New Zealand Telecommunications Forum

Operations and Support Manual for Local and Mobile Number Portability in New Zealand

Version Number and Status:	**ENDORSED**
Version Date:	11 February 2015

This document forms part of the regulation for Number Portability and is enforceable through the IPMS Access Agreement.

Table Of Contents

Quick Start Guide

The Number Portability User Group (NPUG) has identified the following items of particular importance that cause confusion or can create delays in the porting process if they are not well known and understood. Though IPMS users should be aware of all aspects of Number Portability covered in this Operations Manual, the following items are highlighted as having particular importance:

LSP Override
You can check the LSP for a number by doing a number enquiry. Sometimes, IPMS will display a different LSP than that provided by the customer. This will always happen with third party resellers. If IPMS has the incorrect LSP listed, you can:

- Check with the Service Provider that IPMS lists as the LSP first. This is a courtesy, but it is also efficient at identifying whether you can proceed submitting the port to them for them to action on behalf of a reseller, or whether there are any potential issues that might ultimately result in a failed port.
- If the GSP is certain that the details they have been given are correct, or if they are listed as the existing Service Provider, they can put through a port request where they are both LSP and GSP and where they select the correct GC. IPMS will automatically reject this port **but** once that happens, the GSP can check the "LSP Override" box and resubmit it. This is the only legitimate time you can use LSP override.

Emergency Returns

Though IPMS has an Emergency Return feature if a Port needs to be reversed, it is usually **always** more efficient to contact the original service provider and agree to do a normal Port Request, including an associated APC to set the RFS date immediately. This "handshake" process avoids the complications and technical issues of using the inbuilt Emergency Returns process and ensures that the LSP is aware of the issue and able to immediately accept the port.

Planned Outages

The minimum notice period for a Planned Outage is 5 Business Days. Notice must be sent to NP.Outages@tcf.org.nz. However, if the outage will impact a carrier's ability to perform Network Updates, the notice period is increased to 15 Business Days, with a minimum of 10 Business Days between the original planned date and the backup date. This is because incomplete Network Updates halt porting for all parties and have a substantial impact upon the industry. More time is required to plan for these outages.

Explanatory Statement

1.1 The purpose of this Operations and Support Manual for LMNP (the Manual) is for the support and assurance of Local and Mobile Number Portability in New Zealand. Its intent is to ensure that a consistent Customer experience (same processes, same Service Levels) is delivered by LMNP.

1.2 It is intended to provide detailed procedures for operational implementation and management of Porting Processes and multi-lateral issues that Service Providers and Carriers will need to implement to ensure and support the processes defined in the LMNP Terms and the Network Terms and information, such as Carrier contact details, that may vary.

1.3 Whilst this Manual may propose that some processes be subject to Bilateral Agreement, any such agreement shall not, in any way, result in a degradation of the Service Levels and Port Process expectations as laid out in either the LMNP Terms or this Manual.

1.4 The Manual applies to all parties to the Number Portability Determination in relation to either of the designated multi-network services, local telephone number portability service or cellular telephone number portability service.

1.5 This document should be read in conjunction with the following regulatory documentation produced by the Commerce Commission:

(a) The Number Portability Determination Decision 554– "Determination on the Multi Party Application for Determination of 'Local Telephone Number Portability Service' and 'cellular telephone number portability' for Designated Multi-Network Services" and Number Portability Clarification Decision 557 - Clarification of the Determination on the Multi-party Application for Determination of Local and Cellular Telephone Number Portability Designated Multi-Network Services";

(i) Terms for Local and Mobile Number Portability (LMNP Terms);

(ii) Network Terms for Local and Mobile Number Portability (Network Terms).

A copy of these documents can be found on the TCF Website www.tcf.org.nz.

Background

2.1 The Porting arrangements for Local Numbers and Mobile Numbers in New Zealand are provided by the Commerce Commission's Determination on the multi-party application for determination of 'local telephone number portability service' and 'cellular telephone number portability service' designated multi-network services, including any amendments and subsidiary determinations ("Number Portability Determination").

2.2 The Number Portability Determination includes the following:

(a) Terms for Local and Mobile Number Portability (LMNP Terms):

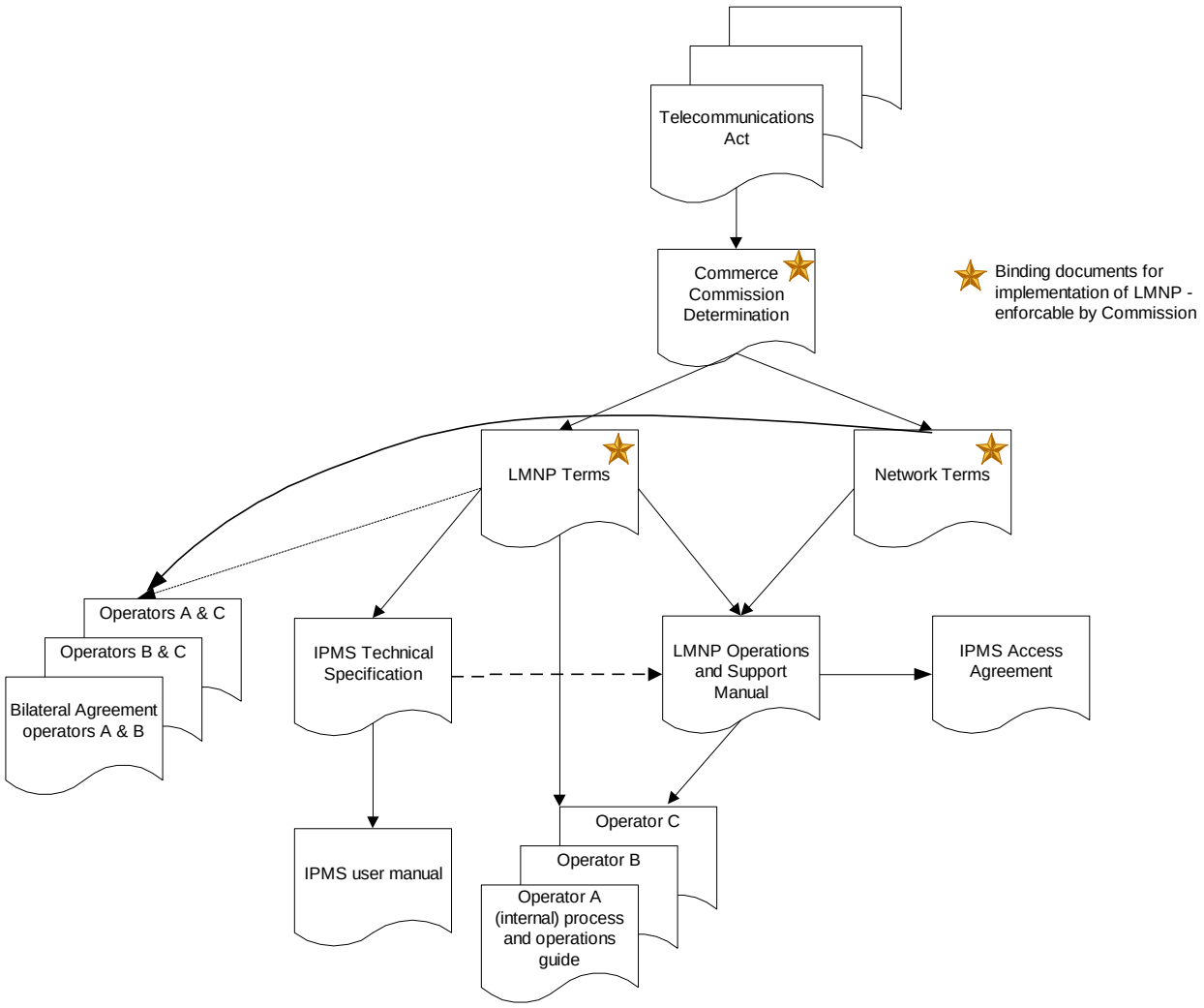
(i) The LMNP Terms detail the processes that enable Customers to Port their Local Numbers and Mobile Numbers and sets out the rights and obligations of parties to the LMNP Terms in a Local and Mobile Number Portability environment.

(b) Network Terms for Local and Mobile Number Portability (Network Terms):

(i) The Network Terms is intended to guide participating Carriers in the development of their own Network solutions and specify the optional and mandatory requirements necessary between Networks for Local and Mobile Number Portability for Voice Services and Short Message Services.

2.3 Included in the LMNP Terms and Network Terms is the timeline and conditions for implementation and on-going maintenance of the Local Number Portability and Mobile Number Portability Services.

2.4 Document Precedence



2.5 Further Explanation

(a) The IPMS Technical Specification document is used to specify the technical implementation of the IPMS.

(b) Each Service Provider and Carrier is to produce their own internal manual of business processes and operational procedures. While their manuals are expected to be consistent with the LMNP Terms, the Network Terms and the Manual, these internal documents have no official status in the context of LMNP.

Change Control Process

3.1 Process for changing Operations Manual

Any changes to this Manual must be made in accordance with the TCF Rules and the IPMS Access Agreement.

3.2 Process for changing IPMS Parameters

The table below describes the process for requesting and implementing a parameter change in IPMS.

Step	Action	Organisation/ Person Responsible
1	Parties to the Number Portability Determination may submit an IPMS parameter change request using the form "Proposal for Parameter Change to IPMS" in Appendix D and submit it to the NP Co-ordinator.	Party requesting parameter change

2	• Assign change number to change request.
	• Check the change, ensure it is consistent with desired result and confirm completed form contains all the required information for the proposed change.
	• Assess whether the change can be expedited or whether it needs to follow the standard change process.
	  ○ number range changes can normally be expedited
	  ○ changes in TEST, DEV, or TRAIN can be done with 24 hours notice and the restart is normally done at 4.00pm
	  ○ changes in PROD require a minimum of 48 hours notice and the restart is normally done at 6pm
	  ○ restarts for configuration changes normally require a 15 minute outage
	• Notify the relevant TCF working parties.
	• Email the change request to the TCF Forum
		NP Co-ordinator

Step	Action	Organisation/ Person Responsible
	Administrator (along with a proposed timetable for all the environments) who will update the Configuration Summary register and upload the change request on the TCF website.	
3	• Report impact of change on IPMS to NPUG	NP Co-ordinator
4	NPUG review: • It is preferred that the change is reviewed at NPUG but for urgent changes it may be distributed by email with at least one Business Day notice before the restart. Any postponement should be done with a minimum of half a day notice. • Confirm all prerequisites are in place to allow the Party to the Number Portability Determination to request parameter change (e.g. the party has executed the IPMS Access agreement) • Agree to roll-out schedule.	NPUG
5	Review by the Parties to the Determination for more complex changes, such as a new Party joining: • Assess impact of parameter change on Carrier's own Network and systems. • Review tentative roll-out schedule and request to amend roll-out schedule if required. • Finalise roll-out schedule. (This may be either by email sign-off by the NPUG or agreed at an NPUG meeting called by the TCF Forum Administrator or the NP Co-ordinator.)	Parties to the NP Determination
6	Manage roll-out of change: • Update the parameter change request form with agreed roll-out dates • Co-ordinate the roll-out of parameter change with the System Administrator and Parties to the Determination. • Advise all NPUG members that the parameter change has been implemented via email • Publish the new IPMS configuration on the TCF website on a regular basis or as required.	NP Co-ordinator
7	If necessary, modify Carrier network and systems as a result of the IPMS parameter changes	Parties to the NP Determination

3.3 Standard or expedited process

The following IPMS parameter changes can follow the expedited process:

1. An existing Number range allocated by the NAD to the Party to the Determination that is already in use or about to be used that needs to be

loaded into IPMS. (This situation may arise if a Carrier has omitted to load one of their existing Number ranges into IPMS).

2. Number range changes or minor changes to the value of fields in existing records for an existing Service Provider or Carrier in IPMS Test, IPMS Train, or IPMS DEV environments.
3. Other changes in TEST, TRAIN, and DEV that are considered urgent and not too complex (there may be limits to how quickly the changes can be scripted) can be expedited if the NP Co-Ordinator deems it to be practical.
4. Changes not requiring restarts of the environments impact others less and are more easily expedited.
5. Private configuration changes, such as parameter changes for a Carrier or Service Provider that impact only the party asking for the change, especially if it is to address something impacting portability in general.

If the NP Co-ordinator believes that a change could follow the expedited process and the change is not listed above, the NP Co-ordinator will send an email to the NPUG requesting to use the expedited process. This process would only occur where there is a change which impacts another Carrier. In these cases unanimous agreement is required by all members of the NPUG to proceed with the expedited process.

In cases where there is no impact on other Carriers and the NP Co-ordinator ascertains there is a benefit to portability in general, the change may be carried out and the NPUG notified afterwards. Once actioned, the configuration change would be posted on the TCF website and the NPUG advised at the fortnightly NPUG meeting.

3.4 Timings

The timings for key steps in the process follow (Note these are the time frames for making changes to the IPMS Prod environment):

Step	Duration (in Working Days)
2	1 day
3-5	10 days (depends on NPUG meeting frequency, currently fortnightly)
6	1 day
7	Depends on nature of change

Definitions and Interpretation

4.1 Terms defined in the Number Portability Determination and the IPMS Access Agreement have the same meaning in this Manual.

