ACCC Report

TELSTRA'S STRUCTURAL SEPARATION UNDERTAKING

Annual Compliance Report 2011–12

Report to the Minister for Broadband, Communications and the Digital Economy

Telstra's Structural Separation Undertaking

Annual Compliance Report

2011–12

Report to the Minister for Broadband, Communications and the Digital Economy

ISBN 978 1 921973 58 1

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

ACCC 04/13_699

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

15 April 2013

Senator Stephen Conroy
Minister of Broadband, Communications and the Digital Economy
Parliament House
CANBERRA ACT 2600

stephen

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 2011–12 financial year. As you are aware, subsection 577A(2) 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

RSims

Rod Sims
Chairman

Contents

Executive summary

Each financial year, the Australian Competition and Consumer Commission (ACCC) is required to report to the Minister on any breaches of Telstra's structural separation undertaking (SSU). This inaugural report outlines breaches of the SSU for the period from its acceptance in March 2012 until 30 June 2012.

The SSU creates obligations for Telstra to self-report on compliance issues on a monthly basis. Telstra brought all the matters in this report to the ACCC's attention pursuant to its monthly reporting obligations under the SSU. Each breach outlined in this report was of an interim equivalence and transparency measure—measures intended to safeguard competition while structural reform is implemented.

More particularly, almost all of the reported breaches concern Telstra's obligations to safeguard Protected Information—confidential or commercially sensitive wholesale customer information provided to Telstra in its capacity as access provider of regulated services—from disclosure to the Telstra businesses that compete against wholesale customers in retail markets.

These breaches arose as Telstra operates shared information systems that support both its retail and network functions, and access controls to those systems—or reports extracted from those systems—were not adequate to prevent disclosure of Protected Information to a Retail Business Unit.

A further reported breach concerns Telstra's obligation to establish order management systems and other measures in order for Telstra to meet specified standards for completing unconditioned local loop (ULL) service activations for wholesale customers. This breach arose from an incorrect configuration of Telstra's workforce management system that resulted in a large number of ULL services being activated outside the required standard.

In responding to the reported breaches, the ACCC's focus to date has been on stopping the conduct and ameliorating its impact. This has included ensuring wholesale customers were alerted to issues so that they could take steps open to them to minimise any impact on their businesses.

The ACCC is further investigating Telstra's failure to comply with its information security obligations and, in particular, the extent to which Telstra has gained or exploited an unfair commercial advantage over its wholesale customers. A decision as to further steps, including any consequential action it considers appropriate, will be made by the ACCC following the conclusion of this investigation.

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 considering whether the conduct has ceased and any harm has been corrected, and whether the conduct involved a blatant and deliberate breach of the law.

The identification of these issues under the compliance reporting mechanisms in the SSU—some of which, while longstanding, previously went undetected—and the work undertaken by Telstra to date, demonstrate that the ACCC is now much better placed to respond to equivalence concerns. Furthermore, it is clear that Telstra is taking its commitments seriously, as evidenced through its internal compliance monitoring, self reporting, and the action it is taking to review its systems, processes and procedures, and make necessary changes, to ensure that they meet the standard of equivalence required by the SSU.

Introduction

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

This is the ACCC's first report on Telstra's compliance with its SSU and migration plan which were accepted by the ACCC on 27 February 2012 and commenced on 6 and 7 March 2012 respectively. This report relates to the financial year 2011–12 and covers the period from 6 March 2012, when the SSU came into force, to 30 June 2012.

The ACCC has prepared this report based on whether in its view, on the balance of probabilities, a breach of the SSU occurred 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 Telstra has expressed to the ACCC. Telstra's views are expressly noted in the body of this report.

The ACCC is further investigating the matters discussed in this report. At the conclusion of that investigation, 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.

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 National Broadband Network (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.[1] Upon the coming into force of the SSU on 6 March 2012, the operational separation regime ceased to operate.

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.[2]

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[3] 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.[4] The migration plan sets out how Telstra will progressively transfer its fixed-line customers onto the NBN.

The ACCC's experience to date in administering the SSU is that it is delivering significantly better outcomes than were realised under the previous operational separation arrangements.

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

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

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

4 Pursuant to section 577BE of the *Telecommunications Act 1997*, when a final migration plan comes into force, the SSU has effect as if the provisions of the plan were provisions of the SSU.

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 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 excellence**—establishing and maintaining ticketing, order management and billing systems that comply with standards in the SSU.
- **Telstra Exchange and Building Access**—commitments around non-discriminatory access to Telstra's exchange and related facilities.
- **Wholesale customer facing systems**—minimum levels of functionality and availability.
- **Information equivalence**—Telstra to 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 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 (further described below), including in relation to the equivalence and transparency metrics and possible breaches of the overarching equivalence commitment.

Compliance reporting

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

- A confidential monthly compliance report on any 'equivalence issues' that have been identified by Telstra or reported to Telstra by the ACCC or wholesale customers.[5]
- 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.

5 An 'equivalence issue' means a possible breach of Telstra's overarching commitment to equivalence or of a specific non-price equivalence and transparency commitment.

The ACCC has considered Telstra's compliance reports relating to the period from 6 March to 30 June 2012. In addition, the ACCC has considered issues identified by Telstra in later compliance reports that relate to issues that arose during the 2011-12 financial year.

