Telstra’s Structural Separation Undertaking

Annual Compliance Report
2015–16

Report to the Minister for Communications and the Arts
20 February 2017

The Hon. Senator Mitch Fifield
Minister for Communications and the Arts
Parliament House
CANBERRA ACT 2600

Dear Minister

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

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

Enclosed is the ACCC’s report for the 2015-16 financial year. Please note that subsection 105C(3) of the Act requires you to table the report in each House of Parliament within 15 sitting days of that House after receiving the report.

Yours sincerely

[Signature]
Rod Sims
Chairman
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>1</td>
</tr>
<tr>
<td>Breaches of the SSU and Migration Plan</td>
<td>1</td>
</tr>
<tr>
<td>ACCC actions</td>
<td>2</td>
</tr>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td><strong>Telstra’s Structural Separation Undertaking</strong></td>
<td>5</td>
</tr>
<tr>
<td>Interim equivalence and transparency</td>
<td>6</td>
</tr>
<tr>
<td>Compliance reporting</td>
<td>6</td>
</tr>
<tr>
<td><strong>The ACCC’s approach to compliance and enforcement</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>Breaches of the SSU</strong></td>
<td>9</td>
</tr>
<tr>
<td>Information security</td>
<td>9</td>
</tr>
<tr>
<td>Price equivalence and transparency</td>
<td>13</td>
</tr>
<tr>
<td><strong>Other SSU developments</strong></td>
<td>17</td>
</tr>
<tr>
<td><strong>Telstra’s Migration Plan</strong></td>
<td>19</td>
</tr>
<tr>
<td>Interim disconnection and migration arrangements</td>
<td>19</td>
</tr>
<tr>
<td>Compliance activity for ACCC approval</td>
<td>20</td>
</tr>
<tr>
<td>Breaches of the Migration Plan</td>
<td>20</td>
</tr>
<tr>
<td><strong>ACCC actions</strong></td>
<td>24</td>
</tr>
<tr>
<td><strong>Further information</strong></td>
<td>25</td>
</tr>
<tr>
<td><strong>ACCC contacts</strong></td>
<td>26</td>
</tr>
</tbody>
</table>
Executive summary

In 2015–16, Telstra continued to demonstrate a commitment to improving its level of compliance with its Structural Separation Undertaking (SSU). There was a reduced number of breaches reported by Telstra during the year, and Telstra continued to dedicate resources to its now completed Information Security Remediation program.

The compliance issues discussed in this report largely arise from errors made by Telstra staff in the course of their day-to-day work which has resulted in the unauthorised disclosure of confidential or commercially sensitive information regarding wholesale customers (Protected Information). Though a small number of SSU breaches have been identified, the ACCC considers that, overall, Telstra’s level of compliance has improved during the year and Telstra has responded to breaches in a positive manner.

The year also marked the conclusion of Telstra’s Information Security Remediation program which was undertaken by Telstra to address a number of significant IT-related breaches identified in previous years. The program included a review of Telstra’s IT systems and remediation to prevent unauthorised disclosure of wholesale customer information. The ACCC engaged Ovum, an external consultant, to conduct a thorough review of the program in early 2015. The ACCC is satisfied that the remediation project is now complete and all outstanding issues in relation to Telstra’s IT systems have been addressed. The program also included the implementation of a new Compliance Management Framework which the ACCC considers should ensure a continued focus by Telstra on its SSU compliance.

The ACCC also continued to monitor Telstra’s performance against its Migration Plan obligations. The Migration Plan outlines how Telstra will progressively migrate its voice and broadband services from its copper and HFC\(^1\) networks to the National Broadband Network (NBN). While Telstra generally complied with its Migration Plan obligations, it reported a small number of minor breaches. These generally relate to delays in publishing disconnection schedules and the reconnection of services to premises previously disconnected or not permitted under cease sale obligations.

Breaches of the SSU and Migration Plan

Information security obligations

The SSU contains a number of obligations that are intended to prevent Telstra from using confidential or commercially sensitive wholesale customer information that it receives in the course of supplying regulated services (Protected Information) to disadvantage wholesale customers in retail markets.

As with previous years, the most common SSU compliance issue during the year was Telstra’s failure to prevent unauthorised disclosure of Protected Information. These issues arose as a result of a number of isolated incidents that occurred due to staff error.

In each of the three reported instances, Telstra took action to contain the risk and sought to address the issue through coaching and ongoing training.

These matters are discussed further on pages 9–13.

---

1 Hybrid fibre-coaxial.
Price equivalence and transparency

The SSU contains various price equivalence and transparency obligations that are designed to improve transparency of Telstra’s internal cost allocations and the prices charged to wholesale customers. These obligations include the requirement that Telstra publish and maintain a rate card specifying the prices for regulated services.

During the year, the ACCC identified two breaches by Telstra of this requirement. The first instance concerned Telstra failing to update its rate card to reflect the ACCC’s October 2015 final access determinations (FAD) for the fixed-line services, until five days after the FADs came into effect (and 15 business days after being notified that the changes would be required).

