduct service qualification for asymmetric digital subscriber line (ADSL) and copper line sharing services (LSS) for lines that are subject to excessive transmission loss. This led to wholesale customers being incorrectly advised that a service could not be supplied in respect of a small proportion of lines. Telstra has dealt with each of these issues by way of formal Rectification Proposals that the ACCC accepted.

Telstra also breached some aspects of its Migration Plan in the 2013-14 reporting period. The Migration Plan is the part of the SSU that sets out how Telstra will disconnect customers from its copper and hybrid fibre-coaxial (HFC) networks and commence supplying services using the National Broadband Network (NBN). Specifically, Telstra failed to provide certain notifications to retail customers and to cease the sale or re-connection of new copper services to consumers that could order an NBN service. These breaches were of a small scale and primarily occurred due to problems in implementing new systems and operational processes.

Telstra also adopted interim arrangements, after advising the ACCC and with the ACCC's consent, for end users in the initial NBN rollout regions that had reached their required disconnection date to allow those end users additional time to migrate to the NBN before their services were disconnected. This was due to significant concern that consumers in those particular regions had not already had a suitable opportunity to migrate their services, and to ensure that further steps could be taken to contact the consumer and confirm they understood the need to migrate to the NBN if they wished to retain service.

Overall, Telstra's level of compliance with the SSU is consistent with it maintaining a suitable level of commitment and resourcing to achieve compliance with its SSU obligations, and acting reasonably to redress breaches as they are brought to light.

In responding to each of the reported breaches outlined in this report, the ACCC has continued to focus on stopping the conduct, ameliorating its impact, and ensuring that Telstra's systems and processes are remediated as soon as practicable to safeguard against recurrence. This has included encouraging Telstra to keep its wholesale customers informed of SSU equivalence and migration issues, conducting consultation on Rectification Proposals submitted by Telstra, and facilitating greater engagement between Telstra and industry through the ACCC's Wholesale Telecommunications Consultative Forums.

# Introduction

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

Telstra's SSU, accepted by the ACCC in February 2012, specifies Telstra's commitments to progressively migrate its fixed line voice and broadband customers onto the wholesale-only NBN and promote equivalence and transparency during the transition period. Given the timeframe required to complete the NBN build, these commitments, including Telstra's overarching commitment to provide equivalence of outcomes, are fundamental to promoting competitive outcomes during the transition period.

This report outlines breaches of the SSU for the period 1 July 2013 until 30 June 2014. The ACCC has prepared this report based on whether in its view, on the balance of probabilities, a breach of the SSU occurred. The ACCC has made its findings after considering information provided by Telstra and making its own enquiries into the matter.

This report identifies a number of breaches of the information security, overarching equivalence and service quality and operational equivalence obligations in the SSU, and identifies the steps taken or proposed to be taken by Telstra to remedy these breaches. The ACCC has accepted Rectification Proposals in relation to two operational equivalence breaches as well as an additional Rectification Proposal in relation to an issue identified in the ACCC's 2012-13 report on BTS fault rectification.

The ACCC has also included in this report details of breaches that were reported in the ACCC's report for 2011-12 (the ACCC's 2011-12 report) and 2012-13 (the ACCC's 2012-13 report), where the conduct continued into the 2013-14 reporting period.

Whilst Telstra has demonstrated its commitment to improving its overall compliance with the SSU, through its remediation action and compliance programs, this report further demonstrates the benefits of achieving structural reform of the telecommunications sector in order to resolve the long-standing competition concerns arising from Telstra's vertical integration.

# Telstra's Structural Separation Undertaking

In late 2010, the Australian Government introduced legislation which created a framework for reforming the telecommunications industry—effecting structural separation of Telstra by the progressive migration of Telstra's fixed line access services to the wholesale-only NBN.

This reform recognised that Telstra, as the vertically integrated access provider over the ubiquitous copper network, operates at all levels of the supply chain and competes with the businesses that it supplies. This has given rise to long standing competition concerns around Telstra's ability and incentive to favour its retail business over other service providers accessing its network, to the detriment of consumers.

Prior to the commencement of the SSU, Telstra was subject to an operational separation regime which was intended to promote equivalence between Telstra's wholesale and retail customers. The ACCC considers, and has previously publicly stated, that the operational separation regime and the ACCC's limited role in investigating and reporting matters to the Minister was largely ineffective in addressing Telstra's ability and incentive to discriminate against its competitors.<sup>1</sup> The operational separation regime ceased to operate when the SSU commenced on 6 March 2012.

The SSU measures are a substantial improvement upon the previous operational separation regime and more effectively promote equivalence and transparency. The SSU provides for stronger enforcement mechanisms, which are particularly important for protecting competition and delivering outcomes in the interests of consumers and businesses during the rollout of the NBN.

The SSU contains four key elements:

- A commitment by Telstra to cease the supply of fixed line carriage services using telecommunications networks over which Telstra is in a position to exercise control from the Designated Day—which is expected to be the day on which the construction of the new wholesale-only national broadband network will be concluded.
- Interim equivalence and transparency obligations regarding access to Telstra's regulated services in the period leading up to the Designated Day.<sup>2</sup>
- Compliance monitoring processes, to provide the ACCC with transparency over Telstra's compliance with the SSU.
- The Migration Plan, which forms part of the SSU.<sup>3</sup> The Migration Plan sets out how Telstra will progressively transfer its fixed line customers onto the NBN.

The ACCC's experience in administering the SSU is that it continues to deliver significantly better outcomes in terms of equivalence for wholesale customers and enhanced transparency regarding Telstra's compliance than were realised under the previous operational separation regime.

1 See for example pages 8 and 9 of the ACCC's submission to the government's 2009 *National Broadband Network: Regulatory Reform for the 21st Century Broadband* discussion paper.

2 Regulated Services include the declared services and the Telstra Exchange Building Access service described in the *Telecommunications (Regulated Services) Determination (No.1) 2011*.

3 Pursuant to s. 577BE of the *Telecommunications Act 1997*, when a final Migration Plan comes into force, the SSU has effect as if the provisions of the plan were provisions of the SSU.

## Interim equivalence and transparency

In order to promote competition during the interim period from the date that the SSU commenced and until the NBN rollout is complete, the SSU includes a broad range of interim equivalence and transparency obligations.

These obligations require Telstra to ensure equivalence of outcomes in relation to the supply of regulated services as between its wholesale customers and its own Retail Business Units. The obligations include:

- Organisational structure—maintaining separate wholesale, retail and network services business units.
- Overarching equivalence—an obligation to ensure that particular aspects of retail and wholesale regulated services will be equivalent.
- Information security—principles governing the use and protection of confidential information of wholesale customers where the information was obtained in respect of regulated services.
- Service quality and operational equivalence—establishing and maintaining ticketing, order management and billing systems that comply with standards in the SSU.
- Telstra exchange building access—commitments around non-discriminatory access to Telstra's exchange buildings and related facilities.
- Wholesale customer facing systems—maintaining minimum levels of functionality and availability.
- Information equivalence—Telstra must keep wholesale customers engaged and provide minimum notifications about network maintenance, outages and upgrades.
- Equivalence and transparency metrics (referred to as Metrics)—objective performance measurement of equivalence regarding provisioning, fault rectification, and systems availability.
- Service level rebates—wholesale customers may 'opt-in' to a rebate scheme where Telstra does not meet the minimum performance standards set out in the equivalence and transparency metrics.
- Price equivalence and transparency—Telstra is to maintain and publish reference prices for regulated services in accordance with the methodology set out in the SSU.
- Accelerated investigation process—a separate 'fast-track' dispute resolution process for wholesale customers to raise equivalence complaints.
- Independent Telecommunications Adjudicator (ITA)—a process and forum for the resolution of equivalence and NBN migration disputes between Telstra and wholesale customers.
- Reporting—Telstra has a number of reporting obligations (further described below), including in relation to the equivalence and transparency metrics and possible breaches of the overarching equivalence commitment.

## Compliance reporting

Telstra's reporting obligations, which facilitate the ACCC's ongoing monitoring of Telstra's compliance with its interim equivalence and transparency commitments, comprise:

- A confidential monthly compliance report on any 'equivalence issues' that have been identified by Telstra or reported to Telstra by the ACCC or wholesale customers.<sup>4</sup>
- A confidential monthly remediation report concerning the program of work Telstra is conducting to ensure that its IT systems are compliant with the information security obligations. This report is provided by Telstra on a voluntary basis.
- A confidential annual compliance report, which includes details of equivalence issues identified by Telstra or reported to Telstra by the ACCC or wholesale customers. This report also states the issues that Telstra has identified as breaches of its SSU obligations.
- Quarterly public operational equivalence reports, which outline Telstra's performance against 33 equivalence and transparency metrics. A confidential version of these reports provides a reasonably detailed explanation of any variances in the Metrics above two percentage points.
- Six-monthly public and quarterly confidential Telstra Economic Model (TEM) reports outlining the list of internal wholesale prices and external wholesale prices.

