ACCC Report

Telstra's Structural Separation Undertaking

Annual Compliance Report

2014–15

Report to the Minister for Communications

Telstra's Structural Separation Undertaking

Annual Compliance Report 2014–15

Report to the Minister for Communications

ISBN 978 1 922145 68 0

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

ACCC 02/16_1060

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

8 February 2016

The Hon Mitch Fifield MP
Minister for Communications
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 2014-15 financial year. Please note that subsection 105C(3) of the Act requires you to table the report in each House of Parliament within 15 sitting days of that House after receiving the report.

Yours sincerely

Rod Sims

Chairman

Contents

Executive Summary

In 2014–15, Telstra continued to demonstrate a commitment to improving its level of compliance with its Structural Separation Undertaking (SSU). As a result, there has been a reduction in the number of breaches reported by Telstra during the year. The ACCC considers that Telstra's overall level of compliance has improved during the year and Telstra has acted reasonably to redress breaches as they arise.

The compliance issues identified in this report largely arise from Telstra's legacy systems not being designed to deliver the outcomes required by Telstra's SSU, limitations in the manual processes Telstra established to safeguard against breaches of the SSU, and errors made by Telstra staff in the course of their day-to-day work.

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. Similar to previous years, the most common SSU compliance issue in the period was Telstra's failure to prevent unauthorised disclosure of Protected Information. These issues have arisen as a result of some outstanding IT system issues and a number of isolated incidents that occurred due to staff error.

Telstra has been working to address issues with its legacy IT systems and continued its wide-ranging IT remediation program during the year. This program included a review of Telstra's IT systems and remediation to prevent unauthorised disclosure of Protected Information. Telstra completed the majority of this remediation work by March 2015, however several new IT system issues have been identified since that time. Telstra is working to address these outstanding issues in cooperation with the ACCC and input from an external consultant. In the meantime, Telstra has taken temporary measures to contain the risk associated with retail business unit staff having access to Protected Information.

In addition to the IT system issues, Telstra identified some isolated instances where Protected Information was inadvertently disclosed to retail business unit staff in error, either by email or verbal disclosure. In each of the reported instances, Telstra took action to contain the risk and sought to address the issue through coaching and ongoing training.

Telstra also reported one minor breach of its obligations to maintain operational and organisational separation of its wholesale, retail and network services business units. In this case, several retail business unit staff accessed a meeting room in Telstra Wholesale secure premises. Telstra has implemented new processes and controls to reduce the risk of this breach occurring in the future.

Transparency

The SSU and Migration Plan contain various reporting requirements that are designed to improve transparency. Telstra failed to report one equivalence issue within the required timeframe, which constituted a breach of its SSU obligations. In relation to its Migration Plan obligations, Telstra failed to publish a disconnection schedule and notify some retail customers of the impending disconnection of their premises within the required timeframes. In these particular instances, it is unlikely that the breaches resulted in significant detriment.

Migration Plan obligations

Telstra also breached some other aspects of its Migration Plan in the 2014–15 reporting period. These breaches occurred where Telstra failed to block orders from being provisioned or other requests from being processed, as required to promote migration to the National Broadband Network (NBN) and realisation of structural reform. 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 breaches primarily occurred due to process and data quality issues, which Telstra is working to improve.

ACCC actions

During the 2014–15 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.

In March 2015, the ACCC initiated an independent review of Telstra's IT systems to assess whether they had been fully remediated so as to prevent staff in a retail business unit from accessing wholesale customer Protected Information. The review identified issues in three of Telstra's IT systems. Telstra is working in cooperation with the ACCC and the external consultant to address the remaining IT system issues.

The ACCC continued to consult on two breaches of Telstra's overarching equivalence commitment during the year that were raised in previous reporting periods. The ACCC previously accepted rectification proposals in relation to these breaches and has been overseeing their implementation. The ACCC is satisfied that the rectification proposals provided an effective means of remedying the relevant equivalence issues. The ACCC has also monitored Telstra's performance against the equivalence and transparency metrics in the 2014–15 reporting period and conducted investigations where variances have been identified.

Introduction

The ACCC accepted a SSU from Telstra in February 2012. 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 for the period 1 July 2014 until 30 June 2015. The report also includes details of breaches that were reported in previous annual SSU compliance reports, where the conduct continued into the 2014–15 reporting period.

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. The report describes several breaches of Telstra's SSU obligations and identifies Telstra's actions to remedy these breaches.

During the 2014–15 reporting period, some changes were made to the obligations contained in Telstra's Migration Plan. These changes operated with ACCC agreement from the time Telstra submitted its revised Migration Plan and prior to its formal acceptance by the ACCC in June 2015. The 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. This has included encouraging Telstra to keep its wholesale customers informed of SSU equivalence and migration issues and conducting consultation on rectification proposals submitted by Telstra.

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 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.[1] 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[2]
- compliance monitoring processes, to provide the ACCC with transparency over Telstra's compliance with the SSU, and
- the Migration Plan, which forms part of the SSU.[3] 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.