The second instance related to the ACCC’s April 2016 FAD for the domestic transmission capacity service. Telstra updated the rate card 40 business days after the FAD came into effect.

While Telstra does not consider these matters to be breaches of the SSU, it has advised the ACCC that where necessary, a billing adjustment was made to reflect the new prices set in the FADs. In these particular circumstances, the ACCC considers that the breaches did not have a material adverse impact on wholesale customers. However, the ACCC expects that Telstra will update its rate card promptly following any future price changes for declared services.

The ACCC notes that in different circumstances, relating to newly-declared services, the SSU specifies a timeframe of five business days in which Telstra must publish a new rate card.

The SSU does not specify a timeframe within which a rate card must be updated following a price change to an already-declared service. In the ACCC’s view, in these circumstances the SSU requires a revised rate card to be published within a reasonable time, considering all the circumstances.

These matters are discussed further on pages 13–16.

Migration Plan obligations

Telstra also breached some aspects of its Migration Plan obligations during the 2015–16 reporting period. These breaches occurred where Telstra failed to block orders from being provisioned or other requests from being processed, as required to support migration to the NBN.

Specifically, Telstra identified a small number of instances where it supplied premises that had previously been permanently disconnected, or connected services that were not permitted under Telstra’s cease sale obligations. These identified breaches were attributed to system or data quality issues and/or human error. Telstra reaffirmed its commitment to actively identify opportunities to improve its Migration Plan compliance. Telstra will continue to coach staff on their obligations and seek to resolve any issues within its systems in the next reporting period.

These matters are discussed further on pages 19–23.

ACCC actions

During the 2015–16 reporting period, the ACCC continued to focus on stopping conduct of potential concern and ameliorating its impact. The ACCC has also continued to focus 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.

In March 2015, the ACCC initiated an independent review of Telstra’s IT systems, engaging external consultant Ovum to assess whether the systems were fully remediated so as to prevent staff in a retail business unit from accessing wholesale customer Protected Information. The
review identified a small number of outstanding issues in three of Telstra’s IT systems. During the 2015–16 year, Telstra has worked in cooperation with the ACCC and Ovum to resolve the remaining IT system issues, and the remediation project is now complete.

The ACCC has also monitored Telstra’s performance against the equivalence and transparency metrics in the 2015–16 reporting period and will continue to monitor these in upcoming reporting periods so as to identify and prevent any patterns of concern emerging.
Introduction

On 27 February 2012, the ACCC accepted a Structural Separation Undertaking (SSU) from Telstra. The SSU 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 are fundamental to promoting competitive outcomes during the transition period.

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.

This report outlines breaches of the SSU by Telstra for the period 1 July 2015 until 30 June 2016 and the steps Telstra has taken or proposes to take in order to remedy these breaches.

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 matters. Some of the ACCC’s findings that a breach has occurred do not accord with views Telstra has expressed to the ACCC. Telstra’s views are expressly noted in the body of this report.

During the 2015–16 reporting period, several variations were made to the obligations contained in Telstra’s Migration Plan. These changes were necessary to support the June 2015 variation of the Migration Plan to facilitate NBN’s shift to a multi-technology mix (MTM) rollout model. The revised Migration Plan obliged Telstra to develop and publish replacement measures with updated disconnection processes to ensure that the framework supported a smooth transition for end-users to the NBN.

Following the approval of the MTM variation to the Migration Plan, Telstra and NBN Co identified aspects of the Migration Plan where further changes were needed to ensure service continuity for end-users. The ACCC exercised regulatory forbearance with respect to Telstra’s Migration Plan obligations and permitted an interim extension of the disconnection timeframes for certain services (such as, fire alarms and lift phone services). These arrangements were permitted on the basis that they were consistent with the Migration Plan Principles and with the expectation that Telstra would proceed to incorporate these changes in a formal variation to the Migration Plan.

Telstra lodged a proposal to vary the Migration Plan on 9 May 2016 and this variation was accepted by the ACCC on 20 July 2016. This report has been prepared on this basis.

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. The ACCC continues to encourage Telstra to keep its wholesale customers informed of any SSU equivalence and migration issues.
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 framework 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.\(^2\) 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 framework 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 NBN will be concluded.
- Interim equivalence and transparency obligations regarding access to Telstra’s regulated services in the period leading up to the Designated Day.\(^3\)
- 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.\(^4\) 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 arrangements.

---

2 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.

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

4 Pursuant to section 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

Telstra’s structural separation will occur progressively as Telstra ceases to supply fixed line voice and broadband services over its copper and HFC networks and commences to supply those services over the NBN as it is rolled out. In order to promote competition during the interim period from the commencement of the SSU 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—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.  

---

5 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.
• 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 matters 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.

In addition to Telstra’s reporting obligations, the ACCC may detect non-compliance in other ways such as directly receiving complaints from wholesale customers or through the ACCC’s own independent monitoring.