4.2 This section is intended to provide examples of the common expressions used for operational purposes.

Expression	Clarification Explanatory Note
Bilateral Agreement	Bilateral Agreements may be established between participants in LMNP may be used to enhance the Service Level obligations of the Terms or to expedite the Porting Process. Care should be taken by parties entering into Bilateral Agreements, that the obligations outlined in the Terms are not compromised. A Bilateral Agreement check list is included in Appendix A.
BAU	Means business as usual.
Business Day	Means a day on which registered banks are open for normal banking business, excluding Saturdays, Sundays and nation-wide public holidays. Regional public holidays are considered to be Business Days.
Carrier	A Carrier is defined in the LMNP Terms. As at the date of this Manual, the Carriers and their allocated Hand Off Code (HOC) are available on the TCF website.
Customer	Unless specifically stated within the Manual – a person that has a bona fide retail billing relationship with a Service Provider.
Contractor	Means an onsite technician.
Manual	Means the Operations and Support Manual for LMNP.
NP Co-ordinator or TCF Coordinator	means the party appointed by the by TCF to liaise with the System Administrator and is to be the primary contact point for any queries in respect of matters relating to the IPMS. The name and contact details of the NP co-ordinator are available on the TCF website.
Service Provider	Service Provider is defined in the LMNP Terms. The list of Service Providers bound by the Number Portability Determination as Access Seekers or Access Providers is available on www.tcf.org.nz.
Terms	Means the LMNP Terms and Network Terms (as the context requires)

Overview of the IPMS Environment

a) The IPMS has three environments visible and accessible by IPMS users:

   i. IPMS TEST – The primary purpose of this environment is to load new builds of IPMS so that they can be acceptance tested by IPMS users before being deployed into PROD.

   ii. IPMS DEV – This is used for parties to test their own systems, APIs and processes against a copy of the system that uses the same version of IPMS as PROD to ensure that parties own internal changes will be compatible with IPMS. Once a new build is accepted and loaded into PROD, it is loaded into DEV also.

   iii. IPMS PROD – The live number portability environment.

b) References to IPMS in this Operations Manual refer only to the PROD environment, though the processes described can be recreated in TEST for the purposes of new build testing and DEV for the purpose of internal testing, without impacting real world users and other parties.

c) Development by the Application Support team is tested on another environment that is inaccessible to all but that team. A fifth environment, IPMS TRAIN, is currently inactive.

d) Both TEST and DEV contain additional fictional parties (not found in PROD) to make testing easier. The original LMNP parties have FBN (Fly By Night) versions of their own companies (ie Spark and FBN Spark). Parties that were loaded into IPMS subsequently all use the Dummy Company, and are given userids for this company. These fictional parties can be used to act as the other party (eg GSP or LSP etc) for testing work because all porting activity requires responses from at least one other party for activities to be completed.

e) Number ranges in TEST and DEV can be very different to those in PROD. In particular, because there is no real-world call routing occurring in these two environments, there are a number of ranges that have a reduced set of networks that receive network updates. This facilitates faster testing. A list of these Queue By Number Range (QBNR) numbers can be found in Appendix M.

Security of IPMS

a) Given the critical nature of the IPMS system, the TCF recognises the importance in having oversight of who uses the system and ensuring that Parties to the Determination and other authorised entities that use IPMS adhere to good security practices.

b) Access to IPMS is only granted to users with the appropriate security credentials. All users, as well as all IPMS related activity, must adhere to the TCF's approved Security Policies for IPMS, as set out in Appendix N.

Code of Conduct

6.1 Good Faith

(a) All parties shall act co-operatively and in good faith to facilitate Porting Processes.
(b) All parties must act in a non-discriminatory manner and must facilitate Porting by acting in compliance with principles and processes that are consistent with section 18 of the Telecommunications Act.
(c) Each party subject to the LMNP Terms must comply with the Service Levels. If a party fails to meet the Service Levels, the provisions set out in sections 7.4 to 7.7 of the LMNP Terms will apply.

Resellers

7.1 The Service Provider or Carrier is responsible for ensuring, to the best of its abilities, that any of its Resellers do not withhold Porting consent from a Customer. This obligation includes ensuring that approval for porting steps is granted in a timely manner so that the Service Provider or Carrier can comply with its Service Level obligations under the LMNP Terms. Each Service Provider and Carrier shall include a clause in its contract with its Resellers that binds the Reseller to support the Service Provider or Carrier in their obligation to support Number Portability in accordance with the LMNP Terms and this Manual. These terms may include an ability for the Service Provider or Carrier to approve porting steps on behalf of the Reseller if the Reseller's delay is at risk of forcing the Service Provider or Carrier to breach a Service Level under the LMNP Terms.

Porting Process

8.1 The Porting Process means the process described in section 8 of the LMNP Terms.

8.2 From the Customer perspective, a porting instance is any case where a change of Service Provider of a Local Service or a Mobile Service[1] is implemented. Refer to section 8.4d) of the Manual for further details.

8.3 There may be other porting instances that involve interaction with IPMS capability and are not directly initiated by Customers. These instances are to be dealt with as Special Projects, as described in section 0 of the Manual.

8.4 Port Initiation Process

This section of the Manual relates to section 5.1 and 5.2 of the LMNP Terms.

Objectives

a) This section provides guidelines to ensure a smooth transition from a Customer request to Port to an industry fulfilment of that request.

1 Refer the Terms documents for Service definitions

It is to be noted that the Terms section 5.2.4, Informed Consent (iv), specify the GSP's obligations to advise the customer of existing obligations they may have to the LSP. This is to include any and all services the customer may have that do not relate to LMNP. An example might be their broadband data services which may or may not be included in the Terms and Conditions of their local or mobile services. Where not included, the LSP has no obligation to relinquish these services part of the porting process.

Port Categories

b) There are four Port categories outlined in the Terms.

c) General guidelines for use of each of the Port categories set out in clause 5.1.3 of the LMNP Terms are provided below. A single Port Request shall not exceed 500 Numbers.

(a) **Simple Local -** A Port for 20 numbers or less will typically be managed as a Simple Port.

(b) **Simple Mobile -** A single consumer connection will typically be managed as a Simple Port.

(c) **Complex Local** - A Port for more than 20 numbers and / or ISDN will typically be managed as a Complex Port.

(d) **Complex Mobile** - Multi-connection and / or Business connections will typically be managed as a Complex Port.

Scenarios / Examples

d) A Customer wishes to change Service Providers of their Local or Mobile Service

(a) A Customer must provide as a minimum the following information: their current Service Provider, their phone number, and their (LSP) account number, or handset reference number for Prepay mobile. Beyond knowing this information, the Customer may not to be able to provide any additional information to assist the Gaining Service Provider structure the Port Request.

(b) In addition to the Customer being unlikely to be able to provide additional information beyond the name of the Service Provider, it is possible that the Gaining Service Provider has no knowledge of the identity of the Losing Carrier.

(c) IPMS should be used wherever a Customer submits a valid request to change Service Provider unless specifically excluded by Bilateral Agreement between the respective parties.

e) A Ported Customer wishing to move premises and retain the Local Number may be allowed to provided that the new premises are within the same Donor Carrier's Local Calling Area

(a) In this scenario, a Customer moving would not normally represent a change in Service Provider. It may however represent a change in Carrier.

(b) An example here may be where one Carrier does not have infrastructure in the area a Customer is moving to, but access can be provided by reselling another Carrier's infrastructure.

(c) Therefore where there is a change in Carrier in this "move" scenario, a Port shall be initiated through IPMS by the Customer's Service Provider to maintain call handling integrity in the Network. A new Customer Authorisation is not required for this type of scenario. [2]

8.5 Port Request Phase

This section of the Manual relates to section 8.1 of the LMNP Terms.

Objectives

a) The objectives for the Port Request phase are to:

(a) Start the Port Process (GSP) by submitting the Port request:

(i) Service Levels start upon submitting the Port Request – IPMS tracks progress of the Port Request;

(ii) The IPMS ensures that no other Port Requests for the same Number can be started while the current Port is in progress.

(b) Allow the LSP to validate the data – check that the details provided by the GSP match with LSP records. The details that are checked depend on the type of Port Request (see Appendix Table 1 of the LMNP Terms).

(i) The LSP responds to the Request

(c) Allow the GSP, based on the LSP response, to approve, reject or resubmit the Port Request.

2 This assumes the clarification has gone through

(i) If the Port is approved, the Approved Port is now scheduled to begin Port Activation on RFS date / time

(ii) If the Port is rejected, the Number(s) involved can be included in another Port Request

(iii) The GSP has the option to make changes to the Port details and resubmit the Port in some circumstances; e.g. Customer wishes to add / remove numbers or the Customer / GSP changes the RFS date / time for Port Activation.

Guidelines

b) Guidelines for when the Port Request process should be used:

(a) The Port Request process should be used where the Customer requests that a GSP Port a Number on their behalf. Please refer to the 'Scenarios / Examples' section below. Note that in the port request screen, IPMS allows you to input a range of numbers with "From Number" and "To Number" columns. These must be numeric with no spaces or other punctuation (dashes, dots, commas etc). If you enter a non-numeric number in the "To Number" field, IPMS may return a non-descriptive error and the entire SOM will have to be re-entered.

(b) The Port Request process may also be used to 'reverse' a Port that has completed previously, but since then the LSP and GSP have mutually agreed that the Port was either a mistake or that the Port was unauthorised. In order to bring the Number back to the original Service Provider (i.e. the LSP in the original Port transaction), this Service Provider will now act as the GSP and submit a Port Request.

(c) A Port Request must only be submitted after Customer Authorisation (including informed consent[3]) has been obtained from the Customer.

(i) Port Requests should only be submitted after the GSP has completed all reasonable steps and checks to ensure that the Port will be able to be completed, from a GSP and GC point of view.

(ii) Such checks may include (but are not be limited to) confirming with the intended Gaining Carrier that the Number can be activated on the Network, and completing a credit check and other steps that the GSP typically completes before accepting a new Customer.

3 Refer section 5.2.3 and 5.2.4 of the LMNP Terms.

(iii) No Port Requests should be submitted pending the outcomes of any steps on the GSP or GC side that may cause the GSP to withdraw the Port. The Port withdrawal process (see section 8.11 of the Manual) should be initiated by the GSP in exceptional cases only; not as a common way to stop a Port should one of the GSP or GC checks fail.

(iv) No Port Requests must be submitted if there is material doubt about the completeness or correctness of the data provided to the LSP, or if there is doubt about validity of the Customer Authorisation – the Port Request process must not be used on a 'trial and error' basis.

(d) Where the LSP and GSP agree to 'reverse' a previously completed Port as a result of a Customer complaint, both parties need to agree that the Port is unauthorised based on a documented audit trail, complaint, or other valid evidence. In this case, the Customers documented audit trail or complaint constitutes an Authorisation by the Customer (see also sections 8.12a) and 8.13b) of the Manual).

(e) A Port Request must be submitted within 30 calendar days of obtaining Customer Authorisation to Port the particular number, from the Customer.

(f) It is recommended that Port Requests are not clustered by the GSP – Port Requests are expected to be submitted as they arise from a Customer request. This is to prevent the situation where a LSP is inundated with Port Requests.

(g) A single Port Request can include up to 500 numbers for Local Ports, across multiple carriers. Despite this technical ability, the GSP should avoid, wherever possible:

(i) submitting a Port Request that includes more than 100 numbers at a time. Since a SOM with 100 numbers is expected to be completed in the same timeframe as a SOM with 1 number, large SOMs can unfairly impact the LSP/LC and swamp their systems. In addition, if a single number in a SOM incurs an error, the entire SOM will be held up and unable to complete. This unfairly impacts numerous numbers.

(ii) Submitting a Port Request where the GSP knows that several LCs will be impacted. This increases the complexity of the Port and increases the risk of errors holding up the majority of the numbers in the SOM. The GSP may not always be aware what LCs will be impacted, but submitting Port Requests with a limited volume of numbers will reduce the risk of involving multiple LCs.

(h) For Mobile Ports, a Port Request should not mix Prepay and Postpay LSP numbers unless agreed bilaterally to do so.

(i) A Port shall include one or more Postpay numbers – in which case a single LSP account reference must be included, or

(ii) Shall include one or more Prepay numbers – in which a handset reference must be included for each number to be Ported.

c) Guidelines for when the Port Request process should not be used:

(a) By the LSP – the LSP cannot request a Number to be Ported away. If a Customer requests to Port away, they should be referred to the appropriate Gaining Service Provider.

(b) If there is already an 'open' Port request in IPMS for that Number. This will be the case if a Port for that Number has previously been submitted, and that Port has not been withdrawn, expired or completed.

(c) If details of an approved Port Request need to be changed (e.g. change to the RFS date), the Approved Port Change process should be used instead of submitting a second Port Request for the same Number.

(d) If the LSP or GSP determines within 1 Business Day of Port completion that the completed Port must be reversed. Instead the GSP should use the Emergency Return (see section 8.12 of the Manual) process.

Scenarios / Examples

d) The LMNP Terms specifically mention a co-operative period, during which either the GSP or LSP can contact each other to discuss the Port Request. Examples of when this may be appropriate include:

(a) During a review of the Port request by the LSP, the LSP notices that information provided is incorrect or incomplete. Rather than respond with 'can not match', the LSP may contact the GSP to clarify to facilitate the Port process.

(b) The LSP response indicates that (some of) the data provided is incorrect, and the GSP wants to clarify before making a decision to reject the Port, or to approve the Port using either the GSP data or the LSP response. While the LSP must act in good faith it is not obliged to provide the information requested by the GSP.

(c) Where the details match on the LSP side, but the LSP has genuine concerns that Porting that particular Number will cause a problem or service interruption for the Customer, the LSP shall notify the GSP by email of these concerns:

(i) if the request is to Port away a pilot Number, without any / all of the other Numbers;

(ii) the LSP has a genuine concern around the Customer Authorisation of the Port;

(iii) the LSP believes that the Customer may have intended to Port other Numbers as well, but only requested a sub-set of Numbers;

(iv) no additional Numbers will be offered for Porting by the LSP. It is the GSP's responsibility to ensure that as part of the pre-Port process, all Numbers are captured.

(d) The GSP has the obligation to liaise with the Customer in correcting the Porting information. The LSP has no obligation to provide the GSP with specific information regarding the Port or Customer account.

Explanatory note

e) This section aims to clarify some of the terminology and statements in the Terms in the context of the Port Request process.

f) Category of Port changed from Simple to Complex

(a) The LSP can, as part of their review of the Port, request that the Category of Port be changed from Simple to Complex (but not the other way around).