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 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—through Telstra ceasing to supply fixed line voice and broadband services over its copper and HFC networks and commencing to supply those services over the NBN as the network 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.[4]

4 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 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 was provided by Telstra on a voluntary basis until March 2015, when Telstra advised the ACCC that it had completed its original IT systems remediation program.
- 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 2014 and 30 June 2015 and Telstra's Annual Compliance Report for 2014–15 (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 2014–15 financial year.

Matters reported in Telstra's Annual Compliance Report

In its Annual Compliance Report, Telstra reported 10 matters as being possible breaches of the SSU. These matters include:

- six instances (two of which were reported in the ACCC's 2013–14 report) where Telstra possibly breached its obligation to safeguard Protected Information pursuant to clause 10.4 and/or 10.5 of the SSU[5]
- two operational systems (one of which was reported in the ACCC's 2013–14 report) which provided Telstra retail business unit staff with access to Protected Information in breach of clause 10.4 or 10.5 of the SSU
- continuing information security issues in parts of three IT systems previously reported in breach of clause 10.4 of the SSU, and
- one matter which related to Telstra's organisational structure commitments, where several retail business unit staff accessed a meeting room in Telstra Wholesale premises without being appropriately escorted, in breach of clause 8.3 of the SSU.

5 In one of these instances, Telstra self-reported the matter to the ACCC but after further assessment determined that it was not a breach of clause 10 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.

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.[6] These tools range from administrative resolutions—for example, a commitment by the business 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.

6 Available at https://www.accc.gov.au/publications/compliance-and-enforcement-policy.

Breaches of the SSU

This report 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 Telstra's organisational structure 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, and
- Telstra's conduct was reported by the ACCC in a previous report but the conduct continued during the 2014–15 reporting period.

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 four breaches of its information security obligations in 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. One of these breaches involved an IT system issue which Telstra is addressing through its IT system remediation program. Two of the breaches were due to inadvertently sending an email in error, while the remaining breach was reported by Telstra as an isolated incident of verbal disclosure.

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—Back of house call centre staff with authority to process orders

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

Description of the breach	Cause of the breach
Two back of house call centre teams who receive incoming customer phone enquiries about existing Telstra Retail services have the authority to process new orders for services if a customer initiates a request for a new service during the call. The work in processing these new orders constitutes about 3 per cent of the work of these teams. It is possible that these staff have access to systems containing wholesale customer Protected Information.	These back of house call centre staff had not previously been identified as being part of a retail business unit because sales constitutes a very small part of their job and is only done in response to a request for a new service by the retail customer who calls in to Telstra for another purpose. They were therefore not accounted for in the remediation of systems previously notified to the ACCC.

ACCC findings

In November 2014, Telstra became aware that two back of house call centre teams had the authority to process retail orders. In processing such orders, these teams had access to systems containing wholesale customer Protected Information.

The two teams only perform the function of a retail business unit for a very limited portion of their role. The primary function of these two teams is to deal with incoming customer queries about existing products, which ordinarily includes billing enquiries, order status enquiries or configuration changes (for example, for line hunt groups). The teams do not receive incoming calls where the customer has indicated that the primary purpose of the call is to request a new service, as those calls are directed to other teams. In addition, these back of house teams do not make outbound sales calls and are not rewarded for any sales they make.

The ACCC considers that this matter constitutes a breach of clause 10.4 of the SSU because Telstra has failed to adequately ensure that wholesale customer Protected Information is not disclosed to any retail business unit.

Remediation undertaken by Telstra

Since identifying the issue, Telstra has undertaken remediation work to protect wholesale customer Protected Information from being disclosed to staff in these teams. Remediation work included applying retail business unit access profiles to those staff, which mask wholesale customer Protected Information in shared IT systems. In addition, access to some other systems was removed entirely. New processes were also developed to allow these staff to perform their role without access to wholesale customer Protected Information, or systems where access had been restricted or removed.

Telstra completed its remediation for all but two of the affected systems by 30 June 2015. Telstra is continuing remediation in respect of the two remaining systems and expects to implement solutions for these two systems by the second quarter of 2016.

In addition to the IT system remediation work, Telstra notified affected staff of system changes and reminded them that they must not access or use wholesale customer Protected Information. Telstra also required all staff in the two teams to complete their annual SSU compliance training by 30 June 2015, and reported a completion rate of 99.7 per cent.

The ACCC considers that, when completed, Telstra's remediation in relation to these systems should ensure that Telstra is compliant with its information security obligations in the SSU in the future. In the meantime, the ACCC is satisfied that the actions undertaken by Telstra minimises the risk associated with the outstanding system issues.

Item 2—Email sent in error

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

Description of the breach	**Cause of the breach**
An email chain between Telstra Wholesale employees was inadvertently copied in error to one retail business unit employee. The email contained the names of some wholesale customers and their service qualification volumes over a very limited time period as well as a reference to a particular wholesale customer not being involved in 'resale'.	The incident was attributable to human error by an individual Telstra Wholesale employee. The issue arose as a result of a wholesale business unit employee mistakenly choosing the wrong name from the Outlook address book.

ACCC findings

On 9 February 2015, a wholesale business unit employee sent an email to a number of Telstra Wholesale employees regarding intermittent performance issues. The email was copied in error to one retail business unit employee, whose name was mistakenly selected from the Outlook address book. This employee was then included on the subsequent email chain, which contained Protected Information in breach of clause 10.4 and other restricted information in breach of clause 10.5.