The ACCC has considered Telstra's monthly compliance reports relating to the period between 1 July 2013 and 30 June 2014 and Telstra's Annual Compliance Report for 2013-14 (Annual Compliance Report). In addition, the ACCC has considered issues identified by Telstra in later monthly compliance reports that relate to conduct that occurred during the 2013-14 financial year.

### Matters reported in Telstra's Annual Compliance Report

In its Annual Compliance Report, Telstra reported 14 breaches of the SSU. These breaches comprise:

- seven instances (one of which was reported in the ACCC's 2012-13 report) where Telstra breached its obligation to safeguard Protected Information pursuant to clause 10.4 of the SSU
- five operational systems (all reported in the ACCC's 2012-13 report) which provided Telstra Retail staff (i.e. staff in a Retail Business Unit) with access to Protected Information in breach of clause 10.4 of the SSU
- two breaches of the overarching equivalence and service quality and operational equivalence obligations in clauses 9 and 11 of the SSU in relation to the retesting of BTS line faults and the ADSL and LSS service qualification process.

<sup>4</sup> An 'equivalence issue' means a possible breach of clause 9.1 (Telstra's overarching commitment to equivalence) or a breach of a specific non-price equivalence and transparency commitment.

## The ACCC's approach to compliance and enforcement

Telstra is obliged to comply with the SSU under the *Telecommunications Act 1997*. If the ACCC considers that Telstra has breached the SSU it may apply to the Federal Court for a range of remedies, including penalties, compensation and any other order that the Court considers appropriate.

The ACCC has discretion over whether to take enforcement action in relation to breaches of the SSU and the nature of that action. The ACCC will only commence court proceedings where there are reasonable grounds for starting the proceedings and where it considers litigation to be the most suitable method of resolving a matter.

As outlined in the ACCC's *Compliance and Enforcement Policy*, the ACCC uses a range of compliance and enforcement tools in order to encourage compliance and resolve matters.<sup>5</sup> These tools range from administrative resolutions—for example, a commitment to stop engaging in the conduct—to litigation. Administrative resolutions are generally used where the ACCC assesses the potential risk of harm flowing from conduct as low. Legal action is more likely in circumstances where the conduct is egregious, where there is reason to be concerned about future behaviour or where the party involved is unwilling to provide a satisfactory resolution.

In respect of breaches of the SSU, the ACCC is more likely to take legal action if it considers it to be necessary to prevent ongoing or systemic breaches of the SSU or to obtain a remedy to undo any harm. The ACCC would also consider litigation if it concludes that Telstra engaged in particular conduct in order to damage its competitors or otherwise provide itself with a commercial advantage.

The ACCC's overall objective is to ensure that Telstra has the requisite systems and processes in place to enable it to fully comply with the commitments in the SSU, in order to promote equivalence and transparency during the period of transition to the NBN.

For each breach, the report notes whether the ACCC considers that Telstra's remedial steps are sufficient to address any competitive detriment that may arise as a result of the breach and to ensure future compliance with the SSU. The ACCC's position on the adequacy of Telstra's remediation is based on the information provided to date by Telstra and its wholesale customers.

---

<sup>5</sup> Available at <https://www.accc.gov.au/about-us/australian-competition-consumer-commission/compliance-enforcement-policy>.

## Breaches of the SSU

This report details a number of instances where the ACCC considers, on the balance of probabilities, that Telstra breached its SSU. These breaches relate to:

- Telstra's information security obligations, in circumstances where:
  - Telstra has reported that it has breached the SSU in its Annual Compliance Report
  - Telstra identified the conduct after the end of the reporting period and so did not express a view on whether the conduct was in breach of the SSU in its Annual Compliance Report
  - Telstra's conduct was reported by the ACCC in 2011-12 and/or 2012-13 but the conduct continued during the 2013-14 reporting period
- Telstra's obligation to provide overarching equivalence and service quality and operational equivalence in the supply of regulated services to wholesale customers and its Retail Business Units in circumstances where Telstra has reported that it has breached the SSU in its Annual Compliance Report.

The majority of breaches reported in 2013-14 involve cases where Protected Information has been disclosed to Retail Business Unit staff inadvertently or as a result of Telstra not yet fully completing its IT systems remediation. Telstra has provided additional training to relevant Wholesale Business Unit staff and, where possible, revised its processes to ensure such breaches do not reoccur.

In addition, Telstra has continued to take steps to properly ring fence wholesale customer Protected Information in its operational and data warehouse systems. These steps include removal of Telstra Retail access to wholesale customer Protected Information through partitioning of shared systems, implementation of user access management controls, process changes as well as behavioural controls. Overall, Telstra has made significant progress in relation to the remediation of its IT systems in the 2013-14 reporting period. Whilst the majority of Telstra's systems were remediated in December 2014, an additional information security issue was identified in late 2014 which may necessitate further systems remediation.

The ACCC considers that, when fully completed, Telstra's IT system remediation program, as well as Telstra's ongoing commitment to ensuring compliance with the SSU, will be capable of preventing the types of breaches that are outlined in this report from recurring. However, the ACCC intends to test the solutions implemented by Telstra to ensure they operate correctly.

### Information security

The SSU contains information security obligations designed to safeguard wholesale customer Protected Information obtained by Telstra in the course of supplying regulated services to wholesale customers. By virtue of Telstra's vertical integration, Protected Information could potentially be used to Telstra's advantage in downstream 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.

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.

### *The SSU and information security*

**Clause 10** of the SSU sets out how Telstra must act in relation to Protected Information. The definition of Protected Information includes:

- (a) confidential information identifying a wholesale customer or a wholesale customer's end user, supplied by that wholesale customer to Telstra for the purpose of, or in the course of, supplying regulated services to that wholesale customer
- (b) information that is commercially sensitive information to a wholesale customer, supplied by that wholesale customer to Telstra for the purpose of, or in the course of, supplying regulated services to that wholesale customer
- (c) confidential information and commercially sensitive information which is derived from information of the kind described in (a) and (b) above, whether or not in an aggregate form, that: (i) would enable the identity of that wholesale customer to be ascertained; or (ii) would enable the identity of a customer of that wholesale customer to be ascertained.

These types of information will not be Protected Information if they are obtained by, or disclosed to, Telstra other than by a wholesale customer; provided by a customer of the wholesale customer directly to Telstra; or if the information was provided by the wholesale customer to a Telstra business unit other than Telstra Wholesale or other than in connection with the supply of regulated services.

The SSU provides examples of information that would constitute Protected Information relating to a wholesale customer, if it was provided by the wholesale customer to Telstra in the manner outlined above. These examples include:

- the wholesale customer's ordering and provisioning details (including details of when and where orders are submitted)
- details of a wholesale customer's end users, such as name, address, contact details, account and service numbers
- information about that wholesale customer's network or facilities.

**Clause 10.3** of the SSU provides that, subject to clause 10.4 (outlined below), Telstra will not use or disclose Protected Information relating to a wholesale customer in a manner which would be likely to enable Telstra Retail to gain or exploit an unfair commercial advantage over that wholesale customer in any market.

**Clause 10.4** of the SSU provides that Telstra will ensure that Telstra Wholesale will not disclose Protected Information relating to a wholesale customer to:

- any Retail Business Unit unless authorised to do so by that wholesale customer
- any Telstra Network Services Business Unit otherwise than on a 'need-to-know' basis or where authorised to do so by that wholesale customer
- an employee (not working for a Retail Business Unit) performing any of the functions specified in clause 8.1(f) otherwise than on a 'need-to-know' basis or where authorised to do so by that wholesale customer.

**Clause 10.5** of the SSU provides that Telstra will not disclose certain wholesale customer information to Telstra Retail unless, with the approval of the ACCC, it makes the information available to wholesale customers at the same time. This clause relates to information which is not Protected Information because it has been aggregated on a national basis or has been aggregated on a sub-national basis but the identity of wholesale customers cannot be ascertained.

Telstra is permitted to disclose Protected Information relating to a wholesale customer where it is authorised to do so by that wholesale customer. This reflects that there could be some circumstances where it would be in a wholesale customer's interests to consent to a particular use or disclosure of its Protected Information. However, as a consequence, the overall efficacy of these arrangements will rely upon wholesale customers carefully considering any proposed use or disclosure of their Protected Information by Telstra.