(b) Changes to the Category of Port must be driven by technical or business complexity and not as a default response, to extend the allowed response time.

(c) The overall guideline is that both the GSP and LSP must make every effort to allow the Port to be completed within the timeframes originally given to the Customer (the RFS date).

g) Validation and Approval

(a) If the LSP indicated on the Port Request is incorrect, the LSP will indicate 'incorrect LSP' and send the response – no data is validated.

(b) If the Account Number on the Port Request is invalid or absent when checked against existing Customer record, the LSP will indicate accordingly on response – phone numbers are not validated with regard to format, close matches or mistyping. For the assistance of the GSP, the minimum and maximum length of the Account Numbers, and the format used, is set out in Appendix L.

(c) If the LSP cannot match the line item details provided in the Port Request, they will indicate this on the response. If more than one Number is included in the same Port Request, the LSP will validate all the Numbers that do match.

(d) The LSP does not reject a Port Request; only the GSP can approve or reject a Port upon reviewing the LSP response.

(e) When the GSP approves the Port Request, they may choose to use the details of their original request, or use the LSP response details.

(f) Upon retrieving the Port Request from the IPMS queue, the LSP checks the details of the Port. Only certain details are required to match:[4]

h) For Mobile Ports, Postpay (Postpay with the LSP):

(a) Phone Number

(b) LSP Account Number

i) For Mobile Ports, Prepay (Prepay with the LSP):

(a) Phone Number

(b) Handset reference number

(i) The handset reference number for GSM phones (used by Vodafone, M2 Communications (including Black and White), Two Degrees Mobile, Vodafone, Compass, CallPlus and some Spark Customers) is the SIM card number. This number is printed on the actual SIM card. For the assistance of the GSP, the relevant number length is set out in Appendix L.

(ii) The handset reference of CDMA phones (used by some Spark Customers) is the unique hardware number on the phone (ESN), typically on the back of the phone under the battery.

NOTE: When the prepay/prepaid box is ticked, the handset reference column should become available for text input. This works in IE8 in compatibility mode, but does not in Chrome or Firefox browsers. In these two browsers you must submit the port request without entering the handset reference, let IPMS check and reject the request and then the field will be available for input. Full Chrome and Firefox functionality will be added in a future release.

j) For Local Ports

(a) Phone Number

4 Refer Table 5, Appendix 1 of the LMNP Terms.

(b) LSP Account Number

k) Not Required flag

(a) If the not-required flag is set to 'yes', it means that the Number will be relinquished by the LSP (ie the number is no longer required by the customer). If you want to have the number excluded from the Port but not relinquished, then do not include the Number in the Port and it will be ignored. Bilateral Agreements may also define additional specific meaning to the 'not-required' flag, e.g. triggering a specific process at the LSP side.

l) Number Blocks

(a) If the GSP is Porting a block of Numbers that cannot be entered as part of a single Port Request, they will need to split the Numbers over more than one Port. This will be the case if the Number Block is bigger than 500 Numbers (limit of the Port Request) or is split across multiple accounts at the LSP side.

Note: in the port request screen, IPMS allows you to input a range of numbers with "From Number" and "To Number" columns. These must be numeric with no spaces or other punctuation (dashes, dots, commas etc). If you enter a non-numeric number in the "To Number" field, IPMS may return a non-descriptive error and the entire SOM will have to be re-entered.

m) Residual Numbers

(a) The Customer may need to contact the LSP to manage any residual Numbers and / or close their account with the LSP. The LSP may need to contact the Customer regarding any residual Numbers that may affect their existing service. Any contact with the Customer by the LSP must be in accordance with Section J of the TCF Customer Transfer Code (extracted in Appendix G).

n) Customer Information Field

(a) The 'additional Customer information' field in IPMS should be used for the full account code when it is above the 20 characters allowed for in the primary 'Customer Account' field when required for ID reasons (some Symbio Customers are most likely to have account numbers greater than 20). The 'additional Customer information' field can also be used for other information as required.

o) Guidelines for Using the Standard Port Request Process for Porting Partial Call Readdressed Numbers

(a) The GSP is to initiate the port request with the correct LSP and Customer account number as identified on the Customer invoice.

(b) The GSP is to include all related partial readdressed numbers in the Port Request. (Due to the linked nature of the numbers the LSP has the right to reject the request if linked numbers are missing.)

(c) The GSP is to use the "not required" checkbox and tick it if specific numbers are not to be ported. The LSP will interpret and action this as part of the manual intervention process. See section k) for further information on the “not required” checkbox.

(d) The port must be submitted following the standard rules.

(e) IPMS will invoke its standard LSP validation and reject the Port Request giving a reason that a specific number requested is not owned by the LSP specified. The GSP re-confirms that the LSP is correct and ticks the "Override Service Provider" checkbox and resubmits.

(f) The LSP will undertake a manual validation of the Port Request and will approve or reject the Port Request providing the reason for the rejection is in accordance with the standard LMNP processes.

(g) Once approval has been gained, the standard LMNP processes are applicable.

8.6 Port Activation Phase

This section of the Manual relates to section 8.2 of the LMNP Terms and sets out the objectives where a Customer Number is being Ported from one Carrier to another including third party updates.

The IPMS enforces rules around when a SOM is permitted to be activated. The column for ‘Window’ below is the time detailed in the LMNP Terms, the grace period is added to this time to allow activations outside of hours (where agreed, see sections 8 and 9). The total window is the total length of time in which a SOM can be activated without requiring an Approved Port Change (APC) to reschedule it.

Port Type	Window	Grace Period	Total Window
Simple Local	Half Day	4 hours	8 hours (morning) 9 hours (afternoon)
Complex Local	Half Day	15 hours	19 hours (morning) 20 hours (afternoon)
Simple Mobile	10 minutes	230 minutes	4 hours
Complex Mobile	Half Day	60 minutes	5 hours (morning) 6 hours (afternoon)

Objectives

a) Customer Number is being Ported from one Carrier to another including third party updates.

b) Explanatory note for clause 8.2 of LMNP Terms

Port Activation

c) Port Activation process

(a) Port Activation will begin when a GSP moves an approved Port to 'in progress' status.

(b) The end-to-end Port Activation process must be managed within Working Hours as defined in LMNP Terms except where extended hours are agreed between the GSP and LSP, and GC and LC.

(c) Where a Port Request results in a change of Service Provider but not of Carrier it will still progress through all activation phases but there will be no changes to Network information or third party updates.

(d) If any complexities are present for a particular Port Request, impacted parties shall use the co-operative periods to work closely together to facilitate the successful Port rather than relying solely on the automated process.

(e) It is recommended that Port Activations are not clustered by the GSP – Port Activations are expected to be scheduled as they arise from a Customer request. This is to prevent the situation where a LC is inundated with requests to action Port Activations.

(f) If a GSP has requested more Numbers to be activated than the LSP indicated in their response, it is highly probable that the additional Numbers will not be Ported and the GSP should expect these Numbers to fail at the activation stage.

(g) If Porting is successful for only some Numbers within a single Port Request the GC and LC must agree with input from the GSP to:

(i) reverse successful Numbers, and fail the Port Request if there are no successfully Ported Numbers, or

(ii) complete the SOM if there are any successfully Ported Numbers.

Done / Undone / Done Loop

d) While IPMS will allow the GC and LC to update each Number many times, it is agreed that procedures will only allow GC Complete to be set to "Done" twice only. If the LC or GC fails the activation at any stage IPMS will reset these number progress states in the same function that the Gaining Carrier uses to restart the process for that number. For each number where the Gaining Carrier is set to "Done" the values of Losing Carrier fields and Test & Complete fields will be set to "Not Done" if they are set to anything other than "Not Done". The other Carrier will need to be aware so that

they reset their network as if the activation had not started. If a Number is left in an "Undone" state it will not be updated to the Ported Number Register.

Only the Gaining Service Provider may set the Activation Status to "Reversed.

A Port Request will need to be raised for any outstanding Numbers.

(a) The LC cannot activate a Port for a Number until GC sets status to "Done". However, any pre-work may be performed up to this point.

(b) Any billing issues arising out of lengthy Port Activation processes are to be resolved between the Customer and the appropriate Service Providers directly. There is no obligation for Service Providers to manage the billing in any way other than business as usual.

(c) The LSP and LC have no obligation to continue processing activation work if it extends past agreed timeframes but best efforts will be made to complete the Port once it has commenced.

(d) It is GSP's responsibility to ensure that the Port Activation process is started at a time that means it has a realistic expectation of being completed within the agreed timeframes (Working Hours, or extended hours if agreed between the parties).

(e) If the start of Port Activation is delayed by the GC such that an RFS Date / Time is missed, it will be necessary to raise an APC.

(f) Mobile Number Port Activation should not result in any loss of service for outgoing calls for the Customer as both the old and new handset can be active on the same Number on each Network, at the same time. Incoming calls may or may not be impacted depending on the call routing solutions deployed by Carriers.

(g) Local Number Port Activation may result in loss of service for outgoing calls for the Customer during activation. This is due to the need to provide a physical connection between the new GC's Network and the Customer's equipment. Incoming calls may or may not also be impacted, depending on the call routing solutions deployed by Carriers.

(h) The Service Levels for Local Number Porting allow up to 'within half day' for Port Activation to occur, however Carriers will use their best endeavours to ensure the impact on the Customers' incoming and outgoing calls is likely to be no more than 15 minutes where those calls are between the GC and LC, and will be as per agreed update periods for third party Carriers.

8.7 Approved Port Change Process

This section of the Manual relates to section 8.3 of the LMNP Terms.

Objectives

a) The objective of the Approved Port Change (APC) Process is to allow the LSP / GSP and Customer (via the GSP) to:

(a) change the RFS Date and / or

(b) change the numbers

and to allow the LSP to:

(c) change the RFS Date

Guidelines

b) An APC is not permitted once a Port Request has commenced Port Activation ("In Progress").

c) Provisions of the co-operative period apply throughout the APC process.

d) Based on Table 8.3.2 in the LMNP Terms, Approved Port Changes have maximum process completion times of:

Flowchart	**APC Process**	**Response Times**		
		Simple Local Port	**Complex Local/Mobile Port**	**Simple Mobile Port**
APC3 to APC5	Responding Party checks change queue and responds	Two Working Hours	Four Working Hours	Two Working Hours
		Frequency		
APC7 and APC8	Gaining Carrier(s) and Losing Carrier(s) should review this queue regularly	Every Working Hour	Every Two Working Hours	Every Working Hour

e) This needs to be factored into any decisions about the use of APC. Given the short timeline for Simple Mobile Ports the use of APC is not recommended if the RFS Date is less than 3 Working Hours in the future.

f) An APC is not possible once a Port is expired or withdrawn. A Port expires 5 Business Days after the RFS Date if an APC is not initiated and the Port has not been activated.

g) An APC may not be used more than five times on a Port before the RFS Date but can be raised many times after the RFS Date.

h) Once an APC is raised the original Port remains in place and, if the APC is declined, will revert to its original status.

i) An APC cannot be used to extend the RFS Date beyond the 30 calendar-day maximum when the Port Request is submitted.

j) This process is not to be used by the LSP to delay the loss of a Customer. The LSP must not raise an APC to add Numbers to the Port Request after the RFS Date has been agreed.

Explanatory Note

k) An APC can only be applied to an Approved Port. If the Port Request is still in the Port Request Process the options are to wait until the request is approved or withdraw the request and initiate a new request or re-submit the same request with amendments.

8.8 Port to Donor

Under section 13 of the Network Terms it states that Carriers may enter into Bilateral Agreements on the method of handing over calls between their networks.

In general, attaching a HOC to a call indicates that the Carrier has identified a call to a ported number and that the Carrier is aware of the correct Host Carrier. Where a number is ported back to the donor Carrier, the provisions of section 13 of the Network Terms shall apply and the call should not have a HOC added unless bilaterally agreed to the contrary and subject to the conditions outlined section 13.3 of the Network Terms.

8.9 Ported Number Relinquishment (including Quarantine) Process

This section of the Manual relates to section 8.4 of the LMNP Terms.

Objectives

a) To provide Ported Number relinquishment protocol including quarantine process.

Guidelines

b) Relinquishment

(a) A Service Provider shall relinquish a Ported Number where:

(i) The Customer has disconnected the Number

(ii) A Service Provider has disconnected the Number as part of BAU.

(b) A Ported Number may not be relinquished where:

(i) The Number is part of a contiguous Number Block unless it is the last remaining Number in the Number Block. In this case the whole Number Block is then relinquished.

(c) After the Host Carrier has relinquished the Number it will be quarantined by the IPMS for 30 calendar days. During the quarantine check period, the Host Carrier terminates the call with an appropriate call treatment.

(d) Cancellation of Relinquishments

Should the Customer change their mind and request the reactivation of their number once the number has been relinquished the process below should be followed if it is within the 30 calendar days.

(i) In IPMS Number Enquiry, if the user has the relinquishment cancel option enabled in their IPMS user profile, enter the SOM number of the relinquishment and press the Cancel button.

(ii) Failing that the Service Provider must supply the following data to the NP Co-Coordinator:

- SOM number of the relinquishment - The affected phone number(s).

NB: The requesting Service Provider must be the Service Provider that raised the relinquishment in IPMS.

Once the details are confirmed the NP Co-Coordinator will instruct HP to change the date on the RQ SOM so that it will be relinquished in the overnight processing that day. HP will confirm this has been completed and the NP Co-Coordinator will advise the requesting Service Provider the next morning when it is shown to be completed.

This allows a Service Provider to allocate the number to the Customer. If the requesting Service Provider does not have a relationship with the Donor Carrier of the number range they must arrange with the Service Provider that does have a relationship, to allocate the number and subsequently port the number if required.