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

- names of wholesale customers
- Telstra Wholesale employee analysis of the service qualification outage, and
- commercially sensitive information regarding a wholesale customer's involvement in 'resale'.

The email also contained aggregated service qualification volumes over a specific, limited time period.

Remediation undertaken by Telstra

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

Telstra has advised that the mistake was identified on the same day that the email was sent, and a recall message was issued. Telstra has also advised that the retail business unit employee was contacted on that day and instructed to delete the email. Telstra has confirmed that the email was deleted and was not forwarded or otherwise distributed to any other retail business unit employee. Telstra also provided coaching to the wholesale business unit employees involved in this incident regarding 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—Verbal disclosure of Protected Information

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

Description of the breach	Cause of the breach
A retail business unit employee received a call from a retail customer enquiring why the customer's order for a retail ADSL service had failed. During the call, the retail business unit employee called a network services business unit employee for further information and was provided information to the extent that a conflicting order for wholesale ADSL existed in respect of the same full national number.	The incident occurred because of an individual error and failure to follow established Telstra procedure.

ACCC findings

On 28 January 2015, a Telstra retail business unit employee received a call from a retail customer enquiring why the customer's order for a retail ADSL service had failed. The retail business unit employee accessed an IT system that included a note made by another Telstra employee to the effect that there was a held wholesale order on the relevant line. The retail business unit staff member called a network services business unit employee for further information. During the call, the network services business unit employee confirmed the existence of the wholesale order but provided no further details.

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

Remediation undertaken by Telstra

Telstra considers that the verbal disclosure was an isolated, one-off incident rather than a systemic issue. Telstra acknowledges that the advice from the network services business unit employee which resulted in the disclosure of this information was contrary to Telstra's SSU obligations and Telstra policy. Telstra has provided coaching to the relevant employees in both the network services and retail business units. Telstra has also continued to provide training and awareness-raising regarding its SSU obligations in order to prevent disclosure by employees.

The ACCC accepts that providing staff training on the inclusion of Protected Information in notes in Telstra retail systems and coaching for the staff members involved was an appropriate measure in response to this incident of verbal disclosure.

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
A retail business unit employee was inadvertently sent an email containing information on a wholesale customer's consumption volumes of a regulated service.	The issue arose because the retail business unit recipient had been included in an email distribution group because of her prior employment in Telstra Wholesale. It occurred on her first day of employment in a retail business unit.

ACCC findings

In May 2015, a Telstra retail business unit employee was sent an email containing restricted information and Protected Information. The email was sent to the retail business unit employee because that employee was included in a distribution group due to her previous role in Telstra Wholesale. The information in the email was nationally aggregated monthly services in operation data, peak bandwidth data and service in operation speed data regarding a particular wholesale customer. To the extent that the aggregated information constitutes restricted information, we consider that this incident amounts to a breach of clause 10.5. Where Protected Information was disclosed, we consider that a breach of clause 10.4 has occurred.

The ACCC understands that a number of control measures were in place for situations where a wholesale business unit employee moves to a position in a different business unit at the time the incident occurred. These measures include removing wholesale business unit employees from distribution lists and following a checklist to ensure the employee no longer has access to any Telstra Wholesale information, either in IT applications or software, shared information repositories or in emails relevant to the employee's role in a wholesale business unit. The incident occurred due to a failure to comply with existing processes.

Remediation undertaken by Telstra

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

Telstra has advised that the retail business unit employee was contacted to confirm that the email had been deleted and had not been disclosed or used in any way. Owners of all email distribution lists that included the employee's name as a wholesale business unit employee were contacted to ensure that the employee's name had been removed from those lists. Telstra advised that confirmation was received from each distribution list owner that the employee's name had been removed.

In addition, all current and future meeting invitations relating to the employee's wholesale business unit activities were reviewed and re-issued to ensure the employee had been removed from those invitations. The wholesale customer was also contacted and advised of the requirement to remove the employee from all meeting invitations or distribution lists that may have included the employee.

The ACCC is satisfied that the actions taken by Telstra have minimised the risk of recurrence.

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 2014–15 financial year, but were only subsequently identified as equivalence issues.

Telstra has identified four additional information security issues in its confidential monthly compliance reports for July, August and October 2015 which were not included in its Annual Compliance Report for 2014–15 but relate to conduct that occurred during the 2014–15 financial year. These matters are reported below.

Item 5—System information may contain Protected Information

In Telstra's monthly compliance report for July 2015, Telstra identified a potential breach of clause 10.4 of the SSU in relation to one of its IT systems. This system provides an integrated platform for Telstra's major marketing, sales and customer relationship management applications. Telstra has advised that information being included in a free text notes field may contain Protected Information which confirms the existence of a wholesale product on the relevant line or an association with a wholesale line. The notes are visible in a part of the system that is accessible to retail business unit users, so there is a risk that disclosure of this information has occurred.

ACCC findings

The work instructions in place at the time referred staff to use template responses that included information that would constitute Protected Information. The work instructions and automated responses had been in place since prior to the commencement of the relevant information security provisions of the SSU (6 March 2012) and continued until they were remediated in May 2015.