## Breaches reported by Telstra

In its Annual Compliance Report, Telstra identified six breaches of clause 10.4 of the SSU which have not previously been reported by the ACCC. These are outlined below and relate to Protected Information being disclosed to staff in a Retail Business Unit. Four of these breaches were inadvertent. The remaining two breaches have been remedied as part of Telstra's IT systems remediation project.

Telstra provided a description and explanation for the cause of each breach (identified in the tables below) in its Annual Compliance Report and outlined the steps it has taken to remediate the breaches. Telstra also provided further particulars in relation to each of these items on request by the ACCC.

### *Item 1—Report sent in error*

In its Annual Compliance Report, Telstra provided the following details in relation to item 1:

#### **Description of the breach**

A report containing Protected Information was emailed by a non-separated business unit employee to a list of project stakeholders, which included Retail Business Unit staff. This list was then forwarded by a Retail Business Unit employee to a distribution list that included other Retail Business Unit staff.

#### **Cause of the breach**

This specific incident was attributable to a human error by individual Telstra representatives.

## ACCC findings

The report was generated by a non-separated business unit employee in March 2013 for the purpose of facilitating the cancellation of 'Telecards' which had been inactive for five years.<sup>6</sup> The report contained wholesale customer Protected Information including the information of around 500 wholesale end users with inactive Telecards. The report was distributed by email to a group which included one Telstra Retail employee who then forwarded the report to 17 other Telstra Retail employees (two of which opened the attachment).

<sup>6</sup> Non-separated business units are those which do not fall within the definition of Separated Business Units within the SSU, namely the Wholesale, Retail and Network Services Business Units.

The Protected Information disclosed to the Retail Business Unit employees included:

- end user details (name, address and the customer identification number)
- wholesale ownership codes and information which identified that the end user order originated from a Wholesale Business Unit.

### Remediation undertaken by Telstra

Telstra has advised that, upon becoming aware of the error, the email attaching the report was immediately recalled by the non-separated business unit employee. In addition, Telstra has confirmed that the email attaching the report has been deleted by all Telstra Retail recipients and that the wholesale customer information was not used for any purpose.

The ACCC considers the action taken by Telstra following its identification of the issue minimised the risk of any competitive harm occurring as a result of the conduct.

### *Item 2—Email with wholesale orders sent to Retail Business Unit*

Telstra provided the following information in its Annual Compliance Report for item 2:

Description of the breach	Cause of the breach
An email containing both retail and wholesale delayed orders was sent to eight Retail Business Unit employees and the wholesale orders were potentially identifiable by a particular code.	This specific incident was attributable to a non-separated business unit employee using an out-of-date code list when identifying wholesale orders for the purpose of removing these orders from the list of delayed orders contained in the email. As the code list was out-of-date the employee did not identify that six orders were wholesale.

### ACCC findings

The email was generated by a non-separated business unit employee in late August 2013 and sent to employees from a number of business units, including eight Telstra Retail employees. The email contained a list of delayed orders for the purpose of requesting employees in the relevant business units to confirm or cancel the relevant orders. Due to the use of an out-of-date code list to manually filter out wholesale customer information from one of Telstra's shared operational systems, the list contained wholesale customer Protected Information, namely information relating to six wholesale orders.

The Protected Information disclosed to the Retail Business Unit employees included:

- end user order details (order numbers, order date and order status)
- full national numbers.

The email also contained codes which may have enabled Retail Business Unit employees to identify that a Wholesale Business Unit initiated the order.

### Remediation undertaken by Telstra

Telstra has confirmed that the email was not forwarded or otherwise distributed to any other Retail Business Unit employee. An up-to-date code list was provided to the non-separated business unit employee and Telstra took steps to train the relevant employee on how to recognise and appropriately segregate wholesale customer information.

In January 2014, Telstra remediated the relevant operational system so that manual filtering of codes is no longer required in order to remove wholesale customer information from the list of delayed orders.

The ACCC is satisfied that the steps taken by Telstra minimised the risk of competitive harm arising from the conduct and, in addition to remediation of the relevant operational system, should ensure that Telstra complies with the information security requirements in the SSU in respect of such emails in the future.

### ***Item 3—Email attaching wholesale customer agreement sent in error***

Telstra provided the following information in respect of item 3 in its Annual Compliance Report:

<b>Description of the breach</b>	<b>Cause of the breach</b>
An email attaching a draft novation agreement for a Wholesale Customer containing Protected Information was erroneously sent to a Retail Business Unit employee after the sender inadvertently selected the Retail Business Unit employee from the global email address book.	This specific incident was attributable to a human error by an individual Telstra representative.

#### **ACCC findings**

The email was sent by a Telstra Wholesale employee in August 2013 to several other Telstra Wholesale employees and one Telstra Retail employee. The Telstra Retail employee was added to the distribution list by mistake, which Telstra has advised was due to the fact that the intended recipient had the same name as the Telstra Retail employee. A 'reply all' response was sent by one of the Telstra Wholesale employees, which resulted in the email being sent to the Telstra Retail employee a second time. The email attached a draft novation and service migration agreement for a wholesale customer.

The Protected Information disclosed to the Retail Business Unit employee included:

- the name of the wholesale customer (in the subject line and body of the email)
- contractual terms relating to the supply of regulated services to that wholesale customer
- information which identified that the wholesale customer was involved in the process of novating the terms to a new wholesale customer.

#### **Remediation undertaken by Telstra**

Telstra has advised that, upon becoming aware of the error, the Retail Business Unit employee contacted the sender advising that the emails had been received in error and confirming that they did not open or read the document attached to the email. Telstra has also informed the ACCC that the Telstra Retail employee deleted the emails and did not use them for any purpose.

In December 2013, Telstra made changes to its global email address book so that Wholesale Business Unit employees are identified by the word 'Wholesale' appearing after their name. Telstra has also implemented processes and conducted training to assist in ensuring wholesale contracts are not inadvertently sent outside of the Wholesale Business Unit.

The ACCC considers that the actions taken by Telstra following this incident minimised the risk of competitive harm arising from the conduct and should reduce the risk of Telstra breaching its information security obligations due to such errors in the future.

**Item 4—Email sent in error**

In its Annual Compliance Report, Telstra provided the following details in relation to item 4:

Description of the breach	Cause of the breach
An email containing Protected Information namely the names and details of Wholesale Customers and feedback provided by some Wholesale Customers in relation to services acquired from Telstra, was erroneously sent to one Retail Business Unit employee.	This specific incident was attributable to a human error by an individual Telstra representative.

**ACCC findings**

The email was sent by a Telstra Wholesale employee in March 2014 and contained feedback provided by wholesale customers in relation to regulated and non-regulated services. Whilst it was intended to be sent to several Telstra Wholesale employees, a Telstra Retail employee was erroneously included in the distribution list as a result of a typing error.

The Protected Information disclosed to the Retail Business Unit employee included:

- wholesale customer names
- details of the feedback provided by the wholesale customers.

**Remediation undertaken by Telstra**

Telstra has advised that, upon becoming aware of the error, the Telstra Retail employee forwarded the email to the correct recipient and deleted the message. The employee confirmed the information had not been used for any purpose.

The ACCC considers that the actions taken by Telstra following this incident minimised any risk of competitive harm and changes to the global email address book (as per item 3) should reduce the risk of Telstra breaching its information security obligations in the future.

**Item 5—Enquiry about a pending wholesale order**

Telstra reported the following details about item 5 in its Annual Compliance Report:

Description of the breach	Cause of the breach
In response to a request for information by a Retail Business Unit employee about a pending Wholesale Customer order that was preventing the submission of a retail broadband transfer request, a Telstra Wholesale employee erroneously disclosed Protected Information, including the wholesale order number, disconnection order and status of the Wholesale Customer's order.	This specific incident was attributable to a human error by an individual Telstra representative.

## ACCC findings

In March 2014, a Telstra Retail employee emailed a Telstra Wholesale employee to follow up on a wholesale ADSL service cancellation order which had not yet been processed and was holding up the submission of a retail ADSL transfer request. Telstra has advised that this email was not in accordance with Telstra's standard practice.

The Telstra Retail employee enquired about the pending order prior to submitting the transfer request. When responding to the enquiry, the Telstra Wholesale employee mistakenly disclosed Protected Information, including:

- the wholesale order and disconnection order numbers
- the status of the wholesale customer's order.

### Remediation undertaken by Telstra

Telstra has confirmed that the email was not distributed or disclosed in any way by the Retail Business Unit employee and was deleted. Telstra has also advised that it provided additional training to the relevant Wholesale Business Unit, including the specific employee involved.