(e) Relinquishment Fast Track

If the Customer wants to be activated on the Donor Network, the relinquishment can be Fast Tracked. The Service Provider must supply the following data to the NP Co-Coordinator:

(i) SOM number of the relinquishment - The affected phone number(s)

NB: The Service Provider that wants the Fast Track is normally not the Service Provider that requested the Fast Track. Therefore, the Service Provider who created the relinquishment must request the Fast Track (often, a Service Provider associated with the Donor Carrier will originate this request and be copied on the request).

Once the details are confirmed the NP Co-Coordinator will instruct HP to change the date on the RQ SOM so that it will be relinquished in the overnight processing that day. HP will confirm this has been completed and the NP Co-Coordinator will advise the requesting Service Provider that the number should be available the next morning when it is shown to be completed.

8.10 Port Expiry Process

This section of the Manual relates to section 8.5 of the LMNP Terms.

Please refer to clause 8.5 of the LMNP Terms for the Port Expiry Flowchart and the Service Levels that apply to the Port Expiry process.

Approved or failed ports where the end of the RFS window was more than one Business Day ago will be changed in IPMS to expiring at midnight.

An APC can be used to reschedule, and an expiring SOM may stay there until the LC confirms if they are configured to require it (in the carrier config field CONFIRMPORTWITHDRAWALIFLC).

A Port Request that is awaiting approval goes in to an expiring state. Then it is expired five days later, for example:

RFS Date - 13/8
Midnight 14/8 set to Expiring (1 day, as per parameter)
You can APC it to reschedule

Midnight 19/8 set to Expired (5 days after, as per parameter)
Now need a new port request to port the number

NB: Once a port goes into an 'expired status' in IPMS, Carriers and Service Providers are responsible for cleaning up this information.

If this expired port is left open, it leaves a potential problem for other Service Providers being able to port that mobile number in the future.

Because of this the SLA to withdraw expired ports will be the next working day.

Objectives

a) The main reason for having a Port Expiry process is to "clean up" overdue Approved Ports or Port Requests in IPMS and prevent the situation where a Number cannot be Ported at some stage in the future because it's still part of a previously Approved Port.

b) The objectives of the Port Expiry process are:

(a) For IPMS to notify the GSP that an Approved Port has not been activated within the expected time window and that, unless the GSP initiates a specific action, the Port will expire.

(b) To expire Approved Ports five Business Days after the RFS date has passed, and thus "releasing" the Number(s) included in the Port.

(c) To confirm that both the Gaining Carrier and Losing Carrier no longer have the Port scheduled to be activated.

Guidelines

c) The Port Expiry process is not triggered by the LSP or GSP it is triggered by the IPMS. As such, there are no user guidelines as to when to use this process.

d) There are guidelines however around the response required from the GSP. When the GSP is notified by IPMS that an Approved Port will expire in 5 Business Days, the GSP has three options for its response:

(a) Respond by initiating a Port Change Request to schedule a new RFS date. This course of action should only be taken after agreeing a new date/time to Port the Customer. This response must not be the default response to an expiry notification, in order to allow more time (e.g. for discussions with the Customer) and keep the Number(s) locked in a Port Request.

(b) Respond by withdrawing the Approved Port. This action should be taken if the GSP establishes that the Port is no longer required to be activated (either confirmed by the Customer, or because of a business or technical issue being experienced by the GSP or GC), or if the GSP cannot agree a new RFS date with the Customer.

(c) Do nothing, and let the Port expire. This 'approach" should be an exception: the GSP must make a reasonable effort to respond with an APC or a withdrawal, and not use this third option as their default 'response'. While the Port Expiry process waits for the 5 Business Days to elapse, the Number(s) included in the Port are still prevented from being included in new Port requests.

e) In general, the guideline is that the GSP should withdraw the Port once they become aware that the Port will not be activated. The default action by the GSP must not be to let the RFS date pass, and wait for the Port Expiry process to be triggered before withdrawing the Port.

f) A Port Request that is not yet approved can expire in the same manner as an Approved Port.

Scenarios / Examples

g) No points of interaction between the GSP and LSP are identified in the Terms in relation to the Port Expiry process. Possible scenarios where direct contact between the GSP and LSP will be beneficial include:

(a) Before requesting a new RFS date (through the APC process), the GSP may want to discuss an appropriate date / time with the LSP, to prevent unnecessary further delays in setting a new RFS date.

(b) The LSP may contact the GSP once the RFS date has passed, requesting that the GSP withdraws the Port (prior to the Port expiring). This may be appropriate if the Customer has contacted the LSP and as a result the LSP wants to perform an account maintenance activity (e.g. disconnect the Customer, or transfer the Number) that is typically not carried out while a Port-out request is in progress.

h) Note that the LSP is expected to refrain from disconnecting a Customer while a Port is in progress, and charges may continue to be incurred by the Customer for the duration of the Port. If required, a Losing Service Provider may 'bar' all services while a Port Request is 'In Progress' so that the Customer can retain ownership of the Number but not continue to accrue charges (in a credit situation).

Explanatory Note

i) All Ports once approved, must eventually reach a final status thus making the Number available again for future Ports. There are three possible ways that the status is changed to a finalised state:

(a) The GSP withdraws the Port

(b) A Port Activation occurs

(c) The Port Expires – this process ensures that the Port Request is ended even if the GSP takes no further action on the Approved Port.

8.11 Port Request Withdrawal Process

This section of the Manual relates to section 8.6 of the LMNP Terms.

(a) A Port Request Withdrawal can be requested by the Customer or initiated by the GSP on behalf of Customer, in order to support the overall Customer experience.

(b) New Port Requests cannot be made against the Numbers in a Port Withdrawal until the Port Withdrawal has been completed. This process may take up to 4 Working Hours.

8.12 Emergency Return Process

This section of the Manual relates to section 8.7 of the LMNP Terms.

Objectives

a) This process is required to quickly, and at reduced notice periods, return a Customer's Number to the Customer's previous Service Provider and Carrier and to restore all routing as if the Port had not been performed.

Guidelines

b) Emergency Returns may only be used within one Business Day of the completion of the Port Activation.

c) Ideally, a problem with a port should be identified before the Port is completed. The Test and Complete phase of the porting process, while the Port status in "in progress" is designed specifically for the purpose of identifying any issue. Automation, though enabling ports to be completed in a timely manner, can remove the ability to spot errors before the Port is complete.

d) It is possible for parties to agree bilateral procedures for handling emergency returns of this nature. These bilateral agreements should take preference over use of the inbuilt IPMS Emergency Return Procedure. In the absence of a bilateral agreement it is expected that Emergency Returns would be used very sparingly.

e) To use the Emergency Return Process effectively, parties will need to proactively communicate with the former LSP to ensure they are ready for the return Port and are able to accommodate the return. It will normally be easier and faster to ask the former LSP to lodge a new port request and supply details for the request to them to facilitate fast completion, rather than use the Emergency Return procedure. IPMS users should contact the alternate party by phone and remain on the phone while the two of you complete the porting process to ensure that both sides are aware of what is happening and that the action is complete. IPMS users should note that there is a good chance that an Emergency Return may be rejected by the new GSP if they are not fully informed about the situation through this "handhold" process.

f) The Gaining Carrier(s) and the Losing Carrier(s) must agree that an Emergency Return is required. The Losing Carrier(s) and Gaining Carrier(s) must coordinate the Emergency Return as mutually agreed. Notice periods for RFS Dates do not apply.

g) The Emergency Return must use an existing completed Port Activation as a reference. The Emergency Return does not have to reverse all Numbers in a given Port. An Emergency Return will be processed in exactly the same way as a normal Port Activation, except that the RFS Date rules are not enforced.

h) The IPMS will require the SOM Number of a previously completed Port. The IPMS will check that the Port was activated within one (1) Business Day of the request of the Emergency Return. Numbers that did not Port successfully in the original Port Activation cannot be returned. The original Gaining Service Provider becomes the new Losing Service Provider once an emergency request is initiated.

i) Emergency Return can be used if:

(a) The Port was not authorised by the Customer and if it is within one Business Day of the completion of the Port Activation

(b) The Customer requests it where the Customer's level of service is technically impacted due to Carrier problems.

(c) Emergency Return cannot be used if:

(i) A Customer changes their mind

(ii) Impacted parties do not reach agreement.

Scenarios / Examples

j) Customer discovers that they have accidentally Ported a Number, as part of a Number Block that should have been left with the Losing Service Provider.

k) A Carrier discovers that when they connect the numbers involved in the Port, the resultant call service delivered is unacceptable. An example might be where although the Port itself has worked, a reconfiguration of Customer premises equipment associated with the Port has failed and the only way to regain service is to regress the Port.

8.13 Unauthorised Ports

For a definition of what constitutes 'Customer Authorisation', 'Informed Consent', the 'Customer Authorisation Validity Period' and when a Port is deemed to be unauthorised, refer to the LMNP Terms section 5.2.

Objectives

a) The objectives of this section are to:

(a) Clarify how the LSP can query the Customer Authorisation for a particular Port, and what the expected response from the GSP will be

(b) Clarify the interaction and cooperation between LSP and GSP in establishing and agreeing whether a Port is authorised or unauthorised by the Customer

(c) Describe the process to follow in cases where it is agreed a Port is unauthorised

(d) Describe the process to escalate disputes when the LSP and GSP do not agree whether a Port is authorised or unauthorised.

Guidelines

b) At the time that the Port Request is submitted by the GSP, the Port is deemed to be authorised. If subsequently the LSP discovers that the Customer Authorisation may not be valid, they need to contact the GSP. The general process by which a Port can become unauthorised is as follows:

(a) The LSP discovers that the Customer Authorisation for the Port is not valid (e.g. the wrong person signed for the Port) and the LSP contacts the GSP to discuss or dispute the Customer Authorisation.

(b) The GSP and LSP agree that the Port is unauthorised.

c) Note that if the GSP becomes aware (or suspects) that the Port is unauthorised, prior to Port Activation, they must reject or withdraw the Port – no agreement from the LSP is required.

d) Once the LSP and GSP agree that a Port is unauthorised, they must, depending on the phase in the Port process:

(a) Cancel the Port (GSP) - prior to Approval

(b) Withdraw the Port (GSP) - prior to Port Activation

(c) GC to stop processing (GSP to inform GC) - during Port Activation. GSP to fail the Port

(d) Emergency Return – within 1 Business Day of Port Activation

(e) The original LSP submits a Port request to bring the number back (act as the GSP in this request) – more than 1 Business Day after Port Activation.

e) If the LSP believes that the Port is unauthorised, but the GSP does not agree, the following guidelines must be followed:

(a) LSP to respond a per normal; RFS changed (APC by LSP or GSP) to allow time for investigation- prior to approval

(b) APC to push back RFS, to allow time for investigation – prior to Port Activation

(c) Continue Port Activation - during activation. Then wait for agreement to Port back or do emergency return

(d) Wait for LSP and GSP to agree – any time after Port Activation (whether within 1 Business Day or more than 1 Business Day after Port Activation.

Process to agree that a Port is Unauthorised

f) LSP enquiry about the Port Authorisation[5]

(a) The LSP can contact the GSP directly to request a copy of the Customer Authorisation obtained for a specific Port.

(i) The LSP can request the copy at any time during the Port process or up to 12 months after the Port Request where the Customer queries the validity of the Port. The Service Level defined in the LMNP Terms specifies that the GSP must provide the copy within 5 Business Days after the request.

(ii) Particularly when a Port has not been activated yet, the GSP should make all reasonable endeavours to supply the copy of

5 Should CA forms have a disclosure statement on them – re: privacy laws

the Customer Authorisation as soon as possible. In general, it will be less impacting to the Customer, the GSP and the LSP if a Port is found to be unauthorised prior to Port Activation (so the Port can be withdrawn by the GSP), compared to the scenario where the Port is found to be unauthorised after completion.

(b) The LSP can contact the GSP to discuss doubts about the Customer Authorisation for a specific Port Request – this may or may not lead to the LSP requesting a copy of the Customer Authorisation.

Guidelines

g) As a general guideline, the LSP must only enquire about the authorisation of a Port and / or request a copy of the Customer Authorisation in cases where the Customer queries the validity of the Port – the process must not be used by the LSP to try and delay or prevent a Port. Both the LSP and GSP must act in good faith. The LSP must act on specific information provided by the Customer ('the bill payer') that suggests that the Port may not be authorised.

h) If, in order to verify the authorisation of a Port, more time is required, i.e. the validity of the Customer Authorisation can not be established before the RFS date arrives, either the GSP or the LSP can initiate the Approved Port Change (APC) process. If, as a result of a Customer query regarding the validity of the Port, the LSP and GSP should agree to reschedule the Port (change RFS), and the GSP must inform the Customer of the delay.

Good Faith

i) As a general guideline, if there are material doubts about the Customer Authorisation (after the Port Request has been submitted), and more specifically, about whether the person who requested the Port is authorised to do so, the GSP and LSP will work together to establish the validity of the Customer Authorisation. The objective is to prevent an unauthorised Port from being activated in the first place, as there is a significant impact on the legitimate owner of the number if the Port does proceed, and then needs to be reversed.

j) Given the typical timing for completing a Port, if the GSP and LSP intend to establish if a Port is unauthorised during the available time between the GSP submitting the Port Request, and Port Activation being triggered (on RFS date), the parties will need to cooperate and exchange information. The process mentioned in the Terms where the LSP requests a copy of the Customer Authorisation is more suitable to prove authorised / unauthorised after the Port has completed. Due to the nature of the Port process (GSP led process), each party has part of the information required; the LSP

only has visibility of the Customer's current account structure, and therefore is more likely to know who is authorised to Port a number (the Customer / bill payer; not necessarily the connection holder); the GSP only has visibility of the Customer Authorisation and only the GSP has direct contact with the 'Customer' during the process.

