Australian Competition & Consumer Commission

ACCC Report

Telstra's Structural Separation Undertaking

Annual Compliance Report 2012–13

Report to the Minister for Communications

www.accc.gov.au

Australian Competition & Consumer Commission

Telstra's Structural Separation Undertaking

Annual Compliance Report 2012–13

Report to the Minister for Communications

ISBN 978 1 922145 11 6

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

ACCC 02/14_839

www.accc.gov.au

EXECUTIVE OFFICE

Australian Competition & Consumer Commission

GPO Box 3131
Canberra ACT 2601

23 Marcus Clarke Street
Canberra ACT 2601

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

www.accc.gov.au

Contact Officer: Michael Cosgrave
Contact Phone: (03) 9290 1914

17 February 2014

The Hon Malcolm Turnbull MP
Minister for Communications
Parliament House
CANBERRA ACT 2600

Dear Minister

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 2012–13 financial year. As you are aware, 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

Telstra's Structural Separation Undertaking (SSU) and migration plan, accepted by the ACCC in February 2012, specify Telstra's commitments to progressively migrate its fixed line voice and broadband customers onto the wholesale-only National Broadband Network (NBN) and promote equivalence and transparency during the transition period.

Given the timeframe required to complete the NBN build, Telstra's equivalence and transparency commitments, and particularly the commitment to overall equivalence of outcomes, are a vitally important component of the regulatory regime to promote competitive outcomes during the transition period.

In 2012–13, Telstra continued to implement the SSU and migration plan and took a number of steps to promote compliance with the commitments it has given.

However, Telstra continued to encounter difficulties in fully complying with several of its SSU commitments and in some instances failed to deliver similar outcomes to wholesale and retail customers. The breaches that occurred in 2012–13 fall into two broad categories:

- Failing to properly ring fence the Protected Information of Telstra's wholesale customers—that is, the ordering and provisioning and other information that wholesale customers must provide to Telstra in its capacity as the provider of access to regulated services. This is largely a continuation of conduct that came to light immediately following the commencement of the SSU and which was the subject of the ACCC's inaugural compliance report.
- Failing to introduce Asymmetric Digital Subscriber Line (ADSL) service enhancements contemporaneously to retail and wholesale customers. This meant that wholesale customers were not able to migrate an existing ADSL service to a better ADSL service supplied from a Telstra cabinet when retail services could be migrated in that way, and wholesale customers having fewer line configurations available to optimise consumers' services.

Telstra is continuing to respond to these breaches in a positive manner and has provided industry with additional transparency both at the ACCC's Wholesale Telecommunications Consultative Forum and through email updates.

Telstra's internal governance arrangements and compliance training programs were generally successful in identifying the majority of the issues at an early stage, although the ACCC and wholesale customers also identified several equivalence issues.

That said, the potential for competitive harm remains ongoing, and hence there is a need for Telstra to safeguard against these breaches of the SSU continuing or recurring during the transition to the new industry structure. Telstra has undertaken and continues to undertake significant remediation of these breaches. While this work is ongoing, at this stage, Telstra does not expect that it will have fully remediated its operational systems to properly ring fence the Protected Information of Telstra wholesale customers until the end of 2014. Telstra will need to carefully manage these operational support systems in order to fully comply with the SSU's equivalence obligations. The ACCC considers that on the information currently available, Telstra's remediation program, which is scheduled for completion by 31 December 2014, as well as Telstra's ongoing commitment to ensuring compliance with the SSU, will be capable of preventing the type of breaches that are outlined in this report from recurring.

In responding to each of the reported breaches outlined in this report, the ACCC has focused 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 ensuring regular updates to wholesale customers, requiring additional regular reporting and conducting consultation on rectification proposals submitted by Telstra.

The ACCC continues to investigate Telstra's failure to comply with its information security obligations to determine whether Telstra has gained or exploited an unfair commercial advantage over its wholesale customers. A decision as to any further action will be made by the

ACCC following the conclusion of these investigation and remediation activities in accordance with the ACCC's *Compliance and Enforcement Policy*.[1] 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.

Under its *Compliance and Enforcement Policy*, the ACCC considers a range of factors when deciding whether and what compliance and enforcement action to take. In respect of the matters discussed in this report, this would include consideration of whether the conduct has ceased, whether any harm has been corrected and whether the conduct involved a blatant and deliberate breach of the law.

1 http://www.accc.gov.au/about-us/australian-competition-consumer-commission/compliance-enforcement-policy.

Introduction

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

The ACCC has prepared this report based on whether in its view, on the balance of probabilities, a breach of the SSU occurred. The ACCC has made its findings after considering information provided by Telstra and making its own enquiries into the matter. Some of the ACCC's findings that a breach has occurred do not accord with views that Telstra has expressed to the ACCC. Telstra's views are expressly noted in the body of this report.

In addition, this report outlines the steps that Telstra has taken to remedy the breaches. Importantly, even in those instances where Telstra disputes that its conduct breaches the information security provisions in the SSU, Telstra is taking steps to safeguard against the relevant systems being the source of a breach in future. These steps include removal of Telstra Retail access to wholesale customer Protected Information through internal partitioning of shared information systems, masking or removal of wholesale customer Protected Information from systems and the implementation of user access controls.

As noted above, the ACCC considers that on the information provided, Telstra's remediation program will be capable of preventing the type of breaches that are outlined in this report from recurring. That said, there are specific instances where Telstra's conduct may have provided it with a commercial advantage or had a detrimental impact on its competitors. The ACCC is further investigating these matters. At the conclusion of these investigations, the ACCC will consider the reported breaches against its compliance and enforcement priorities to determine whether further action is appropriate. The ACCC's approach to enforcement and compliance is discussed later in this report.

The breaches identified in this report demonstrate both the importance of Telstra implementing the equivalence and transparency measures contained in the SSU in a robust manner, and the benefits of achieving structural reform of the telecommunications sector in order to resolve the perennial competition concerns resulting from Telstra's vertical integration.

Telstra's Structural Separation Undertaking

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

This reform recognised that Telstra, as the vertically integrated access provider to the ubiquitous copper network, operates at all levels of the supply chain and competes with the businesses that it supplies to. 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 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.

In introducing structural reform of the telecommunications industry, the Government recognised that the ACCC would need stronger enforcement mechanisms than those under the operational separation regime to ensure transparency and equivalence.[3]

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 National Broadband Network will be concluded
- interim equivalence and transparency obligations regarding access to Telstra's regulated services[4] in the period leading up to the Designated Day
- compliance monitoring processes, to provide the ACCC with transparency over Telstra's compliance with the SSU
- the migration plan, which formed part of the SSU when it was accepted by the ACCC.[5] 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 the SSU continues to deliver significantly better outcomes in terms of equivalence for wholesale customers and enhanced transparency over 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 discussion paper *National Broadband Network: Regulatory Reform for the 21st Century Broadband*.

3 Explanatory Memorandum to the Telecommunications Legislation Amendment (Competition and Consumer Safeguards) Bill 2010, p. 22.

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

5 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.

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 fibre network is rolled out. In order to promote competition during the interim period from the date that the SSU commenced until the NBN fibre network is complete, the SSU includes a broad range of obligations. These interim equivalence and transparency obligations require Telstra to supply regulated services to wholesale customers on equivalent terms to those on which it supplies its own Retail Business Units. The obligations include:

- organisational structure—maintaining separated Business Units (that is, 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—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 (described further 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[6]
- 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 above 2 per cent
- six-monthly public and quarterly confidential Telstra Economic Model (TEM) reports outlining the list of internal wholesale prices and external wholesale prices.

In addition, the ACCC imposed an additional monthly remediation reporting framework in July 2012 concerning the program of work Telstra is conducting to ensure that its IT systems are compliant with the information security obligations in the SSU.

The ACCC has considered Telstra's confidential compliance reports relating to the period between 1 July 2012 and 30 June 2013 and Telstra's Annual Compliance Report for 2012–13 (Annual Compliance Report). In addition, the ACCC has considered issues identified by Telstra in later compliance reports that relate to conduct that occurred during the 2012–13 financial year.

The ACCC has also included details of breaches that were reported in the ACCC's report for the 2011–12 financial year, where the conduct continued to occur in 2012–13.

Matters reported in Telstra's Annual Compliance Report

In its confidential Annual Compliance Report, Telstra reported 21 breaches of the SSU. These breaches comprise:

- 15 operational and 'data warehouse' systems that disclosed Protected Information, or generated reports disclosing Protected Information, to Telstra Retail users—that is, the relevant conduct is reported on a per system basis, with each system as a 'count'
- two reports containing Protected Information that were accessible to Telstra Retail users
- one instance where an email sent to a Telstra Retail call centre team encouraged Telstra Retail staff to access and use Protected Information
- the ability of Retail Business Unit users to cancel wholesale orders
- one instance where Telstra breached the overarching equivalence obligation by failing to introduce ADSL service enhancements to retail and wholesale customers at the same time
- one instance where a TEM report was not submitted within the required timeframe.

6 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.

ACCC approach to compliance and enforcement

As noted above, the ACCC is further investigating Telstra's failure to comply with its information security obligations and, in particular, any extent to which Telstra may have gained or exploited an unfair commercial advantage over its wholesale customers. Pursuant to the *Telecommunications Act 1997*, Telstra is obliged to comply with the SSU and 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. These tools range from administrative resolutions—for example, a commitment to stop engaging in the conduct—to court cases. Administrative resolutions are generally used where the ACCC assesses the potential risk flowing from the 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 the matters the subject of this report, the ACCC would be more likely to take court enforcement 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. For example, the ACCC may consider court action if Telstra does not take effective measures to remediate its systems and processes and to remedy any harm that may have occurred as the result of Telstra's failure to comply with its information security obligations. The ACCC would also consider enforcement action if, after its investigations, it concludes that Telstra engaged in this 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. 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 report details a number of instances where the ACCC considers, on the balance of probabilities, that Telstra breached its SSU in the 2012–13 financial year. These breaches relate to:

- Telstra's obligation to secure wholesale customer Protected Information, in circumstances where:
  - Telstra concedes that it has breached the SSU in its Annual Compliance Report
  - the ACCC considers that Telstra has breached the SSU but Telstra disagrees
  - Telstra reported the conduct after the end of the reporting period and so did not express a view on whether the conduct was in breach of the SSU in its Annual Compliance Report
  - Telstra's conduct reported in 2011–12 continued during the reporting period.
- Telstra's obligation to provide equivalence in the supply of regulated services to wholesale customers and its Retail Business Units, in circumstances where:
  - Telstra concedes that it has breached the SSU
  - the ACCC considers that Telstra has breached the SSU but Telstra disagrees.
- Telstra's obligation to submit TEM reports within 60 days of the end of each quarter.

Information security

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

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

- a strict prohibition on disclosure of Protected Information to Retail Business Units unless the wholesale customer has authorised the disclosure
- a prohibition on Telstra using or disclosing Protected Information in a way that would be likely to enable its Retail Business Units to gain or exploit an unfair commercial advantage over its wholesale customers.

Importantly, Telstra must protect any:

- confidential 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, date of birth and service type in an order or a fault report
- confidential and commercially sensitive information derived from confidential or commercially sensitive information supplied by a wholesale customer and obtained by Telstra for the purpose of or in the course of supplying regulated services to that wholesale customer—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:

- a 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 a 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.

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

This report discusses information security breaches that became known during the 2012–13 financial year (the reporting period), as well as breaches that were previously known and continued into this reporting period. The report separately discusses breaches that Telstra has itself acknowledged, and those where Telstra disputes that the underlying conduct constitutes a breach.

The steps that Telstra is taking to remediate its systems to prevent information security breaches occurring are also outlined. Importantly, even in those instances where Telstra disputes that its conduct breaches the information security provisions of the SSU, Telstra is taking steps to safeguard against the relevant systems being the source of a breach in future.

Telstra's position on 'disclosure' of Protected Information

As outlined above, the SSU prohibits Telstra from 'disclosing' Protected Information to Retail Business Units (among others) in particular circumstances. Where the ACCC and Telstra take differing views as to whether particular conduct is a breach of the information security provisions of the SSU, this is typically due to a fundamental disagreement as to what amounts to 'disclosure' and/or whether the relevant information is 'Protected Information' for the purpose of the SSU.

As 'disclose' is not defined in the SSU, the ACCC has interpreted this according to its ordinary meaning, including 'allow to be seen' or 'make known'. The ACCC considers that where Telstra populates systems with Protected Information and the Protected Information is visible to Business Units as a result, the relevant 'disclosure' has occurred.

For example, where Telstra populates Protected Information into information systems typically used by a Retail Business Unit and has set the access privileges of Retail Business Unit staff such that Protected Information is visible to those staff when accessing the system, then in the ACCC's view this constitutes disclosure to that Retail Business Unit. Actual use of the information accessible in the system is not required to establish disclosure has occurred.

On this basis, where this report refers to Protected Information being accessible to Retail Business Units, the ACCC considers that Telstra has disclosed the Protected Information.

The ACCC acknowledges 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 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). As a consequence, Telstra does not agree that some of the systems discussed in this report have been the source of information security breaches.

Information security breaches conceded by Telstra in 2012–13

Protected Information accessible to Telstra Retail users in operational and 'data warehouse' systems

Appendix 1 contains details provided by Telstra in relation to the disclosure to Telstra Retail users of Protected Information in 14 operational and 'data warehouse' systems that disclosed wholesale customer Protected Information in breach of clause 10.4 of its SSU. Telstra also identified an additional 'data warehouse' system that disclosed wholesale customer Protected Information in breach of clause 10.4 of its SSU, however this system was included in the ACCC's 2011–12 report to the Minister on Telstra's SSU compliance (the ACCC's 2011–12 report) and so is discussed in the 'continuing information security breaches' section below.