As the information was requested in the course of actioning a transfer request, Telstra has advised that the information was of limited value to the Retail Business Unit employee. The ACCC is satisfied that the steps taken by Telstra minimised any risk of recurrence.

### ***Item 6—Auto-population of an email template when rejecting Telstra Retail fixed voice service orders***

Telstra provided the following information in respect of item 6 in its Annual Compliance Report:

Description of the breach	Cause of the breach
<p>An industry partner of Telstra's was using an email template for an order rejection notice that auto-populated using Protected Information from an operational system, namely the full national number, the fact a wholesale service existed on the line and in some cases, the name of the Wholesale Customer end user. These order rejection notices were sent to Retail Business Unit staff in circumstances where fixed voice services were requested but rejected because of incompatible wholesale products on the same line.</p>	<p>Not all Protected Information in the relevant system which fed into these forms had been masked or otherwise segregated from Retail Business Unit users, and remediation to the system had not been implemented. Further, the order rejection notices containing wholesale information were being sent to Retail Business Unit staff due to non-compliance with existing work instructions.</p>

## ACCC findings

A non-separated business unit was using several email templates ('order rejection notices') to advise Telstra Retail employees that their fixed voice service orders were rejected due to incompatible wholesale services. The order rejection notices were created using a process which auto-populated information from an operational system containing wholesale customer Protected Information. This resulted in wholesale customer Protected Information being disclosed to Retail Business Unit staff.

Telstra has provided an example of an order rejection notice below:

*Your request has been received however we are unable to complete the request due to the following:*

*The FNN 07xxxxxxx & 07xxxxxxx has wholesale services so the request for conversion cannot be provisioned. Hence your request is rejected.*

The Protected Information disclosed to Retail Business Unit employees included:

- end user names
- full national numbers
- advice that there is a wholesale service on the line.

Telstra has advised that only a small portion of the total orders handled by the relevant business unit were affected by order rejection notices of this nature and that these templates were sent to Telstra Retail staff contrary to work instructions. Telstra has also advised that no other business units use these templates.

### Remediation undertaken by Telstra

Telstra took action in May 2014 and August 2014 to remind the relevant business unit to follow the relevant work instructions to ensure that order rejection notices containing wholesale customer information are dealt with by staff in a non-separated business unit that does not have any retail sales function in relation to regulated services.

Telstra has advised that the relevant operational system was remediated in December 2014. The ACCC considers that Telstra's remediation in relation to this system and the actions taken by Telstra should ensure that this breach does not reoccur.

### Matters identified after the end of the reporting period

The SSU requires Telstra's Annual Compliance Report to include details of equivalence issues identified by wholesale customers, the ACCC or by Telstra during the relevant financial year. Consequently, Telstra's Annual Compliance Report does not contain those equivalence issues that occurred during the 2013-14 financial year, but were only subsequently identified as equivalence issues.

Telstra has identified three additional information security issues in its confidential monthly compliance reports for July and September 2014 which relate to conduct that occurred during the 2013-14 financial year.

#### ***Item 7—Data warehouse reporting tool***

In its monthly compliance report for July 2014, Telstra identified a potential breach of clause 10.5 of the SSU in relation to a reporting system which delivers operational data from different databases in a summarised format to Telstra Retail staff.

Telstra has advised that the system removes wholesale data based on filters at different database layers but that, due to an incomplete set of wholesale ownership codes, the filters failed to remove some wholesale customer Protected Information from the system. This issue was identified by Telstra in June 2013 but it did not consider at that stage that a breach had occurred.

Telstra has now confirmed that certain wholesale customer Protected Information was available to Telstra Retail staff in summary form. Telstra advised that the information was aggregated, incomplete and inaccurate and, as a result, was not of any real use to Telstra or its Retail Business Units. Telstra has also confirmed that, apart from certain wholesale ownership codes, there

was no information available that enabled the identification of wholesale customers or their end users. Telstra has advised that these codes are not known or generally accessible to Retail Business Unit staff.

### ACCC findings

Telstra has advised that the filters were in place prior to the commencement of the SSU and that 211 Retail Business Unit staff have accessed the reporting system since that time. The system made available wholesale ownership codes as well as the following partially aggregated wholesale customer information:

- the number of new, disconnected and existing copper-based services by business unit code
- the number of services associated with a particular pre-selection override code
- a sub-set amount of domestic transmission capacity services (DTCS) services-in-operation.

The information and wholesale ownership codes do not appear to readily enable Retail Business Unit staff to ascertain the identity of wholesale customers.

Telstra is restricted from disclosing information of this nature unless, with the approval of the ACCC, it makes the information available to wholesale customers at the same time. As this was not done, the ACCC considers Telstra has breached clause 10.5 of the SSU.

### Remediation undertaken by Telstra

Telstra has advised the ACCC that the filters were updated on 24 October 2013 to ensure that they were operating as they were designed to and that any sub-aggregated wholesale customer information linked to the relevant wholesale ownership codes was removed. Accordingly, the wholesale customer Protected Information is no longer visible to Retail Business Unit employees.

The ACCC considers that this remediation should ensure that Telstra is compliant with the information security requirements in the SSU in relation to this system.

### *Item 8—Report regarding 'mixed services'*

In its confidential monthly compliance report for July 2014, Telstra identified a potential breach of clause 10.4 of the SSU in respect of a report containing information about 'mixed services'.

Telstra has advised that the report was prepared by a non-separated business unit for Retail Business Unit staff. The report contained information which identified a number of end users as having 'mixed services', meaning that they are customers of both Telstra Retail and a wholesale customer. In some instances, the report also indicated that the end user was acquiring an LSS-based product.

### ACCC findings

The report was provided to nine Retail Business Unit staff and contained information on the customers with active Telstra services in areas where the NBN had been declared 'Ready for Service' that were within four months of their Disconnection Date (the date from which Telstra's obligation to disconnect the copper service commences).<sup>7</sup> The relevant Retail Business Unit staff were employed as team managers, project managers, product specialists and business analysts.

The report included a list of 7985 end users with active Telstra services, of which 490 were also identified as having wholesale services. Of these 490 customers with 'mixed services', six were identified as having an LSS-based service. As a result of this report being distributed, Protected Information was disclosed to a Retail Business Unit in breach of Clause 10.4 of the SSU.

<sup>7</sup> The 'Ready for Service' Date is defined in Schedule 9 of the Migration Plan to mean either the date notified by NBN Co as the Disconnection Commencement Date or the date advised by NBN Co in a notice published on its website that Fibre Services will be able to commence to be supplied in the Rollout Region.

The Protected Information disclosed to the Retail Business Unit employees included:

- information identifying the end users as customers of wholesale customers
- the wholesale product (LSS) being acquired by wholesale customers for the end user.

The Protected Information outlined above was set out clearly and in an easy to follow format in the report. The report also contained detailed end user contact information and significant contextual information about the end users' premises' state of NBN readiness. The Protected Information, accompanied by this additional information, would have been likely to enable the Retail Business Unit to offer discounts and/or other special deals on retail services likely to interest the end user. Further, it would have been likely to enable Telstra to gain a competitive advantage when developing marketing strategies aimed at these end users. The ACCC considers that disclosure of the Protected Information in the form of this 'mixed services' report constituted disclosure in a manner which would have been likely to enable Telstra to gain or exploit an unfair commercial advantage over the relevant wholesale customers in breach of clause 10.3 of the SSU, particularly as these wholesale customers would not have equivalent information and could not identify or act upon similar opportunities.

Telstra disagrees that the above conduct amounts to a breach of clause 10.3 of the SSU. Telstra has stated that the email was sent to a small number of Retail Business Unit staff on Saturday 25 January 2014 and identified and deleted by the relevant staff on Tuesday 28 January 2014 (the first business day after the Australia Day long weekend). Telstra considers that, in circumstances where the report was only available to limited staff for a limited amount of time, there was no opportunity for or evidence that the report resulted in any unfair commercial advantage to Telstra or a loss to wholesale customers.

The ACCC notes, however, that the actual gaining or exploiting of an unfair commercial advantage over wholesale customers is not required to establish a breach of clause 10.3 of the SSU. The ACCC considers that disclosure of the Protected Information in the form of the 'mixed services' report was disclosure in a *manner which would have been likely to enable* Telstra to gain or exploit an unfair commercial advantage in breach of clause 10.3 of the SSU regardless of whether any material competitive harm eventuated.

### Remediation undertaken by Telstra

Telstra has advised that, as soon as the issue was identified, it took the following steps:

- all recipients of the report were contacted immediately and asked to delete the report. Telstra has advised that the recipients confirmed that this had been done and that they had not forwarded or uploaded the file
- a meeting was convened to reiterate Telstra's SSU information security requirements to the relevant staff members.