The ACCC has considered Telstra’s monthly compliance reports relating to the period between 1 July 2015 and 30 June 2016 and Telstra’s Annual Compliance Report for 2015–16 (Annual Compliance Report).

Matters reported in Telstra’s Annual Compliance Report

In its Annual Compliance Report, Telstra reported eight matters as being possible breaches of the SSU. These matters include:

• three instances where Telstra possibly breached its obligation to safeguard Protected Information pursuant to clause 10.4 of the SSU

• four instances (all of which were reported in the ACCC’s 2014–15 report) where Telstra retail staff had access to systems that contained Protected Information in breach of clause 10.4 of the SSU, and

• continuing information security issues in parts of four IT systems previously reported in breach of clause 10.4 of the SSU.
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. A breach of the SSU is also a breach of Telstra’s carrier licence conditions, which can attract a fine of up to $10 million.

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. 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 Telstra complies with its 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.

---

Breaches of the SSU

This section details several instances where the ACCC considers, on the balance of probabilities, that Telstra breached its SSU obligations. These breaches relate to Telstra’s information security obligations and price equivalence and transparency obligations in circumstances where:

• Telstra has reported that it has breached the SSU in its Annual Compliance Report, or
• the ACCC has identified the conduct and considers it a breach of the SSU.

Information security

The SSU contains information security obligations designed to safeguard Protected Information obtained by Telstra in the course of supplying regulated services to wholesale customers. 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, and
• further restrictions on disclosing other information unless, with the approval of the ACCC, it makes the information available to wholesale customers at the same time.

Importantly, Telstra must protect any:

• confidential or commercially sensitive information obtained directly from wholesale customers for the purpose of, or in the course of, Telstra supplying regulated services—such as the end-user’s name, address and service type, and
• 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 provision recognises 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 three breaches of its information security obligations in the SSU which have not previously been reported by the ACCC. These are outlined below. Two breaches relate to Protected Information being disclosed to staff in a retail business unit while the other relates to Protected Information being disclosed to a network services business unit employee. All three breaches were due to emails sent in error.

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 at the request of the ACCC.

In addition to the remediation action set out below, Telstra has indicated it will also undertake the following tasks to prevent, to the extent that it can, future similar instances from occurring:

- encourage staff to turn off auto-populating and suggested names in Outlook
- encourage staff to seek management or legal advice before any sort of information is distributed to non-Telstra Wholesale workgroups, and
- continue emphasising the importance of checking email recipients before hitting ‘send’ in all induction and refresher SSU staff training.

**Item 1—Email sent in error**

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

<table>
<thead>
<tr>
<th>Description of the breach</th>
<th>Cause of the breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>An email including an attachment with wholesale customer Protected Information was mistakenly sent by a wholesale business unit staff member to one retail business unit staff member.</td>
<td>This incident was attributable to human error by an individual wholesale business unit employee who sent the email to the wrong person.</td>
</tr>
</tbody>
</table>

**ACCC findings**

On 10 August 2015, a wholesale business unit employee mistakenly sent an email containing Protected Information to a retail business unit employee in breach of clause 10.4.

The Protected Information disclosed to the retail business unit employee included:

- names of wholesale customers
- service numbers
- order numbers, and
- LinxOnline Ordering (LOLO) references.

**Remediation undertaken by Telstra**

Telstra considered that this was an isolated incident of inadvertent disclosure due to human error. Remediation focused on mitigating the risk associated with the disclosure and reducing the risk of recurrence.
Telstra has advised that it became aware of the error on the same day and immediately contacted the retail business unit employee to delete the email and confirm the information was not distributed, disclosed, stored or used in any way. The retail business unit employee confirmed the necessary actions had been taken.

Telstra also advised that it has provided coaching to the wholesale business unit employee about the importance of checking recipient names before sending emails and the importance of complying with the obligations under the SSU.

The ACCC is satisfied that the actions taken by Telstra were appropriate in minimising the risk of any competitive harm occurring, and the risk of recurrence.

**Item 2—Email sent in error**

In its Annual Compliance Report, Telstra provided the following details in relation to item 2:

<table>
<thead>
<tr>
<th>Description of the breach</th>
<th>Cause of the breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>An email containing limited information that may constitute wholesale customer Protected Information was mistakenly sent by a wholesale business unit staff member to one network services business unit staff member who did not have a need to know the information contained in the email.</td>
<td>This incident was attributable to a human error by an individual Telstra wholesale business unit staff member who sent the email to the network services business unit staff member who had the same name as the intended recipient of the information.</td>
</tr>
</tbody>
</table>

**ACCC findings**

In February 2016, a Telstra network services business unit employee was sent an email containing Protected Information. The email was sent to the network services business unit employee because that employee had the same name as the intended recipient of the email.

The information in the email included the name of a wholesale customer, the fact that the wholesale customer obtains particular services as a bundle and the price the wholesale customer pays for one of those services.

The ACCC considers that in this instance, wholesale customer Protected Information was disclosed by the wholesale business unit employee to the network services business unit employee in breach of clause 10.4.