In its confidential annual compliance report for 2012, Telstra identified four instances where it breached its obligation to safeguard Protected Information pursuant to clause 10.4 of the SSU. These instances are outlined below as breaches of the SSU.

In subsequent monthly compliance reports, Telstra identified a further equivalence issue in relation to Telstra's obligation to safeguard Protected Information. The issue concerns a limited number of Telstra Retail staff having access, including during the 2011-12 financial year, to several 'data warehouse' systems. These systems are used for business reporting and contain detailed wholesale and retail customer data. Based on further information provided by Telstra, the ACCC considers that this also amounts to a breach of Telstra's information security obligations in clause 10.4 of the SSU.

In its 2011-12 confidential annual compliance report, Telstra reported an equivalence issue that arose because a product manager in the Telstra Innovation Products and Marketing Business Unit with responsibility for retail pricing decisions had access to Protected Information in a Telstra billing system. Although Telstra does not agree, the ACCC considers that the reported conduct resulted in a breach of clause 10.5 of the SSU.

In addition to those breaches concerning Telstra's information security obligations, in its 2011-12 confidential annual compliance report Telstra reported an equivalence issue stemming from an error with its workforce management system. However, Telstra expressed the view that any potential failure to comply with the service quality and operational equivalence obligations in clause 11.4 of the SSU was trivial and so did not breach the SSU. The ACCC does not consider the matter to be trivial because the incorrect configuration of Telstra's workforce management system resulted in Telstra failing to activate several thousand ULL services within the standard required by the SSU.

Breaches of the SSU

Information security breaches identified by Telstra

The information security obligations in the SSU are designed to safeguard Protected Information obtained by Telstra in the course of supplying regulated services, which—by virtue of its vertical integration—Telstra could potentially use to its advantage in downstream markets.

These obligations include:

- a strict prohibition on disclosure of Protected Information to Telstra 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 name, address, date of birth and service type together in an order or a fault report, and
- 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:

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

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

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

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

Clause 10.4 also provides that Telstra Network Services must not disclose Protected Information relating to a wholesale customer to Telstra Retail unless authorised to do so by that wholesale customer.

Clause 8.1(g) also provides that an employee (not working for a Retail Business Unit) that performs functions set out in 8.1(f) of the SSU, including network planning, wholesale pricing, processing and implementing churn requests or local number portability is subject to the provisions of clause 10. Therefore, an employee will not be able to use or disclose Protected Information except on a need-to-know basis or where authorised to do so by that wholesale customer.

Clause 10.5 of the SSU provides for further restrictions on the use of information.

Clause 10.5(a) provides that Telstra will not disclose to a Retail Business Unit:

- information that is derived from certain types of Protected Information
- but is not Protected Information because it has been aggregated (other than on a national basis) and the identity of wholesale customers or their customers cannot be ascertained

unless, with the approval of the ACCC, it makes the information available to wholesale customers at the same time.

Clause 10.5(c) provides that if an employee who works for a Business Unit which is not a Separated Business unit has responsibility for decisions about pricing of retail services, Telstra will ensure that Protected Information is not disclosed to that employee (subject to the exceptions in clause 10.5(d)).

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.

As outlined above, the SSU prohibits Telstra from 'disclosing' Protected Information to Retail Business Units (among others) in particular circumstances. 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 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. 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 Business Units, the ACCC considers that Telstra has disclosed the Protected Information. The ACCC acknowledges that Telstra does not consider that mere accessibility of Protected Information is in itself a breach of clause 10 of the SSU.

In the period from 6 March to 30 June 2012, Telstra identified four breaches of clause 10.4 of its SSU. These identified breaches all relate to Protected Information being disclosed to staff in a Retail Business Unit (including front of house staff) as a result of access to information systems, or reports extracted from them. These identified breaches are summarised below.

1 and 2. Protected information accessible to Telstra Retail in shared systems

Telstra provided the following details in its confidential annual compliance report in relation to these identified breaches of clause 10.4 of the SSU:

Due diligence around SSU implementation has identified a potential problem with the transparency of information via our IT systems to RBUs. The general issue is the transparency of network codes (required for the processing of services in the Telstra systems and to avoid the creation of incompatibilities between services) which could be used to determine the existence and type of wholesale services being supplied over Telstra's network not otherwise available through industry churn and other processes available to Wholesale Customers.	Some of Telstra's legacy systems contain Wholesale Customer Protected Information which may be available to staff in a RBU [Retail Business Unit] who have access to that system. Not all Wholesale Customer Protected Information has been masked from, or otherwise segregated from, users of the system who are from a RBU. The business has been reliant upon behavioural rules, training and policies to promote compliance.
Employees in Retail and Network Services are 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 has led to employees seeking to withdraw an order. For example, as part of the activation process, employees contact Wholesale Customer end-users to confirm details such as connection address and whether a lead-in has been installed. There have been limited instances of employees cancelling Wholesale Customer orders at the direction of the Wholesale Customer's end-user, believing they are fulfilling the customer's wishes.	Telstra believes this issue has been caused by: a. The visibility of certain Wholesale orders to staff outside the WBU (including RBU staff); and b. In most cases where a RBU staff member is involved, a request from the end-user of the service to be provisioned from the order, seeking its cancellation.