In addition, Telstra has advised that the report template has been modified and will no longer disclose that the end user acquires services from a wholesale customer or that they are acquiring an LSS product.

The ACCC is satisfied that the steps taken by Telstra minimised any risk of competitive harm arising from the conduct. The ACCC considers that removal of the information identifying the end users as customers of wholesale customers and the wholesale products being acquired by them should ensure that Telstra does not breach the information security requirements in the SSU in respect of this report in future.

### ***Item 9—Email attaching wholesale customer agreement sent in error***

In Telstra's confidential monthly compliance report for September 2014, Telstra identified a second instance where a wholesale customer's novation agreement was disclosed in breach of clause 10.4 of the SSU.

In this instance, an email attaching the wholesale customer's novation agreement was sent to an employee with responsibility for decisions about the pricing of retail services which are not regulated services as well as two employees in a Network Services Business Unit.

#### **ACCC findings**

In August 2013, an email was sent from Telstra Wholesale to two Network Services Business Unit employees and an employee responsible for making decisions about the pricing of retail services. Whilst the email itself related to non-regulated services, a wholesale customer agreement was mistakenly attached to the email and contained wholesale customer Protected Information relating to the supply of regulated services. Neither of the Network Services Business Unit employees that received the email had a need to know the Protected Information contained in the agreement.

The Protected Information disclosed to the relevant employees in breach of clause 10.4 of the SSU included:

- the name of the wholesale customer
- contractual terms relating to the supply of regulated services to that wholesale customer.

#### **Remediation undertaken by Telstra**

Upon becoming aware of the error, Telstra directed the retail pricing employee to delete the email and has confirmed that this was done. In addition, Telstra has confirmed that the employee did not distribute or use the information contained in the email or attachment for any purpose. Telstra has also advised that the two Network Services Business Unit employees have deleted the email and did not distribute or use the email or the contents of the attachment for any purpose. Telstra has provided coaching to the Telstra Wholesale employees responsible for the distribution of the email and its attachment on the processes that should have been followed.

The ACCC considers the action taken by Telstra following its identification of the issue minimised the risk of any competitive harm occurring as a result of the conduct and should ensure that this breach does not reoccur.

### **Continuing information security breaches**

In the ACCC's 2012-13 report, the ACCC reported 40 breaches of the SSU's information security obligations. Twenty four of these breaches, each relating to individual operational and data warehouse systems, continued in 2013-14. Four breaches, relating to six operational and data warehouse systems, also continued from the 2011-12 reporting period.

Further detail on each of these breaches is available in the ACCC's 2011-12 and 2012-13 reports to the Minister on Telstra's SSU compliance.<sup>8</sup>

### ***Summary of Telstra's information security remediation***

Telstra has continued to undertake a number of remediation activities throughout the reporting period to bring its IT systems into compliance with the SSU information security obligations. In particular, Telstra has now remediated 39 of the 41 operational and data warehouse systems which have been reported to breach clauses 10.4 and 10.3 since the ACCC commenced reporting on Telstra's compliance with the SSU.

<sup>8</sup> <http://www.accc.gov.au/publications/telstras-structural-separation-undertaking>.

Telstra has implemented the following remediation in relation to these systems:

- systems changes, including:
  - the introduction of user profiling and filtering to block wholesale customer Protected Information from being visible to Telstra Retail staff
  - the modification and/or removal of particular functions and messages
  - introduction of pop-up screens to ensure that wholesale customer Protected Information is not inadvertently disclosed or accessed
- process and operational changes (for example, moving particular functions to non-separated business units where it involves the handling of Protected Information)
- the implementation of behavioural controls, either as an interim measure until the relevant system is fully remediated, where the system is unable to be fully separated or where necessary to support systems or other process changes.

As part of the final stages of Telstra's IT systems remediation project, Telstra identified end users that have had no prior retail relationship with Telstra and removed Telstra Retail access to information regarding these customers. The majority of this project was completed in December 2014 with only two systems still awaiting remediation. Telstra has advised that remediation of these two systems will be completed in March 2015.

Telstra has however recently identified two back of house call centre teams that have limited Retail Business Unit functions which were previously unidentified. Telstra has advised that, as these teams had not previously been accounted for in Telstra's IT systems remediation project, they may have access to wholesale customer Protected Information in Telstra's shared IT systems in breach of the SSU. In that case, further systems remediation will likely be required in 2015.

Telstra has continued to educate its staff on and raise awareness of its information security obligations under the SSU, including training to assist staff in identifying wholesale customer Protected Information. In this context, the ACCC notes that a number of the reported breaches in 2013-14 have arisen from human error where wholesale customer Protected Information has been mistakenly disclosed to Telstra Retail staff. Telstra has indicated that this is a result of increased awareness of Telstra's SSU information security commitments and willingness to report potential non-compliance—rather than deficiencies in its compliance program. In the 2013-14 reporting period, Telstra has taken action to address these breaches through individual coaching, additional training and education as well as making it easier to identify Wholesale Business Unit staff in its email system.

The ACCC considers that, when fully completed, Telstra's IT system remediation program and its ongoing commitment to ensuring compliance with the SSU will ensure that wholesale customer Protected Information is properly ring fenced. This will further ensure that Telstra is unable to gain an unfair informational advantage in the retail market due to its vertically integrated position. However, the ACCC intends to test the solutions implemented by Telstra to ensure that they operate effectively.

### ***Breaches of clause 10.4***

A number of Telstra's systems were not fully remediated prior to the commencement of the reporting period. As a result, wholesale customer Protected Information continued to be visible to Telstra Retail staff when they accessed a number of operational and data warehouse systems for part of the period.

- Protected Information continued to be available to Telstra Retail over Telstra's ordering and provisioning, and billing systems. This matter is outlined in full in items 1 and 2 of the ACCC's 2011-12 report.
- Protected Information relating to faults continued to be accessible to Telstra Retail in a shared system. This matter is outlined in full in item 3 of the ACCC's 2011-12 report.

- Protected Information contained in data warehouse systems reported in 2011-12 continued to be available to Telstra Retail staff in three of the four reported systems. This matter is outlined in full in item 5 of the ACCC's 2011-12 report.
- Protected Information continued to be accessible to Telstra Retail staff in 24 of the 33 operational and data warehouse systems identified in the ACCC's 2012-13 report. These matters are outlined in full in Appendices 1 and 2 and pages 24-25 of the ACCC's 2012-13 report.

### Remediation undertaken by Telstra

As outlined earlier in this report, Telstra has undertaken a significant amount of remediation, with many system remediation projects being finalised, during the reporting period and prior to finalisation of this report.

Telstra has now remediated 28 of the remaining 30 systems that continued to make Protected Information available to Retail Business Unit staff during the 2013-14 reporting period. The remaining two systems are expected to be remediated in March 2015.

The ACCC considers that, when completed, Telstra's proposed remediation in relation to these remaining systems should ensure that Telstra is compliant with its information security obligations in the SSU.

### ***Breaches of clause 10.3***

There was one continuing breach of clause 10.3 in the 2013-14 reporting period. The breach related to Telstra's primary ordering and provisioning system for fixed line services which was not fully remediated prior to the commencement of the reporting period. This matter is outlined in full in item 7 of the ACCC's 2011-12 report.

Until 18 April 2014, the system continued to disclose wholesale customer Protected Information and display a prominent 'NON-TEL' indicator notifying Telstra Retail staff that there were non-Telstra services on a particular line. As noted in the ACCC's 2011-12 report, Telstra does not agree or concede that there has been a breach of clause 10.3 of the SSU in relation to this indicator. However, Telstra cannot rule out the possibility of some Retail Business Unit staff disregarding its guidelines and using the indicator to gain or exploit an unfair commercial advantage. The actual gaining or exploiting of an unfair commercial advantage over wholesale customers is not required to establish a breach of clause 10.3 of the SSU.

### Remediation undertaken by Telstra

Telstra removed the NON-TEL indicator on 18 April 2014. Final remediation of the ordering and provisioning system was completed in December 2014. The ACCC considers that Telstra's remediation of this system should ensure that Telstra is compliant with the information security requirements in the SSU.

## Equivalence in the supply of regulated services

The SSU contains a number of commitments designed to ensure that Telstra provides equivalence in the supply of regulated services to wholesale customers and its Retail Business Units.

These obligations include:

- An overarching equivalence commitment—a broad obligation to ensure that Telstra's retail and wholesale regulated services will be supplied to an equivalent standard.
- Service quality and operational equivalence commitments—specific commitments to establish and maintain operational systems and processes so that tasks are performed in an equivalent manner for retail and wholesale customers and otherwise those customers are treated equivalently.