There are currently around 5000 retail business unit users with access to this system, and all of these staff have access to the notes. However, not all users with access actually use the system and not all notes contain Protected Information.

The ACCC understands that Telstra is not aware of any specific situations where retail business unit staff have accessed Protected Information as a result of this issue. However, Telstra acknowledges that it is possible that at least one retail business unit staff member would have viewed the information in the context of them assisting to resolve the rejected order status.

The ACCC notes that Telstra does not consider that the presence of Protected Information in a system that Telstra Retail employees have access to is in itself a breach of clause 10 of the SSU. Rather, Telstra considers that the Protected Information must be revealed to the retail business unit employee in order for there to be a breach of clause 10 of the SSU (for example, if an employee actually viewed the Protected Information in the system).

However, the ACCC considers that given Protected Information is included in some notes, retail business unit staff would have been able to view that information in the context of assisting to resolve a rejected order status. The ACCC considers that where Telstra populates systems with Protected Information and the Protected Information is visible to retail business unit staff as a result, the relevant 'disclosure' has occurred.

On this basis, the ACCC considers that Telstra has breached clause 10.4 of the SSU in relation to this system.

Remediation undertaken by Telstra

Telstra has advised that the work instructions have been updated and no longer refer staff to use templates that list wholesale services or orders as a reason for order failure. Telstra is also sending six monthly communications to all users of this system, reminding retail business unit users that they cannot contact other areas to find out more information about why an order has failed. In addition, Telstra undertook remediation of the tools that inserted automated comments into the free text fields to ensure that no automated interaction comments refer to wholesale services or orders. This remediation work was completed on 14 May 2015. Telstra has also advised that compliance with the amended work instructions will be monitored and further instances of non-compliance will be referred for disciplinary action where appropriate.

The ACCC considers that the remediation action undertaken by Telstra minimises the risk of Protected Information being disclosed to retail business unit staff in this system in the future.

Item 6—System may disclose Protected Information

In Telstra's monthly compliance report for August 2015, Telstra identified a potential issue in relation to another IT system. This system is used by all business units to receive notifications of dirty tickets of work and return orders to the initiating business unit for remediation and progression of the order. Dirty tickets of work are errors in tickets of work which may result in delays or rework in completing a ticket of work.

As part of a regular review, Telstra identified a limited situation where the system tool will issue a ticket to alert the retail business unit staff member that the Telstra retail broadband order cannot progress. The ticket issued to the retail business unit staff member contains a free text field that is populated by Telstra back of house staff. Telstra has identified a small number of new cases where the free text field on the issued ticket has been completed in a way that confirms the existence of a wholesale broadband service on the line. None of the instances identified include any information identifying the wholesale customer concerned or the specific wholesale service being acquired. Telstra identified that the free text field was completed in this manner based on a separate standard template that was not corrected as part of initial remediation works in 2013.

ACCC findings

The ACCC understands that the work instructions had been in place since prior to the commencement of the relevant information security provisions of the SSU (6 March 2012) and continued until they were remediated. Remediation was completed by 30 December 2014.

Telstra identified about 150 tickets out of approximately 131 000 in the system during the period between May and July 2014, where the ticket confirmed there was a wholesale service on the line. Most of the 150 tickets confirmed the existence of a wholesale broadband service. There were a small number that referred to a wholesale PSTN service and a small number referring to the existence of a wholesale relationship without specifying the particular service being provided.

The ACCC considers that Telstra has breached clause 10.4 of the SSU in relation to this system issue.

Remediation undertaken by Telstra

Telstra has issued updated work instructions to the back of house teams completing the free text fields so that retail business unit users are not notified of the existence of a wholesale broadband service. Telstra has also conducted regular SSU training and issued regular reminder notices to staff to help prevent the recurrence of the issue.

Telstra has also advised that it will review the process for accepting retail broadband orders and compliance with the updated work instructions in the system. If necessary, Telstra will make further changes to reduce the risk of disclosure in the free text field occurring again in the future.

The ACCC considers that the steps undertaken by Telstra minimises the risk of Protected Information being disclosed to retail business unit staff in the free text field in the future.

Item 7—System displaying Protected Information

In Telstra's monthly compliance report for October 2015, Telstra identified a historical issue with an IT system. This particular system is an application that displays information about the incoming call to the recipient of an inbound call to Telstra. It is mainly used in relation to Telstra Business customers.

ACCC findings

From a time prior to the commencement of the SSU until 6 December 2013, the ACCC understands that the system was capable of displaying information that constituted Protected Information in breach of clause 10.4. The specific information was displayed in a field in the user interface for a full national number which in some cases may have identified that the caller was calling from, or calling about, a full national number associated with a current wholesale eBill service.

The ACCC notes the delay in Telstra reporting this matter and considers that it is a breach of Telstra's reporting requirements. Under clause 23.3 of the SSU, Telstra is required to provide the ACCC with a report within 10 business days after the end of each calendar month with any equivalence issues identified within that month. As the issue was identified and remediated in 2013, Telstra's reporting of this issue to the ACCC was outside the reporting requirement timeframes.