Telstra has stated that the limited number of instances in which wholesale orders were withdrawn was in breach of company policy and against training/instructions to staff.

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.

Telstra's information systems, used by both Telstra Retail and Telstra Operations staff, contain wholesale customer Protected Information. This information is populated into Telstra's information systems after it is supplied by the wholesale customer. Information relating to an order is passed from the wholesale customer ordering system (LOLO) through to an ordering and provisioning system and from there into a variety of other systems. The diagram in **Appendix 1** illustrates how information flows from an initial wholesale order into the ordering and provisioning system and a Telstra billing system.

Telstra's information systems are access controlled, with classes of staff given different access privileges. Telstra uses access controls for business assurance purposes as well as to facilitate compliance with its information security obligations. Notwithstanding the existence of these arrangements, not all wholesale customer Protected Information has been masked or segregated from users with access privileges typically given to Telstra Retail staff. Consequently, in certain cases, this Protected Information was visible to Retail Business Unit staff.

Further, access controls could be overridden in certain circumstances which would allow a broader cross section of information to be visible to Telstra Retail staff members than would otherwise be available under their assigned access privileges.

Accessible Information

Prior to and during the reporting period, the following protected information concerning wholesale orders was visible to Telstra Retail staff:

- end-user details (name, address details)
- in limited circumstances, dates in relation to wholesale orders (application date, appointment date, date the order was completed)
- the wholesale customer's 'financial identifier'—a unique code that Telstra's systems allocate for each wholesale customer.

Protected Information may be disclosed to Retail Business Units if the wholesale customer authorises disclosure or to fulfil requirements under a legislative instrument, industry standard or industry code.

Telstra Retail employees were also able to see the type of wholesale services supplied. This information was visible in a Telstra billing system for eBilled services (comprising wholesale line rental and wholesale DSL services) and visible in an ordering and provisioning system for shared retail/wholesale customers. **Appendix 2** provides an overview of the information visible to Telstra Retail Business Units in the ordering and provisioning system and the Telstra billing system.

In addition to passing through Protected Information, Telstra's information systems also generate product codes (known as PCMS codes) based upon Protected Information. These product codes are required to process service orders in Telstra systems and other business processes. For instance, an order for a DSL service will attract a DSL product code that will affect how the order is fulfilled, including the steps to be taken to avoid the creation of incompatibilities between services.

Prior to and during the reporting period, these product codes were visible to Telstra Retail staff and, as different product codes are assigned to wholesale and retail services, Telstra Retail staff could identify whether an end-user customer was acquiring a wholesale service and if so, the general type of service.

During the reporting period, Telstra Retail employees were also able to cancel pending wholesale orders. This occurred on a small number of occasions (on average, 21 each month). 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. To illustrate, a shared end-user could potentially contact Telstra Retail

to cancel their services, including a pending wholesale order, because the end-user had decided to use mobile instead of fixed-line services, or because their business was closing and services were no longer required.

Telstra has indicated that not all information contained in the relevant ordering and provisioning system or billing system record will disclose wholesale customer Protected Information, as some records could contain information, in particular the end-user's name and date of birth, which was first provided when the end-user was in a retail relationship with Telstra. However, the ACCC notes this would not be the case for end-users who have never previously been Telstra Retail customers.

In addition, the ACCC notes that information supplied by wholesale customers and obtained by Telstra for the purpose of, or in the course of, supplying regulated services to that wholesale customer is current information (rather than historical information) that Telstra would not otherwise have access to, unless the end-user also acquires services from Telstra Retail. For example, the end-user's address, name or types of services may have changed.

Remediation undertaken by Telstra

Telstra has taken a number of remedial steps to minimise the risk of Protected Information being used by Telstra Retail. In particular, Telstra has:

- Revoked access from all Telstra outbound call centres.
- Removed the process whereby employees could override their access privileges.
- Removed the visibility of wholesale customer financial identifiers for wholesale DSL orders.
- Removed guides to interpreting and identifying wholesale customer Protected Information in the relevant ordering and provisioning and billing systems.
- Issued instructions to Telstra Retail employees and industry partners to cease the use of wholesale customer Protected Information and replaced materials on the Telstra staff intranet with warnings to not seek out or use wholesale customer Protected Information.
- Conducted staff training on information security issues.
- Implemented a number of processes to monitor compliance.
- Removed the ability for Telstra Retail staff to withdraw wholesale LSS orders in August 2012.
- Advised that it implemented a system fix in November 2012 to remove the ability of Telstra Retail staff to withdraw any wholesale orders and modify most wholesale orders, with further IT changes planned to restrict the ability to modify wholesale orders.

In the period from Telstra first reporting the issue to the implementation of the systems fix, Telstra took steps to establish a process to identify and reinstate orders that were incorrectly withdrawn, employees that cancelled wholesale orders were provided with further training/coaching to avert reoccurrence, and at the ACCC's request Telstra advised wholesale customers of the steps that they could take to reinstate orders that were incorrectly withdrawn.

As described further below, Telstra is currently undertaking further remediation work to ensure that its IT systems are compliant with the information security commitments in the SSU.