Telstra's operational systems have a broad range of functions including sales, customer management, order entry, service assurance, billing and credit management. These systems are used by both Telstra Retail and Telstra Operations staff and in some cases contain wholesale customer Protected Information. A number of 'data warehouse' systems, which are used by Telstra to enable business reporting, contain extensive wholesale customer Protected Information. There are differing amounts of wholesale customer Protected Information visible to Retail Business Unit users of each system.

Telstra's operational and 'data warehouse' systems are access controlled, with classes of staff given different access privileges. For example, Retail Business Unit staff are given access to view information relating to retail orders and services, whereas Wholesale Business Unit staff are given access to view information relating to wholesale orders and services. Notwithstanding the existence of these arrangements, Telstra has reported that in 15 of its operational and 'data warehouse' systems, not all wholesale customer Protected Information has been masked or segregated from Telstra Retail staff. Telstra has either partially or fully remediated a number of these systems, with the balance to be completed by December 2014.

ACCC findings

The ACCC sought further particulars from Telstra in relation to these issues. The ACCC's findings, including the wholesale customer Protected Information visible to Retail Business Units in each system, are detailed in appendix 1.

Telstra states that some of the information contained in these systems could have been provided to Telstra when the end-user was previously a retail customer of Telstra, particularly the end-user's name and date of birth. However, for each of these systems, Telstra has reported that some information relates to end-users that have never previously been Telstra Retail customers. In this case, the information could only have been provided to Telstra by the relevant wholesale customer.

Below are examples of a number of the systems identified as breaches of clause 10.4. The examples detail the general functions that Telstra Retail staff undertake when using the relevant system, the type of wholesale customer Protected Information that is visible in the system and the steps that Telstra has taken during the reporting period to remediate the system.

Customer relationship management and ordering tool

In its confidential Annual Compliance Report, Telstra states that:

Protected Information contained in a Customer Relationship Management and ordering tool used by Telstra Business and Telstra Enterprise & Government staff is likely to have been disclosed to RBU [Retail Business Unit] users in circumstances where the RBU staff searched for information regarding Retail customers, particular end-users or specific FNNs [full national numbers].

Prior to and during the reporting period, the following types of Protected Information concerning wholesale customers were visible to Retail Business Units if they conducted a search on an end-user of a wholesale customer by name, full national number or customer identification number:

- end-user details (full national number, name, customer identification number, address, other contact details)
- Telstra reference number
- wholesale products (for example, WLR, W-ADSL (Wholesale ADSL), LSS (Line Sharing Service), ULL (Unconditioned Local Loop))
- dates associated with the service (for example the created date and cancellation date if applicable)
- work required and other order details.

Telstra states that there were a significant number of Telstra Retail users of this system during the reporting period. This system is used by Telstra Retail for inbound and outbound sales, customer management and credit management.

In October 2013 Telstra implemented a systems change to mask wholesale customer Protected Information relating to wholesale orders for Retail Business Unit users. Full remediation is expected to occur by mid-2014.

Order entry and provisioning system for voice services

In its confidential Annual Compliance Report, Telstra states that:

Protected Information in a provisioning system for voice services is likely to have been disclosed to RBU users in certain circumstances where the information was associated with the FNN of a mixed Wholesale/Retail end-user or the FNN of an end-user with wholly eBilled Wholesale services.

Prior to and during the reporting period, the following types of Protected Information concerning wholesale customers were visible to Retail Business Units when accessing the system about end-users who acquired services from both Telstra and a wholesale customer:

- end-user details (including name and full national number)
- wholesale product codes for eBilled services* associated with the full national number.

Where a Retail Business Unit staff member searched on a full national number relating to an end-user of a wholly eBilled wholesale service (an end-user that has no services with Telstra Retail), the following Protected Information was available:

- end-user details (name, address)
- wholesale product codes associated with the full national number.

This system is a front-of-house system used by Retail Business Unit staff to provision voice services for business and corporate customers. Telstra states that there were a significant number of Telstra Retail users of this system during the reporting period.

Telstra has begun work to remediate this system to remove visibility of wholesale customer Protected Information to Retail Business Units. This remediation is expected to be completed in June 2014.

Fault and connection tracking tool

In its confidential Annual Compliance Report, Telstra states that:

Protected Information in a tool used to track the status of faults or orders and for web reporting is likely to have been disclosed to RBU users in circumstances where the RBU staff searched on a Wholesale FNN or Order Number or searched based on Region.

Prior to and during the reporting period, the following types of Protected Information concerning wholesale customers were visible to Retail Business Unit staff searching by full national number, order number or region and wholesale customer name:

- end-user details (name, full national number, plant details and service notes)
- wholesale customer orders.

This system tracks the status of faults and orders and is used by Retail Business Unit staff to check the status of a customer's fault or connection. Telstra states that there were a significant number of Telstra Retail users of this system during the reporting period.

In October 2013, Telstra made changes to this system to ensure that Retail Business Unit users cannot view the fields in the system that contain wholesale customer Protected Information and by removing staff access to the system where it is not required in their normal job function.

Corporate-wide 'data warehouse'

In its confidential Annual Compliance Report, Telstra states that:

Protected Information contained in an information repository storing subject-oriented data from customer billing, complaints, faults, provisioning and activation, credit management and marketing was accessible to and was likely to have been disclosed to RBU users.

Prior to and during the reporting period, the following types of Protected Information concerning wholesale customers were visible to Retail Business Unit staff accessing the system:

- end-user details
- eBill product details
- service and order information associated with full national numbers with wholesale eBill arrangements.

This system stores data from multiple source systems for reporting purposes. Telstra states that approximately 103 Retail Business Unit employees had access to this system in the reporting period.

Telstra states that Retail Business Unit access to this system has been revoked. Full remediation is expected to occur in 2014. Telstra states that this remediation will ensure that wholesale customer information flowing from other systems is segregated and Retail Business Unit staff are prevented from gaining access to the system.

* eBill is a Telstra business-to-business system for billing of wholesale fixed line voice and some data services (including wholesale Digital Subscriber Line (DSL)).

Remediation undertaken by Telstra

Telstra has undertaken a number of remediation steps in relation to the systems that it identified as breaches of clause 10.4 of the SSU. In particular, Telstra has:

- implemented a system change that redirects users to use a manual process to request documents, which are then manually edited to ensure that they do not contain wholesale customer Protected Information
- removed the visibility of wholesale customer Protected Information in one system, and removed visibility of wholesale customer Protected Information in certain views in two systems
- implemented data segmentation through defined access profiles in three 'data warehouse' systems and assigned all Retail Business Unit users the appropriate access profile
- removed Retail Business Unit user access in two 'data warehouses' where access is not required and developed processes to prevent new Retail Business Unit staff gaining access in the future.

In addition, Telstra has conducted SSU training and implemented behavioural rules and policies to promote SSU compliance and minimise the risk of Retail Business Units accessing and using wholesale customer Protected Information in breach of the SSU.

Telstra also decommissioned one system in June 2013 and intends to decommission another.

Telstra's proposed information security remediation for these systems includes removal of Telstra Retail access to wholesale customer Protected Information through internal partitioning of shared information systems, masking or removal of wholesale customer Protected Information from systems and the implementation of user access controls.

The ACCC considers that, when fully completed, Telstra's proposed remediation in relation to these systems should ensure that Telstra is compliant with the information security requirements in the SSU. However, the ACCC continues to closely monitor the progress of Telstra's remediation program and the effectiveness of interim controls put in place by Telstra. The ACCC intends to test the solutions implemented by Telstra in order to ensure that they operate correctly.

Protected Information contained in reports available to Telstra Retail staff

In its confidential Annual Compliance Report, Telstra identified two types of reports containing wholesale customer Protected Information that were made available to Telstra Retail staff either directly or on the Telstra intranet. Telstra provided the following details in relation to these two identified breaches of clause 10.4 of the SSU:

[Service Delivery] Reports which at times contained Protected Information, were prepared by a Corporate business unit for the Network Services Business Unit and may have been visible to RBU users who conducted searches on the Telstra intranet.	Access to the relevant intranet site had not been restricted at the relevant time. Since 18 December 2012, Telstra has restricted access to the intranet site to only those non RBU staff who need to know the information contained in the reports.
[Service Exception] Reports prepared for and received by RBU employees to implement large customer contracts may have included Protected Information in relation to Wholesale Services also acquired by the specific large customers involved.	Protected Information in particular Service Exception Reports was not masked or otherwise segregated from RBU Users. The Customer Billing Solutions Team stopped providing these reports to the relevant RBU users in January 2013.

ACCC findings

The ACCC sought further particulars from Telstra in relation to these issues. After considering the information provided by Telstra and making its own enquiries into the matters, the ACCC has made the following findings.

The Service Delivery Reports were available on the Telstra intranet and could be accessed by the majority of Telstra staff. These reports contained extensive wholesale customer Protected Information, including the type of wholesale service and the Telstra account number. In some cases the reports also included the names of wholesale customers and end-user contact details in a free-text comment field. The Telstra account number could then be entered into other Telstra systems in order to obtain the end-user's contact details.

The Service Delivery Reports were in a spreadsheet format which included the underlying data used to compile the reports, enabling Retail Business Unit employees to filter the information by type of service (for example, 'Wholesale Business DSL') and Telstra Business Unit.

The Service Delivery Reports contained a range of information relating to faults and were prepared for a service delivery team in a Network Services Business Unit that rectifies faults.

During the reporting period, 498 Service Delivery Reports were generated and accessible to Retail Business Units on the Telstra intranet. Some of these reports contained wholesale customer Protected Information, including:

- customer identification numbers and full national numbers
- end-user names and addresses
- wholesale product codes
- wholesale customer names
- Telstra Business Unit identifiers, for example 'TW' refers to 'Telstra Wholesale'.

The Service Exception Reports were prepared by a customer solutions team specifically for Telstra Retail account managers following Telstra winning a corporate or business customer.

The Service Exception Reports were generated to assist the corporate or government customer to accurately confirm the services that were to move to Telstra Retail. Some reports contained wholesale customer Protected Information relating to services that would continue to be provided by a wholesale customer. This Protected Information included:

- the service number
- invoice arrangement identification number
- whether the service was preselected to another carrier and whether the service was ported in, ported out or a non-Telstra access customer.

Remediation undertaken by Telstra

As noted above, in December 2012, Telstra restricted access to the intranet site containing the Service Delivery Reports to staff who are not in Retail Business Units and need to know the information contained in the reports. Telstra's Customer Billing Solutions Team also stopped providing the Service Exception Reports containing Protected Information to Retail Business Unit users in January 2013. The ACCC considers that this action by Telstra should ensure that Telstra is compliant with the information security requirements in the SSU.

Instruction email sent to a Telstra Retail call centre

In its confidential Annual Compliance Report, Telstra identified that an email sent to a call centre team breached clauses 10.3 and 10.4 of the SSU. Telstra provided the following details:

On 10 December 2012, a team leader in a Telstra Business inbound call centre sent an email to their team prompting them to use Protected Information that was accessible in Telstra's systems in a manner which was contrary to Telstra policy.	This specific incident was attributable to a breach of Telstra's policies by an individual Telstra representative. Upon becoming aware of the issue on 17 December 2012, Telstra sent an email to the recipients of the original email clarifying that staff must not use Telstra systems to determine whether a customer was acquiring services from a Wholesale Customer and conducted additional SSU training with staff to further reinforce the importance of these obligations and individual staff responsibility for complying with them. Investigations by Telstra have revealed that no loss or damage was suffered by any Wholesale Customer as a result of this incident. Accordingly, Telstra does not believe any use or disclosure of Protected Information which may have resulted from the issuing of this email could have been likely to, or did, enable a RBU to gain or exploit an unfair commercial advantage over any Wholesale Customer in any market.

ACCC findings

The ACCC sought further particulars from Telstra in relation to this issue. After considering the information provided by Telstra and making its own enquiries into the matter, the ACCC has made the following findings.

The instruction email sent to the Telstra small business call centre team was reported through Telstra's established processes for potential SSU compliance issues after an employee who was forwarded a copy of the email identified the potential SSU concerns. The email contained the following, which highlights the SSU concerns:

Use your prompts and triggers – wholesale internet on the line = "I notice that you don't have an internet service with Telstra, may I ask if there is a reason behind it?"

This email was sent to 120 recipients, all staff within an inbound call centre team that is responsible for Telstra's small business customers and receives service-related calls. The team generates 'leads' from these inbound calls which are then referred to sales teams. The team uses a large number of Telstra's systems, including some systems that contain wholesale customer Protected Information. In the period immediately following receipt of the instruction email (between 10 December and 24 December 2012), the team received more than 10,600 calls. 780 of these calls were labelled as leads and referred to the relevant sales team.

Telstra conducted an investigation into the leads generated by the team and isolated a number of calls for further review. Telstra's investigation concluded that for the majority of calls, the end-user either volunteered that they had services with a wholesale customer or asked, unprompted, what offers were available, either before the consultant accessed or without the consultant accessing any of Telstra's systems. On two occasions, the Telstra staff member queried the end-user's services after checking a Telstra system. However, these calls did not result in the end-user churning their services back to Telstra.

Telstra states that its enquiries indicate that the instruction email did not result in any end-users churning away from a wholesale customer to Telstra Retail. On this basis, Telstra does not believe any use or disclosure of Protected Information which may have resulted from the issuing of this email could have been likely to, or did, enable a Retail Business Unit to gain or exploit an unfair commercial advantage over any wholesale customer in any market.

However, the actual gaining or taking of an unfair commercial advantage to wholesale customers is not required to establish a breach of clause 10.3. It is only necessary that Telstra has used or disclosed Protected Information in a manner which *would be likely to enable* a Retail Business Unit to gain or exploit an unfair commercial advantage.