Telstra disagrees that the reporting of this matter amounts to a breach of clause 23.3 of the SSU. Telstra has noted that investigations into SSU compliance matters can be complex and take time to resolve. Telstra has stated that, in this case, it only determined that the matter was reportable as a breach following the receipt of further information after undertaking some remediation.

Remediation undertaken by Telstra

Telstra has advised that it remediated the issue with the system on 6 December 2013.

Item 8—Reporting portal capable of displaying Protected Information

In Telstra's monthly compliance report for October 2015, Telstra advised that it has identified a corporate reporting portal that is capable of displaying Protected Information in a 'Pre-selected Services' report. This reporting portal allows users to request reports for retail accounts based on a retail customer identification number.

The portal is mainly used for teams that support enterprise and government customers. However, in addition to information about the retail accounts, Telstra has identified that some of these reports have included information relating to wholesale services.

ACCC findings

The ACCC understands that two 'Pre-selected Services' reports containing Protected Information were requested by retail business unit users during the period 1 July 2014 to 30 June 2015. The Protected Information disclosed in these reports, in breach of clause 10.4 of the SSU, included the full national number and an 'N' in the 'with Telstra' column of the report, indicating that the service is not with Telstra retail. In the two reports requested by retail business units in the period, there were a total of 6337 full national numbers, of which 21 were for wholesale eBill services.

Remediation undertaken by Telstra

Telstra completed remediation of the portal in November 2015. Telstra has also advised that, prior to remediation, there were controls in place to limit unauthorised access to Protected Information in the system. For example, there is a behavioural control which asks the person requesting the report to tick a box that the customer has authorised the report to be run, and the portal will not allow the report to be run unless that box is ticked. Further, for the report to be run, the customer's identification number is required. Telstra has advised that retail business unit staff would not have access to wholesale customer identification numbers for a report to be run for a wholesale customer.

The ACCC considers that the remediation work undertaken by Telstra minimises the risk of Protected Information being disclosed to retail business unit staff in 'Pre-selected Services' reports in the reporting portal in the future.

Continuing information security breaches

During 2014–15, Telstra progressively addressed the IT information security system issues that were notified to the ACCC during 2012–13 and 2013–14, but were not yet remediated at the time of Telstra's Annual Compliance Report submission for 2013–14.

Summary of Telstra's information security remediation

Telstra identified 42 IT systems that required remediation throughout the IT system 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. During the 2014–15 reporting period, remediation work continued on the relevant remaining systems. Telstra has advised that it completed remediation of these systems by the end of March 2015.

Telstra also completed some scheduled primary remediation activities for two systems during the 2014–15 financial year.

Review of IT remediation work

On 5 March 2015, the ACCC engaged an external 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 some Protected Information that may have been visible to retail business unit users under specific, limited circumstances. This included:

- archive reporting—online archive reports were available to some retail business unit users. These reports may have contained historical wholesale customer information, wholesale product code information and information about the current status of a wholesale customer full national number.
- billing platform—wholesale product code information was not masked from the retail business unit profile view on one screen in the billing platform. However, this screen is used mainly for actioning customer billing enquiries and is not commonly used by retail business unit users.
- data warehouse reporting—historical wholesale customer information, including order information and other information regarding a small percentage of wholesale customer end users was able to be accessed by retail business unit users via reports prepared from the system's staging area.

These ongoing system issues resulted in a continuing breach of clause 10.4 of the SSU in the reporting period.

Telstra remediated the first two systems on 27 June 2015, and completed remediation in respect of the data warehouse reporting system on 28 September 2015. While remediation of the data warehouse reporting system was taking place, retail business unit staff who attempted to access the staging area were directed to cease using the system.

Telstra internal due diligence review

From July 2015 until November 2015, Telstra undertook an internal due diligence review of its IT remediation project. As part of this review, Telstra assessed all 24 systems where retail business unit staff still had access to the system.

Telstra identified that the remediation work had been effective for 20 of the systems, but there were some minor issues in four of the systems which arose in specific, limited situations. These four systems were re-reported in Telstra's monthly compliance report for October 2015. Telstra found that in each of these systems, Protected Information may be accessible by retail business unit staff, in breach of clause 10.4 of the SSU. Telstra has advised that it intends to commence remediation work for these systems in December 2015, which will likely continue into 2016. Telstra will also continue to monitor and improve its compliance management framework to strengthen controls, promote consistency in the approach to remediation across systems and reduce the potential for future breaches.

The ACCC has retained an external consultant to examine and report on the thoroughness of Telstra's internal due diligence review and consider how Telstra's internal due diligence review has improved Telstra's ongoing compliance program. We expect that consultant's report will be completed in early 2016.

The ACCC recognises that Telstra has made a significant investment in its IT system remediation project and appears committed to improving compliance with its SSU obligations in this area. The ACCC will continue to monitor Telstra's IT system remediation project to ensure that the outstanding issues are resolved.

Organisational structure commitments

Telstra's SSU sets out certain commitments regarding Telstra's organisational structure.[7] The main focus of the organisational arrangements is on separating retail business units from the wholesale and network services business units, and vice versa. For example, only wholesale business units have control over wholesale customer sales and management of service delivery. This prevents retail business units, who have competing incentives, from performing these functions. Similarly, the separation of network services business units is primarily to ensure that staff are not incentivised to give preference to retail customers or orders.