3. Protected information relating to faults accessible to Telstra Retail in a shared system

Telstra provided the following details in its confidential annual compliance report in relation to this identified breach of clause 10.4 of the SSU:

Wholesale Customers can log service faults in relation to Regulated Services via the online portal LinxOnline Service (LOLS) available by TW website. The service fault / assurance dockets are then raised in the fault reporting system. Wholesale Customers can also raise service faults by phone in which case the Telstra Operations team will raise a trouble ticket of work directly in the fault reporting system (bypassing LOLS). In some instances, the information provided contains Wholesale Customer Protected Information.	Not all Wholesale Customer Protected Information has been masked from, or otherwise segregated from, users of the fault reporting system who are from a RBU. The business has been reliant upon behavioural rules, training and policies to promote compliance and Telstra is investigating remediation options.

Telstra has stated that an employee of a Retail Business Unit could access the fault reporting system, for example to check on the status of a fault in the system relating to an end-user of a wholesale customer (in breach of Telstra's policies).

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 response to targeted searches for certain regulated services, the following Protected Information was accessible to some members of a Retail Business Unit:

- end-user details
- a high level product description
- the wholesaler/rebiller name
- the source of the fault notification ticket which, on occasion, identifies the wholesale customer
- fault description
- case history associated with a full national number (FNN).

This information is available for 13 months after a fault is logged in the fault management system.

Remediation undertaken by Telstra

Particular searches in the fault reporting system create prompts or flags advising that the end-user should contact its service provider to report a fault. Telstra is currently implementing system changes by adding 'splash screens' reminding Retail Business Unit employees to only access the system for permitted purposes and not to use any wholesale customer Protected Information. Telstra has also conducted training, reiterating the importance of compliance with its SSU obligations and has updated its information security policies, standards and processes to incorporate the new obligations. In addition, Telstra has commenced longer term remediation to ensure that its fault management system is compliant with the information security obligations in the SSU.

4. Protected information distributed to Telstra Retail employees as part of a cross-company project

Telstra provided the following details in its confidential annual compliance report in relation to this identified breach of clause 10.4 and 10.5 of the SSU:

A Cross-Company Project Team for the South Brisbane Exchange Project included representatives of a Retail Business Unit (RBU). Material distributed to the team included aggregated numbers of wholesale services migrated and to be migrated. Additionally, a daily report from Service Delivery containing details of specific faults and incomplete connections had been, until 2 April 2012, sent to select project members, including those from a RBU. Two Wholesale Customers were specifically mentioned in one message.	Human error: a failure of relevant staff to identify Wholesale Customer Protected Information in materials distributed to members of the project team.

Telstra has also stated that:

The aggregated material distributed to a small number of Retail BU staff did not identify a wholesale customer or end user. It therefore did not contain Protected Information and there was no breach of clause 10.4 of the SSU.

However, the use or disclosure of this type of aggregated information is subject to restrictions in clause 10.5 of the SSU that were not followed. Telstra took steps to remove information regarding the number of wholesale services from the material distributed to the Project Team.

In the small number of instances where a daily report referred to a Wholesale Customer, some of the information may not have related to a Regulated Service, and therefore may not have fallen within the definition of Protected Information. The breach of clause 10.4 was very limited and Telstra ceased circulation of the daily report to project team members.

Remediation undertaken by Telstra

Telstra took steps to remove information regarding the number of wholesale services migrated and to be migrated from the material distributed to the project team, and ceased circulation of the daily report to project team members. Telstra also reminded relevant staff of the SSU obligations.

Further information security breaches identified by the ACCC

5. 'Data warehouse' systems

Telstra identified the following equivalence issues in its September and October 2012 confidential monthly SSU compliance reports in respect of four IT systems or databases that store data:

1. A mainframe data mart that acts as a reporting platform and data staging area for downstream systems. Users of the system run reports from it to extract information, rather than accessing the system via a user interface. We have identified that there is a small number of users in a Retail BU (approximately 13) who may have access to Wholesale Customer information through this system.
2. A database that receives information from Operational Support Systems that support the network, including information about service provisioning, faults, billing and some customer information. We have identified that staff in a Retail BU are able to query the system in a way that allows access to Wholesale Customer information, including where the end-user has services with both wholesale and retail.
3. A data warehouse storing services related data, including activation, assurance, outage and complaint data. There are currently approximately 63 users from a Retail BU with access to this data warehouse. We have identified that these users may be able to conduct searches that reveal some Wholesale Customer information.
4. This system is an information repository storing subject-oriented data from customer billing, complaints, faults, provisioning and activation, credit management and marketing. This data is provided to this system by multiple source systems such as an ordering and provisioning system, CDBOR and a Telstra billing system. This system contains both Retail and Wholesale information. Wholesale Customer information includes eBill product codes under a Retail CIDN, customer information including contact name, address, phone number, service and product details. There are approximately 103 Retail staff and 426 corporate users. Users require specialist knowledge about the data tables in order to conduct searches.

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 'data warehouse' systems, which are used by Telstra to enable business reporting, contain extensive wholesale customer Protected Information. The information which was visible includes customer details, product and service details, billing information, and wholesale customer service orders.

During the 2011-12 financial year, a small number of Telstra Retail employees were able to access visible Protected Information in Telstra's 'data warehouse' systems and conduct searches/queries and run detailed reports that included wholesale customer Protected Information.

The ACCC considers that by making wholesale customer Protected Information stored in these 'data warehouse' systems, or reports extracted from them, accessible to Telstra Retail staff, Telstra breached the information security obligation in clause 10.4 of the SSU.