Escalation process to establish if a Port is Unauthorised

k) If after discussing the Port and exchanging information, the LSP and GSP cannot agree on whether the Port is unauthorised or not, the following process will be followed:

Reversal of an Unauthorised Port

l) The GSP and LSP agree that the Port is unauthorised. An audit trail must be kept by both parties; both parties should send an email to confirm that they are satisfied that the Port is unauthorised, and should be reversed. If only certain numbers in a Port are deemed to be unauthorised, the specific numbers must be listed in the email.

m) The 'new GSP' will not have a Customer Authorisation from the Customer in this case; the email confirmation by LSP and GSP will serve as proof of Authorisation, and must be kept for a minimum of 12 months. The 'new GSP' must be able to reproduce the confirmation (agreement) from the LSP upon request; either when audited or if the LSP asks for a copy.

n) The 'new LSP' will confirm the details of the Port – provided that only numbers agreed to be reversed are included. The LSP will approve 'as soon as possible' – prioritising approval for this type of Port reversal over BAU Port out requests.

o) The GSP will Approve the Port. Approval will be given 'as soon as possible' - prioritising approval for this type of Port reversal over BAU Port in requests.

p) The GSP will initiate Port Activation once the Port is approved.

q) During the Port reversal process, communication to the 'Customer' will be as follows: The original GSP (the SP that requested the Port that is now deemed to be unauthorised) will communicate with their newly acquired Customer – their number(s) are being Ported back, but at the start of the Reversal process, the original GSP has the billing relationship with this person. The original LSP will communicate with their Customer – the person who has legitimate 'ownership' of the number that is being Ported back.

Special Projects

9.1 In addition to the four types of Ports listed above, there may be a need to update IPMS and / or third party Carriers outside the provisions of the standard Simple and Complex porting process. This update will require the IPMS manager to

generate a ported number change file which is to comply with the structure shown in Appendix H, Special Projects Upload File Structure.

(a) A Special Project necessitating update of IPMS would involve a direct load of Numbers or changes to the IPMS database, bypassing the Port processes (i.e. the messages and SLA's) as they exist for Simple and Complex Port types.

(b) A Special Project may involve any combination of change of Service Provider, change of Carrier and change of Donor Carrier or any instance where IPMS needs to 'know about' changes in order to either maintain network call handling integrity, or allow future Ports on the affected Numbers[6]

(c) This type of update must not be used for Customer initiated Ports.

(d) Special projects should be clearly defined upfront by means of a terms of reference. This document should clearly outline and include the scope of the project, impacted stakeholders, roles and responsibilities and a schedule of events. The scope should be agreed prior to the start of the project. It will be the role of the NP Co-ordinator to ensure the Terms of Reference template is completed and to manage the project from start to end.

9.2 All LMNP parties have a responsibility to fully disclose to the NPUG, any planned work on internal systems which interface to IPMS or as may enable third parties, such as resellers, to provide porting capabilities.

The NPUG has a responsibility to ensure a consistent customer experience (ref clause 1.1 of this Manual). To ensure this consistency, they may implement governance in a manner similar to that of a Special Project.

9.3 Third party updates may be implemented:

(a) Updates shall be implemented through the Special Project migration file.

Obligations

9.4 As the SLA's defined in the LMNP Terms do not apply to the Special Project event, the following obligations shall apply:

(a) The initiating party must provide a minimum notice period of 20 Business Days prior to the generation of the Terms of Reference notification to all parties to the Number Portability Determination.

(b) Special Project timelines are to be developed with all parties impacted by the Special Project, working in good faith on an individual project basis. This notwithstanding, any party unable to fulfil the requirements of the Terms of Reference within 40 Business Days of its formal notification shall formally notify the NP Co-ordinator of this.

9.5 The addition of new Parties to IPMS will be completed in accordance with the 3 month timeframe in the LMNP Terms. The addition of a reseller, or a change to

6 Per line set-up costs may be applicable

an existing Party's configuration, is not subject to the same timeframe requirements in the Terms. All Parties will act in good faith to implement a requested change in a timely manner. The Party requesting the change should have a reasonable expectation of the time it will take to implement such changes. The following is a guideline to help set expectations for common changes, noting that each situation will be different and will need to be reviewed on its own merits:

Approximate Time to Complete	Action Required of other Parties
2 weeks	New Carrier-Service Provider relationship to be created between existing Carrier and existing Service Provider
4 weeks	New Service Provider created within an existing Party, and an associated new Carrier-Service Provider relationship created in a service area where the Party already operates (eg an additional mobile Service Provider added to an existing mobile Carrier)
6 weeks	New Service Provider created within an existing Party, and an associated new Carrier-Service Provider relationship created, in a service area where the Party does not already operate (ie adding a mobile service to a Party that has previously been local only).
8 weeks	New Carrier created for an existing Party, using existing interconnection methods
10 weeks	New Carrier created for an existing Party using new interconnection methods (eg new locations)

Service Level Expectations and Operating Hours

Objectives

10.1 To provide an understanding of the operating hours for each of the parties to the LMNP Terms and how this impacts the Service Levels.

10.2 The Service Level provisions in Table 2, Appendix 1 of the Terms, in respect to Simple Ports and Complex Ports apply.

Guidelines

10.3 These are the guidelines for Service Provider and Carrier Extended Hours of Business for Simple and Complex Port Categories.

(a) During Working Hours the Service Levels defined in the LMNP Terms shall apply.

(b) For Port Request activities processed during hours outside of Working Hours the same Service Level timeframes stated in the Terms are applicable but the level of commitment to meet these Service Levels may be reduced.

Extended Hours

10.4 Any Porting activity between GSP's and LSP's may be performed outside Working Hours, as agreed to in Bilateral Agreements. Examples include:

(a) Simple Mobile Ports carried out in stores that are open during weekends and late nights

(b) Large business Customers requesting after hours cutover to reduce business risk.

10.5 Relaxed Service Level obligations may be agreed between parties for Extended Hours of Business.

10.6 The following constraints shall apply to any Bilateral Agreements for Extended Hours of Business

(a) The "Simple Mobile" port category Ports would have RFS windows set within standard hours of business as specified in the Terms i.e. 8 and 5 but the IPMS is set up with a 3 hour 50 minute grace period which would allow port activations to take place up to, but not beyond, 5pm unless mutually agreed. (The grace period increases the window in which the port can be activated.)

(b) Complex Mobile Ports would be provisioned in a similar manner but a 15 hour IPMS grace period will allow any "Complex" port category to have RFS windows set 24 x 7.

(c) These constraints may be subject to review as a result of the current PCR Change Process.

Third Party Update Phase

10.7 By definition, third party updates are required by all participating Carriers. They are required once a Port is deemed by the GSP, GC and LC to be complete.

10.8 The synchronisation of third party updates is critical to ensure the Customer experience during the Port is not adversely impacted.

10.9 Parties to the Determination are to use best endeavours to implement 3rd party updates at least hourly, between the hours of 05:00 am and 03:00 am, seven days per week.

Scenarios / Examples

10.10 Even though Service Levels / Working Hours govern response time maximum periods, IPMS will be available and will process requests on a 24 x 7 basis, except in agreed downtimes allowed within the contract agreed between the Systems Administrator and the TCF.

10.11 The Port Request phase is to establish agreement between the GSP and LSP and Customer to allow Porting to occur, so there is no Network dependency, therefore there is no issue with Service Level spanning multiple calendar days.

10.12 Port Activation has a Network dependency and therefore the Service Level should not span more than one single Working Day.

Explanatory note

10.13 The RFS Date / Time will be the start of the Port Activation window

10.14 For a Simple Mobile Port the expectation to be set with the Customer should be that the Port will be completed within 30 minutes following the RFS Date / Time

10.15 The activation window will be 4 Working Hours for all other Ports

10.16 Parties must adhere to the Service Levels at all times; this includes ports involving third party resellers. If a third party reseller is slow to respond to a Port Request or other porting step, the party acting on their behalf inside IPMS must still take the appropriate action required within the time allowed by the Service Level. It is up to the party acting within IPMS to manage their third parties and ensure that porting continues in accordance with the Service Levels, regardless of delays or complexities caused by third parties.

10.17 For further explanation of the Service Levels, refer to Appendix F.

Agency & Special Services Requirements (Emergency Services)

Agencies requesting information under legal compulsion

11.1 "Legal Compulsion" is defined as any legal obligation to provide call tracing services, Customer information, call records, or technical data for Government Agencies or where necessary in public safety situations.

11.2 It is each Service Provider/Carriers responsibility to have internal processes in place to satisfy any legally compelling request that is served on that Service Provider or Carrier.

Public Safety - Emergency Services

11.3 The Police or other government agencies may require urgent access to Customer details from the Service Provider or Carrier under certain circumstances (e.g. threat to life, public safety). The Service Provider and Carrier must have internal processes in place to provide coverage to deal with these requests in a timely manner to comply with its own obligations.

11.4 Where there is any impact to **111** as a result of work undertaken - ensure that the 111 emergency service is always protected by alternative route.

Access to the IPMS by Government Agencies

11.5 Section 4.5 of the LMNP Terms states that:

> *Government agencies (including without limitation emergency services such as the Police and Fire Service) and third parties will be entitled to access the IPMS for information purposes only in the conduct of their lawful operations. The terms on which these parties will be granted access will be specified by the TCF and set out in an IPMS access agreement between the TCF and the party seeking access.*

11.6 Currently, this requirement has been satisfied by allowing Government agencies and third parties to access IPMS using the report download web service and download IPMS reports such as the Full Ported Number register report. As at June 2007, no Government agency had taken advantage of this capability.

Customer Fault Handling and Testing Procedures

Objectives

12.1 To identify how Carriers / Service Providers will act in the event of a Ported Number fault and provide processes and requirements for the management/resolution of Network faults involving Number Portability.

Guidelines

12.2 Each Carrier will progress their own fault handling within their own Network. Each Service Provider is responsible for their Customer base and as such will have control of any service fault reports.

12.3 The specific inter-Carrier process for Number Portability fault handling and resolution are to be developed by Carriers as amendments to existing Bilateral Agreements regarding fault handling.

12.4 If the location of the fault is determined to be in the Host Carrier network then responsibility for management and repair of the fault shall be with the Host Carrier.

12.5 If the location of the fault is determined to be in the Donor Carrier network then responsibility for management and repair of the fault shall pass to the Donor Carrier.

12.6 The party responsible for the fault shall repair the fault within the clearance times given in the tables at sections 12.15 to 12.18 (inclusive) unless the fault has no impact on services provided to the other party under this agreement. If temporary repairs are made, the other party shall be informed and agree to the estimate of the timescale to full repair and the expected impact on the service.

12.7 The party responsible for fault repair shall inform the other party using an agreed communication format as soon as the fault is resolved.

12.8 The Host Carrier and the Donor Carrier will agree all service contacts (refer TCF Website www.tcf.org.nz).

Standard Testing / Fault Analysis

12.9 Before reporting a fault to another Carrier, each Carrier must ensure that the:

(a) Port Activation time for Porting has expired

(b) Customer Equipment is correctly terminated

(c) Dial tone or an outgoing call capability is available on the Gaining Carrier service

(d) Test calls from within the Gaining Carrier telecommunications Network are successful; and

(e) Test calls from other Carrier Telecommunications Network are unsuccessful.

12.10 Each Carrier whilst diagnosing a fault must use sufficient analysis to identify which Carrier Telecommunications Network may be causing the fault and then direct the fault report to the now identified Carrier in the first instance.

Additional Testing / Analysis for Complex Ports

12.11 In the case of a fault with a Complex Port, the Gaining Carrier must conduct the Standard Tests however the Gaining Carrier does not need to test all Numbers if there are more than 10 Numbers associated with a service which are in a sequential Number range.

12.12 In the case where there are more than 10 sequential numbers, the Gaining Carrier must apply Standard Tests for the following Numbers:

(a) the first Number in the range

(b) the last Number in the range

(c) a selection of Numbers in the range representing an even spread of the range, such that five Numbers or 3% of the range (which ever is greater) are tested, ensuring that testing includes a minimum of three Numbers in each 100 Number Block.

Guide to LMNP Fault Management Timetable

12.13 Further evaluation of the impact on existing BAU fault management processes. Each needs to be checked against existing Bilateral Agreements.

12.14 This section is intended to provide guidelines for inter-company fault resolution Service Level Agreements.

12.15 Fault priority levels are defined as follows:

(a) Upon initial contact between the parties involved in the fault process, the party receiving the fault will set the initial priority, and confirm status and priority to the other parties, observing response times as specified in the Service Level table in this section.

Priority	Fault
1	Critical impact, e.g. Complete outage of a service or loss or severe degradation of inter-Carrier exchange capability.
2	One or more Customers are experiencing partial loss of service to access either inbound or outbound calling (not both) impacted
3	All other faults

12.16 Either party may request reclassification of a priority 2 fault to priority 1- this reclassification must be agreed between the parties.

12.17 The quality of service parameters appropriate to the fault management procedure is specified below.

Period Title	Value
Response Time	Time between an intercompany fault report and the first response from the Service Provider/Carrier that clearly indicates expected resolution time, progress information and fault diagnoses.
Resolution Time	Time between fault report and fault resolution.
First Escalation Time	Time between the Fault initially being reported and the relevant escalation contact point first being informed.
Second Escalation Time	Time between an intercompany fault being reported to the first escalation point and the relevant second escalation point contact first being informed.

Note: a fault may be escalated if the agreed resolution time is not met, or updates are not received within the agreed timeframes.

12.18 The service parameter values for all services are specified below:

(a) The Service Levels in the table below relate to Business Days and Working hours. After hours fault Service Level timeframes to be checked through Bilateral Agreement process.

	Priority 1	Priority 2	Priority 3
Response Time	< 30 min	< 120 min	< 2 days
Resolution Time	4 hours	8 hours	3 days
First Escalation Time	2 hours	8 hours	3 days
Second Escalation Time	4 hours	2 days	5 days

Porting Contact and Escalation Points

This section provides guidelines on how and when to contact other parties in regards to Porting.