The ACCC considers that this breach is illustrative of the importance of Telstra's longer term systems-based remediation as Telstra's interim behavioural controls and compliance training only reduce, but do not eliminate, the risk of Retail Business Units accessing and misusing wholesale customer Protected Information.

Remediation undertaken by Telstra

As noted above, upon becoming aware of the instruction email, Telstra took a number of remedial steps:

- a follow-up email was sent to the original email recipients clarifying that staff must not use Telstra systems to determine whether a customer is a wholesale customer's end-user
- Telstra conducted refresher SSU training
- additional materials were provided to the team that included Telstra's SSU compliance rules for Telstra systems used by Telstra Retail users which contain wholesale customer information and internal Telstra rules for using Telstra systems.

Telstra has remediated systems to remove 'conversion opportunity' messages and some other wholesale customer Protected Information from being displayed by systems used by Retail Business Unit staff. In some cases, further remediation is required to ensure that no wholesale customer Protected Information, including wholesale service details and in the case of one system, a prominent indicator that there are non-Telstra services on the line, is disclosed to Retail Business Unit staff. This indicator was partially removed from the system in April 2013 and is no longer visible when Retail Business Unit users view services. Further changes in 2014 will completely remove the indicator from the system.

Further information security breaches identified by the ACCC in 2012–13

Protected Information accessible in Telstra operational and 'data warehouse' systems

In its confidential Annual Compliance Report, Telstra reported an additional 13 operational and 'data warehouse' systems that, based on its assessment, raised concerns as having the potential to disclose wholesale customer Protected Information but which it does not consider breach clause 10 of the SSU. In addition, Telstra sought to withdraw two systems that it reported in the 2012–13 financial year on the basis that they do not contain wholesale customer Protected Information. The ACCC does not accept Telstra's position in relation to these systems. The details provided by Telstra are contained in appendix 2.

These systems have a broad range of functions including, sales, customer management, order entry, service assurance, billing and credit management and reporting. These systems are used by staff in Telstra Retail and contain information relating to wholesale customers that could be viewed by Telstra Retail users of the system.

Telstra states that these systems do not breach the information security commitments in the SSU for the following reasons:

- eight of the systems contain wholesale customer Protected Information, however Telstra considers this Protected Information has not been disclosed to Telstra Retail as no Telstra Retail users have accessed the Protected Information during the reporting period
- the information visible to Retail Business Units in the seven remaining systems does not meet the definition of wholesale customer Protected Information in clause 10.1 of the SSU.

The ACCC's position in relation to these points is set out below.

ACCC findings

The extent of wholesale customer Protected Information contained in each system varies. The ACCC's findings, including on the nature of wholesale customer Protected Information visible to Retail Business Units in each system, are detailed in appendix 2. Telstra's reasons as to why it considers each of the systems included in appendix 2 do not constitute a breach of clause 10 of the SSU are also included in appendix 2.

'Disclosure' of wholesale customer Protected Information

As noted above, the ACCC considers that where Telstra populates wholesale customer Protected Information into information systems typically used by a Business Unit and has set the access privileges of Business Unit staff such that Protected Information is visible to those staff when accessing the system, then this constitutes disclosure to that Business Unit.

Accordingly, as Telstra Retail staff had access to eight systems containing wholesale customer Protected Information that was not masked, the ACCC considers that Telstra has breached clause 10.4 of the SSU in relation to each of these systems.

As noted above, Telstra considers that the Protected Information must be revealed to a Retail Business Unit 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. Telstra does not accept that there was disclosure of this type in relation to these eight systems and believes that it has not breached clause 10.4 of the SSU.

Definition of wholesale customer Protected Information

Telstra considers that the wholesale customer information in seven systems is not Protected Information for three reasons:

- The wholesale customer information does not disclose the wholesale customer's identity, the wholesale relationship or regulated service details.

  In its confidential Annual Compliance Report, Telstra states that four of its systems/data stores may contain details of a wholesale customer's end-user. Telstra considers that end-user details on their own are not wholesale customer Protected Information as they do not disclose or enable a Telstra Retail user to ascertain:

  – that the end-user is a customer of a wholesale customer (that is, it is silent on this matter)

  – the identity of a wholesale customer

  – any regulated service details for the end-user.

  Telstra considers that in order for end-user details to amount to wholesale customer Protected Information those details must be confidential and/or commercially sensitive and show a wholesale relationship (that is, they must identify the end-user as a customer of that wholesale customer).

  As noted above, clause 10.1 of the SSU defines Protected Information as confidential information identifying a wholesale customer or a customer of that wholesale customer, which was supplied by that wholesale customer and obtained by Telstra for the purpose of, or in the course of, supplying regulated services to that wholesale customer.

  Clause 10.2 of the SSU also contains examples of information which would constitute Protected Information. One example is the details of customers of the wholesale customer, such as name, address, contact details, account and service numbers.

  The ACCC considers that confidential information identifying a customer of a wholesale customer, including end-user names and contact details, is wholesale customer Protected Information if it is supplied by the wholesale customer and obtained by Telstra for the purpose of or in the course of supplying regulated services. It does not matter whether, of themselves, the end-user details disclose that the end-user is a customer of a wholesale customer, the identity of the wholesale customer or any regulated service details.

- The information does not relate to a regulated service.

  In its confidential Annual Compliance Report, Telstra states that one of its operational systems contains wholesale customer information (end-user names, addresses, full national numbers and in some cases, records of customer interactions). Telstra considers that this information is not wholesale customer Protected Information as it relates to interim medical priority assistance services which are not regulated services.

  The *Priority Assistance for Life Threatening Medical Conditions Code (ACIF C609:2007)* provides that where a medical priority assistance service is unworkable due to a fault on the Unconditioned Local Loop Service (ULLS), suppliers and underlying carriers will supply an interim service to priority customers (including provisional priority customers) until the fault is rectified. While it is possible for medical priority assistance services to be provided over other technologies, the ACCC considers that the vast majority of priority assistance services offered by wholesale customers will be provided in connection with ULLS or the Wholesale Line Rental (WLR) service.

  The ACCC therefore considers that the information in Telstra's systems relating to interim medical priority assistance services for end-users of wholesale customers will generally have been provided to Telstra by the wholesale customer for the purpose of, or in the course of, supplying a regulated service.

- The information that discloses end-user details is populated from another source.

  The two systems that Telstra sought to withdraw are systems that automatically pre-populated end-user details in an order form when an order was placed prior to 31 October 2012. These details included the Telstra account number where the end-user never had a retail relationship with Telstra.

  Telstra considers that these systems do not disclose wholesale customer Protected Information as:

  - neither the form itself, nor the information returned by the system to complete the form, discloses (or at any time has disclosed or enabled the Retail Business Unit user to ascertain) that the end-user is a customer of a wholesale customer, nor does it disclose (or at any time has disclosed or enabled the Retail Business Unit user to ascertain) the identity of the wholesale customer, so a Retail Business Unit user of the system would be unaware that the end-user has any relationship with a wholesale customer
  - neither the form, nor the information returned by the system to complete the form, discloses any service details for the end-user or any wholesale service information
  - the only information populated in the form is the end-user's name, address and account number, which on their own is neither confidential nor commercially sensitive because they do not disclose any wholesale relationship details, or enable the identity of a wholesale customer or the identity of customer of a wholesale customer to be ascertained, and is therefore not Protected Information within the meaning of the SSU
  - the Retail Business Unit user will only be accessing the system following a request by an end-user for Telstra to provide a service
  - the standard ordering practice requires the Retail Business Unit user taking the order to confirm the end-user details which are populated with the end-user, meaning the Retail Business Unit user does not save any time in taking the order as a result of the pre-population of the end-user's contact details, and
  - Telstra also notes that clauses 7.21 and 7.22 of the Standard Terms of the generic Customer Relationship Agreement permit Telstra to use end-user details received from a wholesale customer where Telstra is supplying a telecommunications service to the end-user.

  The ACCC considers that the presence of a Telstra account number in an order form for an end-user that does not have any services with Telstra Retail clearly indicates that the end-user is a customer of a wholesale customer. Accordingly, this information is Protected Information within the meaning of the SSU. In addition, as these end-users have never had a service with Telstra, Telstra was not currently supplying a telecommunications service to the end-user and so the exception to the definition of Protected Information referred to above does not apply.

Remediation undertaken by Telstra

Telstra has taken steps towards removing access to these operational and 'data warehouse' systems, or put filters in place to limit access to wholesale customer Protected Information in those systems.

In particular, Telstra has continued to refine its access management processes for each of the systems to ensure access requests by Telstra Retail staff undergo a thorough review before access is granted.

Telstra has also continued to implement general training and has put in place policies to promote compliance with the SSU and prevent the use of wholesale customer Protected Information in Telstra's systems. It is also continuing to investigate longer term remediation options.

Telstra's proposed information security remediation for these systems includes removal of Telstra Retail access to wholesale customer Protected Information through internal partitioning of shared information systems, masking or removal of wholesale customer Protected Information from systems and the implementation of user access controls.

The ACCC considers that, when fully completed, Telstra's proposed remediation in relation to these systems should ensure that Telstra is compliant with the information security requirements in the SSU. However, the ACCC continues to closely monitor the progress of Telstra's remediation program and the effectiveness of interim controls put in place by Telstra.

Communication with end-users

Telstra provided the following details in its confidential Annual Compliance Report in relation to an instance where it had communicated with the end-users of wholesale customers:

> Letters were sent to end-users of Wholesale Customers in relation to the Warrnambool Exchange fire. A Telstra staff member had requested a list of contact information for services at the Exchange and the list provided included 3185 Wholesale fixed line services. A small number of Retail BU employees had access to the list.

ACCC findings

The ACCC sought further particulars from Telstra in relation to this issue. After considering the information provided by Telstra and making its own enquiries into the matter, the ACCC has made the following findings.

The contact information disclosed to Retail Business Unit employees included:

- end-user details (name, address, associated account numbers)
- full national numbers.

Telstra states that at least 400 of the end-users contacted also had services with Telstra Retail and approximately 1037 end-users had previously been Telstra Retail customers. Accordingly, Telstra considers that some of the end-user information disclosed to Retail Business Unit employees was not provided to Telstra by a wholesale customer and so does not meet the definition of Protected Information in the SSU.

With regard to those end-users that had never been customers of Telstra Retail, Telstra contends that this information was not wholesale customer Protected Information as it did not disclose any wholesale relationship details or enable the identity of a wholesale customer or the identity of the end-user as a customer of a wholesale customer to be ascertained.

The ACCC does not accept Telstra's position. The ACCC considers that any confidential information identifying a wholesale customer's end-user (where it meets the other requirements in clause 10.1) is wholesale customer Protected Information, regardless of whether it discloses wholesale relationship details or the wholesale customer's identity.

The ACCC considers that by misclassifying end-users' services and supplying lists of end-users that included end-users of wholesale customers to Telstra Retail staff, Telstra has breached clause 10.4 of the SSU.

Remediation undertaken by Telstra

Upon becoming aware of the conduct, Telstra wrote to affected wholesale customers to inform them of, and apologise for, the reported conduct. The ACCC considers that Telstra's actions following its identification of this issue minimised the risk of any competitive harm occurring as a result of the conduct.

Disclosure of information in a system also breached clause 10.3

Telstra did not report any of its operational and 'data warehouse' systems that disclose wholesale customer Protected Information as breaches of clause 10.3 of the SSU.

ACCC findings

The ACCC sought further particulars from Telstra in relation to the matters described above and considers that one order management system also breaches clause 10.3 of the SSU.

In its confidential Annual Compliance Report, Telstra provided the following information about this system:

Protected Information in a web-based tool that supports the management and delivery of customer solutions where there is an infrastructure shortfall (held orders) is likely to have been disclosed to RBU users in circumstances where the RBU staff searched for details on a ticket of work via service FNN, customer name, region, ticket of work ID and other criteria.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users and access controls were not fully in place. Telstra took steps to reduce the number of RBU users with access and, after a further systems remediation, the final 19 RBU users had their access revoked between 19 April and 13 September 2013.

Telstra does not consider there has been a breach of clause 10.3 as it has no evidence that the order management system has been used by Retail Business Unit users in any widespread or systemic way to access or use Protected Information or in order to gain any unfair commercial advantage.

This system has a number of search capabilities, including the ability to search by Business Unit. Conducting a search by 'TW' (Telstra Wholesale) will give a list of all Telstra Wholesale tickets of work for 'held orders'—orders that are unable to be provisioned, for example because of a lack of available infrastructure. Searches can also be conducted by region.

The search results include a list of end-user names and the status of the ticket of work. Users of the system can then select the ticket of work ID to obtain further details, including the end-user's contact number and relevant dates associated with the ticket of work (including the application date).

The ACCC considers that Telstra has used wholesale customer Protected Information in a manner which would be likely to enable Telstra Retail to gain or exploit an unfair commercial advantage over wholesale customers in downstream markets, including by:

- populating wholesale customer Protected Information into an order management system used by Telstra Retail staff
- enabling Telstra Retail staff to search by Business Unit from the main screen and create a list of tickets of work for end-users of wholesale customers
- enabling Telstra Retail to view details of wholesale customers' end-users, including contact number, by clicking on tickets of work.

The ACCC notes that it has previously received complaints from wholesale customers alleging that some retail orders have been provisioned in circumstances where a wholesale order is 'held'. That is, the wholesale customer's end-user contacts Telstra Retail after experiencing lengthy provisioning delays and is able to obtain the same service from Telstra Retail with shorter or no delay. The ACCC considers that end-users whose orders are 'held' may be more likely to take up an offer to churn to an alternative provider, particularly if they have been waiting for a significant period of time for a service to be provisioned and do not fully appreciate that the delay is not the

responsibility of the provider. While Telstra orders may also be 'held', it is clear from the ACCC's enquiries that Telstra's wholesale customers did not have the same degree of visibility over their competitors' 'held orders' as was available to Telstra Retail.