Remediation undertaken by Telstra

Telstra has taken steps to limit access to the 'data warehouse' systems. In particular, Telstra has refined 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. This will potentially limit the number of Telstra Retail staff with access to these systems. In addition, Telstra is currently investigating longer term remediation options.

6. Telstra product manager accessed protected information

Telstra provided the following details in its confidential annual compliance report in relation to this identified equivalence issue:

A product manager in the Telstra Innovation Products and Marketing Business Unit with responsibility for retail pricing decisions had access to Protected Information in a Telstra billing system.	A failure to identify that an employee had a level of access in Telstra's billing system for eBilled services that was not appropriate for the employee's duties.

ACCC findings

The ACCC considers that by providing access to Protected Information to an employee who works for a Business Unit which is not a Separated Business Unit and who had responsibility for decisions about pricing of retail services, Telstra breached the information security obligation in clause 10.5(c) of the SSU.

Telstra has stated that it does not accept that there has been a breach of clause 10.5(c) of the SSU in respect of the circumstances reported to the ACCC. Telstra's stated reasons for this position include that the pricing manager was responsible for a pricing decision that was initiated and occurred before the introduction of the SSU. Accordingly, Telstra concludes that there can be no inference drawn that the employee did access Protected Information when the SSU was in force.

In addition, Telstra states that the ACCC's findings do not reflect the correct approach to assessing whether information is Protected Information under the SSU. Telstra contends that because the product manager had responsibility for a product that was not a regulated service, the information that could be accessed by the product manager was presumably supplied by wholesale customers for the purpose of, or in the course of, obtaining a wholesale product that is not a regulated service and therefore not Protected Information under the SSU.

The ACCC does not accept that it is necessary for the employee to have made a retail pricing decision during the reporting period to establish a breach of clause 10.5(c) of the SSU. The relevant question is whether the employee had responsibility for retail pricing decisions during the reporting period. The ACCC considers that retail pricing decisions were within the employee's authority during the reporting period. In addition, the employee had access to the Telstra billing system and Protected Information was visible in the Telstra billing system during that time. The ACCC does not accept that actual use of the information accessible in the Telstra billing system is required to establish that disclosure by Telstra has occurred.

Further, the ACCC does not accept that the information accessible by the employee was not Protected Information. Given that wholesale customers would have needed to acquire an underlying PSTN service (a regulated service) before acquiring the non-regulated service in question, the ACCC considers that the relevant information was supplied by wholesale customers and obtained by Telstra for the purpose of, or in the course of, supplying a regulated service to those wholesale customers, thereby bringing it within the meaning of 'Protected Information' set out in clause 10.1(a) of the SSU.

Accordingly, the ACCC considers that Protected Information was accessible to the Telstra employee notwithstanding that the employee's responsibilities related to a non-regulated service.

The ACCC has considered Telstra's views, but is of the view that Telstra breached the information security obligation in clause 10.5(c) of the SSU.

Remediation undertaken by Telstra

Telstra removed the employee's access to wholesale customer Protected Information.

7. Breaches of Clause 10.3

Telstra did not report any matters as identified breaches of clause 10.3 of the SSU in its confidential annual compliance report.

ACCC findings

The ACCC sought further particulars from Telstra in relation to the matter described in items 1 and 2 above. After considering the information provided by Telstra and making its own enquiries into these matters, the ACCC has made the following findings.

In addition to populating its primary operational support system for fixed line service orders with the Protected Information detailed in **Appendix 2** which was visible to, or accessible by, Telstra Retail staff, Telstra configured an ordering and provisioning system to display a prominent 'NON-TEL' indicator notifying Telstra Retail staff that there are non-Telstra services on a particular line. Telstra has stated that the 'NON-TEL' code was introduced onto ordering and provisioning system screens in June 1998.

Similarly, a Telstra sales transaction system (STS), used by some inbound sales and lead teams (including Telstra Retail consultants) for billing and order purposes, was configured by Telstra to display 'conversion opportunity' messages where an end-user acquired one or more non-Telstra services. For example, on the customer record of an end-user to whom services are supplied by a wholesale customer, STS displayed the following message:

'Conversion Opportunity—ebill Service. This customer has services supplied and billed by a Service Provider other than Telstra.

Please refer the customer to their Service Provider for any Account or Billing enquiries.'

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 is 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. Despite Telstra's guidelines, Telstra cannot rule out the possibility of some Retail Business Unit staff disregarding the guidelines and used the 'NON-TEL' indicator and STS 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. Telstra has stated that STS displayed these conversion opportunity messages and the 'Convert to Telstra' option from its initial deployment in 2000.

In June 2012, Telstra reported to the ACCC the discovery of an internal guide titled 'Churn Types – STS Quick Reference' which was published on the Know How section of Telstra's staff intranet site. The stated purpose of the guide was to assist STS users to determine a customer's relationship with Telstra for a particular service, and to explain the 'conversion opportunity' messages in STS. Telstra also reported the publication of a 'Know How' page available on its staff intranet site which explained how to interpret wholesale product codes.

Telstra stated in its May 2012 confidential monthly SSU compliance report that it appears that Telstra Business industry partners have at times accessed systems to inform themselves of the existence/nature of the wholesale services for marketing purposes, for example, during an outbound telemarketing call to a customer.