### *The overarching equivalence obligation*

**Clause 9** of the SSU contains an overarching equivalence obligation which applies to Telstra's supply of regulated services generally.

**Clause 9(a)** requires that Telstra ensure equivalence, on an equivalence of outcomes basis, in relation to its supply to wholesale customers and Telstra's Retail Business Units in respect of:

- (i) the technical and operational quality of the relevant regulated service
- (ii) the operational systems, procedures and processes used in the supply of the relevant regulated service
- (iii) information about the matters specified in clause 9(a)(i) and clause 9(a)(ii)
- (iv) the price that is charged for supplying the regulated service.

**Clauses 9(b) and (c)** provide a number of qualifications to the overarching equivalence obligation, limiting its application and enforcement. In particular, clause 9(b)(x)(B) provides that clause 9(a) will not apply to the extent that it would have the effect of preventing Telstra from obtaining a sufficient amount of a regulated service to supply services in accordance with its Priority Assistance Policy.

**Schedule 11** of the SSU sets out the manner in which the ACCC may enforce clause 9 of the SSU. It requires Telstra to submit a 'Rectification Proposal' to the ACCC to remedy possible breaches of clause 9. The ACCC may either accept a Rectification Proposal or, if it considers that the proposal is inadequate, issue a direction that Telstra take alternative steps to remedy the possible breach.

### *Specific interim equivalence and transparency obligations*

**Clause 11** of the SSU contains a number of specific equivalence and transparency obligations relating to Telstra's operational processes. In particular:

- **clause 11.1** provides that Telstra must maintain systems and processes for issuing tickets of work to field staff so that tickets of work in relation to regulated services supplied to wholesale customers and comparable retail services supplied to Telstra Retail customers are (a) issued and processed in Telstra's systems using equivalent order management and (b) managed and performed by Telstra field staff in an equivalent manner
- **clause 11.2(b)** provides that Telstra will rectify BTS faults reported by wholesale customers and Telstra Retail customers using equivalent order management and otherwise in an equivalent manner
- **clause 11.3(a)** provides that Telstra will use equivalent order management to process all ADSL service activation orders received from wholesale customers and Retail Business Units.

**Clause 11.7(b)** and **paragraph 1(b) of Schedule 11** provide that Telstra will not breach the equivalence commitments in the SSU in circumstances where it fails to comply with the requirements of the equivalence commitments and the failure is trivial.

In its Annual Compliance Report, Telstra reported two breaches of the overarching equivalence and service quality and operational equivalence obligations. Both breaches were brought to Telstra's attention by wholesale customers, but were reported to the ACCC at an early stage by Telstra following in-depth investigation. The identification of these additional instances of non-equivalence demonstrates the importance of Telstra implementing the equivalence and transparency commitments in the SSU in a robust manner, and the benefits of achieving structural reform of the telecommunications sector in order to resolve the long-standing competition concerns resulting from Telstra's vertical integration.

## Breaches reported by Telstra

### *Item 10—Wholesale ADSL service qualification*

Telstra provided the following details in its Annual Compliance Report in relation to this issue:

#### **Description of the breach**

Existing systems and processes for handling service qualifications and the subsequent decision regarding the provisioning of orders for ADSL and LSS services—where a service qualification query or ADSL/LSS order is performed using a full national number and the existing PSTN service is affected by excessive transmission loss—were different for Wholesale and Retail Customers. In this limited situation, Wholesale Customer systems would produce a 'Fail' result, while Telstra Retail systems would assess the suitability of the current and alternative paths, meaning there was a potential for different treatment by Telstra of service qualification queries or ADSL/LSS orders for Retail and Wholesale Customers in those circumstances.

#### **Cause of the breach**

This matter arose from Telstra Wholesale's current systems and processes which are limited to assessing the suitability and provisioning option of the current path for the existing full national number only. Where the current path used for the existing full national number was affected by excessive transmission loss, the results received by Telstra Wholesale Customers would indicate a 'Fail'. In contrast, where the current path of the existing full national number was affected by excessive transmission loss, Telstra Retail's systems and processes would assess the suitability of the current and alternate paths that were not affected by excessive transmission loss. The service qualification results received by Telstra's Retail Business Units would not indicate an 'Unavailable' result but would allow an assessment of the potential to provision the ADSL service by way of that alternate path, if one was available.

#### **ACCC findings**

In January 2014, Telstra received a complaint from a wholesale customer through its accelerated investigations process that it was unable to acquire a wholesale ADSL service for premises where the wholesale customer had previously acquired a PSTN and LSS service. This occurred in circumstances where, several days later, Telstra Retail was able to provision an ADSL service to the premises.

In March 2014, Telstra identified that, within its operational systems, procedures and processes, there was potential for different treatment of requests by wholesale customers and Telstra Retail when provisioning ADSL or LSS services (where there was an existing PSTN service), in circumstances where the PSTN provisioned line was affected by excessive transmission loss.

Further investigations by Telstra identified that when a request was made by Telstra Retail using a full national number search in such circumstances, the system explored provisioning options over alternate copper paths and in the event that possible alternatives were identified, would advise Telstra Retail that further investigation was required. However, when a request was made by a wholesale customer using the full national number search, the service would be rejected without the system first exploring alternate copper paths.

Telstra identified that this led to different outcomes for the ordering and provisioning of some wholesale ADSL services when compared to Telstra's Retail Business Unit. Telstra has advised that the breach is likely to have affected 282 wholesale customer end users from May 2012 to October 2014.

The overarching equivalence commitment in the SSU requires that Telstra ensures equivalence in the supply of regulated services, including wholesale ADSL and LSS, to wholesale customers and its Retail Business Units in respect of the operational systems, procedures and processes used in the supply of the relevant regulated service (clause 9(a) of the SSU). The SSU also requires Telstra to use an equivalent order management process to process all ADSL service orders received from wholesale customers and Retail Business Units (clause 11.3(a) of the SSU).

### Rectification proposal

Telstra submitted a Rectification Proposal to the ACCC on 12 June 2014 in relation to this issue, and provided a further revised Rectification Proposal to the ACCC on 26 August 2014. The ACCC accepted the revised Rectification Proposal on 26 September 2014.

As part of the Rectification Proposal, Telstra has:

- undertaken to implement system and process changes to ensure that full national number service qualification tests and results provide the same outcome for wholesale customers and Telstra Retail—through removal of the system's consideration of alternative copper paths for Telstra Retail queries
- as an interim measure, promoted alternative ordering options which will enable Telstra to select the copper pair capable of supporting ADSL until system and process changes are implemented
- communicated with its wholesale customers about the issue and its proposed solution
- offered free transfer of affected end users and compensation for affected wholesale customers.

The ACCC is satisfied that that these measures provide an effective remedy for the breach.

### *Item 11—Retesting of Line Fault (ROLF) process*

Telstra provided the following details in its Annual Compliance Report in relation to the breach:

#### **Description of the breach**

Systems and processes for handling BTS fault requests, for cases the subsequent retesting of the line fault indicated there is 'No Fault Found', caused Retail and Wholesale Customers to be placed in different 'ring-back queues' which had different processes for closing a fault report. This created the potential for differential treatment by Telstra of faults for the BTS for Retail and Wholesale Customers.

#### **Cause of the breach**

This matter arose from process and systems issues in respect of a subset of BTS faults. These issues meant that Retail Customers' fault tickets were placed in a 'ring-back queue' and these Retail Customers were then contacted to confirm the service had been restored before the fault report was closed, or if the Retail Customers were not contacted or indicated their service still had a fault, then Telstra proceeded with the commitment or appointment. In contrast, Wholesale Customers' fault tickets were placed in a different 'ring-back queue' and, in some circumstances, an automatic email notification was generated informing the Wholesale Customer that the fault report was closed. In other cases Wholesale Customers' fault tickets were automatically closed without any further contact made to the Wholesale Customer.

## ACCC findings

In 2013, Telstra became aware of an issue regarding the process it applies to BTS fault requests following inquiries by wholesale customers as to why some of their fault tickets had been closed without notice.

Where a fault report is received for BTS which requires a technician to attend to the fault, the report is allocated a fault ticket. If the technician's visit is scheduled more than 24 hours into the future, the ticket is subjected to a line testing process, called the 'Retesting of the Line Fault Test' (ROLF), to confirm that there is a fault in Telstra's network. Where the ROLF process returns a 'No Fault Found' (NFF) result, there were different processes for wholesale customer and Telstra Retail tickets.