**Remediation undertaken by Telstra**

Telstra considered that the disclosure was an isolated incident, so its remediation efforts focused on mitigating the risk associated with the disclosure and coaching staff to minimise the risk of recurrence.

Telstra advised that the mistake was identified the following business day that the email was sent, and the network services business unit employee was contacted and instructed to delete the email. Telstra has advised that the network services business unit employee confirmed that the email was deleted and that they did not forward the email or use the information contained in the email.

Telstra also advised that it has provided coaching to the wholesale business unit employee about their obligations under the SSU in relation to wholesale customer Protected Information.

The ACCC considers that the action taken by Telstra following identification of the issue minimised the risk of any competitive harm occurring as a result of the conduct.
Item 3—Email sent in error

In its Annual Compliance Report, Telstra provided the following details in relation to item 3:

<table>
<thead>
<tr>
<th>Description of the breach</th>
<th>Cause of the breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>An email containing information that is potentially wholesale customer Protected Information was sent in error by a network services business unit staff member to one retail business unit staff member. A second retail business unit staff member was sent this email for the purposes of submitting the web form for the SSU investigation of this matter.</td>
<td>This incident was attributable to a human error by an individual network services business unit staff member who sent the email to the retail business unit staff member in error. The email was then sent on to another retail business unit staff member for the purpose of lodging a web form to trigger an investigation.</td>
</tr>
</tbody>
</table>

ACCC findings

On 14 January 2016, a network services business unit employee inadvertently sent an email containing Protected Information, including the service address of a wholesale customer, to a retail business unit employee. The retail business unit employee forwarded the email to another retail business unit employee for the purposes of initiating an SSU investigation.

The ACCC considers wholesale customer Protected Information was disclosed by the network services business unit employee to the retail business unit employees in breach of clause 10.4.

Remediation undertaken by Telstra

Telstra considered that the disclosure was inadvertent and isolated in nature. As such, its remediation efforts focused on mitigating the risk associated with disclosure and minimising recurrence.

Telstra has advised that upon becoming aware of the error six days later, it contacted the retail business unit employees and requested that they delete the email. Telstra advised that the retail business unit employees confirmed that they had done so and did not forward or use the information contained in the email (other than for the purpose of the SSU investigation).

Telstra also advised that it has provided coaching to the network services business unit employee who sent the email to help prevent the occurrence of an email being sent with Protected Information to a retail business unit employee in the future.

The ACCC is satisfied that the actions taken by Telstra were appropriate in minimising the risk of any competitive harm occurring, and the risk of recurrence.

Price equivalence and transparency

The SSU also contains price equivalence and transparency obligations. These are designed to ensure transparency of Telstra’s internal cost allocations and the prices charged to wholesale customers.

Telstra’s price and transparency obligations are contained in clause 18 of the SSU. These obligations include a requirement that Telstra update and maintain a rate card which specifies the prices for regulated services as set by the ACCC.
The SSU and price equivalence and transparency

Clause 18 of the SSU sets out what Telstra must do to meet its price equivalence and transparency obligations.

Clause 18.3 (in conjunction with Schedule 8) of the SSU provides that Telstra will publish and maintain a rate card with prices for:

- the unconditional local loop service, line sharing service, wholesale line rental, local carriage service, public switched telephone network originating access, public switched telephone network terminating access, domestic transmission capacity service, mobile terminating access service and the wholesale asymmetrical digital subscriber line service
- the Telstra Exchange Building Access service, and
- any other declared service.

The relevant prices for each service are those specified by the ACCC from time to time in:
- a binding rule of conduct
- a final access determination, or
- an interim access determination.

Telstra is not required to publish a price for the above listed services for any period that there is no final access determination (FAD), interim access determination or binding rule of conduct in force.

Breaches identified by the ACCC

During the reporting period, the ACCC identified two technical breaches of Telstra’s price equivalence and transparency obligations under the SSU. These breaches related to delays by Telstra in updating its wholesale rate card to reflect the ACCC’s final access determinations for the fixed-line services and domestic transmission capacity service.

In each instance, Telstra provided a description and explanation for the conduct on request by the ACCC. Telstra disagrees that its failures to promptly update the rate card amount to breaches of clause 18.3 of the SSU. Telstra has noted that the SSU does not specify a timeframe in which the rate card must be updated and that it has worked on the understanding that it will update the rate card within a reasonable time for already-declared services.

Item 4—Failure to promptly update the rate card—Fixed Line Services FAD

ACCC findings

Under clause 18.3 of the SSU, Telstra is required to publish and maintain a rate card setting out the prices of regulated services as determined by the ACCC. On 9 October 2015 the ACCC made a FAD setting out the price and non-price terms for the seven fixed-line services. The FAD came into force on 1 November 2015. Telstra updated the rate card on 6 November 2015.