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, by:

- populating wholesale customer Protected Information into systems used by both Telstra Retail and Telstra Operations staff
- drawing the attention of Telstra Retail staff to that information on each occasion they viewed the relevant record in circumstances where Telstra Retail staff could use the information in a manner likely to enable Telstra Retail to gain or exploit an unfair commercial advantage, including by:
    - prompting the Telstra Retail staff to ask targeted questions about the end-user's existing service(s)
    - enabling Telstra Retail staff to proactively offer competing Telstra products based on the visibility of the end-user's specific product configurations, and
    - in some cases, cancelling wholesale orders.

It is clear from the ACCC's enquiries that Telstra's wholesale customers did not have the same degree of visibility over their competitors' supply of services as was available to Telstra Retail.

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

- the NON-TEL indicator, the messages displayed in STS and the quick reference guides available to Retail Business Unit staff do not prompt Retail Business Unit staff to engage in activities that would provide any unfair commercial advantage to a Retail Business Unit, or be likely to do so
- the type of information that was accessible to Retail Business Unit staff was of a very high level
- the ability to access the Protected Information did not lead or was not likely to lead to wholesale customer orders being cancelled in a manner that would result in a Retail Business Unit gaining an unfair commercial advantage.

Telstra has also stated that it has not uncovered any widespread and systemic use of Protected Information in its shared systems in a manner that has resulted in Retail Business Units gaining any unfair commercial advantage. As noted above, 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 use or disclosure is in a manner which would be likely to enable a Retail Business Unit to gain or exploit an unfair commercial advantage.

Remediation undertaken by Telstra

The 'conversion opportunity' messages and 'Convert to Telstra' option were removed from Telstra's STS within one month of Telstra reporting the issues to the ACCC. In addition, Telstra has removed the relevant Know How pages from its staff intranet site. As described further below, Telstra is currently undertaking significant remediation work to ensure that its IT systems are compliant with the information security commitments in the SSU, and has indicated that this will include the removal of the 'NON-TEL' indicator from the ordering and provisioning system.

As noted above, Telstra removed the ability for Telstra Retail staff to withdraw wholesale LSS orders in August 2012 and has advised that it implemented a systems fix to remove the ability of Telstra Retail staff to withdraw and modify all other types of wholesale orders in November 2012.

Summary of Telstra's information security remediation

Telstra is currently undertaking significant remediation work to ensure that its IT systems are compliant with the information security commitments in the SSU.

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.

The ACCC recognises the need for Telstra to exercise care in modifying these systems as changes may have unforeseen consequences for both wholesale and retail end-users if not properly scoped. In this regard, Telstra has stated that the affected systems are mostly legacy systems that have evolved over long periods of time, and therefore core systems changes are complex and the development and implementation of fundamental solutions may take considerable time.

The ACCC has therefore sought to ensure that Telstra establishes appropriate interim remediation measures. The interim remediation steps taken by Telstra include:

- revoking access to some systems from all Telstra outbound call centres
- removal of the 'conversion opportunity' message and 'convert to Telstra' option in STS
- in particular systems, implementing 'splash screens' or warnings to Telstra Retail staff and contractors to further facilitate the protection of wholesale customer Protected Information
- introducing 'golden rules' reminding all Telstra Retail employees and industry partners of the SSU information security obligations
- conducting additional employee training and issuing further guidelines on the SSU information security obligations.

At the date of this report, Telstra has completed some long term remediation, including:

- the development of new access controls
- removing the visibility of wholesale customer financial identifiers for wholesale DSL orders
- blocking the ability of Telstra Retail and Network Services staff to modify or cancel wholesale customer orders.

Service quality and operational equivalence

Telstra is obliged to establish and maintain ticketing, order management, fault rectification and billing systems that comply with standards prescribed in the SSU.

Clause 11.4 of the SSU provides that Telstra will establish order management systems and other measures in relation to:

a. completing activations of LSS

b. completing ULL individual cutovers, and

c. rectifying faults relating to the LSS and the ULL service,

in order for Telstra to meet the equivalence and transparency metrics applicable to those services.

Clause 11.7(b) of the SSU provides that Telstra will not be in breach of this clause 11 in circumstances where Telstra fails to comply with a requirement of this clause 11 and the failure to do so is trivial.

In its confidential annual compliance report, Telstra identified an equivalence issue in relation to its obligation to establish order management systems and other measures in order for Telstra to meet specified standards for completing ULL individual cutovers for wholesale customers.

Telstra reported this issue in the following terms:

> In November 2011, Telstra began to bring contractors and the allocation of tickets of work on to a workforce management system. Due to an error in the system, appointments for ULL cutovers were being allocated in four hour blocks rather than 15 minute timeslots. After mass service disruptions are accounted for, Telstra met the customer request date on 90.23% of ULL cutovers orders in April 2012 and 90.41% in May 2012.

Telstra has stated that any potential failure to comply with clause 11 of the SSU is trivial for the purposes of clause 11.7(b) of the SSU because this issue was limited to a short period of time, was promptly fixed, was confined to one geographical area and involved conduct which was not deliberate in terms of any potential impact on wholesale customers. Telstra has also stated that this matter is trivial on the basis that the reported metric outcomes did not indicate a Reporting Variance. A Reporting Variance occurs for the relevant metric outcomes when Telstra's performance level for wholesale customers is two per cent or more below the performance threshold.