Contact Procedures

13.1 Communication

(i) Communication should include:

Initiator of the contact	First level contact (refer to contact list)
Contact at other provider	First level contact (refer to contact list)
Method of contact	Email shall be the primary method of contact between parties Phone calls should be used where Service Levels are short (e.g. simple mobile) or the issue is critical (e.g. emergency return) Phone contact should be followed up by the initiator with an email to confirm the issue discussed and the agreed outcome.
Minimum information to supply (requestor)	SOM Phone number Reason for contact and action requested Priority of request
Optional information to share	Copy of Customer Authorisation form Customer name, address Further information as appropriate
Response time	Resolution during initial contact where possible. Otherwise response within 2 hours by the contacted party to provide an update on the request, and an estimated time for resolution where applicable. Different response times may apply outside of Working Hours

13.2 Escalation points

‘

(ii) Escalation points for Porting will be maintained on the TCF web site at www.tcf.org.nz.

IPMS Fault Management

14.1 **In** the case of IPMS issues or faults, refer to Appendix B - IPMS Management.

Capacity Forecasting Procedures

15.1 If activity is planned outside the normal operating levels, reasonable notice should be given to all other parties.

15.2 Refer to section 18 of the Network Terms for further detail. Capacity forecasting shall be agreed in Bilateral Agreements, as required for exceptional Porting volumes.

New Participants Procedures

16.1 The Number Portability Determination identifies a limited number of Access Seekers and Access Providers; companies that have been determined to be bound by that Determination. Appendix H of the Manual describes how new parties who wish to participate in Number Portability need to work with the TCF and the parties to the Number Portability Determination to provide a satisfactory Porting experience for Customers.

16.2 The TCF may, at their discretion, appoint a third party to manage the introduction of the new entrant as a programme of work and the existing participants and new entrant will work in good faith to facilitate the new entrant being able to Port Numbers.

16.3 Existing Parties to the Number Portability Determination must review internal Porting processes and systems to incorporate the new Service Provider.

Enforcement Agency Procedures

17.1 The Enforcement Agency

(a) The Enforcement Agency is a person nominated by the TCF and approved by the Commerce Commission or, where the TCF has failed to nominate a person, a person appointed by the Commerce Commission. The Enforcement Agency is envisaged in clause 14.5 of the Network Terms and clause 7.4 of the LMNP Terms.

(b) The Enforcement Agency is not a specifically constituted body, but rather will be appointed on an ad hoc basis and will perform its functions in accordance with the powers and processes set out in this part of the Manual.

(c) The role of the Enforcement Agency under the Network Terms and the LMNP Terms (collectively "the Terms") is to monitor and as required by the Terms measure and enforce compliance with:

(i) the Equivalent Service provisions in accordance with clause 14.4 of the Network Terms (the Equivalent Service Criteria); and

(ii) the specified service levels set out in clause 7.4 and Table 2 of the LMNP Terms (the LMNP Service Levels).

(d) Where necessary, the Enforcement Agency will conduct audits of Carriers (Audit Carriers) to assess compliance with the Equivalent Service Criteria and/or the meeting of LMNP Service Levels. For the purposes of section 0 where the context requires, Audit Carrier shall include reference to an Audit Carrier under the Network Terms and an Audit IPMS Client under the LMNP Terms.

(e) The Enforcement Agency may conduct such audits itself, or appoint an independent expert to conduct the audit on its behalf. Reference to "Enforcement Agency" should be read to include any duly appointed independent expert.

(f) An expert appointed by the Enforcement Agency is to be independent of both the Audit Carrier and any Carrier whose complaint to the Enforcement Agency initiated the Audit. An expert will be deemed independent of a Carrier if they have not (and no member of their staff involved with the audit have) been retained by that Carrier on any matter within the previous three (3) year period.

(g) The powers and processes set out here are additional to, and not exclusive of, any other rights a Carrier may have under the Telecommunications Act, at law or in equity. In particular, nothing in this part in any way prevents a party from, in accordance with section 61 of the Telecommunications Act 2001:

(i) exercising its right to enforce compliance with the Equivalent Service Criteria;

(ii) exercising its right to enforce compliance with the LMNP Service Levels; or.

(iii) exercising its right to generally enforce the Commerce Commission LMNP Determination.

Powers of the Enforcement Agency

17.2 Carrier Non Compliance

(a) Where a Carrier complains in writing to the Enforcement Agency that another Carrier is either not complying with the Equivalent Service Criteria or not meeting the required LMNP Service Levels, the Enforcement Agency may initiate an audit of the Carrier in question. The Enforcement Agency

may only commence an audit where a complaint is supported with evidence that, in the view of the Enforcement Agency, establishes reasonable grounds of non-compliance to commence an audit. The Enforcement Agency has the discretion to decline to conduct an audit if it reasonably considers that the breach complained of is not of a significantly material nature to warrant an audit of the relevant Carrier or if the relevant Carrier satisfies the Enforcement Agency that it has remedied the breach.

(b) The purpose of undertaking an audit is for the Enforcement Agency to assess and determine whether, as the case may be, the Audit Carrier has:

(i) complied with the Equivalent Service Criteria; or

(ii) met the LMNP Service Levels; subject to any exemptions granted to the Audit Carrier in respect of the Equivalent Service Criteria or the LMNP Service Levels.

(c) If, prior to the commencement of an audit an Audit Carrier accepts that it has not complied with the Equivalent Service Criteria or the LMNP Service Levels, the Audit Carrier may request that the Enforcement Agency waive the requirement for an audit and move directly to whatever enforcement action is appropriate under the Terms.

(d) A Carrier who having been audited is found to comply with the Equivalent Service criteria cannot be subject to another Enforcement Agency audit to assess compliance with the same Equivalent Service Criteria within the six (6) month period following the completion of that audit.

(e) A Carrier who having been audited is found to comply with the LMNP Service Levels cannot be subject to another Enforcement Agency audit to assess whether it has met the same LMNP Service Levels within the six (6) month period following the completion of that audit.

(f) Where the Enforcement Agency has commenced or proposes to commence an audit of a Carrier, that Carrier must advise the Enforcement Agency of any exemption granted to it by the Commerce Commission relevant to the commenced or proposed audit.

(g) Where the Audit Carrier is exempted from complying with some of its obligations either under the Network Terms in respect of the Equivalent Service Criteria or under the LMNP Terms in respect of the LMNP Service Levels and it is those obligations that would be the subject of the audit the Enforcement Agency will suspend any audit or sanction of the Audit Carrier. Any such suspension will be:

(i) for as long as, and to the extent that, the exemption exempts compliance with the Equivalent Service Criteria or the meeting of LMNP Service Levels; and

(ii) notified to all interested parties by the Enforcement Agency.

17.3 Where requested by the board of the TCF the Enforcement Agency may perform an investigatory and reporting function in respect of the enforcement of Carriers and Service Providers obligations under the IPMS Access Agreement provided to those parties by the TCF.

Audit Procedures

17.4 Notice Period to any Carrier of Audit

(a) The Enforcement Agency shall give not less than five (5) Business Days prior written notice to any Carrier of a decision to undertake an audit of the Audit Carrier. The Enforcement Agency shall specify in reasonable detail those aspects of the service and documentation it proposes to audit and will advise the Audit Carrier who is to undertake the audit.

(b) Any written notice of the Enforcement Agency's intention to conduct an audit must be addressed to the General Counsel/Chief Legal Advisor of the Carrier in question.

(c) The Audit Carrier shall have five (5) Business Days to agree to the audit, accept the allegation of non-compliance with the LMNP Service Levels or the Equivalent Service Criteria and request that the audit not be undertaken, or submit in writing to the Enforcement Agency why the audit should not be undertaken.

(d) The Enforcement Agency will consider any submission made in good faith and will then advise the Audit Carrier within five (5) Business Days whether or not an audit will be undertaken. If no submission is received from the Audit Carrier, or the Audit Carrier advises that it agrees to the audit, the Enforcement Agency may, but is not required to, undertake the audit.

(e) If the Enforcement Agency decides to undertake an audit then the Enforcement Agency shall:

(i) provide to the Audit Carrier, not less than five (5) Business Days notice of the date of the commencement of the audit;

(ii) provide the Audit Carrier a written list of those documents, or such descriptions of the type of documents, it wishes the Audit Carrier to provide to it. Such documents must in the Enforcement Agency's view be necessary to assess whether the Audit Carrier has complied with, as the case may be, the Equivalent Service Criteria or the LMNP Service Levels. Without limitation, this may include documentation pertaining to those documents, records, written practices, data and other documentation within its control that is reasonably necessary to complete an audit; and

(iii) use its reasonable endeavours to conduct the audit in a manner so to provide minimal disruption to the day-to-day business activities of the Audit Carrier.

(f) Within 10 Business Days of receiving a written request from the Enforcement Agency for documents or such longer period as is reasonably required by the Audit Carrier given the nature and volume of the documents requested, the Audit Carrier must supply the Enforcement Agency with the requested documents within its control and that are reasonably necessary to complete an audit.

(g) The Audit Carrier will co-operate fully with the Enforcement Agency to facilitate a timely audit process. Such co-operation extends to an Audit Carrier responding to any reasonable written questions from the Enforcement Agency seeking clarification on any of the documents supplied to the Enforcement Agency.

(h) Where an Audit Carrier fails to supply any requested document(s) it must provide reasons to the Enforcement Agency.

(i) An Audit Carrier is under no obligation to provide the Enforcement Agency with any documentation for which privilege is claimed or in respect of which the Audit Carrier owes obligations of confidentiality to a third party and that third party does not consent to the disclosure.

(j) Failure by an Audit Carrier to supply the Enforcement Agency with requested documentation or respond to written questions clarifying such documentation will be deemed to constitute a non-compliant audit, unless such requests and/or questions are not reasonably necessary to complete an audit. Within 20 Business Days of receiving such requested documents, the Enforcement Agency will provide a copy of the Audit Report to the Audit Carrier setting out its determination (being only a positive or a negative determination) on whether the Audit Carrier has either complied with the Equivalent Service Criteria or met the Service Levels in the LMNP Terms. Such an Audit Report will detail the reasons behind the Enforcement Agency's determination.

(k) The Enforcement Agency will provide the Audit Carrier five (5) Business Days to comment on any audit report provided to it before a final audit report is issued. The Enforcement Agency will forward a copy of the final audit report to all Carriers who were a party to the Number Portability Determination.

17.5 Confidentiality

(a) All confidential information obtained by the Enforcement Agency in conducting an audit must be kept confidential to the Audit Carrier and the Enforcement Agency.

Audit Cost Allocation

17.6 Audit Costs

(a) The Audit Costs associated with completing an Audit Report will comprise of both:

(i) The Enforcement Agency's reasonable direct costs in respect of the audit (including auditing and legal fees); and

(ii) Such costs of the Audit Carrier in respect of time involved in assisting the audit as submitted by the Audit Carrier to the Enforcement Agency and determined by the Enforcement Agency to be fair and reasonable.

(b) The Enforcement Agency is responsible for determining and notifying the costs associated with completing an Audit Report ("Audit Costs") within 10 Business Days from when it determines the costs of the Audit Carrier as submitted are fair and reasonable.

(c) Such Audit Costs as determined by the Enforcement Agency will be payable by:

(i) the Audit Carrier, where an Audit Report concludes that the Audit Carrier has not complied with the Equivalent Service Criteria set out in the Network Terms or the LMNP Service Levels set out in the LMNP Terms, (whichever were alleged to have been breached) irrespective of whether or not the Audit Report was undertaken due to a request from another Carrier; or

(ii) the Carrier at whose request the Audit Report was completed, where the Audit Report concludes that the Audit Carrier has complied with the Equivalent Service Criteria set out in the Network Terms or the LMNP Service Levels set out in the LMNP Terms (whichever were alleged to have been breached).

(d) Where an Audit Report was completed otherwise than due to a request of a Carrier, each of the Enforcement Agency and the Audit Carrier will bear their own costs in the event the Audit Report concludes that the Audit Carrier has complied with the Equivalent Service Criteria set out in the Network Terms.

(e) An Audit Carrier is entitled to be reimbursed its costs by the Enforcement Agency where:

(i) The Audit Report concludes that it has complied with the Equivalent Service Criteria set out in the Network Terms or the LMNP Service Levels set out in the Terms(whichever were alleged to have been breached) ;

(ii) The Enforcement Agency has received payment in full of the Audit Costs from the Carrier at whose request the Audit Report was completed; and

(iii) The Enforcement Agency has determined that the costs of the Audit Carrier are fair and reasonable.

(f) All amounts payable to the Enforcement Agency under this part must be paid in full to the Enforcement Agency within 30 days from when the Service Provider or Carrier (as applicable) is notified of the amount payable. Failure to pay monies due will be treated as a breach of the Terms.

(g) Any reimbursement due of an Audit Carrier's costs must be received within 30 days from receipt in full of the Audit Costs by the Enforcement Agency.

(h) Where a payment is due and not received in full by the Enforcement Agency by the due date, the Enforcement Agency is entitled to interest on the amount outstanding on a daily basis at the rate of the current 90 day bank Bill Rate plus 4%.

17.7 Appendix J outlines which service levels are actively monitored by the Enforcement Agent.

Issues Escalation

18.1 All issues raised are to be entered into the NP Issues Register. The Issues Register will be reviewed monthly at the regular meetings held by the Number Portability User Group and the Issue Register updated where necessary. If the issue is unable to be resolved by the NP User Group or a party feels the issue is taking too long to resolve, the issue can be escalated to the TCF Board for resolution and if necessary further escalated to the Commerce Commission.