---

7 ACCC, Public inquiry into final access determinations for fixed line services, Final Decision, October 2015. Accessed here: http://www.accc.gov.au/system/files/FSR%20FAD%20Final%20Decision%20Report%20-%20Public%20Version.pdf. The fixed line services are: the unconditioned local loop service, line sharing service, fixed originating access service (previously the public switched telephone network originating access service), fixed terminating access service (previously the public switched telephone network terminating access), wholesale line rental, local carriage service and wholesale ADSL service.
The ACCC considers the five business day delay—from the date the FADs took effect—in Telstra updating the rate card amounts to a technical breach of Telstra’s price equivalence and transparency obligations. Given Telstra had 15 business days’ notice that references prices for the seven fixed-line services were going to change, the ACCC considers it reasonable to expect the rate card to have been updated on 1 November 2015.

Telstra disagrees that the failure to update the rate card on 1 November 2015 when the FAD came into effect amounts to a breach of clause 18.3 of the SSU. Telstra has argued that the SSU does not specify a particular timeframe in which the rate card must be updated when the price for an already-declared service is changed, and attributes the delay to issues around its appeal of the decision and how to address this when updating the rate card. The ACCC does not consider this interpretation aligns with Telstra’s express obligation to ‘maintain’ a rate card setting out prices for declared services as specified from time to time by the ACCC in a FAD, interim access determination or binding rule of conduct.

The ACCC considers that, when the price for an already-declared service is changed, Telstra must update the rate card to reflect the change within a reasonable period of time, taking into account the date when Telstra is notified of the price change and the date when it comes into effect. In this case, when Telstra had 15 business days’ notice of the price change, then took over 5 business days following the price change to update the rate card, the ACCC considers Telstra breached clause 18.3 of the SSU.

Remediation undertaken by Telstra

Telstra advised that where necessary, wholesale customers received a billing adjustment (for the period between 1 November 2015 and 6 November 2015 when Telstra updated the rate card) to reflect the new prices set by the ACCC in the FAD.

In these circumstances, the ACCC does not consider the breach had a material adverse impact on wholesale customers.

Item 5—Failure to promptly update the rate card—DTCS FAD

ACCC findings

Under clause 18.3 of the SSU, Telstra is required to publish and maintain a rate card setting out the prices of regulated services as determined by the ACCC. On 21 April 2016, the ACCC made a FAD setting out the price and non-price terms for the domestic transmission capacity service (DTCS), with immediate effect. Telstra updated the rate card on 16 June 2016.

The ACCC considers the 40 business days’ delay in Telstra updating the rate card from the date the price changed amounts to breach of Telstra’s price equivalence and transparency obligations (see the above discussion of the ACCC’s views on Telstra’s obligations under clause 18.3 in these situations).

While immediately updating the rate card would not have been a reasonable expectation on Telstra given the FAD was released on the same day it took effect and the pricing model for DTCS is fairly complex, the ACCC considers that the 40 business days’ delay is an unreasonably long period to update the rate card and amounts to a breach of clause 18.3 of the SSU.

---

Remediation undertaken by Telstra

Telstra advised that where necessary, wholesale customers received a billing adjustment (for the period between 21 April 2016 and 16 June 2016 when Telstra updated the rate card) to reflect the new prices set by the ACCC in the FAD.

Given this, the ACCC does not consider the breach had a material adverse impact on wholesale customers.
Other SSU developments

In 2015–16, Telstra completed its Information Security Remediation program that it commenced in 2012 to address a number of significant IT information security system issues. These issues related to Telstra’s SSU commitment to prevent the unauthorised disclosure of Protected Information to Telstra retail business units so as to not disadvantage wholesale customers.

Summary of Telstra’s information security remediation

Telstra remediated a total of 42 IT systems as part of its remediation project. The ACCC understands the remediation project has been complex and has involved systems changes, process and operational changes as well as behavioural controls where the system is unable to be fully separated.

While Telstra had completed the majority of its remediation work by March 2015, it continued working during the 2015–16 year to address a small number of outstanding issues identified in a review by Ovum—an external consultant engaged by the ACCC to assess the thoroughness of the remediation program.

Remediation of all systems was completed by June 2016, with minor residual work relating to a data clean up exercise occurring in July and August 2016.

The ACCC notes that as part of the IT remediation project, Telstra also developed a new Compliance Management Framework which is now part of its business as usual operations.

Review of IT remediation work

On 5 March 2015, the ACCC engaged Ovum as an independent expert consultant to examine and report on Telstra’s IT system remediation program. As part of this review, the ACCC selected a sample of eight systems for independent testing. The review identified that three of these systems still contained Protected Information that may have been visible to retail business unit users under specific, limited circumstances. These systems have now been remediated, and Ovum has verified the remediation.

In February 2016, Ovum concluded in its final report to the ACCC that Telstra’s approach to its remediation project was appropriate considering its scale, and that Telstra has brought its systems into compliance with the SSU. Ovum recommended that the ACCC continue to rely on Telstra’s internal Compliance Management Framework and self-reporting mechanisms in the SSU.