While Telstra has not found any examples of its staff using this system to identify and approach end-users whose orders with a wholesale customer are 'held', clause 10.3 does not require a Retail Business Unit to have actually used the information to gain or exploit an unfair commercial advantage over its competitors. Rather, clause 10.3 will be breached where wholesale customer Protected Information is used or disclosed in a manner which would be likely to enable a Retail Business Unit to gain or exploit an unfair commercial advantage over the wholesale customer.

Telstra does not agree or concede that there has been a breach of clause 10.3 as outlined above. Telstra states that:

- *the number of RBU users during the Reporting Period who had access to [the system] was relatively low (at its highest 72) and has been reduced over this time;*
- *as at 19 September 2013, there were no RBU users who had access to the system. Any future request by RBU employees for access to the system will be assessed to determine if they need access to the system for purposes that fall within one of the SSU exceptions under clause 8.4 (e.g. provision of emergency services or payphones);*
- *RBU staff typically use the system to address retail customer concerns and check the status of held retail orders;*
- *in May 2012 Telstra removed intranet guides for interpreting and identifying wholesale customer information in ordering and provisioning and billing systems to minimise the interpretation and use of any wholesale customer information; and*
- *Telstra has implemented general training and policies to promote compliance with the SSU and to prevent the use of Protected Information in Telstra's systems.*

Remediation undertaken by Telstra

In September 2013, Telstra removed Retail Business Unit access to the system. Telstra also developed processes to prevent new Retail Business Unit staff gaining access in the future.

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

Matters reported after the end of the reporting period

The SSU requires Telstra's confidential Annual Compliance Report to include details of equivalence issues received from wholesale customers or from the ACCC or identified by Telstra during the relevant financial year. Consequently, Telstra's confidential Annual Compliance Report does not contain those equivalence issues that occurred during the 2012–13 financial year, but were subsequently identified as equivalence issues.

In this regard, Telstra has identified a number of equivalence issues in its confidential monthly SSU compliance reports for July, August and September 2013 that relate to conduct that occurred during the 2012–13 financial year. These equivalence issues comprise:

- five operational systems that disclose wholesale customer Protected Information
- an email forwarded in error to a Telstra Retail employee.

Protected Information accessible in Telstra operational systems

Telstra provided the following information in its confidential monthly SSU compliance reports in relation to five matters that may breach clause 10.4 of the SSU:

(i) Field and exchange appointment management system

There are approximately 6500 RBU employees with access to the system. It is possible to search by customer reference number (CRN), order number or full national number (FNN) and recognise that an exchange appointment has been created or initiated for that CRN or FNN. If a user knew of the Wholesale end customer's FNN and then attempted to cancel an exchange appointment for that FNN, the wholesale product codes for that end-user's service will be displayed. We do not have any evidence that RBU users have been modifying or cancelling exchange appointments for Wholesale end customers.

(ii) Dirty tickets of work (DToW) and coaching feedback management tool

DToW are errors in tickets of work which may result in delays or rework in completing a ticket of work. The tool receives notifications of DToW and returns orders to the initiating business unit for business remediation and progression of the order. While the tool can be accessed by many users via the intranet, users can only view the DToW that they, or someone in their work group, have logged and/or been allocated for follow up. A small proportion of DToW allocated to RBU users for follow up have been found to contain Wholesale Customer information such as wholesale products on the line and the name of the Wholesale Customer.

(iii) Fault testing system for ADSL, fibre to the premises (FTTP) and Public Switched Telephone Network (PSTN) services used by wholesale and retail staff

The system also tracks testing and fault data for compliance reporting, performs automated fault queue testing and testing and diagnostic functionality for various interfacing systems. The system receives data from a number of upstream systems. The system also sends ADSL/PSTN test results to a number of other systems.

Approximately 357 [Telstra Retail] users have access to the system. These retail users access the system to check for faults in relation to retail services. The majority of [Telstra Retail] users only view a results page, which does not reveal Protected Information.

However, Telstra has identified that it is possible to view other screens where some wholesale customer information is visible to retail users including the name of a wholesale customer and the product and service reference codes for wholesale services associated with a wholesale FNN.

(iv) Archive facility that extracts data from a service order engine for provisioning Enhanced Business Services

The archive facility has different access for wholesale and retail users based upon the use of a filter which has been identified as being incomplete. Our investigation has identified that it is possible to search using a wild card function, for example, when there is an incomplete FNN, and that wildcard searches can be performed for information such as Order Number, Customer Name, FNN, Customer Reference and Account Number. If a wildcard search was performed, it is possible that information regarding a wholesale customer that is Protected Information could be disclosed to the RBU user, including Wholesale customer name details, FNN, Order Number and CIDN [customer identification number].

Of the 45 RBU users who have accessed the archive facility only five users have used the wildcard search function. While we do not have any evidence that Wholesale Customer Protected Information has been disclosed to any of the RBU users, due to our discovery of the incomplete filtering there is a theoretical risk that a RBU user could use wildcard searching to access information relating to a wholesale customer's order.

(v) Front-end interface used by Telstra's Channel Partners and Dealers

The search functions allow the disclosure of some wholesale customer end-user information, that is, if a RBU user conducts a serviceability check in response to an end-user inquiry to Telstra regarding the availability of a service at a particular address, information regarding the presence of the active or inactive ULLS or a pending disconnection of the ULLS at the address may be visible. This system is a different interface of the system described in item 13 of appendix 1. Telstra states that it reported the different interface out of an abundance of caution and to reflect the fact that there is a different user group of this system. Apart from one remaining issue, both interfaces have been remediated.

ACCC findings

The ACCC sought further particulars from Telstra in relation to these equivalence issues. After considering the information provided by Telstra and making its own enquiries into the matter, the ACCC has made the following findings.

Each of the systems contain a range of wholesale customer Protected Information. During the 2012–13 financial year, Telstra Retail employees were able to access this Protected Information.

The ACCC considers that by making wholesale customer Protected Information stored in these systems accessible to Telstra Retail staff, Telstra breached the information security obligation in clause 10.4 of the SSU.

Remediation undertaken by Telstra

Telstra has introduced warning screens into the DToW and coaching feedback management tool and made changes to ensure users do not enter wholesale customer Protected Information into free text fields. Telstra has also blocked the visibility of wholesale product codes in the front-end interface used by Telstra's Channel Partners and Dealers. Telstra expects that the remaining remediation will be completed in 2014.

Telstra's proposed information security remediation for these systems includes removal of Telstra Retail access to wholesale customer Protected Information through internal partitioning of shared information systems, masking or removal of wholesale customer Protected Information from systems and the implementation of user access controls.

The ACCC considers that, when fully completed, Telstra's proposed remediation in relation to these systems should ensure that Telstra is compliant with the information security requirements in the SSU. However, the ACCC continues to closely monitor the progress of Telstra's remediation program and the effectiveness of the interim controls put in place by Telstra. The ACCC intends to test the solutions implemented by Telstra in order to ensure that they operate correctly.

Email sent in error

Telstra included the following information in its confidential monthly SSU compliance report for July 2013:

> An email received from a Wholesale Customer with an inquiry about an end-user's service was mistakenly forwarded to an employee in a RBU by a person who mistakenly thought the query related to a Telstra Retail customer. The sender was seeking to provide information to respond to the query. The purpose of the email was to clarify why the particular order was in 'held' status and it contained details of an order reference, site property information and the end-user name. There was no intention to provide any advantage to a RBU and no obvious advantage for the RBU to know the existence of the order. The RBU staff member was requested to delete the email and has confirmed that this was done.

ACCC findings

The ACCC sought further particulars from Telstra in relation to this issue. After considering the information provided by Telstra and making its own enquiries into the matter, the ACCC has made the following findings.

In late March 2013, a Telstra wholesale customer sought clarification in an email to Telstra Wholesale as to why Telstra had rejected its service request on behalf of a large corporate end-user to install new copper infrastructure in an industrial estate in Western Australia. This email disclosed both the wholesale customer's name and the end-user's identity.

Telstra rejected the wholesale customer service request on the basis of its business decision not to sell copper into Greenfield NBN estates. The service request related to an area marked as an NBN Co site, although the site was not currently serviced by NBN infrastructure and Telstra did not expect NBN construction to start until March 2015.

The wholesale customer's enquiry was forwarded to a Telstra Retail employee by a person in a non-Separated Business Unit. When forwarding the email, the person in the non-Separated Business Unit requested that the Telstra Retail employee provide advice on the retail services that may be appropriate for the end-user.

Telstra states that the person in the non-Separated Business unit forwarded the email mistakenly as they thought that the enquiry related to the Telstra Retail employee's customer. The Retail Business Unit employee's primary role and responsibility was to assist the Telstra team in the transition to the NBN. Telstra states that the Telstra Retail employee did not take any action with the email or provide any advice in relation to it.

Telstra reported these circumstances as giving rise to a breach of clause 10.4 of the SSU.

Telstra states that there was no intention to provide any advantage to a Retail Business Unit and no obvious advantage for the Retail Business Unit to know the existence of the order, and as such Telstra does not consider that the circumstances gave rise to a breach of clause 10.3 of the SSU.

In this regard, the ACCC does not consider intent to be relevant to whether a breach of clause 10.3 has occurred. It is apparent from the relevant email chain obtained by the ACCC that, whether inadvertently or otherwise, a wholesale customer's enquiry containing Protected Information was forwarded to a Retail Business Unit employee in a manner which was likely to enable the relevant Retail Business Unit to gain or exploit an unfair commercial advantage over the wholesale customer. This is evidenced by the nature of the email forwarded to the Retail Business Unit employee which:

- suggested that, as a large customer, the end-user should consider using mobile phones for the voice service and mobile broadband for their internet services
- requested the Telstra Retail employee advise on the options for Telstra Enterprise and Government customers for NBN
- identified the Telstra Retail employee as the lead at Telstra's NBN Centre of Excellence for Telstra Enterprise and Government customers.

The ACCC considers that in these circumstances Telstra has used wholesale customer Protected Information in breach of clause 10.3 of the SSU.

Remediation undertaken by Telstra

As noted above, Telstra has stated that the Retail Business Unit employee that received the email was asked to delete the email. Telstra states that the email was deleted and the employee did not take any action with the email or provide any advice in relation to it.

Continuing information security breaches

In its confidential Annual Compliance Report for 2011–12, Telstra identified four breaches of the SSU's information security obligations. The ACCC identified an additional three breaches. Five of these breaches continued in 2012–13. Further detail on each of these breaches is available in the ACCC's 2011–12 report to the Minister on Telstra's SSU compliance (the ACCC's 2011–12 report).[7]

Continuing breaches of clause 10.4

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

- Protected Information is accessible to Telstra Retail in shared systems.

  This matter is outlined in full in items 1 and 2 in the ACCC's 2011–12 report. The wholesale customer Protected Information visible during the reporting period included network codes, end-user details and product codes that enabled Telstra Retail staff to identify whether an end-user customer was acquiring a wholesale service and if so, the general type of service.

  Employees in Telstra Retail and Network Services were also able to identify in an IT system whether there is a pending order for a wholesale service on a particular line. In a small proportion of instances, this led to employees seeking to withdraw an order.
- Protected Information relating to faults is accessible to Telstra Retail in a shared system.

  This matter is outlined in full in item 3 in the ACCC's 2011–12 report. The wholesale customer Protected Information visible during the reporting period included end-user details, a high level product description, the wholesaler/rebiller name and fault description.
- 'Data warehouse' systems contain wholesale customer Protected Information.

  This matter is outlined in full in item 5 in the ACCC's 2011–12 report. The wholesale customer Protected Information visible during the reporting period included customer details, product and service details, billing information and wholesale customer service orders.

Remediation undertaken by Telstra

Telstra undertook a significant amount of remediation during the reporting period. In particular:

- In April 2013, it implemented system changes to block the ability of Telstra Retail users to view or modify wholesale customers' orders for one shared system. It is currently considering broader user access management system changes and processes to manage Telstra Retail users' access to two shared systems.
- In March 2013 Telstra introduced splash screens to warn users not to enter wholesale customer information into a fault management system.
- Telstra has sought to remediate the four 'data warehouses' reported in 2011–12. In particular, it fully remediated one of the four systems in September 2013 by removing access to all existing Telstra Retail users and developing processes to prevent Telstra Retail users gaining access in future. The other 'data warehouse' systems have been partially remediated by removing those Telstra Retail users' access and Telstra is exploring options to further segregate Protected Information within the systems.

Telstra's proposed information security remediation for these systems includes removal of Telstra Retail access to wholesale customer Protected Information through internal partitioning of shared information systems, masking or removal of wholesale customer Protected Information from systems and the implementation of user access controls.

7 http://www.accc.gov.au/publications/telstras-structural-separation-undertaking

The ACCC considers that, when fully completed, Telstra's proposed remediation in relation to these systems should ensure that Telstra is compliant with the information security requirements in the SSU. However, the ACCC continues to closely monitor the progress of Telstra's remediation program and the effectiveness of the interim controls put in place by Telstra.

Continuing breach of clause 10.3

This matter is outlined in full in item 7 in the ACCC's 2011–12 report.

Until November 2012, Telstra Retail employees were still able to cancel pending wholesale orders. This occurred on a small number of occasions (for example, 21 in July 2012 and 18 in October 2012). Until March 2013, Telstra Retail employees were also able to release 'held' wholesale orders. This occurred on a small number of occasions (for example, two in January 2013). In almost all cases where a Telstra Retail staff member cancelled a wholesale order, this occurred at the request of the end-user of the service.

In addition, Telstra's primary ordering and provisioning system for fixed line services continued to display a prominent indicator notifying Telstra Retail staff that there are non-Telstra services on a particular line.