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 ACCC considers that Telstra breached its service quality and operational equivalence obligation in relation to establishing order management systems for completing ULL individual cutovers.

Due to the error in Telstra's workforce management system, which is used to allocate tickets of work to technicians for completing service activations, appointments for in-use ULL cutovers were being allocated in four-hour blocks when in most cases only a single exchange jumper task was involved requiring a 15 minute time period.

Based on confidential service level performance data provided by Telstra, the ACCC considers that the error in Telstra's workforce management system had a significant negative impact on the number of individual ULL cutovers completed on the customer requested date in the months of April and May 2012. The delayed provisioning of ULL services over a period of two months is likely to have resulted in material detriment to as many as 15 wholesale customers and several thousand end-users. Consequently, the ACCC does not consider that Telstra's failure to comply with the service quality and operational equivalence commitments in clause 11 of the SSU was trivial, even when the fact that the reported metric outcomes did not show a Reporting Variance is taken into account. In this regard, the ACCC notes that under Schedule 3, paragraph 1(c) of the SSU the extent to which a matter involves or is reflected in a Reporting Variance is not determinative of whether the matter is trivial.

Telstra implemented a systems fix in order to allocate 15 minute timeslots for the completion of in-use ULL individual cutovers in mid-May 2012. This resulted in a substantial improvement in Telstra's performance in the month of June 2012, with Telstra completing 99.53% of ULL individual cutovers on the customer requested date. This improved service level in June 2012 provides a strong indication of the significant impact that the system error had in April and May 2012.

Breaches of the migration plan

The ACCC has not identified any breaches of the migration plan in the period between 7 March 2012 and 30 June 2012.

ACCC action

In responding to the reported breaches, the ACCC's focus to date has been on stopping the conduct and ameliorating its impact. This has included ensuring wholesale customers were alerted to issues so that they could take steps open to them to minimise any impact on their businesses.

Shortly after Telstra first reported the information security issues, the ACCC set out a number of principles to which Telstra broadly agreed, consistent with the general approach to remediation in the SSU. In particular, the compliance arrangements should:

- Promote compliance with information security requirements in the SSU and wholesale customer contracts, as well as SSU equivalence and standard access obligations more broadly.
- Generally take the form of 'bright line' compliance measures, rather than be based upon purely behavioural controls—these are measures that are clearly stated and readily allow for an objective assessment of whether the measure is being complied with.
- Be supported by appropriate and well documented internal policies (and where industry partners are concerned, by clear contractual materials) and robust audit arrangements.
- Until such time as 'bright line' arrangements can be implemented, include additional monitoring of potentially high risk systems use and business practices to reduce the potential for misuse of systems access, such as:
    - additional staff training and management reinforcement of the behavioural rules
    - regular monitoring and auditing of behavioural rules including reviewing samples of customer interaction records
    - following up on all ordering and provisioning system enterprise user code changes, and wholesale service or order modifications made by retail staff and industry business partners; and
    - reviewing sales remuneration models to ensure that they do not incentivise retail staff and/or industry business partners to seek out and misuse Protected Information.

The ACCC also imposed an additional monthly reporting framework around Telstra's systems remediation program, requiring Telstra to identify the status of remediation underway and completed. In addition, the ACCC required the withdrawal of problematic access privileges from outbound call centres. Telstra agreed to these measures.

Importantly, the ACCC sought to provide transparency around the information security issues by encouraging Telstra to provide timely updates to wholesale customers, to ensure that wholesale customers were able to take steps to minimise any ongoing competitive detriment. In this regard, as well as keeping wholesale customers informed through ongoing correspondence from Telstra Wholesale, Telstra has provided detailed updates at the ACCC's Wholesale Telecommunications Consultative Forum, which was established by the ACCC to encourage open communications between Telstra, wholesale customers and the ACCC.

In addition to closely overseeing Telstra's ongoing remediation activities, the ACCC is further investigating Telstra's failure to comply with its information security obligations and, in particular, the extent to which Telstra has gained or exploited an unfair commercial advantage over its wholesale customers. A decision as to further steps, including any consequential action it considers appropriate, will be made by the ACCC following the conclusion of this investigation.

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 dispute resolution.

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 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.