Telstra’s internal due diligence review

Following Ovum’s initial review which identified a small number of outstanding IT issues, Telstra decided to conduct a further ‘due diligence’ review of its remediation project. As part of this review, Telstra assessed all 24 of its systems accessible by its retail business unit staff.

As part of its due diligence review, Telstra identified a small number of additional issues in four of the systems which arose in specific, limited situations. These issues were reported by the ACCC in last year’s report.⁹

Telstra commenced remediation of these systems in December 2015 and completed remediation in the first half of 2016.

Compliance Management Framework

Telstra’s IT remediation project also included the development of a new Compliance Management Framework for the ongoing protection of wholesale customer information under the SSU. The Framework is built to help embed Telstra’s SSU responsibilities across the company through changes in system and product development processes, and staff training. It focuses on promoting awareness, implementing preventive controls, and detective controls to ensure preventative controls are working effectively.

In its final report to the ACCC, Ovum concluded that the implementation of Telstra’s Compliance Management Framework should prevent new issues from arising or alternatively, allow the reporting of new issues as they arise (through compliance checks and company training).

The ACCC considers the implementation of the Framework is a positive initiative which should help strengthen controls and reduce the potential for future breaches.

ACCC conclusions

The ACCC is satisfied that the remediation project is now complete and that the actions taken by Telstra were appropriate in remedying the outstanding IT systems issues. The ACCC is also satisfied that Telstra’s SSU reporting measures can be relied on to identify any further information security issues, should they arise.

Telstra has dedicated a significant amount of resources to the completion of its Information Security Remediation project and appears committed to improving compliance with its Information Security obligations under the SSU.
Telstra’s 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. Telstra’s obligation to disconnect customers from its copper and HFC networks changed during the year, following re-negotiation of the agreements between Telstra and NBN Co. Telstra operated under regulatory forbearance from the ACCC during the period of negotiation, which allowed Telstra to implement modified arrangements which resulted in a better migration experience for end-users and industry.

Interim disconnection and migration arrangements

During the 2015–16 reporting period, Telstra operated under a revised Migration Plan that was modified to facilitate the shift to a multi-technology mix rollout model adopted by NBN Co.

Following the ACCC’s approval of the MTM variation to the Migration Plan, Telstra and NBN Co identified aspects of the Migration Plan that required additional flexibility to ensure service continuity for some end-users that have placed an order for an NBN service, or acted late in deciding to migrate their services to the NBN. The arrangements also provided industry participants affected by the increased number of premises subject to NBN migration and disconnection activity additional time to service these premises.

Specifically, the following interim arrangements were consented to by the ACCC:

- August 2015, the implementation of transitional managed disconnection arrangements for In-Train orders, fire alarms and lift phone services. This provided additional time for NBN Co to connect an increased number of premises to the NBN and allowed Retail Service Providers (RSPs) to complete the installation of their servicing equipment.
- September 2015, an extension to the Disconnection Date for registered fire alarm and lift phone services, so these services do not face mandatory disconnection until after 30 June 2017.
- October 2015, the implementation of transitional arrangements for premises with disconnection scheduled to occur over the 2015–16 Christmas and New Year period. This also provided a short extension to promote customer awareness and minimise disruption to customers before disconnection steps were taken.
- February 2016,
  - a further extension of the interim arrangements for In-Train order premises that allowed RSPs additional time to connect NBN services prior to Telstra commencing service disconnection.
  - an extended disconnection timeframe equivalent to In-Train order premises for some Service Class 0 premises (i.e. premises that are planned to be serviced by fibre) with a Disconnection Date occurring between February and October.
  - a deferred Disconnection Date for some premises that were subject to a change in NBN technology from fibre to the premises to fibre to the basement. This also provided additional time for RSPs to develop products to service these premises.

On 9 May 2016, Telstra proposed a revision to the Migration Plan for ACCC approval. These changes were designed to formalise the interim migration and disconnection arrangements that had already been implemented by Telstra and NBN Co with ACCC consent. It also included a proposal to amend the framework for disconnecting Special Services (business grade services) to accommodate NBN Co’s release of additional wholesale product functionality by access technology. The ACCC approved the variation on 20 July 2016 as the proposed variations were considered to be consistent with the Migration Plan Principles.
The ACCC’s role in approving the revised Migration Plan was limited to determining whether the proposal was consistent with the legislative requirements and complies with the Migration Plan Principles issued by the Australian Government in 2015.

Compliance activity for ACCC approval

Under the revised Migration Plan approved in June 2015, Telstra was required to reassess its disconnection and migration related processes set out in the Migration Plan, and develop and publish changes to those processes to reflect the transition to the multi-technology NBN rollout model. During the reporting period, the ACCC accepted the following replacement Required Measures:

1. Pull Through Consents and Pull Through Exception Event and Installation of Temporary Cable Notifications (Required Measures 1 (a) and (b))
2. Process for Managed Disconnection of Copper Services from the Disconnection Date (Required Measure 2)
3. Process for Managed Disconnection of HFC Services from the Disconnection Date (Required Measure 3), and
4. Process for Telstra to Build Copper Paths at Premises which had been Permanently Disconnected in order to Supply Special Services and Special Service Inputs (Required Measure 4).