During part of the reporting period, a Telstra sales transaction system, used by some inbound sales and lead teams (including Telstra Retail consultants) for billing and order purposes, continued to display 'conversion opportunity' messages where an end-user acquired one or more non-Telstra services. The Telstra Retail consultant could then navigate to a 'Convert to Telstra' option which provided an additional message advising the sales consultant that the service was supplied and billed by a provider other than Telstra, and that they may attempt to convert the customer to Telstra if the customer has agreed to be told information about Telstra products, or where the customer has made a request to be converted.

Telstra cannot rule out the possibility of some Retail Business Unit staff disregarding the guidelines and used the indicator and conversion messages to gain or exploit an unfair commercial advantage. The actual gaining or exploiting of an unfair commercial advantage over wholesale customers is not required to establish a breach of clause 10.3 of the SSU.

Remediation undertaken by Telstra

Telstra undertook a significant amount of remediation during the reporting period. In particular, Telstra:

- removed the 'conversion opportunity' messages in July 2012
- removed the ability for Telstra Retail staff to withdraw wholesale LSS orders in August 2012
- removed the ability for Telstra Retail staff to modify/withdraw other wholesale orders in March 2013
- removed the ability for Telstra Retail staff to release 'held' wholesale orders in March 2013.

In addition to the remediation outlined above, Telstra's proposed remediation includes masking or removing wholesale customer Protected Information from the systems and removing the prominent indicator that there are non-Telstra services on a particular line.

The ACCC considers that, when fully completed, Telstra's proposed remediation in relation to these systems should ensure that Telstra is compliant with the information security requirements in the SSU. However, the ACCC continues to closely monitor the progress of Telstra's remediation program and the effectiveness of the interim controls put in place by Telstra. The ACCC intends to test the solutions implemented by Telstra in order to ensure that they operate correctly.

Summary of Telstra's information security remediation

Telstra has undertaken a number of remediation activities throughout the reporting period to bring its IT systems into compliance with the SSU's information security obligations. Telstra anticipates that all systems-based remediation will be completed by the end of 2014.

The remediation implemented by Telstra during the reporting period included:

- segregating wholesale customer Protected Information in its systems from Telstra Retail user access
- removing Retail Business Unit user access to systems (or certain fields or windows in systems) that contain wholesale customer Protected Information
- placing other controls on its systems, such as preventing Retail Business Unit users from viewing or modifying wholesale customers' orders, removing search functions or access to archived material that could provide access to Protected Information.

Telstra has faced difficulties remediating some of its systems, and has had to reconsider its remediation options. Telstra has stated that many of these are critical systems that assure service provision and fault rectification in respect of all Telstra's fixed line services, both retail and wholesale, and process hundreds of thousands of transactions each day.

As such, the ACCC has recognised the need for Telstra to exercise care in modifying these systems as changes may have unforeseen consequences for both wholesale customer and Telstra Retail end-users if not properly scoped.

In addition, Telstra has conducted training on the SSU's equivalence obligations and put in place behavioural rules and policies, to promote compliance and prevent the use of wholesale customer Protected Information by Telstra Retail staff. Telstra has also sought to communicate relevant breaches of the SSU with affected wholesale customers.

The ACCC considers that, on the information currently available, Telstra's remediation program will ensure that Telstra complies with the information security obligations in the SSU. The ACCC intends to test the solutions implemented by Telstra in order to ensure that they operate correctly.

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 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 those customers are otherwise 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* supplied to Telstra Retail customers are (a) issued and processed in Telstra's systems using equivalent order management and (b) managed and performed by Telstra field staff in an equivalent manner
- **clause 11.2(b)** provides that Telstra will rectify Basic Telephone Service (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.

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

In its confidential Annual Compliance Report, Telstra identified one breach of the overarching equivalence obligation. This breach related to the unavailability of ADSL profiles to wholesale customers when these profiles were available to Retail Business Units.

The ACCC has also identified an additional breach of the overarching equivalence obligation and specific interim equivalence and transparency obligations in clause 11 of the SSU.

Overarching equivalence breach conceded by Telstra

Wholesale ADSL 'profiles'

In 2011 Telstra released two new ADSL 'profiles' that were part of a new retail product called 'Digital Business'. Digital Business bundled a broadband internet connection with a voice over internet protocol (VoIP) telephony service. In support of the Digital Business product, Telstra developed two new ADSL 'profiles' to assist in managing lines experiencing problems with interference.

ADSL 'profiles' are normally available for both retail and wholesale services where supported by Telstra equipment. However, the two new ADSL profiles that were developed to support the Digital Business product were not made available to wholesale customers.

Telstra provided the following details in its confidential Annual Compliance Report in relation to this identified breach of the overarching equivalence commitment in the SSU.

Two new ADSL profiles which were offered as part of a Retail Bundled Layer 3 product (which is a bundle of ADSL2+ broadband, IP telephony over ADSL2+ and mobile services) were available to Telstra Retail but not Wholesale Customers.	When the New Profiles were developed, Telstra understood that they formed an integral part of an innovative Layer 3 product that was not subject to the SSU. Telstra subsequently formed the view that the New Profiles applied over and operate at Layer 2. Upon becoming aware of the issue, Telstra took immediate steps to make the New Profiles available to Wholesale Customers as soon as practicable and, on 13 May 2013, submitted a rectification proposal detailing these steps to the ACCC.

ACCC findings

The ACCC sought further particulars from Telstra in relation to this issue. After considering the information provided by Telstra and making its own enquiries into the matter, the ACCC has made the following findings.

The overarching equivalence commitment in the SSU requires that Telstra ensure equivalence in its supply of regulated services, including ADSL, to wholesale customers and its Retail Business Units in respect of its technical and operational quality. The ADSL profiles Telstra developed for its Digital Business product are technical settings applied at Layer 2 and were provided to its Retail Business Units. The overarching equivalence commitment therefore required that they also be made available to wholesale customers. The ACCC considers that this matter breaches clause 9(a)(ii) of the SSU.

Rectification proposal

As required by the SSU, Telstra submitted a rectification proposal setting out the steps it proposed to take to remedy the possible breach. The ACCC consulted with affected wholesale customers about whether Telstra's proposal was an effective remedy for the possible breach and no submissions were received. The ACCC subsequently accepted the rectification proposal in July 2013 as it considered that it provided an effective remedy for the breach.

As part of the rectification proposal Telstra has:

- made the new ADSL profiles available to wholesale customers on an equivalent basis to Retail Business Units
- published an up-to-date list of available ports in each exchange service area where the new ADSL profiles are available
- communicated these changes to wholesale customers.

Further equivalence breaches identified by the ACCC

Order management of wholesale ADSL service upgrades

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

> Following an issue raised by the ACCC in respect of a complaint by an end-user of a wholesale customer regarding the availability of ADSL 2+ services, Telstra undertook an analysis to determine whether any other services could have been similarly affected. As a result of these investigations, Telstra identified that a small number of wholesale DSL requests to upgrade were not progressing in its wholesale customer ordering system in circumstances where a transposition would be required to configure or transfer an ADSL1 service to an ADSL2+ service. Some of these orders would have been allowed to progress through Telstra Retail's ordering processes.

Telstra does not consider that a breach of the equivalence commitments in the SSU occurred as it considers that any failure to comply with the requirements of the SSU in this instance was trivial. Telstra states in its confidential Annual Compliance Report that:

- the issue only affected service qualification requests for upgrades from ADSL1 to ADSL2+ for a small number of services with a "particular, unusual network topology"
- of the services affected, only a small number of services churned to Telstra Retail
- the issue did not result in any significant negative or material impact on wholesale customers
- Telstra could not reasonably be expected to have identified the issue earlier than it did.

ACCC findings

The ACCC sought further particulars from Telstra in relation to this issue. After considering the information provided by Telstra and making its own enquiries into the matter, the ACCC has made the following findings.

In 2011 Telstra commenced a project to upgrade existing infrastructure (TopHat upgrades) across its network so that customers in areas where no broadband services were available, or where only ADSL1 was available, could obtain an ADSL2+ service.

The overarching equivalence commitment in the SSU requires that Telstra ensure equivalence in its supply to wholesale customers and its Retail Business Units in respect of the operational systems, procedures and processes used in its supply.

In some limited circumstances where a TopHat upgrade had taken place, Telstra's wholesale customer ordering system did not allow a wholesale order to upgrade an end-user's service from ADSL1 to ADSL2+ to be fulfilled. In the same circumstances, a Telstra Retail order could have been completed.

The ACCC considers that this reported issue breaches clauses 9(a)(ii) and 11.3(a) of the SSU. The ACCC does not consider the reported issue to be trivial because:

- in upgrading its network, Telstra failed to implement changes to its wholesale ordering platform to enable wholesale customers to upgrade customers in an equivalent way to Retail Business Units
- the time taken to rectify the problem was substantial—the changes required to enable equivalence were not made until 18 months after the commencement of the TopHat upgrade project
- there was a demonstrable impact on a number of wholesale customers who were unable to upgrade their end-users
- a small number of end-users chose to churn to Telstra Retail in order to upgrade their services after a wholesale provider was unable to do so.

Rectification proposal

As required by the SSU, Telstra submitted a rectification proposal setting out the steps it proposed to take to remedy the possible breach. The ACCC consulted with affected wholesale customers about whether Telstra's rectification proposal was an effective remedy for the possible breach and each of the affected wholesale customers indicated that the steps outlined in Telstra's rectification proposal were adequate to address the issue. The ACCC subsequently accepted the rectification proposal in July 2013 as it considered that it provided an effective remedy for the breach.

As part of the rectification proposal Telstra has:

- implemented a system change to correct information displayed in its wholesale customer ordering system in relation to affected order types and communicated with wholesale customers in relation to the system change
- contacted the wholesale customers whose services were impacted by the order failure and dealt with their affected orders
- contacted end-users who were "gained" by Telstra Retail as a result of the breach and offered to transfer (at no charge to the end-user) their services to the wholesale customer whose order had failed.

Reporting obligations

Clause 18(c) of the SSU provides that Telstra will promote and facilitate the ACCC's monitoring of Telstra's compliance with the SSU by, amongst other things, providing the TEM report in accordance with the requirements of Schedule 9.

Paragraph 2.1(a)(ii) of Schedule 9 states that a confidential TEM Report will be prepared for each three month period commencing on 1 April 2012.

Paragraph 2.1(c) of Schedule 9 provides that Telstra must submit TEM Reports within 60 days after the end of the Reporting Period to which it relates.

Telstra provided the following details in its confidential Annual Compliance Report in relation to this identified breach of the SSU:

The TEM Report filed in December 2012 was not submitted to the ACCC by the due date, resulting in a technical non-compliance with the SSU. While the Report was prepared within time to be submitted by the due date, a discrepancy in the report was identified immediately prior to its submission. The materiality of this discrepancy required further analysis, resulting in a request to the ACCC for an extension of the report's submission date. This request was granted by the ACCC. As the SSU does not provide for extensions to the timeframes for submitting reports, this could be taken to be a technical non-compliance with the SSU. Since this occurrence, our TEM governance structures have been strengthened, and parts of the reporting process have been automated to stop this recurring.

Other rectification proposal submitted during the reporting period

Fault rectification of the BTS

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

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

Background

Relevant clauses of the SSU

Clause 9(a)(i) of the SSU requires that Telstra must ensure equivalence, on an equivalence of outputs basis, in relation to its supply to wholesale customers and Retail Business Units in respect of the technical and operational quality of the relevant regulated service. Clause 16.1 of the SSU provides that Telstra has identified equivalence and transparency Metrics that are relevant to the operational quality of relevant regulated services. Metric 5 is relevant to the operational quality and delivery standard of the BTS, a regulated service.

Clause 9(a)(ii) requires that Telstra ensure equivalence, on an equivalence of outputs basis, in relation to its supply to wholesale customers and Retail Business Units in respect of the operational systems, procedures and processes used in the supply of the relevant regulated service.

Clause 11.1 of the SSU requires that Telstra maintain systems and processes for issuing tickets of work to field staff so that wholesale and retail tickets of work are issued and processed in Telstra's systems using equivalent order management and also managed and performed by Telstra field staff in an equivalent manner. Clause 11.2(b) of the SSU requires Telstra to rectify wholesale and retail BTS faults using equivalent order management and otherwise in an equivalent manner.

Equivalence and transparency Metrics

The SSU requires Telstra to submit quarterly operational equivalence reports to the ACCC measuring its performance against a number of measures known as 'Metrics'. In these reports, Telstra compares its operational performance for wholesale customers with its operational performance for its Retail Business Units.

These Metrics are set out in Schedule 3 of the SSU, and are used to assist both Telstra and wholesale customers to assess over time:

- the operational quality of relevant regulated services
- the standard of delivery of service activation and provisioning, fault detection, handling and rectification and availability of LOLO (LinxOnline Ordering web services)
- the adequacy and timeliness of wholesale processes including billing accuracy.

Variances in favour of Telstra Retail do not, of themselves, breach the SSU. However, where there is a variance of more than 2 per cent in favour of Telstra Retail (which is termed a 'reporting variance' for the purpose of the SSU), the SSU requires Telstra to promptly investigate the cause of the non-compliant result and provide an explanation of the reasons for the reporting variance.

Metric 5 variance

Metric 5 measures the percentage of BTS faults that are rectified within particular timeframes. In calculating the variance for this Metric, Telstra compares how often it rectifies Telstra Retail faults within the set timeframes with how often it rectifies wholesale faults within the set timeframes. Telstra must report its Metric 5 results for business and residential customers separately.

In its operational equivalence report for the September 2012 quarter, Telstra reported Metric 5 variances in favour of Telstra Retail of 4.9 per cent for business faults and 4 per cent for residential faults. For the December 2012 quarter, Telstra reported Metric 5 variances in favour of Telstra Retail of 3 per cent for business faults and 3.3 per cent for residential faults.