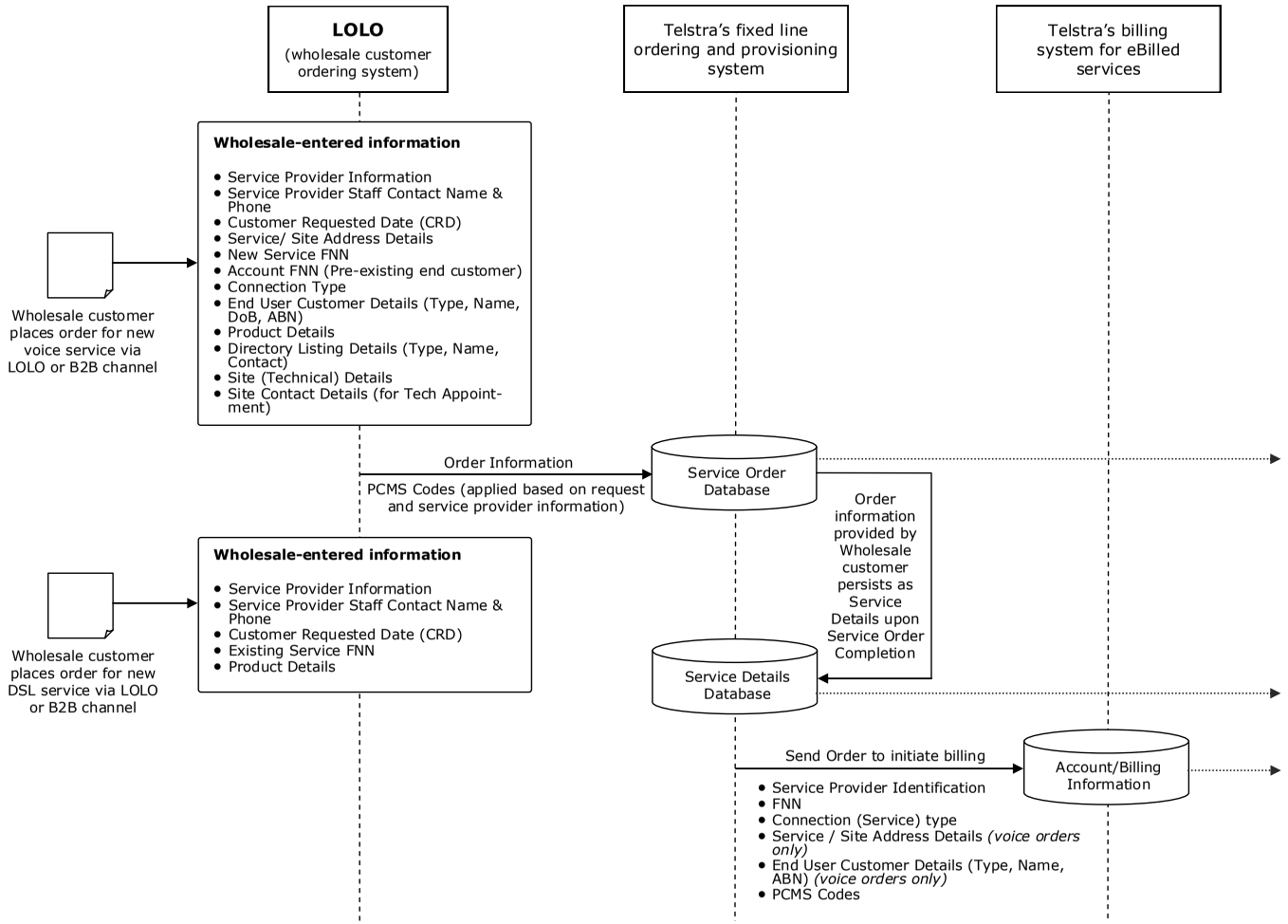
In respect of the matters the subject of this report, the ACCC would be more likely to take court enforcement action if it considers it to be necessary to prevent ongoing or systemic breaches of the SSU or to obtain a remedy to undo any harm. For example, the ACCC may consider court action if Telstra 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 to damage its competitors or otherwise provide itself with a commercial advantage.

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 Broadband, Communications and the Digital Economy** website: http://www.dbcde.gov.au
- Information on the NBN rollout is available at the **NBN Co** website: http://www.nbnco.com.au

Appendix 1

Diagram illustrating the flow of information from an initial wholesale customer orders for voice and DSL services



Appendix 2

Information available to Telstra Retail users accessing Telstra's fixed line ordering and provisioning system and Telstra's billing system for eBilled services between 6 March 2012 and 30 June 2012

	A Retail user of Telstra's fixed line ordering and provisioning system attempts to view an order[1] for a customer with a mixed Telstra (PSTN) & Wholesale DSL/Spectrum Sharing relationship	A Retail user of Telstra's fixed line ordering and provisioning system attempts to view a service record for a customer with a mixed Telstra (PSTN) & Wholesale DSL/Spectrum Sharing relationship	A Retail user of Telstra's fixed line ordering and provisioning system attempts to view a service record for a customer with a mixed Telstra DSL & Wholesale (PSTN) service	A Retail user with general access to Telstra's billing system for eBilled services attempts to view a record for eBilled[2] services by searching on a FNN, address or other search field
FNN	Yes	Yes	Yes	Yes
Wholesale product code	Yes, PCMI	Yes, PCMI	Yes, PCMI	Yes, PCMI and PBI
Service address	Yes	Yes	Yes	Yes
Service name	Yes	Yes	Yes	Yes
Billing address	No	No	No	No
Date of birth	Yes	No	No	No
Lists of services held by a customer	No	No	No	Yes
Service provider financial identifier	Yes	Yes	No	No
Service provider name and number	Yes	Yes	No	No
Enterprise unit code	Yes	Yes	Yes	No
Dates in relation to orders[3] / services	Yes	No	No	Yes
Install remarks	Yes	No	No	No

Notes:

1 An order record remains accessible in Telstra's billing system for eBilled services from the date the order is submitted until 126 days following the order being fulfilled.

2 eBill is a Telstra business-to-business system for billing of fixed line voice and some data services (including Wholesale DSL).

3 Application date, customer request date, Telstra commitment date, appointment date, completion date.

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
61–63 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