In particular, where a Telstra Retail ROLF test resulted in a NFF result, the fault ticket was placed in the 'ring-back queue' whereby the retail customer would be contacted to confirm that their service was operational. If they were not contacted or they advised their service still had a fault, the Telstra technician proceeded with the visit. On the other hand, wholesale customers were required to request to be contacted if the ticket returned a NFF result. If the wholesale customer did not request to be contacted, the fault would remain open for seven days prior to being closed. If the wholesale customer did request to be contacted, they were required to respond within 24 hours of the notification (whether or not they were able to contact their end user). If they did not respond within 24 hours, Telstra would close the fault ticket.

Telstra has advised that between 1 October 2013 and 10 April 2014, over 7,200 wholesale customer BTS fault tickets went through the ROLF process and 5,700 of these returned a NFF result and were subsequently closed. Over 3200 of these tickets which had been closed were re-reported by the wholesale customer within seven days and around 1800 of them were shown to arise from a fault on Telstra's network.

In addition to the overarching equivalence commitment in clause 9(a), the SSU requires Telstra to maintain systems and processes for issuing tickets of work to field staff so regulated services are managed and performed by Telstra field staff in an equivalent manner (clause 11.1(a)) and to rectify BTS faults in an equivalent manner (clause 11.2(b)).

## Rectification proposal

Telstra submitted a Rectification Proposal to the ACCC in relation to this issue, which was accepted on 4 August 2014. Telstra implemented changes to its ROLF process on 8 May 2014, prior to acceptance of the proposal.

As part of the Rectification Proposal, Telstra has amended the ROLF process so that wholesale customers whose fault tickets return an NFF result are contacted by phone or email to either confirm or withdraw their fault report, consistent with the Telstra Retail process. The fault ticket will remain open until the wholesale customer responds, providing them with an opportunity to contact their end user and confirm that the fault is ongoing. If the wholesale customer does not respond by the due date, the technician's scheduled visit will proceed.

Telstra has also made a commitment that where further changes are necessary to its ROLF process during the operation of the Rectification Proposal, it will ensure that the changes are equivalent for retail and wholesale customers and that wholesale customers are advised of any changes which may affect them. The ACCC is satisfied that these measures provide an effective remedy for the breach.

## Other Rectification Proposals submitted during the reporting period

### *Fault rectification of the BTS*

Telstra provided the following details in its Annual Compliance Report in relation to this identified equivalence issue. This matter was reported in detail in the ACCC's 2012-13 report.

On 15 November 2012, Telstra notified the ACCC that, following continuing investigations into the Reporting Variance for Metric 5 in relation to fault rectification of the BTS, while inclement weather, high demand and the high number of medical priority tickets of work for Retail Customers remained possible reasons for the Reporting Variance, Telstra had identified two additional factors relating to the use of a severity level and the inadvertent removal of a Wholesale Customer code in its systems for processing faults which may have also contributed to the Reporting Variance in respect of BTS fault rectification.

## Background

In Telstra's operational equivalence reports for the June, September and December 2012 quarters, Telstra reported variances of more than two per cent in favour of Telstra Retail in relation to the performance measure for BTS faults (known as Metric 5). Metric 5 measures the percentage of BTS faults that are rectified within set timeframes for both Telstra Retail and wholesale customers. The reports indicated variances between the treatment of wholesale and retail faults as large as -5.79 per cent in relation to business customers and -4.36 per cent in relation to residential customers. As noted in the ACCC's 2012-13 report, the ACCC considers this issue raised concerns under clauses 9(a)(i), 9(a)(ii) and 11.1 of the SSU.

Telstra identified a number of potential reasons for the reporting variances, including that some contact centre staff had been incorrectly allocating an increased level of severity to a number of Telstra Retail BTS faults, the treatment of medical priority assistance faults as well as the removal of a wholesale code (the ZZZ code) which inadvertently resulted in wholesale customer faults being allocated a lower level of priority.

On 14 December 2012, Telstra submitted a Rectification Proposal to the ACCC in relation to this issue. At the ACCC's request, Telstra engaged the ITA Adjudicator to prepare a report on whether the Rectification Proposal would effectively address the issues identified and the cause(s) of the reporting variances. The ITA Adjudicator was also asked to consider any alternative measures that would be effective in addressing the cause(s) of the variances.

The ITA Adjudicator concluded that the most likely explanation for the reporting variances was the effect of dealing with medical priority assistance faults under Telstra's Universal Service Obligation and that the measures in the Rectification Proposal would be unlikely to lead to a change in the reporting variances or deal with the cause(s) of the reporting variances.

## Rectification proposal

In May 2014, Telstra submitted a revised Rectification Proposal in relation to this issue. Following ACCC consultation with wholesale customers on the revised Rectification Proposal, Telstra provided a further revised Rectification Proposal to the ACCC in September 2014.

The ACCC accepted the further revised Rectification Proposal on 15 October 2014. As part of the Rectification Proposal, Telstra has:

- committed to using a workforce management tool which operates during periods of high fault rates to better align resources with the volume of work required
- implemented changes to training materials and introduced prompts to ensure staff do not incorrectly allocate increased severity levels to Telstra Retail BTS faults, and will report to the ACCC on whether staff are allocating correct severity levels
- reinstated, as at November 2012, the ZZZ code.

The ACCC is satisfied that Telstra's Rectification Proposal provides an effective remedy and will result in competition and consumer benefits from Telstra allocating greater resources during periods of high faults rates. Since Telstra implemented the above steps, the ACCC has observed a noticeable improvement in Telstra's performance against Metric 5.

# Breaches of the Migration Plan

The Migration Plan governs the manner in which Telstra will cease to supply services over its copper and HFC networks and ultimately achieve structural separation. During the 2013-14 reporting period, a number of additional obligations under the Migration Plan came into effect—including Telstra's 'cease sale' and managed disconnection obligations.

Whilst Telstra generally complied with its Migration Plan obligations during this period, it reported a number of breaches of the new obligations in its Annual Compliance Report. The majority of these breaches were of a small scale and arose due to problems implementing new systems and operational processes. However, Telstra also adopted (with the ACCC's consent) a number of interim arrangements which were outside the Migration Plan in order to promote a more positive end user migration experience and to address ACCC concerns regarding service continuity and a lack of consumer awareness about the need to migrate.

## Cease sale

Telstra's cease sale obligations under clause 17 of the Migration Plan commenced in July 2013. These obligations require Telstra to cease supplying new copper and HFC services in NBN rollout regions 10 business days after the region has been declared Ready for Service by NBN Co.<sup>9</sup>

In its Annual Compliance Report, Telstra acknowledged that there were some initial compliance issues caused by pre-existing data quality issues and human error. As a result, a number of customers were provided with new copper or HFC services after the relevant region had been declared Ready for Service in breach of the cease sale provisions of the Migration Plan. Telstra has advised that the breaches occurred due to the following:

- missing data and misaligned end user address data causing incorrect service qualification results
- incorrect use of override codes by front-of-house staff
- front-of-house staff following the incorrect process for cease sale premises
- orders not being assessed properly for the cease sale by the cable assigner.

Telstra has advised that it has taken steps to:

- implement additional training and regular communication for front-of-house staff to remind them of Telstra's cease sale obligations
- provide coaching to staff involved in relevant instances of non-compliance.

Telstra is continuing to consider options for remediating the data quality issues within its systems and processes. Telstra has also undertaken to monitor and report to the ACCC on use of the relevant manual override codes by front-of-house staff.

In addition, Telstra reported some instances where it allowed connection of retail and wholesale services after the cease sale date in respect of end users whose retail service provider has exited the market in order to ensure that these end users were able to maintain continuity of service while they obtained a replacement NBN service.

In June 2013, Telstra requested ACCC approval to vary the Migration Plan so that the cease sale obligation would apply only to premises that are NBN serviceable or are determined by NBN Co to be 'Frustrated Premises' (for example, where there has been a conscious and persistent refusal by the owner of the premises to allow NBN Co to install infrastructure to enable the premises to be NBN connected). Telstra requested the proposed variation in response to

<sup>9</sup> The decision to declare a region as Ready for Service has been based on a 'properties passed' metric which does not require NBN Co to install all the necessary infrastructure to support an NBN service (for example, to connect the cable in the street to the customer's premises).

industry concerns about the need to reduce the likely number of end users who would not be able to obtain an NBN or copper fixed line service during the switchover period. The effect of the variation is to exclude premises from the cease sale obligation that are not yet capable of being connected to the NBN.

The ACCC considers that the revised cease sale arrangements ensure a better end user experience in migrating to the NBN and consented to Telstra implementing the arrangements prior to formal ACCC approval of the proposed Migration Plan variation, pending NBN Co and the Department of Communications settling the definition of Frustrated Premises.