7 Clause 8 of the SSU.

The SSU and organisational structure commitments

Clause 8 of the SSU sets out certain organisational arrangements, including how Telstra must maintain separate business units for wholesale, retail and network services functions.

Clause 8.3(c) provides specific requirements regarding wholesale business unit premises. It states that employees engaged to work for a wholesale business unit must be located in premises that:

(i) are physically separate from any premises occupied by employees engaged to work for a retail business unit (although this does not mean that the employees need to be located in a separate building)

(ii) have security measures in place that prevent an employee who is engaged to work for a retail business unit from gaining access to the premises where the employees working for that wholesale business unit are located unless:

- A the employee who is engaged to work for a retail business unit enters the premises for the purposes of a meeting with an employee who is engaged to work for that wholesale business unit, and
- B the entry to the premises by the employee who is engaged to work for a retail business unit is authorised by an employee who is engaged to work for that wholesale business unit, and
- C the employee who is engaged to work for a retail business unit is accompanied, to the extent practicable, while in the premises by an employee who is engaged to work for that wholesale business unit.

Item 9—Retail business unit staff meeting held on Telstra Wholesale secure premises

In its Annual Compliance Report, Telstra provided the following details in relation to item 9:

Description of the breach	**Cause of the breach**
Eleven retail business unit employees held a meeting in Telstra Wholesale secure premises without a Telstra Wholesale employee being in attendance.	The incident arose due to an individual staff error as the meeting was inadvertently scheduled on a Telstra Wholesale secure floor. The usual security controls did not prevent the retail business unit employees from entering the floor as some of the employees had required access to that floor previously for an approved purpose and that access had not been removed.

ACCC findings

As retail business unit staff gained access to a Telstra Wholesale secure floor, there was an isolated breach of clause 8.3(c) of the SSU. The usual security controls did not prevent the staff from entering the secure floor. The Telstra retail business unit staff were not entering the premises for the purposes of meeting with a wholesale business unit employee, were not authorised entry by a wholesale business unit employee, and were not accompanied by a wholesale business unit employee.

The ACCC understands that the meeting was inadvertently scheduled to take place on a Telstra Wholesale secure floor because of a mistyped room number identifier in the meeting invitation. The usual security controls did not prevent staff from entering the floor because some of the staff involved had required access to that floor previously for an approved purpose.

Remediation undertaken by Telstra

Following the incident, Telstra ensured that the relevant retail business unit staff had their access to the secure Telstra Wholesale floor removed. Telstra also conducted a review of processes and controls to prevent retail business unit staff having access to Telstra Wholesale secure floors, and took the following action:

- installed clearly visible signage on all entry doors where retail business unit staff are restricted from access
- conducted a re-audit of all sites where wholesale business units are located, including meeting rooms and calendars
- confirmed that a visitors' log book is available on each floor
- carried out a full review of all quarterly audits, and
- conducted additional training to educate the Building Manager Liaison Officers of their responsibilities in relation to physical access and the associated audit task.

The ACCC is satisfied that the steps taken by Telstra have minimised the risk of recurrence.

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 outputs 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[8] supplied to Telstra Retail customers are (a) issued and processed in Telstra's systems using equivalent order management and (b) are 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.

Telstra did not identify any new breaches of the overarching equivalence commitment or the service quality and operational equivalence commitments in its Annual Compliance Report.

8 Comparable retail service means, in respect of a regulated service, a retail service supplied by Telstra that is comparable to that regulated service.

Rectification proposals

In its Annual Compliance Report, Telstra identified two rectification proposals that were carried forward from previous financial years.

Basic telephone service fault rectification

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 and 2013–14 reports.

> During 2014–15, pursuant to the accepted revised rectification proposal, until 31 March 2015, Telstra implemented workflow management tools to manage the tickets of work within a service delivery area when the volume of basic telephone service faults recorded by Telstra Operations reached the specified high threshold in that area and also confirmed the steps Telstra had taken to address the reported matters in 2012.
>
> In addition to the processes already put in place in 2012–13, these measures provided an effective means of remedying the concerns raised by the ACCC in respect of the reporting variance for Metric 5 in 2012.
>
> Telstra provided the ACCC with quarterly updates on the use of the severity level referenced in the revised rectification proposal. The last update was provided in May 2015 covering the quarter to March 2015.

Background

Telstra is required to provide quarterly reports on various equivalence and transparency metrics in relation to the supply of regulated services.[9] Metric 5 measures the percentage of basic telephone service faults that are rectified within set timeframes for both Telstra Retail and Telstra Wholesale customers. In its operational equivalence reports for the June, September and December 2012 quarters, Telstra identified reporting variances of more than two per cent in favour of Telstra Retail in relation to the performance of Metric 5. This raised potential concerns under clauses 9(a)(i), (9)(a)(ii) and 11.1 of the SSU. Telstra identified several potential reasons for the reporting variances, including inclement weather, high demand and the high number of medical priority tickets of work for retail customers.

On 15 November 2012, Telstra notified the ACCC that it had identified two additional factors that may have contributed to the variance. These included some staff incorrectly allocating an increased level of severity to a number of Telstra Retail basic telephone service faults and the removal of a wholesale code (the ZZZ code) which inadvertently resulted in wholesale customer faults being allocated a lower level of priority. These issues were rectified in 2012–13 and were the subject of a rectification proposal submitted to the ACCC in December 2012.