Telstra was also required to consider whether its business-as-usual disconnection processes that are outlined in Schedules 1 and 2 of the Migration Plan were appropriate. The ACCC accepted the revision to Schedule 1 and noted its consistency with the industry guidelines developed by the Communications Alliance. The revision of Schedule 2 (relating to the disconnection processes for HFC services) remains outstanding, however, pending the finalisation of the relevant Communications Alliance guideline.

Breaches of the Migration Plan

During the reporting period, a further 348 NBN rollout regions reached their Disconnection Date. There are now 452 NBN rollout regions that have reached their Disconnection Date with managed disconnections occurring on a monthly basis. Telstra has indicated that a further 142 NBN rollout regions will occur during the first half of the next reporting period.

Whilst Telstra generally complied with its Migration Plan obligations during the period, it reported a number of minor breaches. Prior to the approval of the May 2016 variation proposal of the Migration Plan, Telstra adopted a number of interim disconnection arrangements. The ACCC has considered Telstra’s compliance with the Migration Plan having regard to these interim disconnection arrangements which were adopted in order to promote service continuity and to ensure that end-users were not left without a working service.

The following sections detail Telstra’s specific breaches of the Migration Plan.

Notification of the disconnection schedule

Under clause 7 of the Migration Plan, Telstra is obliged to publish a disconnection schedule for the benefit of wholesale and retail customers, and to update that schedule within five business days of receiving notification of a change. Following the approval of the varied Migration Plan in June 2015, the disconnection schedule was expanded to include a number of additional reportable fields relating to key roll-out or Disconnection Dates.

Telstra has advised that there were some instances where Telstra published the disconnection schedule later than the prescribed five days after receipt of notification from NBN Co of a new or updated rollout region Ready for Service Date. Telstra attributes the short delay to human
error in not adhering to established processes. Telstra advised that in April 2016, arrangements were implemented to prevent a delay from reoccurring. These measures include republishing the disconnection schedule on a weekly basis, irrespective of whether NBN Co has provided any updates.

Since the implementation of these new arrangements in April 2016, Telstra has identified an additional instance it published the disconnection schedule outside the specified timeframe. This breach was attributable to human error, however it was rectified within one business day after the specified timeframe.

The ACCC has confirmed that the regular updates have occurred and considers that the revised disconnection arrangements implemented are likely to further reduce the risk of reoccurrence and help to keep consumers well informed.

Reconnection of premises previously permanently disconnected

Telstra is required to ensure that no new copper paths or HFC lines are connected to premises that have previously been permanently disconnected, except in some circumstances regarding special services or where a disconnection has occurred in error. Telstra identified a small number of instances where a copper service was supplied to premises that had previously been permanently disconnected.

These instances included where:
- Telstra’s processes did not prevent or detect the reconnection order being accepted
- the end-customers were priority assistance customers that had experienced delays or issues in obtaining a service on the NBN, and
- the disconnection of the copper or HFC service was successful but there was a delay in a customer’s premises becoming NBN serviceable.

Telstra advised that the majority of instances where services were connected without complying with this obligation occurred during the migration window or shortly after the relevant Disconnection Date and prior to managed disconnections commencing. Telstra also advised that most of the non-compliant services have now been disconnected. Telstra has advised that the small number of premises that remain on the network will be disconnected in accordance with the relevant rollout region Disconnection Date. Consistent with previous years, Telstra has provided coaching on the rules that apply to the staff involved.

During the reporting period, Telstra also advised that it had identified address matching inconsistencies in its systems. The system had attributed new paths and lines, not previously associated with premises, to premises that had previously been permanently disconnected. Although not a breach under clause 19.1 of the varied Migration Plan, Telstra has identified this system issue and advised the ACCC that it is working to resolve the anomalies.

The ACCC considers that Telstra’s actions were appropriate in this instance, and further investigations into resolving address matching inconsistencies should help to improve compliance with this obligation in the future.

Cease sale

Telstra’s cease sale obligations are set out in clause 17 of the Migration Plan. The cease sale obligations generally prohibit Telstra from supplying new copper and HFC services to premises after it becomes NBN serviceable, except in limited circumstances.

Telstra has advised that it identified some instances during the year where services were connected that were not permitted under cease sale obligations. These non-compliant connections were attributable to system and data quality issues, and to a lesser extent human error associated with the use of manual processes. Telstra considers that the number of
instances is insignificant compared to the overall population of order requests made or rejected. Telstra has advised that it is working to promote internal compliance with the obligation by improving its automated processes, the quality of service data and has reiterated the importance of compliance to staff through various communications activities. In this regard, Telstra has advised the ACCC that it has regular engagement with NBN Co to analyse identified data inconsistencies and improve the quality of premises data it receives. Telstra has also provided the ACCC with relevant compliance policy and training documents prepared and disseminated by Telstra.