System and Network Outages

19.1 The Network Terms outline the processes surrounding Network Outages and an amendment to the LMNP Terms is proposed to include the same for system outages. Sections a) to e) apply to system outages and Network Outages.

a) Subject to item (c) below, in the event that a Carrier identifies that they require an outage in the Carrier's Network or system that may affect LMNP, that Carrier must advise all Parties to the Determination via email at least 5 Business Days before the Planned Outage occurs. Contact details for all Parties to the Determination in relation to outages can be found on the private section of the TCF website under Number Portability. Parties to the Determination are given access to this webpage by contacting the TCF Forum Administrator. If there is any change to the Planned Outage date or time the change must be advised to all Parties to the Determination via phone call and email as soon as possible.

b) Carriers must provide details of all Planned Outages (including any change to those Planned Outages) to the TCF via email 5 days prior to the Planned Outage and the TCF must ensure those details are provided on the TCF website and updated when there is any change.

c) Notwithstanding the above, if a Carrier identifies that they require an outage in the Carrier's Network or system that will impact their ability to perform Network Updates, that carrier must advise all Parties to the Determination via email at least 15 Business Days before the Planned Outage occurs. The backup date for the Outage must be at least 10 Business Days after the original planned date. This is because:

   (i) This impact is greater than merely one party being able to process their own porting activity. An inability to perform Network Updates will stop porting for all parties as no Ports can be marked complete without all Network Updates being completed.

   (ii) Ports cannot be started during the Planned Outage because an inability to complete Network Updates will risk the customer being without a fully operational service while Network Update remains outstanding.

   (iii) Other parties will have to reschedule third party contractors, internal service provisioning and reset customer expectations to work around the outage. This takes extensive time and planning, requiring more notice.

   (iv) Once the Planned Outage is complete there will be a surge in activity as parties catch up on the backlog; this activity needs to be properly anticipated and managed.

   (v) The backup date should be scheduled at least 10 Business Days after the original Planned Outage date to allow for a large enough window for ports to be moved from the original Planned Outage date and not caught by any slippage to the backup date.

d) A TCF LMNP Outage email address has been set up which should be used by Parties to the Determination to advise other Parties of any

Planned or Unplanned Outages. When an email regarding an outage is sent out the subject line of the email should indicate which environment the outage relates to ie. TEST, TRAIN, DEV or PROD. The TCF email address will be notified to the Parties from time to time. At the date this operations Manual was last amended the email address was NP.Outages@tcf.org.nz.

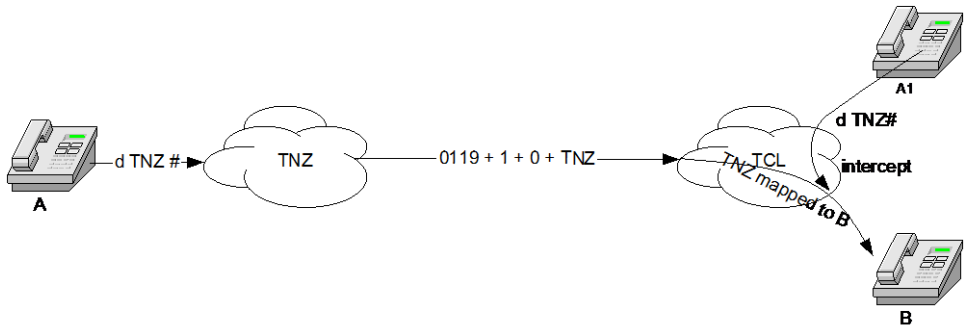
e) Parties to the NP Determination are required to provide the TCF with an email address (and any changes to that email address) to be used by other Parties to the Determination to notify that Party of any Planned or Unplanned Outages. Details of individual Carriers outage contacts can be found on the LMNP Outages/Faults Contacts page which is on the private section of the TCF website. Parties to the Determination are given access to this webpage by contacting the TCF Forum Administrator. These individual email addresses are to be used for any outage notifications if for any reason the TCF email address is not operating correctly.

Call Readdress

20.1 Call Readdress is a network capability between two working numbers, each on a different Service Provider's network that allows one to be diverted to another. Call Readdress is no longer available for new connections to Customers and therefore over time the numbers should diminish with the Porting alternative. There are two types of Call Readdress that exist: Full Call Readdress and Partial Call Readdress.

a) Full Call Readdress

Full Call Readdress, is effectively an alternative name for a donor re route scenario. Donor re route is a valid call forwarding service whereby end-users call the Customer by dialling the listed number which is routed to the donor Carrier. The donor Carrier then Call Forwards to the recipient network with Called Party Number equal to HOC + Call Readdressed Number as shown in the diagram below.



Scenario 1

- Spark Customer (A) dials Spark number that is diverted to VF
- Call forwarded to VF as HOC 0119+1+0+Spark Number

- VF Terminates Call to (B) – Spark Number configured on VF switch to map to (B)

Scenario 2

- VF Customer (A1) dials Spark diverted number
- VF intercepts call and terminates to (B) via Spark # mapped on switch

When a Full Call Readdress Customer originates a call, their CLI is set to the Call Forwarded Number.

Whilst this was a pre-Number Portability mechanism, Full Call Readdress required all calls not ported to the originating Carrier[7] to be sent to the donor Carrier. As this scenario maps simply to the originating Carrier lookup scenario, with its inherent advantages, Full Call Readdressed numbers have been migrated over to the LMNP Port process.

b) Partial Call Readdress

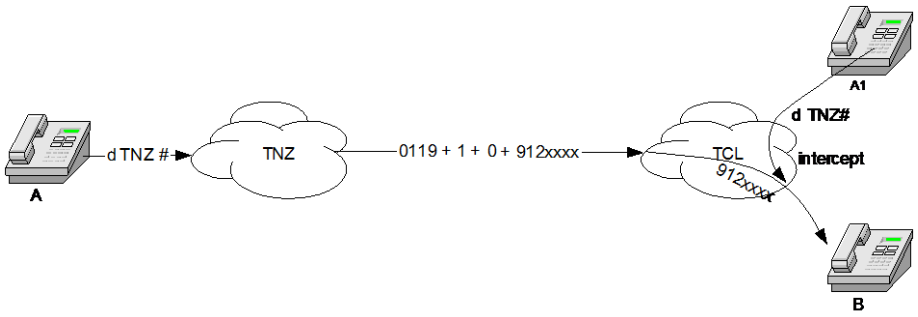
For Partial Call Re-address, the call forwarded Customer is assigned two numbers:

- one number is their original number from the donor network (the "Call Forwarded Number");
- the second number is a number from the call forwarded or recipient Carrier network (the "Recipient Network Number").

End Users can call the Partial Call Readdress Customer by dialling either the Call Forwarded Number or the Recipient Network Number.

If the End User dials the Recipient Network Number, the call is routed directly to the recipient network bypassing the donor switch.

The diagram below illustrates two call scenarios when an End User dials the Call Forwarded Number of a Partial Call Readdress Customer:



Scenario 1

- Spark Customer (A) dials Spark number ported to VF
- Call forwarded to VF as HOC 0119+1+0+VF#
- VF terminates call to (B) VF# e.g. 912 xxxx

Scenario 2

[7] Interceptions are in place to trap calls to numbers ported to the carrier originating the call

- VF Customer (A1) dials Spark number ported to VF
- VF intercepts call and terminates to VF 912xxxx (B)

c) Call Readdress Procedures

The Gaining Service Provider (GSP) is to provide all Customer details including the number to be ported and the Partial Call Readdress number associated to it.

The LMNP Terms state it is the responsibility of the GSP to prepare the Port Request. The Port Request must include the data required as per Appendix 1, table 1 of the LMNP Terms. Subject to clause 4.2.4 of the LMNP Terms, the Losing Service Provider (LSP) is not obliged to advise the GSP of additional Numbers beyond those included in the Port Request (see clause 5.3.1.(c) of the LMNP Terms).

However, when the LSP checks the Port Request, subject to clause 8.1.7(e) of the LMNP Terms, the LSP enters its understanding of the details if they differ from the information presented by the IPMS and this can include the addition or removal of Numbers for a Multiple Number Port (see clause 8.1.7(d) of the LMNP Terms).

d) GSP Rules for Partial Call Readdress

The following rules MUST then be adhered to by the GSP for the successful approval of Partial Call Readdress numbers to be ported via LMNP process.

(a) Load port request with correct LSP and Customer a/c number. All Call Readdress associated numbers to be ported must be shown including numbers that may not be required (i.e. both VF and Spark);[8]

(b) Use checkbox and tick if specific numbers are "not required";

(c) Submit as per standard rules;

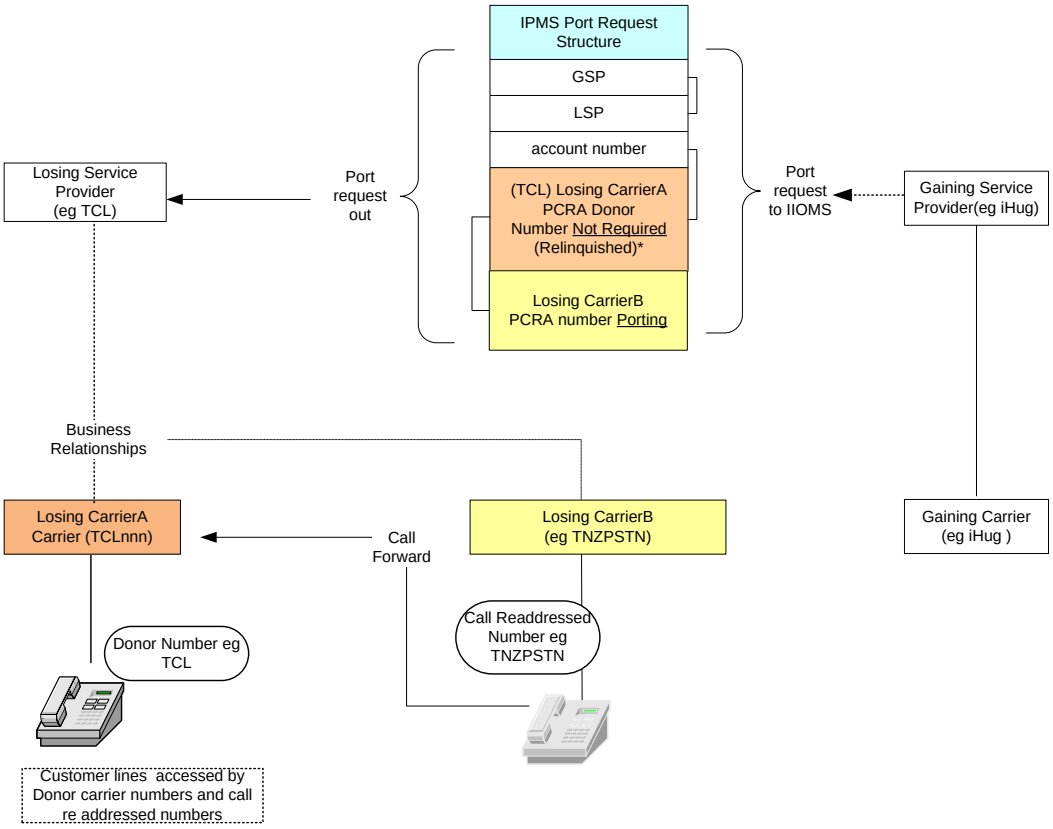
(d) IPMS will reject giving a reason that a specific number requested is not owned by the LSP specified. When this occurs reconfirm that the LSP is correct and tick the "Override Service Provider" checkbox and resubmit; and

(e) In "Additional Customer Information" field please add "Call Readdress".

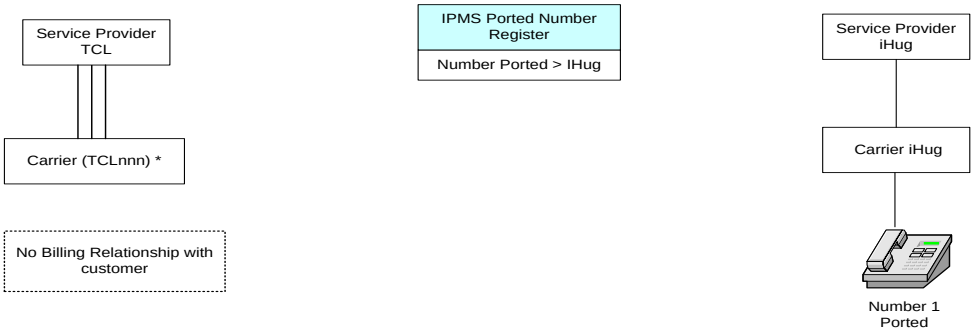
[8] Where Partial Call Readdress numbers are not known by the customer, the customer should in the first instance, seek the information from the LSP. The customer may also authorise the GSP to seek this information on their behalf from the LSP who is to assist in providing it through an agreed escalation process.

Scenario 1

Customer has a call re addressed number and a donor number. They want to port the readdressed number and relinquish the donor number.