## Disconnection obligations

Under clause 14 of the Migration Plan, Telstra is required to commence disconnecting all remaining copper and HFC services in the NBN rollout region from the 'Disconnection Date' (18 months after the relevant NBN Ready for Service date), subject to certain exceptions. The majority of managed disconnections must occur within 10 days of the Disconnection Date.

NBN Co declared the first 15 rollout regions as Ready for Service in November 2012, with the first set of managed disconnections scheduled to occur on 23 May 2014. Another 16 rollout regions were scheduled for disconnection in July and October 2014.

To address significant industry concerns that consumers in the first 31 rollout regions had not had a suitable opportunity to migrate their services due to delays in the physical connection of individual premises to the NBN, and the potential for such customers to be left without a service after the Disconnection Date, Telstra and NBN Co agreed upon revised disconnection arrangements. Under the interim disconnection arrangements, Telstra and other service providers have a further opportunity to contact customers and confirm they understand the need to migrate to the NBN if they wish to retain a service.

The ACCC was advised in advance that Telstra would be acting in this manner and considered the revised disconnection arrangements would reduce the risk of consumers and businesses losing their fixed line service during the migration to the NBN due to a lack of NBN serviceability or awareness of the need to migrate. Consequently, given the timing imperative and potential for significant consumer disruption, the ACCC consented to Telstra immediately implementing the revised disconnection arrangements without proceeding to seek a formal variation to the Migration Plan. Telstra has conducted briefings and provided materials to wholesale customers to ensure that they are aware of and understand what is required of them under these interim arrangements.

The government is now seeking to implement a Migration Assurance Policy and has sought views from the telecommunications industry and other interested stakeholders on the best way to improve the migration process to provide assurance to consumers that they can access services during and following the NBN transition period.

## Reconnection of premises previously Permanently Disconnected

In its Annual Compliance Report, Telstra reported several instances where copper services were supplied to wholesale or retail customers at premises which had previously been, and were required to remain, Permanently Disconnected under clause 18 of the Migration Plan and which did not fall within the relevant exceptions.

Telstra has advised that these instances included where:

- its internal processes had been incorrectly followed
- the end user was a Priority-Assistance customer and there were delays or issues associated with obtaining a required service on the NBN

- premises that were Service Class 1 (which were entitled to reconnection) were later re-classified as Service Class 0 by NBN Co after the premises were permanently disconnected.

Telstra has advised that, with the exception of premises which are classified as Service Class 0, the majority of reconnected services have now been restored to their Permanently Disconnected state. In addition, Telstra has confirmed that it has implemented improvements to its internal processes to further reduce the opportunity for such instances to occur.

The ACCC is satisfied that the steps taken by Telstra should ensure that Telstra complies with its obligations under clause 18 of the Migration Plan in future.

## Communication with Retail Customers about Disconnection Dates

Under clause 8.2 of the Migration Plan, Telstra is obliged to advise retail customers no less than three months before the Disconnection Date of the impending disconnection of their Premises from the copper and HFC networks.

Telstra reported a number of instances where it failed to notify retail customers in the first 15 NBN rollout regions within the required period. Telstra advised that this was due to:

- ongoing and frequent updates to end user address details which resulted in errors in the address list for disconnection for the relevant NBN rollout region
- inconsistencies within the service address data provided by NBN Co that caused confusion as to which end user addresses should be included in the address list for disconnection for the relevant NBN rollout region
- issues with its external mailing house.

The ACCC considers that the revised disconnection arrangements ensured that affected end users did not suffer detriment as a result of these breaches. Telstra is also working with NBN Co to ensure that it is clear which premises fall within the relevant NBN rollout region so that they are contacted in the required period.

## ACCC action

During the 2013-14 reporting period, the ACCC has continued to focus on stopping conduct of potential concern as it comes to light and ameliorating its impact. The ACCC has also focussed on identifying areas for improvement in Telstra's systems and processes to ensure its SSU and Migration Plan obligations are being implemented effectively and in a robust manner.

The ACCC investigated two breaches of Telstra's overarching equivalence commitment and subsequently accepted Rectification Proposals in relation to these breaches. The ACCC also consulted on and accepted a third Rectification Proposal with respect to an issue which had been identified in the 2012-13 reporting period and reported in the ACCC's 2012-13 report. The ACCC is satisfied that these three Rectification Proposals provide an effective means of remedying the relevant equivalence issues.

The ACCC monitors and receives regular updates from Telstra on its information security remediation project in relation to its IT systems and processes. The ACCC has also monitored Telstra's performance against the equivalence and transparency metrics in the 2013-14 reporting period and conducted investigations where variances have been identified.

The ACCC receives a number of additional reports from Telstra in relation to its obligations under the SSU and the Migration Plan. The ACCC continues to critically examine these reports to ensure that any potential equivalence concerns or migration issues are identified, considered and addressed.

The ACCC ran two Wholesale Telecommunications Consultative Forums in 2013-14 in order to facilitate greater engagement between Telstra and industry in relation to potential issues arising under the SSU and Migration Plan. These forums covered a wide range of issues and the ACCC considers that they have provided an effective platform for wholesale customers to raise issues with Telstra.

The ACCC continues to encourage Telstra to provide regular updates to wholesale customers on interim equivalence and Migration Plan issues as they arise so that steps can be taken to minimise any impact on their business.

## Further information

Telstra's SSU and Migration Plan are available at:

- the ACCC website: <http://www.accc.gov.au>
- the Telstra Wholesale website:  
<http://www.telstrawholesale.com.au/about/structural-separation-undertaking/index.htm>  
<http://www.telstrawholesale.com.au/nbn/migration-plan/index.htm>

The legislation and legislative instruments underpinning the SSU and Migration Plan are available at the Department of Communications website: [http://www.communications.gov.au/policy\\_and\\_legislation/telecommunications\\_regulatory\\_reform\\_separation\\_framework](http://www.communications.gov.au/policy_and_legislation/telecommunications_regulatory_reform_separation_framework)

## ACCC contacts

ACCC Infocentre: business and consumer inquiries: 1300 302 502

Website: [www.accc.gov.au](http://www.accc.gov.au)

Translating and Interpreting Service: call 13 1450 and ask for 1300 302 502

TTY users phone: 1300 303 609

Speak and Listen users phone 1300 555 727 and ask for 1300 302 502

Internet relay users connect to the NRS (see [www.relayservice.com.au](http://www.relayservice.com.au) and ask for 1300 302 502)

## ACCC addresses

### National office

23 Marcus Clarke Street  
 Canberra ACT 2601  
 GPO Box 3131  
 Canberra ACT 2601  
 Tel: 02 6243 1111  
 Fax: 02 6243 1199

### New South Wales

Level 20  
 175 Pitt Street  
 Sydney NSW 2000  
 GPO Box 3648  
 Sydney NSW 2001  
 Tel: 02 9230 9133  
 Fax: 02 9223 1092

### Victoria

Level 35  
 The Tower  
 360 Elizabeth Street  
 Melbourne Central  
 Melbourne Vic 3000  
 GPO Box 520  
 Melbourne Vic 3001  
 Tel: 03 9290 1800  
 Fax: 03 9663 3699

### Queensland

*Brisbane*  
 Level 24  
 400 George Street  
 Brisbane Qld 4000  
 PO Box 12241  
 George Street Post Shop  
 Brisbane Qld 4003  
 Tel: 07 3835 4666  
 Fax: 07 3835 4653

### *Townsville*

Suite 2, Level 9  
 Suncorp Plaza  
 61-73 Sturt Street  
 Townsville Qld 4810  
 PO Box 2016  
 Townsville Qld 4810  
 Tel: 07 4729 2666  
 Fax: 07 4721 1538

### South Australia

Level 2  
 19 Grenfell Street  
 Adelaide SA 5000  
 GPO Box 922  
 Adelaide SA 5001  
 Tel: 08 8213 3444  
 Fax: 08 8410 4155

### Western Australia

3rd floor, East Point Plaza  
 233 Adelaide Terrace  
 Perth WA 6000  
 PO Box 6381  
 East Perth WA 6892  
 Tel: 08 9325 0600  
 Fax: 08 9325 5976

### Northern Territory

Level 8  
 National Mutual Centre  
 9-11 Cavenagh St  
 Darwin NT 0800  
 GPO Box 3056  
 Darwin NT 0801  
 Tel: 08 8946 9666  
 Fax: 08 8946 9600

### Tasmania

Level 2  
 70 Collins Street  
 (Cnr Collins and Argyle  
 Streets)  
 Hobart Tas 7000  
 GPO Box 1210  
 Hobart Tas 7001  
 Tel: 03 6215 9333  
 Fax: 03 6234 7796



Australian  
Competition &  
Consumer  
Commission

[www.accc.gov.au](http://www.accc.gov.au)