At the ACCC's request, Telstra engaged the ITA Adjudicator to consider whether the rectification proposal would effectively address the issues identified and the cause(s) of the reporting 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.

9 Schedule 3 of the SSU.

Rectification proposal

In May 2014, Telstra submitted a revised rectification proposal to the ACCC for consideration. 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:

- 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 basic telephone service faults, and reported to the ACCC on whether staff are allocating correct severity levels
- reinstated the ZZZ code.

Service Qualification

- 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 2013–14 report.

> During 2013–14, Telstra identified a potential issue with its systems and processes for handling service qualification (SQ) and the subsequent decision regarding the provisioning of orders for ADSL services and, in the case of Telstra Wholesale services, Line Sharing Service (LSS), in the limited circumstances where the SQ queries or ADSL/LSS order is performed using a full national number and the existing PSTN service is affected by excessive transmission loss. This meant there was a potential for different treatment of SQ queries or ADSL/LSS orders for retail and wholesale customers in this limited circumstance.

Background

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.[10] 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.[11]

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 provide an ADSL service to the premises.

Telstra investigations identified an issue with its systems and processes for handling service qualification that led to different outcomes for the ordering and provisioning of some wholesale ADSL services when compared to Telstra's retail business unit. Telstra advised that the breach was likely to have affected 10 wholesale customers and 282 end users from May 2012 to October 2014.

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.

10 Clause 9(a) of the SSU.

11 Clause 11.3(a) of the SSU.

Pursuant to the accepted further revised rectification proposal, Telstra has:

- deployed IT system changes and alignment of processes
- given notification to wholesale customers of the changes
- promoted the availability of one-step and DSL-capable ordering
- updated the Telstra Wholesale website, and
- implemented a rectification scheme.

The ACCC is satisfied that the rectification proposals for both the BTS fault rectification and service qualification issues provided an effective means of remedying the relevant equivalence issues.

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.

During the 2014–15 reporting period, Telstra submitted a revised Migration Plan for ACCC approval to reflect the revised commercial agreements between Telstra and NBN Co and the move to a multi-technology mix NBN. In addition, the revised Migration Plan includes some modified migration and disconnection arrangements that are intended to promote service continuity. On 26 June 2015, following public consultation, the ACCC approved Telstra's revised Migration Plan. The ACCC's role in approving the revised Migration Plan was limited to assessing whether it was consistent with the legislative requirements.

Breaches of the Migration Plan

During the reporting period, 104 NBN Rollout Regions reached their final disconnection date. This included the initial 31 NBN Rollout Regions which were given an additional six months post the disconnection date for disconnection.

Whilst Telstra generally complied with its Migration Plan obligations during the period, it reported a number of small scale breaches. Prior to approval of the revised Migration Plan, Telstra adopted interim disconnection arrangements under ACCC forbearance from compliance with its original Migration Plan obligations. The ACCC consented to these interim disconnection arrangements in order to promote service continuity and ensure that end-users were not left without a working service.

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. Telstra has advised that on one occasion, Telstra published the disconnection schedule later than the prescribed five business days after receipt of notification from NBN Co of a new or updated Rollout Region Ready for Service date. This delay was caused by human error in not adhering to a timeline associated with a manual process. Telstra has advised that this error has not been repeated.

The ACCC considers that the revised disconnection arrangements which were in place at the time would have likely reduced the risk of consumer harm as a result of this isolated incident.

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.[12] Telstra identified a small number of instances where a copper service was supplied to a premises that had previously been permanently disconnected.

12 Clause 19 of the Migration Plan.

These instances included where:

- Telstra's processes did not prevent or detect the reconnection order being accepted
- the end customer was a Priority Assistance customer and there were delays or issues associated with obtaining a service on the NBN, and
- the disconnection of the copper or HFC service was inadvertently effected prior to the successful connection of the premise to the NBN, including circumstances where the installation of the NBN service had been delayed.

Telstra has advised that in the majority of instances, services that were provided in non-compliance with this obligation have now been disconnected and the staff involved have received coaching.

The ACCC considers that Telstra's actions were appropriate in this instance and 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. A variation to these obligations was incorporated into the revised Migration Plan accepted by the ACCC on 26 June 2015. Telstra has advised that it assessed its compliance with the varied cease sale obligations for the purposes of its Annual Compliance Report.

The cease sale obligations generally prohibit Telstra from supplying new copper and HFC services to a 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 the cease sale obligations. These connections occurred due to data quality issues and human error associated with manual processes. Telstra considers that the number of instances is insignificant compared to the overall population of order requests made. Telstra has advised that it is working to improve the quality of its service data and has reiterated the importance of compliance to staff through various communication activities.

Telstra is required to provide data to the ACCC in its quarterly Migration Plan Compliance Reports on the volume of retail 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.

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 notified later than the specified timeframe. Telstra has stated that this was primarily attributable to limitations with internal processes and systems that did not identify that some customers had been excluded from the mail-out until after the required timeframe had passed. In these instances, further communications were provided to relevant customers, including catch-up notifications. Telstra has advised that enhancements to the notification processes were implemented in March 2015 to improve compliance.