As the variances for Metric 5 were in favour of Telstra Retail in this instance, this raised the possibility of Telstra having breached the SSU. For example, the reporting variances might constitute evidence:

- of Telstra failing to ensure equivalence in relation to the supply of regulated services to wholesale customers and Telstra's Retail Business Units in respect of the technical and operational quality of BTS and/or the operational systems, procedures and processes used in the supply of the BTS contrary to clause 9(a) of the SSU
- that Telstra has not maintained systems and processes for issuing tickets of work to field staff so that tickets of work in relation to BTS supplied to wholesale customers and the comparable retail service supplied to retail customers are issued and processed within Telstra's systems using equivalent order management and managed and performed by Telstra field staff in an equivalent manner in contravention of clause 11.1 of the SSU
- of Telstra not having used equivalent order management to process BTS service activation orders received from a Retail Business Unit and wholesale customers so that the service activation and provisioning of BTS could occur in an equivalent manner. This would be contrary to clause 11.2 of the SSU.

Variances are also relevant in other ways. For example, Schedule 3 of the SSU provides that when determining whether an equivalence issue is trivial (for the purpose of determining whether a breach of the SSU has occurred), the extent to which the matter involves or is reflected in a reporting variance may be taken into account.

In the March 2013 quarter, Telstra implemented a 'jeopardy management' process whereby it monitors its performance against Metric 5 and manually intervenes to ensure that the variance is within the limits established in the SSU. For the March 2013 and June 2013 quarters, Telstra did not report a variance for Metric 5.

Possible reasons identified by Telstra for the reporting variance

In addition to inclement weather, high demand and the high number of medical priority tickets of work for Retail customers, Telstra reported two additional factors in a confidential rectification proposal submitted in accordance with Schedule 11 of the SSU:

Within Telstra's processes for accepting the reporting of faults, Service Delivery contact centre staff are able to allocate different, and higher than 'standard', severity levels for fault rectification for the BTS based on factors such as whether:

- *the customer is a priority assistance customer;*
- *there is damage to Telstra's plant or equipment which poses a risk to the public; or*
- *the customer is a key/corporate customer.*

Telstra's internal inquiries indicated that, since around October 2010, some Service Delivery contact centre staff had been incorrectly allocating an increased key/corporate level of severity to a number of Telstra Retail Customer BTS faults (primarily business customer faults), rather than the standard severity level.

Prior to 4 February 2011, Telstra's IT systems contained a reference data table which automatically recognised a code for particular wholesale customer BTS faults (the ZZZ Code), which resulted in those wholesale customer faults being allocated an elevated level of priority.

Telstra's investigations have indicated that, during a system update on 4 February 2011, the ZZZ Code was removed.

At this stage, it is unclear whether, and the extent to which either of these issues has affected actual fault rectification times for Retail Customers or wholesale customers or Telstra's Metric 5 results.

The ACCC sought further information from Telstra in relation to these two factors and identified that:

- The practical effect of the ZZZ code in Telstra's systems is to elevate all wholesale customer BTS faults to the same level of priority that is allocated to Telstra Retail business faults. While wholesale customers who had not been migrated to eBill were not affected by the system change, where the wholesale customer had not migrated to eBill, their BTS business faults were automatically allocated a lower priority level than Telstra Retail business BTS faults from 4 February 2011.
- Telstra states that the allocation of a lower priority level to wholesale business BTS faults where the wholesale customer had not migrated to eBill and the manual selection of a severity level by Telstra contact centre staff did not necessarily equate to a different level of fault rectification in terms of ultimate outputs.
- Wholesale customers do not have the same ability as Telstra Retail contact centre staff to manually select the severity level when they log a BTS fault with Telstra.

The Independent Telecommunications Adjudicator's report

After submitting the rectification proposal to the ACCC, Telstra engaged the ITA Adjudicator[8] at the ACCC's request to prepare a report on:

- whether the measures set out in the rectification proposal would effectively address the issues identified by Telstra and the cause or causes of the reporting variances; and
- if the ITA Adjudicator considered they would not be effective, to identify any alternative measures that would be effective in addressing the cause or causes of the reporting variances.

8 Telstra established the Independent Telecommunications Adjudicator as a company limited by guarantee (the ITA) under clause 20 of the SSU. The ITA Adjudicator exercises the functions of the ITA, including the resolution of equivalence disputes involving wholesale customers.

The ITA Adjudicator's report examined the measures set out in the rectification proposal and the effect of medical priority assistance faults on BTS fault rectification, and concluded:

- The most likely explanation of the reporting variances is the effect of dealing with medical priority assistance faults, which has a direct impact and correlation on the residential reporting variance and an indirect flow through impact on the business reporting variance.
- The measures in the rectification proposal would be unlikely to lead to a change in the reporting variances and would not effectively address the cause or causes of the reporting variances.
- Although there will be some benefit (in terms of equivalence) obtained from ensuring that priority codes are used appropriately by Telstra Retail customer service representatives, the effect is unlikely to be significant.
- The reinstatement of the ZZZ Code should be beneficial. However, this impact will be small compared to the effects of medical priority assistance faults.
- No further or alternative measures were able to be identified that would provide an effective means of addressing the cause or causes of the reporting variances.

ACCC review of the impact of medical priority assistance on BTS fault rectification

As noted above, Telstra considers that medical priority assistance tickets of work are the most likely cause of the Metric 5 variance.

To explain, Telstra is obliged to fix faults reported by medical priority assistance customers so as to maximise service continuity for those customers, and to do so within specified timeframes (which are less than would otherwise apply).[9] Consequently, Telstra prioritises faults reported by those customers. In circumstances where there are insufficient resources to fix all faults on time, this results in a greater likelihood that medical priority assistance customer faults are fixed on time, and a reduced likelihood that other faults are fixed on time.

In order to test the effect of prioritising faults reported by medical priority assistance customers on the Metric 5 results, the ACCC obtained data from Telstra relating to its BTS fault rectification performance. The ACCC then removed medical priority assistance tickets of work from Telstra's fault rectification data and recalculated Telstra's performance for Metric 5 having regard only to Telstra's performance in fixing other faults. The ACCC shared this analysis with Telstra and presented its findings at a meeting of the Wholesale Telecommunications Consultative Forum on 26 March 2013.

In the relevant period, there were a material number of medical priority assistance tickets for residential BTS customers, and proportionately more of these tickets concerned Telstra Retail customers than wholesale customers. On the other hand, there were few medical priority assistance tickets for business BTS customers.

When medical priority assistance tickets of work were excluded from the data for the September 2012 and December 2012 quarters, the variance in favour of Telstra Retail for residential faults remained but reduced to a level below the threshold for a reporting variance.

This result suggests that, had there been a similar proportion of residential BTS faults that attracted medical priority assistance status for Telstra Retail and Telstra Wholesale respectively, and these were allocated the same priority, then it is likely the Metric 5 result reported for residential customers would have been within this SSU threshold.

The ACCC found that, when the number and distribution of medical priority assistance tickets of work are taken into account, the Metric 5 results are consistent with Telstra fixing residential BTS faults for retail and wholesale customers to a broadly equivalent standard, and supplying the BTS to residential customers with broadly equivalent operational quality.

9 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*, rule 19.

In contrast, in testing the effect of medical priority assistance tickets of work on business BTS faults, the variance in favour of Telstra Retail for business faults did not change significantly and remained above the threshold for a reporting variance.

Telstra has concerns about the study undertaken by the ACCC and, in particular, has noted that it does not take into account the indirect impact of prioritising medical priority assistance tickets of work.

Telstra's position

Telstra does not consider that a breach of the equivalence commitments in the SSU occurred for a number of reasons set out in its confidential Annual Compliance Report:

- The report of the ITA Adjudicator concluded that the prioritisation of medical priority assistance tickets of work for end-users are the most likely cause of the BTS fault rectification variance between wholesale customers and its Retail Business Units.
  - To the extent that the BTS fault rectification variance has been caused by medical priority assistance tickets of work in accordance with its Priority Assistance Policy, clause 9(b)(x)(B) of the SSU excludes the operation of the overarching equivalence commitment.
  - Telstra treats and rectifies medical priority assistance tickets of work on an equivalent basis regardless of whether they are received from a wholesale end-user customer or a Telstra retail end-user customer.
- The additional matters Telstra reported as factors which may have contributed to the variance are unlikely to have had an impact on fault rectification times for wholesale customer end-users and therefore have not given rise to a breach of the SSU.
- Any failure to comply with a requirement of the SSU in this instance was trivial as there is no evidence to show any material adverse impact on wholesale customers.

Rectification proposal

As required by the SSU, Telstra submitted a rectification proposal setting out the steps it proposed to take to remedy the possible breach. The BTS fault rectification variance has been subject to discussions with wholesale customers and the ACCC is continuing to work with Telstra to assess whether the rectification proposal will be an effective remedy for the breach.

In addition to the conduct outlined in the rectification proposal, as noted above, Telstra has implemented jeopardy management to ensure that any variance in its BTS fault rectification performance for wholesale customers and Telstra Retail is within the limits established in the SSU. Telstra has also undertaken a detailed inquiry in an attempt to identify other possible contributing factors to the BTS fault rectification variance.

Current status

The ACCC is continuing to investigate this matter against clauses 9 and 11 of the SSU and assess the adequacy of Telstra's rectification proposal.

Breaches of the migration plan

The ACCC has not identified any breaches of the migration plan in the period between 1 July 2012 and 30 June 2013.

ACCC action

Throughout the reporting period, the ACCC has continued to focus on stopping conduct of potential concern as it comes to light and ameliorating its impact. As noted above, in July 2012 Telstra agreed to implement an additional monthly reporting framework in relation to Telstra's information security remediation program to assist in this work.

The ACCC has worked with Telstra to improve Telstra's SSU compliance framework, resulting in Telstra undertaking a number of additional internal measures during 2012–13 to ensure greater compliance with its interim equivalence and transparency obligations.

The ACCC has also encouraged Telstra to provide regular updates to wholesale customers on equivalence issues so that they could take steps to minimise any impact on their businesses. In this context, the ACCC established a Wholesale Telecommunications Consultative Forum to facilitate greater engagement between Telstra and industry in relation to potential issues arising under the SSU and migration plan.

During the reporting period, the ACCC conducted a number of studies into Telstra's performance against the equivalence and transparency Metrics and interrogated data provided in compliance reports. The ACCC presented its findings to the Wholesale Telecommunications Consultative Forum.

Following consultation with wholesale customers, the ACCC accepted rectification proposals from Telstra in relation to its failure to introduce ADSL service enhancements contemporaneously to retail and wholesale customers, and its failure to make two ADSL line configurations available to wholesale customers when these configurations were available to Telstra Retail. The ACCC considers that the rectification proposals provide an effective means of remedying these equivalence issues.

The ACCC is assessing the further rectification proposal from Telstra concerning its failure to provide equivalence in handling of basic telephone faults.

In addition, the ACCC is continuing to investigate Telstra's failure to comply with its information security obligations and, in particular, whether it has gained or exploited an unfair commercial advantage over its wholesale customers.

Further information

Telstra's SSU and migration plan:

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

The legislation and legislative instruments underpinning the SSU and migration plan are available at the Department of Communications website: http://www.communications.gov.au/policy_and_legislation/telecommunications_regulatory_reform_separation_framework

Appendix 1
Details of identified breaches in Telstra operational, reporting and 'data warehouse' systems

No.	Telstra's summary of identified breach	Telstra's explanation of the identified cause of the breach	Wholesale customer Protected Information disclosed to Retail Business Unit staff
1	Protected Information in a provisioning system for voice services is likely to have been disclosed to RBU users in certain circumstances where the information was associated with the FNN of a mixed Wholesale/Retail and user or the FNN of an end-user with wholly eBilled Wholesale services.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users. Remediation changes to the system are scheduled to be completed by June 2014.	Prior to and during the reporting period, when a Retail Business Unit user accessed the system, the following types of wholesale customer Protected Information regarding end-users that acquire services from Telstra Retail and a wholesale customer (mixed customer) were visible: • end-user details (full national number, name, details) • wholesale product codes for eBilled services associated with the full national number. Where a Retail Business Unit staff member searched on a full national number relating to an end-user of a wholly eBilled wholesale service, the following Protected Information was available: • end-user details (name, address) • wholesale product codes associated with the full national number.
2	Protected Information contained in a system that manages the Customer Access Network and provides for the allocation of telephone numbers is likely to have been disclosed to RBU users in circumstances where the RBU staff searched for information regarding Retail customers.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users. Remediation changes to the system are scheduled to be implemented by the end of June 2014.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to Retail Business Unit staff: • details of wholesale services supplied to end-users • details of the wholesale rebiller name, address and contact details • full national number, plant and cable details associated with the record • the type of service.

No.	Telstra's summary of identified breach	Telstra's explanation of the identified cause of the breach	Wholesale customer Protected Information disclosed to Retail Business Unit staff
3	Protected Information contained in a PSTN and ISDN [Integrated Services Digital Network] order system is likely to have been disclosed to RBU users in circumstances where the RBU staff searched for information regarding Retail customers.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users. Remediation changes to the system are scheduled to be implemented in October 2013.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to Retail Business Unit staff conducting a search in the system against a service: • where there is a Telstra Retail voice service and a wholesale DSL service, the product code for the wholesale DSL service • where there is a Telstra Retail DSL service and a wholesale voice service, a message that the service is charged to a "rebiller" • where there are wholesale DSL and voice services, a message that the service is charged to a "rebiller".
4	Protected Information contained in a service order engine is likely to have been disclosed to RBU users in circumstances where the RBU staff searched for information regarding a retail customer who also happened to have Wholesale services, or where an RBU user sought to create/update and review a service order, amend issued order details, created a completion advice, update details, create a customer entry or re-target or withdraw a service.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users and fix RBU users of the system were incorrectly assigned to a wholesale level access. Remediation changes to the system are due to be implemented in March 2014. The assignment of incorrect access was attributable to human error and has been removed.	Prior to and during the reporting period, information relating to end-users of mixed Telstra Retail and wholesale customers were available to Retail Business Unit staff entering certain commands on customer identification numbers, such as: • customer details including full national number, customer name and address • wholesale product codes • outstanding orders.