Telstra is required to provide data to the ACCC in its quarterly Migration Plan compliance reports on the volume of copper, wholesale copper and retail HFC services where an override code applies or a service is incorrectly provisioned without an override code during the relevant period.

The ACCC has not identified any potential equivalence concerns arising from the limited instances of non-compliance by Telstra with its cease sale obligations and considers the measures Telstra has taken to address these limited instances are appropriate.

**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 has advised that it complied with this obligation in the majority of instances. However, Telstra identified some retail customers who were given less than the specified notification timeframe set out in the Migration Plan. Telstra has stated that this was primarily attributable to limitations with internal processes and systems issues. In these instances, further communications were provided to the relevant customers, including catch-up notifications. Telstra has advised that it has implemented measures to reduce the likelihood of this reoccurring and promoted awareness of the need for these communications.

The ACCC considers that the steps taken by Telstra, including an ongoing retail customer communication campaign and catch up notifications for those notified later than the mandated timeframe set out in the Migration Plan, have reduced the risk of consumer detriment associated with the late notification of disconnection in these instances.

**Order Stability Period**

Clause 13 of the Migration Plan allows Telstra to apply an order stability period in each rollout region immediately prior and after the Disconnection Date for that rollout region. This provides Telstra sufficient time to clear any remaining pending orders before the managed disconnection process commences.

Telstra has advised that there were some instances where it connected services that were not permitted within the order stability period. These instances arose due to data quality issues and human error associated with manual processes. Telstra considers that the volume of these instances is insignificant compared to the number of orders that were completed (or rejected) in accordance with the obligation. Telstra has advised that it is continuing to promote compliance with this obligation by imposing stricter rules to govern the types of orders allowed, improving the quality of service data and reiterating the importance of compliance with staff.

The ACCC considers that the steps taken by Telstra should help to improve compliance with this obligation in the future.
**Managed disconnections**

During 2015–16, Telstra applied the revised arrangements for Managed Disconnection in the first 31 NBN rollout regions. Telstra advised that it had completed managed disconnections for all remaining legacy services by 30 June 2016 with the exception of a small number of premises which received an interim extension to managed disconnection (for example, in the case of premises with a registered fire alarm or lift phone services, premises identified as a multi-dwelling unit common area, or where the service is a Direct Special Service).

Telstra advised there were 13 Disconnection Dates that occurred during the reporting period affecting 348 NBN rollout regions. By the end of the reporting period, the obligation to complete mandatory disconnections for all remaining premises with the exception of those with In-Train Orders (i.e. made within 45 business days after the rollout region Disconnection Date), had occurred for a total of 264 NBN rollout regions.

Telstra noted some instances where disconnection of services (wholesale and retail) did not occur on the required date. Telstra advised that these instances were mainly due to the potential threat to the customer’s well-being if their copper service was disconnected before they had a working NBN service, or for similar reasons of concern regarding the disconnection of safety- or security-critical services. Where this had occurred, Telstra advised that it sought to ensure that disconnection was only suspended for a short period of time, and that any extensions were granted on an equivalent basis across retail and wholesale.

The ACCC considers that the revised disconnection arrangements provide an appropriate set of protections for end-users to promote service continuity and provides end-users with a sufficient opportunity to nominate a RSP supplying NBN services prior to the Disconnection Date. The ACCC has confirmed that the instances where disconnection did not occur on the required date have now been addressed by subsequent disconnection or are now subject to a later Disconnection Date that is yet to be reached.
ACCC actions

During the 2015–16 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 focused 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.

In each case of Telstra’s non-compliance during the 2015–16 reporting period, the ACCC has assessed and found that no instances warrant further enforcement action. The ACCC considers that remediation undertaken by Telstra has been sufficient to address any competitive detriment that may arise as a result of Telstra’s non-compliance.

The ACCC has also monitored Telstra’s performance against the equivalence and transparency metrics in the 2015–16 reporting period.

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

The SSU requires Telstra to report publicly on its costs, revenues and demands associated with its regulated services, and the internal and external prices that apply to those services. In July 2016, the ACCC commenced publishing a time series comprising internal and wholesale price data taken from the TEM reports.

The ACCC continues to encourage Telstra to provide relevant 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. In this regard, the ACCC ran a Wholesale Telecommunications Consultative Forum in April 2016 to facilitate greater engagement between Telstra and industry in relation to potential issues arising under the SSU and Migration Plan. The forum covered a wide range of issues, including Telstra’s IT systems remediation program, NBN migration arrangements and Telstra’s price equivalence reporting.
Further information

Telstra’s SSU and Migration Plan are available at:

- the Telstra Wholesale website:

The legislation and legislative instruments underpinning the SSU and Migration Plan are available at the Department of Communications and the Arts website:

ACCC contacts

ACCC Infocentre: business and consumer inquiries: 1300 302 502
Website: 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 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, 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