The ACCC considers that the steps taken by Telstra, including issuing catch up notifications, should have reduced consumer issues associated with the late notification of disconnection dates in these instances. Further, the ACCC considers that the revised disconnection arrangements that were in place at the time are likely to have reduced the risk of any consumer harm.

Order stability period

Clause 13 of the Migration Plan allows Telstra to apply an order stability period in each rollout region immediately prior to and after the disconnection date for that rollout region to allow Telstra time to clear any remaining pending orders before the managed disconnection process commences. Some changes to the operation of the order stability period and further clarifications to the types of orders that are allowed to be processed during the order stability period were incorporated into the revised Migration Plan accepted by the ACCC in June 2015.

Telstra has advised that there were some instances where it connected services that were not permitted within the order stability period. Similar to the cease sale issues, 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 in comparison 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 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 for first 31 Rollout Regions

During 2014–15, Telstra continued to apply revised arrangements for managed disconnections in the first 31 Rollout Regions. In September 2014, Telstra made a further change to the arrangements for managed disconnections. The ACCC did not object to the implementation of these revised arrangements.

Mandatory managed disconnections commenced in the initial 15 NBN Rollout Regions on 15 December 2014 and in the remaining 16 NBN Rollout Regions between 10 February and 15 May 2015. Telstra has advised that there were a number of retail services scheduled for disconnection in April 2015 that did not receive soft dial tone and service disconnection in accordance with the required timeframe. Telstra explained that this was due to the amount of activity occurring at that time, with two different disconnection processes in place. Telstra also advised that all but a very small number of retail services were permanently disconnected contemporaneously with wholesale services in accordance with the arrangements. The small number of outstanding retail services proceeded to permanent disconnection within a short period after the nominated timeframe.

Telstra noted that during the reporting period, managed disconnections were successfully completed for 20 of the first 31 NBN Rollout Regions. The remaining 11 NBN Rollout Regions are scheduled for completion in early 2015–16.

Managed disconnections and related obligations for Rollout Regions 32+

On 31 January 2015, the ACCC provided consent for Telstra to proceed with a revised disconnection approach for NBN Rollout Regions 32+, which was outside the requirements of the Migration Plan. Telstra designed the changes to provide more flexibility for end-users who place an order for an NBN service, including a final opportunity to place their NBN order within a limited timeframe after the disconnection date. The ACCC consented to these revised arrangements without a formal variation to the Migration Plan on the basis that the revised arrangements would provide a greater level of service continuity and on the expectation that Telstra would shortly submit a formal variation to the Migration Plan.

Telstra submitted a formal variation request in March 2015 and an amended variation request in June 2015. The ACCC accepted the Migration Plan variation on 26 June 2015. The revised Migration Plan included this revised disconnection approach as well as some additional amendments to address further scenarios where the in-train order process required additional flexibility. In addition, the revised Migration Plan sets out transitional provisions that apply to premises with in-train orders in rollout regions with a disconnection date during the 2015

calendar year. The ACCC has consented to the extension of these transitional provisions until 30 June 2016, while Telstra and NBN Co continue to finalise proposed long-term arrangements for in-train orders.

The transitional arrangements include extending the definition of in-train order premises and increasing the time period before managed disconnection occurs from 30 business days to 120 business days for premises that NBN Co notifies Telstra have been connected to the NBN from three months before the Disconnection Date. The ACCC considers that the new disconnection arrangements under the revised Migration Plan are likely to provide greater service continuity assurance for customers in the migration process.

Telstra considers that its operation and compliance with the disconnection rules under NBN Rollout Regions 32+ proceeded relatively smoothly during 2014–15. Telstra has advised that it identified a small number of instances where the permanent disconnection of the service occurred a few days outside the stated timeframe. These instances, however, were rare and were caused by minor process issues.

Telstra has further advised that five disconnection dates were passed during 2014–15, impacting 73 NBN Rollout Regions. At the conclusion of the year, the obligation to complete mandatory disconnections for all remaining premises, with the exception of those with in-train orders, had occurred for 58 Rollout Regions.

ACCC action

During the 2014–15 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 continued to consult with Telstra and wholesale customers on two breaches of Telstra's overarching equivalence commitment during the year that were raised in previous reporting periods. The ACCC accepted rectification proposals in relation to these breaches. The ACCC is satisfied that the rectification proposals provided an effective means of remedying the relevant equivalence issues. The ACCC is also satisfied that Telstra complied with the revised rectification proposals for both the BTS fault rectification and the service qualification issues.

The ACCC has also monitored Telstra's performance against the equivalence and transparency metrics in the 2014–15 reporting period and conducted investigations where variances have been identified. The ACCC did not identify any equivalence issues in the reporting period.

The ACCC monitors and receives regular updates from Telstra on its information security remediation project in relation to its IT systems and processes. Following the completion of Telstra's main remediation project, the ACCC commissioned an external consultant to independently test Telstra's systems remediation work. The ACCC is continuing to work with both the consultant and Telstra to address the remaining IT system issues. Telstra has been cooperative in this process.

The ACCC receives several 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 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: 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 and the Arts website:

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

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
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