No.	Telstra's summary of identified breach	Telstra's explanation of the identified cause of the breach	Wholesale customer Protected Information disclosed to Retail Business Unit staff
5	Protected Information contained in a system used to check the status of orders by Retail and Wholesale staff is likely to have been disclosed to RBU users as RBU users could search for, and access, wholesale end-user orders in the system.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users, and access controls had not been implemented. RBU access controls are scheduled to be implemented in the fourth quarter of 2013.	Prior to and during the reporting period, wholesale customer Protected Information was accessible to Retail Business Unit staff conducting searches by order date, exchange code, order number or full national number, including: • information regarding the status of a wholesale order • end-user details • wholesale product codes • other service-related information that is necessary for the order to be provisioned by a Telstra field technician.
6	Protected Information in a tool used to track the status of faults or orders and for web reporting is likely to have been disclosed to RBU users in circumstances where the RBU staff searched on a Wholesale FNN or Order Number or searched based on Region	Not all Protected Information in the system had been masked or otherwise segregated from RBU users, and remediation had not been completed. Remediation changes to the system are scheduled to be implemented in October 2013.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to Retail Business Unit staff with general access permissions conducting a search on a wholesale full national number or order number: • end-user name, regions and full national number • plant details and service notes.
7	Protected Information contained in an information repository storing subject-oriented data from customer billing, complaints, faults, provisioning and activation, credit management and marketing was accessible to and was likely to have been disclosed to RBU users.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users and system access had not been revoked, and remediation had not been completed. Access to all RBU users has now been revoked and remediation changes to the system are scheduled to be implemented in October 2013.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to approximately 103 Retail Business Unit staff: • end-user details • eBill product details • for services with eBill arrangements, service and order information associated with the full national number.

No.	Telstra's summary of identified breach	Telstra's explanation of the identified cause of the breach	Wholesale customer Protected Information disclosed to Retail Business Unit staff
8	Protected Information contained in a database used to capture and store field tests and activities is likely to have been disclosed to RBU users in circumstances where the RBU staff searched for information regarding specific FNNs. Around 40 RBU users with access to the system may also have been able to access additional information as they were assigned an elevated permission level.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users, and remediation had not been implemented. In April and May 2013, Telstra remediated the system for most RBU users by preventing general users from viewing tickets of work that identify the existence of a Wholesale service associated with the FNN. In addition, from 15 July 2013, a "popup" message was introduced on screens that appear when level 2 users first log in to (and reappears every few weeks) that reminds those users to be mindful of their SSU obligations when using the system. Other remediation work Telstra for RBU users with level 2 access, including segmenting the data in the system so that RBU users' profiles restrict their ability to see Protected Information in the system, is nearly completed, with final verification testing scheduled for the 1st week of October 2013	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to Retail Business Unit staff with general access permissions conducting a search by full national number: • end-user information in relation to field tests and associated activities conducted on the full national number over time. For approximately 40 Retail Business Unit staff with elevated permission levels: • end-user name and address • detailed information linked to the full national number.
9	Protected Information contained in a system containing architectural diagrams, drawings and pictures of equipment, and information about infrastructure (including infrastructure owned or leased by Wholesale Customers) related to PSTN and ADSL Broadband and TEBA [Telstra Exchange Building Access] services is likely to have been disclosed to a small number of RBU users (around 16) who access the drawings to provide technical solutions for large Retail customers.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users, and direct RBU user access had not yet been revoked at the relevant time. Telstra revoked RBU user access to the system on 30 August 2013. Further, any RBU users who require access to drawings stored in the system will be required to request drawings from Telstra Operations staff who will mask Protected Information before providing the drawings to RBU users.	Prior to and during the reporting period, wholesale customer Protected Information was accessible to Retail Business Unit staff with general access permissions: • exact drawings to provide technical telecommunications and IT service solutions to large retail customers • in some cases, information identifying wholesale customers and Telstra Exchange Building Access service-related drawings.

No.	Telstra's summary of identified breach	Telstra's explanation of the identified cause of the breach	Wholesale customer Protected Information disclosed to Retail Business Unit staff
10	Protected Information contained in a system used to track customer requests and orders for PSTN services, and for sending acknowledgements, billing and completion notices, is likely to have been disclosed to a small number of RBU users (approximately three) who may have inadvertently viewed Protected Information on partially eBilled accounts.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users and RBU access controls to the system had not been completed. RBU access to the system was removed on 11 February 2013 and the system was decommissioned in June 2013.	Prior to and during the reporting period, wholesale customer Protected Information relating to end-users of mixed Telstra Retail and wholesale customers and end-users of wholly eBilled wholesale customers was available to Retail Business Unit staff, including: • end-user name, address and full national number • wholesale product codes for eBilled wholesale customers associated with the full national number.
11	Protected Information which is accessible via read-only portal which displays (but does not store) data that is fetched in real time from other Telstra systems is likely to have been disclosed to RBU users in limited circumstances where the filters attached to that system (which are designed to suppress Protected Information from being viewed by RBU users) have failed to operate properly.	In some limited circumstances, the filters applied to the relevant system have failed to operate properly. Telstra is still investigating the solutions that can be implemented to fix the filters.	Prior to and during the reporting period, in limited circumstances, wholesale customer Protected Information was accessible to Retail Business Unit staff, such as: • end-user name, address and account details • in some cases, the regulated services obtained through a wholesale provider.
12	Protected Information contained in a customer relationship management platform used for consumers is likely to have been disclosed to RBU users in circumstances where the RBU staff conducted searches using as a search term an end-user's name, date of birth or FNN, or where the RBU staff conducted a serviceability check in response to an end-user enquiry to Telstra regarding the availability of a service at an address where an active or inactive ULLS was present.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users and remediation had not been implemented. Remediation changes to the system are scheduled to be implemented in October 2013.	Prior to and during the reporting period, when a Retail Business Unit user entered a customer name, full national number, business name (or Australian Company Number/Australian Business Number), date of birth or customer identification number then the search returned the customer record (including full national number, name and address), which after further enquiries may enable the Retail Business Unit user to identify that the telephone service supplied over the full national number is not a Telstra Retail service.

No.	Telstra's summary of identified breach	Telstra's explanation of the identified cause of the breach	Wholesale customer Protected Information disclosed to Retail Business Unit staff
13	Protected Information contained in a Customer Relationship Management and ordering tool used by Telstra Business and Telstra Enterprise & Government staff is likely to have been disclosed to RBU users in circumstances where the RBU staff searched for information regarding Retail customers, particular end-users or specific FNNs.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users. Remediation changes to the system are scheduled to be implemented in October 2013.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were visible to Retail Business Units conducting a search on an end-user of a wholesale customer by name, full national number or customer identification number: • end-user details (full national number, name, customer identification number, address and other contact details) • Telstra reference number • wholesale product codes (for example, WLR, W-ADSL, LSS, ULL) • dates associated with the service (for example the created date and cancellation date if applicable) • work required and other order details.
14	Protected Information in a web-based tool that supports the management and delivery of customer solutions where there is an infrastructure shortfall (held orders) is likely to have been disclosed to RBU users in circumstances where the RBU staff searched for details on a ticket of work via service FNN, customer name, region, ticket of work ID and other criteria.	Not all Protected Information in the system had been masked or otherwise segregated from RBU users and access controls were not fully in place. Telstra took steps to reduce the number of RBU users with access and, after a further systems remediation, the final 19 RBU users had their access revoked between 19 April and 3 September 2013.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to Retail Business Unit staff with general access permissions where searching on a ticket of work, full national number, customer name, region, and other criteria, such as: • end-user name, address and full national number • product codes • product type supplied to the wholesale customer.

Appendix 2
Details of breaches in Telstra data operational systems identified by the ACCC and disputed by Telstra

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
1	Telstra web application used to create and notify third party contractor requests for some fixed line products (i.e. wideband products). The system is used by both wholesale and retail staff. At the time of the MCR, we had identified that some Wholesale Customer information was accessible to RBU staff in the system. In particular, it was understood that for a mixed customer, RBU staff may be able to view PCMS codes [product codes] relating to Wholesale services, and service orders for Wholesale wideband products.	Of the five types of reports available in the system: • two only allowed users to view orders in their own team (so a RBU user could only view RBU reports); • two were not generally known to RBU users and Telstra has no evidence that they were accessed by RBU users, and • one did not contain any Protected Information. There was only a theoretical and remote possibility that RBU users could access any Protected Information in the system by knowing the Wholesale Customer Request ID or entering that number by mistake or at random. Telstra has no evidence of this occurring and there is a lack of any evidence of actual use or disclosure of any Protected Information to any RBU users with access to the system during the Reporting Period. System changes were also implemented in April and September 2013 to remove or mask Protected Information from RBU users.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were visible to approximately 150 Retail Business Unit staff in limited circumstances searching by wholesale customer request identification number: • product codes relating to wholesale services • service orders for wholesale wideband products, which in combination with a full national number or end-user details would be Protected Information.

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
2	Workforce management system used to predict, plan, schedule, dispatch and report on work demands and the resources used to undertake them. The system contains Wholesale Customer information such as name, FNN, address details as well as the types of services that the customer acquires. At the time the system was reported in the MCR, it was believed there were approximately 1600 users, of which two had RBU functions. Neither of the two users with RBU functions were frequent users of the system and both are unable to say why they used the system or even what the system is for.	Further investigations indicated that there were only four RBU users of the system. Of those, two RBU users work for or with employees who are engaged to work for a Network Services Business Unit in relation to payphones and payphone carriage services and have 'a need to know' for the purposes of performing his or her duties effectively and are therefore exempt under clause 10.4(c)(i) of the SSU. The other two RBU users with access to the system both confirmed that they had no knowledge of the system and no recollection of using the system since the introduction of the SSU. Telstra notes that access to the system to those two RBU users was revoked on 23 August and 21 December 2012.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to a small number of Retail Business Unit staff: • end-user name, full national number, and address details • the types of services that the end-user acquires From the above, a Retail Business Unit user may have been able to ascertain the identity of a wholesale customer.

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
3	System used by Telstra Wholesale for registering work requests from customers and access is provided via manual approval. At the time the system was reported in the MCR, it was understood that several RBU employees had access and one had actually logged in post SSU commencement. The system was reported on the basis that access and logging into the system may have provided an opportunity for Wholesale Customer information to have been disclosed to RBU employees.	Only three RBU users had access to the system since the introduction of the SSU, as a result of access not being removed when each employee transitioned to a role in a RBU. None of those three RBU users accessed the system since the introduction of the SSU or since commencing their RBU roles. There is no evidence of actual use of or disclosure to the RBU users who had access to the system during the Reporting Period.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to a small number of Retail Business Unit staff: • full national number • billing information.

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
4	Application available via a web-based portal on the Telstra intranet that allows any user with general account access to submit a fault, service request or password reset, or initiate automated software deployment via an online mechanism. The system has an interface into an Incident Management console for the purposes of raising fault, service request and password reset incidents for the relevant line of business application. Users with general account access can view their own tickets via the system by entering the relevant ticket number, or by searching by employee number. The system allows the user to view a truncated version of incident tickets only. The system was reported as there was a theoretical possibility that an RBU user could enter the employee number of a Wholesale employee into the system and view the details of a Wholesale Customer's incident tickets	The vast majority of information in the IT system relates to internal Telstra system faults, such as requests to reset passwords, logging faults with internal systems or asking for system access to be granted (e.g. access to the internet). Only a small proportion of information relates to external systems and network issues for wholesale customers, only some of which relate to Regulated Services. Until May 2013, it was theoretically possible for a RBU user to have conducted a search of an employee number of a Wholesale Business Unit (WBU) staff member and reviewing the records raised by the WBU staff member which theoretically could display Wholesale Customer information, such as a FNN together with a Wholesale Customer name. However, Telstra has no evidence of this occurring and there is a lack of any evidence of actual use or disclosure to any RBU users with access to the system during the Reporting Period of any Protected Information.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to Retail Business Unit staff with general account access conducting a search on the employee number of a Wholesale Business Unit staff member or by randomly entering a ticket number that relates to a wholesale customer: • full national number • wholesale customer name.

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
5	A read only depository of information used for reporting and data analysis by approximately 219 users in different Telstra business units. The system contains several layers of data. At the time the system was reported in the MCR, it was understood that despite there being restrictions on access for RBU users, some limited Wholesale Customer information was accessible by RBU users through the system. The system was reported on the basis that access and logging into the system may have provided an opportunity for Wholesale Customer information to have been disclosed to RBU employees.	No RBU users accessed the system during the Reporting Period. Telstra therefore has no evidence that RBU users have been using the system to access or use Protected Information. Further, to access wholesale customer Protected Information in the system, a RBU user would have had to conduct targeted searches for specific terms relating to wholesale customer information and combine searches to obtain Protected Information. Telstra notes that the system was partially remediated on 23 January 2013 and is implementing further user access profiling within the system.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to a small number of Retail Business Unit staff: • end-user details • product and service information (such as product codes) and account and billing information • wholesale customer details.

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
6	System for the storage, assignment and management of structured FNNs for leased line special services. These are not normal PSTN FNNs that are issued by the ACMA [Australian Communications and Media Authority] under the Numbering Code; they are FNNs which are part of a numbering system developed internally by Telstra for the purpose of managing special services/data services in other systems. The system is used to assign FNNs for wholesale transmission services but not ULL. At the time the system was reported in the MCR [Monthly Compliance Report], it was understood that in may contain Wholesale Customer information and be visible to RBU users, in the form of details of customer name and address.	Only seven RBU users used the system during the Reporting Period. The only functions that the seven users typically use the system for is to order bulk FNNs which require the RBU user to access a particular screen. That screen does not contain any Protected Information. Further, the other screens in the system contain very limited wholesale customer information that may not relate to a Regulated Service. On the basis that there is very limited Protected Information in the system and it was only visible on the one screen, which was not the screen typically used by the very limited number of RBU users who accessed the system during FY13, Telstra does not consider there is evidence of, and has not identified, any disclosure of Protected Information in breach of clause 10.4 of the SSU. The system has also been partially remediated and the system is expected to be fully remediated by March 2014.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to a small number of Retail Business Unit staff: • customer name, full national number • exchange address details • Points of Interconnect in relation to wholesale Domestic Transmission Capacity services.

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
7	System used to manage Wideband Feasibilities. Feasibilities are conducted by Telstra staff to support or sell products to customers. The system stores Wholesale Customer information including end-user and service details such as Wholesale Customer end-user name, CIDN, product/service requests, bandwidth requests and customer site details. Each feasibility request is given a unique ID which is sequential and can then be used to search the system for that request. The system is accessible via the Telstra intranet by staff with general user access. At the time of reporting in the MCR, the system was reported on the basis that the general user access to the system provided a potential opportunity for RBU users to access Wholesale Customer information, such as the Wholesale Customer end-user name, site details product/service requests and build/upgrade costings.	A RBU user could only have visibility of wholesale customer Protected Information contained in the system by entering the unique ID pertaining to a particular wholesale customer request or report, or incorrectly entering a unique ID and by mistake viewing a wholesale report containing Protected Information. On the basis that the likelihood of RBU users accessing Protected Information in the system was theoretical and remote, Telstra does not consider there is evidence of, and has not identified, any disclosure of Protected Information in breach of clause 10.4 of the SSU, or a breach of any other provision of clause 10.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to a Retail Business Unit staff with general account access conducting a search for a particular feasibility study by entering a unique identification number: • end-user name and customer identification number • product/service requests, bandwidth requests, customer site details, build/upgrade costings and feasibility studies.

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
8	System used to identify bottlenecks preventing retail and Wholesale orders from progressing. At the time the system was reported in the MCR, it was understood that staff with general account access could access orders which may show an FNN or Service Provider, and that Retail Business Unit (RBU) users accessed the system. The system was reported on the basis that access and logging into the system by RBU users may have provided an opportunity for Wholesale Customer information to have been disclosed to RBU users.	At the time of preparing its confidential Annual Compliance Report (ACR), Telstra had not identified any disclosure of Protected Information in breach of clause 10.4 of the SSU, or a breach of any other provision of clause 10, arising from RBU users accessing any Protected Information in the system during FY13. Telstra notes that since preparing the ACR, it identified two RBU users who accessed information in the system from on or about 26 June 2013. The information they accessed was information about wholesale services that were being provided over FNNs of customers who had requested a Telstra retail PSTN service and whose retail orders had been placed in held order status. However, the information in the report accessed by the two RBU users did not identify the wholesale customer and the FNNs in the report were only the FNNs of the customers who had contacted Telstra to request a Telstra retail PSTN service. This system is expected to be remediated in early 2014.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to a small number of Retail Business Unit staff: • full national number • service details • data regarding wholesale services set up under a Telstra Retail customer identification number • during part of the reporting period, enterprise unit codes relating to wholesale customers.
9	PC based application used to activate service features on customers' telephone services by executing commands to activate and deactivate certain services on a line. The system connects to an exchange via the security wall and then interacts with the exchange switches. At the time of reporting in the MCR, it was understood that three RBU employees had access to the CAM system which may have enabled them to access records relating to Wholesale Customer with eBilled services.	The only information in the system which could identify the wholesale customer end-user records as being in relation to an end-user of a wholesale customer (and as acquiring services from a wholesale customer) was the wholesale pre-select override code, which is information which may identify other carriers but for the purposes of respecting the pre-selection or pre-selection override preferences of the end-user, and is not information obtained by Telstra from a wholesale customer for the purpose of, or in the course of, supplying a Regulated Service. This information is only available when a user searches for and retrieves a single customer record by FNN or by order number. There is only a theoretical risk that some RBU users may have visibility of the wholesale customer end-user records by mistake or if they entered the wrong order number or FNN. For these reasons, Telstra does not consider there is evidence of, and has not identified, any disclosure of Protected Information in breach of clause 10.4 of the SSU, or a breach of any other provision of clause 10.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to a small number of Retail Business Unit staff conducting searches by full national number or order number: • end-user name, address, full national number and order number • pre-selection override codes • in some cases, wholesale customer end-user records.

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
10	System that holds information such as Wholesale Customer end-user names and addresses which flow through from a wholesale customer ordering system. At the time of reporting in the MCR, Telstra identified that the system held end customer information, including end-user names and addresses of Wholesale Customers, which flow through from the wholesale ordering system and that some RBU users have access to this system.	The system does not disclose (or enable the RBU user to ascertain from the information in the system on its own) that the end-user is a customer of a wholesale customer, nor does it disclose (or enable the RBU user to ascertain from the information in the system on its own) the identity of the wholesale customer, so a RBU user of the system would be unaware that the end-user details displayed in the system relate to an end-user that has any relationship with a wholesale customer. These details on their own are neither confidential nor commercially sensitive because they do not disclose on their own any wholesale relationship details or enable the identification of a wholesale customer or the identity of the end-user as a customer of a wholesale customer.	Prior to and during the reporting period, the following types of Protected Information concerning end-users of eBilled wholesale customers, and end-users with services with Telstra Retail and a wholesale customer, were accessible to approximately 5,900 Retail Business Unit staff: • end-user name, address, date of birth, Australian Company Number, authorised contact details and customer identification number

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
11	Front of house (FOH) customer relationship management (CRM) system used to support existing Telstra Retail customers who have a BigPond product or service. It allows users to conduct a customer search using an exact CIDN or FNN and retrieves results of this search from a customer database. Searches can be conducted using either an end-user FNN, or a retail CIDN (including retail CIDNs with a Wholesale eBill arrangement), site address or customer name and may display end-user information including CIDN, name, address and date of birth (DOB). The system does not display any service information, the service provider name or the Wholesale product codes or any other information that connects the end-user's details to a Wholesale Customer or otherwise identifies the end-user as a customer of a Wholesale Customer. Further, it is not possible to conduct large scale searches to allow Telstra to identify FNNs which have a Wholesale service on the line; a user can only search one record at a time.	Telstra does not accept that the information visible to RBU users of the system is Protected Information as that information by itself does not disclose or enable the RBU user to ascertain: • that the end-user is a customer of a wholesale customer • the identity of a wholesale customer, or • any Regulated Services acquired by the end-user.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to approximately 5,100 Retail Business Unit staff searching by full national number or customer identification number, site address or customer name: • full national number, customer identification number • end-user name, address, date of birth.

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
12	System that acts as a network/integration layer. It copies or synchronises data from a set of source systems to support functionality of other applications. It does not act as the place of origin or store of any data and it has no user interface. This system runs in the background of a limited group of user interfaces and the system server executes scripts and daemons that assist these user interfaces. At the time of reporting in the MCR, it was understood that Wholesale Customer information was available in the system and it was reported on the basis that a small number of RBU users (six) had access and which provided the opportunity for conduct that may result in a breach.	The system does not store Protected Information as it is not a source or origin of data, a storage system or a user interface system. Rather, it is an intermediate system that copies or synchronises data from a limited set of source systems to support functions of certain front end systems. Telstra also confirmed that no RBU users directly accessed the system during the Reporting Period.	Prior to and during the reporting period, Protected Information sourced from other systems concerning wholesale customers was accessible to a small number of Retail Business Unit staff.

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
13	System that allows users to provision, track and recover interim phones which have been provided to Retail customers and Wholesale end-users (please note that interim services are provided to wholesale customer end-users in the case of Medical Priority Assistance end-users only). It contains information about these end-users only, including FNN, name and address. At the time the system was reported in the MCR, it was understood that RBU users who performed certain searches and investigations to find Wholesale Customer end-users, they could access information about these end-users.	Except for six records contained in the system, the end-user details visible did not disclose or allow a RBU user to ascertain that the end-user was a customer of a wholesale customer. For this reason, the majority of the records in the system do not contain Protected Information. Further, there were only two RBU users of the system during the Reporting Period and Telstra has no evidence that they used or had disclosed to them the wholesale customer information contained in the six records disclosed to them during the Reporting Period.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to two Retail Business Unit staff conducting searches in the system: • full national number • end-user name and address • in some cases, records of customer interactions • in a small number of cases, the relationship with a wholesale customer.

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
14	Order capture tool which is available to managed Telstra Business customers. When users of the system generate an order via the ordering tool, other information about the customer is automatically populated (for example, populating the customer's ABN and account number will then cause the customer's address to automatically populate). The system will automatically populate data for customers who are wholesale end-users of e-bill services. This system only populates customer address and other contact details. It does not populate any service details or indicate whether the customer is an end-user of a Wholesale Customer.	Telstra considers that the matter was reported in error. This system is used by RBU staff to generate orders for retail services when contacted by an end-user seeking to place an order for a particular pricing plan. When contacted by an end-user, the RBU user will generate an order for that end-user. At the time the system was reported in Telstra's confidential monthly compliance report, Telstra thought that in some circumstances, where the end-user is an end-user of a wholesale customer with e-Bill services, it was possible that the details were populated using information provided by that wholesale customer. Telstra considers that the system does not breach clause 10 of the SSU because: • neither the form itself, nor the information returned by the system to complete the form, discloses (or at any time has disclosed or enabled the RBU user to ascertain) that the end-user is a customer of a wholesale customer, nor does it disclose (or at any time has disclosed or enabled the RBU user to ascertain) the identity of the wholesale customer, so a RBU user of the system would be unaware that the end-user has any relationship with a wholesale customer • neither the form, nor the information returned by the system to complete the form, discloses any service details for the end-user or any wholesale service information • the only information populated in the form is the end-user's name and ABN number which on their own is neither confidential nor commercially sensitive because they do not disclose any wholesale relationship details, or enable the identity of a wholesale customer or the identity of customer of a wholesale customer to be ascertained, and is therefore not Protected Information within the meaning of the SSU; • the RBU user will only be accessing the system following a request by an end-user for Telstra to provide a retail service, and • the standard ordering practice requires the RBU user taking the order to confirm the end-user details, meaning the RBU user does not save any time in taking the order as a result of the pre-population of the end-user's contact details. Telstra also notes that clauses 7.21 and 7.22 of the Standard Terms of the generic Customer Relationship Agreement permit Telstra to use end-user details received from a wholesale customer where Telstra is supplying a telecommunications service to the end-user. Following changes which took effect on or around 31 October 2012, the form will not pre-populate with the end-user's account number where the end-user has never had a retail relationship with Telstra.	Prior to, and during the reporting period, the following types of wholesale customer Protected Information were accessible to Retail Business Unit staff and pre-populated into fields in the ordering tool after they enter an end-user's Australian Business Number or account number: • end-user name, address • if the search was against an Australian Business Number, the end-user account number.

No.	Summary of the identified issue reported by Telstra	Telstra's reasons as to why it considers a breach of clause 10 has not occurred	ACCC findings as to the types of wholesale customer Protected Information disclosed to Retail Business Unit staff
15	Order capture tool which is available to managed Telstra Business customers. When users of the ordering tool generate an order, other information about the customer is automatically populated (for example, populating the customer's ABN and account number will then cause the customer's address to automatically populate). This includes end-user data for customers who are wholesale end-users of e-bill services and are not Telstra retail customers. This system only populates customer address and other contact details. It does not populate any service details or indicate whether the customer is an end-user of a Wholesale Customer.	When contacted by an end-user, the RBU user will generate an order for that end-user. At the time the system was reported in Telstra's confidential monthly compliance report, it was thought that in some circumstances, where the end-user is an end-user of a wholesale customer with e-Bill services, it was possible that the details were populated using information provided by that wholesale customer. Telstra considers that the system does not breach clause 10 of the SSU because: • neither the form itself, nor the information returned by the system to complete the form, discloses (or at any time has disclosed or enabled the RBU user to ascertain) that the end-user is a customer of a wholesale customer, nor does it disclose (or at any time has disclosed or enabled the RBU user to ascertain) the identity of the wholesale customer, so a RBU user of the system would be unaware that the end-user has any relationship with a wholesale customer • neither the form, nor the information returned by the system to complete the form, discloses any service details for the end-user or any wholesale service information • the only information populated in the form is the end-user's name and ABN number which on their own is neither confidential nor commercially sensitive because they do not disclose any wholesale relationship details, or enable the identity of a wholesale customer or the identity of customer of a wholesale customer to be ascertained, and is therefore not Protected Information within the meaning of the SSU • the RBU user will only be accessing the system following a request by an end-user for Telstra to provide a service, and • the standard ordering practice requires the RBU user taking the order to confirm the end-user details, meaning the RBU user does not save any time in taking the order as a result of the pre-population of the end-user's contact details. Telstra also notes that clauses 7.21 and 7.22 of the Standard Terms of the generic Customer Relationship Agreement permit Telstra to use end-user details received from a wholesale customer where Telstra is supplying a telecommunications service to the end-user. Following changes which took effect on or around 31 October 2012, the form will not pre-populate with the end-user's account number where the end-user has never had a retail relationship with Telstra.	Prior to and during the reporting period, the following types of wholesale customer Protected Information were accessible to Retail Business Unit staff and pre-populated into fields in the ordering tool after they enter an end-user's Australian Business Number, Australian Company Number or account number: • end-user name, address and account number.

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