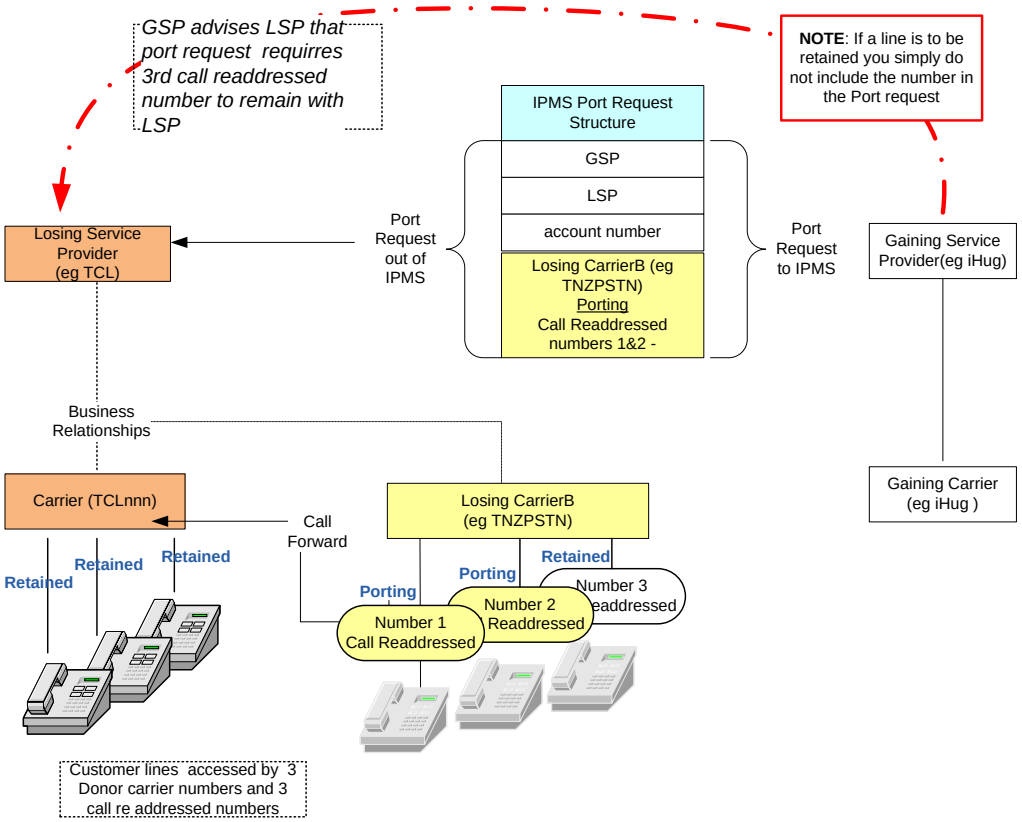
Post Port Status



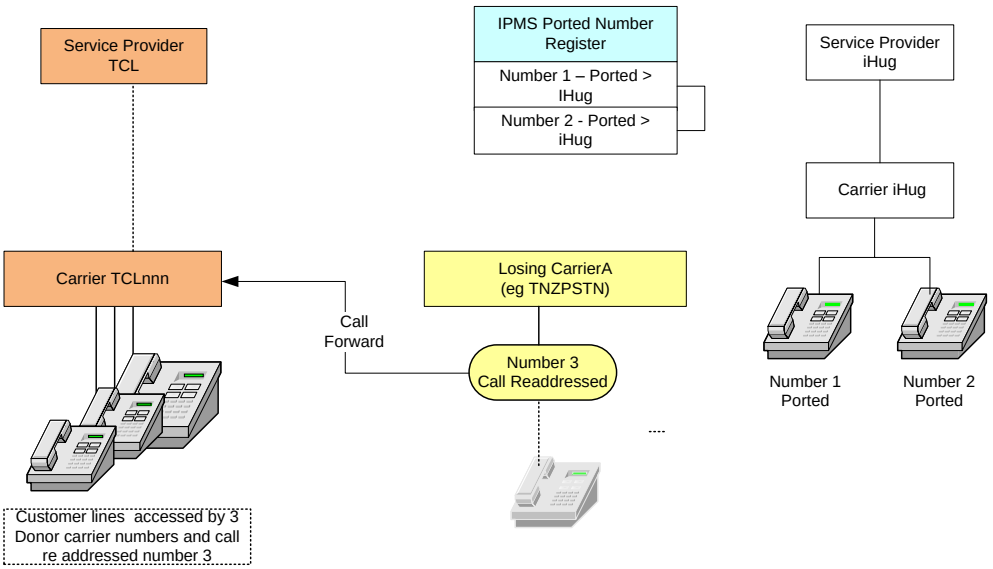
e) Customer has requested that one number remain with the existing network?

If Customer requests to remain with both GSP and LSP by splitting the Call Readdress related numbers this must be communicated through standard escalation process before submitting request for validation

Scenario 1
Customer has three Call Readdressed numbers and three donor numbers. They want to port two of the readdressed numbers and retain the three donor numbers and one of the call readdressed numbers.



Post Port Status



f) Call Readdressed ports involving resellers

Where the LSP is a reseller and the port request includes the porting out of resold Partial Call Readdressed numbers, the wholesaling company is to ensure that business processes are in place whereby the reseller is able to gain access to the Partial Call Readdress number information.

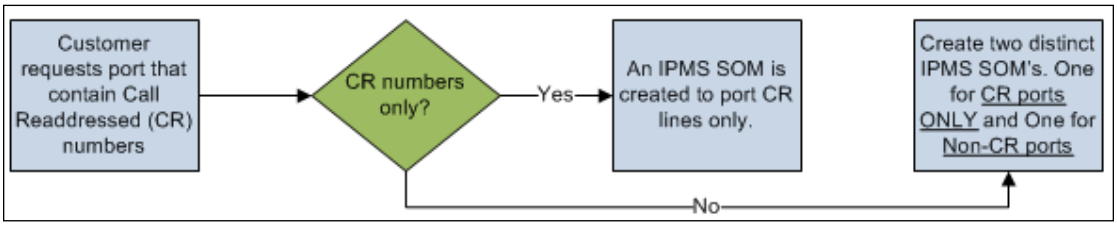
This is applicable to two scenarios:

- Where the GSP has told the Customer to approach the LSP (reseller) to gain the necessary Call Readdress information.
- Where the reseller is both LSP and GSP ie change of Carrier, no change of Service Provider for ports involving Call Readdressed numbers.

Where the LSP is a reseller, the appropriate IPMS Carrier/Service Provider relationships are to be in place such that Port Request of the call readdressed number is validated by IPMS without the need for invoking the SP Override function in IPMS.

g) Customer has requested to port numbers that are Call Readdressed and non-Call Readdressed?

IPMS SOM requests must not contain both Call Readdressed and Non-Call Readdressed lines.


Customer requests port that contain Call Readdressed (CR) numbers
CR numbers only?
Yes
An IPMS SOM is created to port CR lines only.
Create two distinct IPMS SOM's. One for CR ports ONLY and One for Non-CR ports
No

Appendix A. Bilateral Agreement Check List

The purpose of this section is to provide an indicative list of the items which, eventually, would need to be discussed and approved in the Bilateral Agreement between two Service Providers who are parties to the LMNP Terms.

LMNP BILATERAL DISCUSSION KICK-OFF QUESTIONNAIRE

OVERVIEW

> "*In a Number portability environment changes are required to the traditional way in which calls are routed from originating Carriers to terminating Carriers. For voice services, this applies to local, national, fixed-to-mobile, mobile-to-fixed, mobile-to-mobile, incoming and outgoing international and other calls involving local or mobile numbers.*"
> …….……Pg 4 of Network Terms for Local & Mobile Number Portability in New Zealand [29.08.2005]

This document is intended to be used by New Zealand telecommunications network operators to initiate bilateral technical negotiations with other network operators aimed at facilitating agreement about the call handling interworking arrangements to be used in the Local and Mobile Number Portability (LMNP) environment.

Interworking arrangements between networks will need to specify which of the several options allowed for in the Network Terms will be implemented by network operators for handling calls passed across the boundaries between their networks when Number Portability is operational. Specifically, each network that originates calls, or transits toll bypass calls, must either:

- Perform a call-by-call lookup of a Number Portability database to determine whether a called number is Ported, and if it is Ported, determine the Recipient Network (identified by the 011xn7 Handoff Code (HOC) that now hosts the number, and then route the call towards that network by appending the HOC to the Called Party Number,

OR

- Pass the call to another network which is delegated to perform all or part of the above function on its behalf. In this case there are further options allowed by the Network Terms that must be selected. These cover the format of the Called Party Number signalled with the call, and whether the call is to be onward-routed by the delegated network, or released for Query on Release (QOR) action or for Redirection action by the originating (or transit) delegating network.

In addition, network operators need to confirm other aspects of LMNP call handling such as default call routing under abnormal circumstances such as database failure, and methods of protecting the network against call recirculation.

USING THE TEMPLATE

This template is designed as a tool to help network operators implement LMNP. It has been drafted as a guideline only and is not compulsory.

The information collected from this questionnaire will be treated as confidential between the parties and will not be disclosed to any other party, unless such disclosure:

- is agreed to by the parties; or
- is required by law.

The information is intended to be used as an input to bilateral negotiations to determine the necessary changes to call handling functionality required to implement LMNP. The agreed network arrangements will then be documented and included in a revised interconnection agreement between the network operators.

Terminology used in this document is in accordance with the reports "LMNP Terms" and "Network Terms" dated 31.08.2005.

NOTES ABOUT THE QUESTIONNAIRE

Q1 – Q4: relate primarily to your network acting as a Recipient Network hosting numbers Ported from other networks, and will only be applicable if you provide a (terminating and originating) local service to Customers. The information will enable other networks to set up call routing data required to deliver calls to numbers Ported into your network.

Q2: Actual allocation of HOCs is done via the Number Administration Deed (NAD – www.nad.org.nz). Most Carriers are expected to have a single 011xnt (t=7, 8, or 9) value assigned, however some are proposing to use multiple codes where they support two or more distinct networks. Separate HOCs are expected for fixed and mobile applications operated by the same carrier.

Q3 & Q4: This information will assist with confirming that call recirculation cannot occur in abnormal situations.

Q5 & Q6: indicate whether your network will consult a Number Portability database itself to determine call routing [case (a)], or will delegate this function to another network by routing calls to that network without first consulting a database [case (c)].

Case (b) is a mixed case where your network checks some number ranges, and delegates checking other number ranges to another network. For cases (b) and (c) this information in conjunction with **Q7** will enable other network operators to offer to act as a delegated network to consult their Number Portability databases on your behalf.

Note that only Customers' local (fixed network) and mobile numbers are able to be Ported under LMNP. Therefore no changes are required to the routing of calls to numbers delivered on the interconnect boundary in other formats (e.g. 0800, 0900, 010, 111 etc.).

Q7 & Q8: This information will enable the network(s) with which you are directly interconnected to set up call routing data to transit to the relevant Recipient Networks calls destined to Ported (and non-Ported) numbers that have been received from your network. NOTE that the descriptions 0a(2-8) and 0A9 are typical of the ranges described, but not exhaustive.

Q9: covers the details of call handling in the situation where you intend to delegate Number Portability database consultation to another network. It will need to be completed as an

iterative process in conjunction with the delegated network; therefore it may not be possible to complete some parts of Q8 on the initial pass.

Note that the delegated network [identified in Q9(c)] does not necessarily need to be directly interconnected with your network. By using the 011xn8 and 011xn9 HOCs to identify the delegated network, calls can be routed via a transit network [identified in Q9(a)] (which will not consult the database) to the specified delegated network (which will). Where the delegated network is directly connected to your network the use of a HOC is optional if the default action is for the delegated network to consult the database for all incoming calls on a given incoming route (as will be the case for international incoming calls, for example, because they will never include a HOC). In this situation there is no need to change the existing called party number format passed between the delegating and delegated networks.

9(d) is used to identify which of three call routing mechanisms allowed for by the LMNP Terms (Onward Routing, Query on Release [QOR] or Redirection) you wish to operate in conjunction with the delegated network. If QOR or Redirection are to be used there will need to be further detailed technical discussions as these functions are not supported in the PTC331 No.7 Signalling standard currently used for network interconnection in New Zealand.

Q10: This information will assist with confirming that recirculation cannot occur in abnormal situations.

Q11 & Q12: This information will advise other networks whether your network can act as a delegated network and consult a Number Portability database on another network's behalf, and if so, the specific method(s) of call routing available.

Q13 & Q14: This information can be used to progress the resolution of issues concerning geographic-origin based routing in the LMNP environment.

Carrier Name	
Contact Person	
Contact email address/telephone	
Date questionnaire completed	

Q	QUESTION	ANSWER (please ☒ as appropriate)		
1	*Will your network act as a Recipient Network for Ported numbers (i.e. will you be, or host, one or more Gaining Service Providers)?*	(a) NO – go to Q4		☐
		(b) YES – go to Q2		☐
2	*What **011xn7** Hand-off Code(s) (HOC) will your network accept as a prefix to the called party's national number with incoming calls to Ported Customers hosted on your network?* *Please insert HOC values and description if more than one HOC is used* *NOTE: The 011XN7 HOCs are allocated by the NAD*	HOC	Comment	

Q	QUESTION	ANSWER (please ☒ as appropriate)	
		- go to Q3	
3	*What action will your network take if it receives a call from another network with **the called party number prefixed with one of your 011xn7 HOCs** (from Q2), but cannot terminate the call because the number range is not installed or the number is not allocated to a Customer on your network?* *(i.e. other network's database is not up-to-date)* ***NB** the Cause Value in question 3(a) is the Cause Value sent over the interconnect boundary.*	(a) always release the call (Cause Value =)	☐
		(b) other (please describe)	☐
		NOTE: To prevent any possibility of recirculation your network must NOT change or delete the received HOC and onward-route the call! *- go to Q4*	
4	*What action will your network take if it receives a call from another network with **the called party number in the format 0+NN**, where NN is a number range allocated to your network, but cannot terminate the call because the number is not allocated to a Customer on your network?* *NN= National Number* ***NB** the Cause Values in question 4(a) and (b) are the Cause Values sent over the interconnect boundary.*	(a) always release the call (Cause Value =)	☐
		(b) determine if the number has Ported to another network & if so, attach 011xn7 HOC and onward route the call. Otherwise release the call (Cause Value =)	☐
		(c) other (please describe)	☐
		- go to Q5	
5	*For calls to NZ local network Customers' numbers* • *originated by Customers (if any) on your network, and/or* • *transited by your toll bypass network (if any)* ***will your network check a Number Portability database** to determine the Ported status of the called number, and, if Ported, determine the HOC identifying the Recipient Network (before routing the call to another network)?*	(a) YES – for ALL called local network numbers	☐
		(b) YES – for some called local network numbers	☐
		(c) NO	☐
		- go to Q6	

Q	QUESTION	ANSWER (please ☒ as appropriate)		
6	*For calls to NZ mobile network Customers' numbers* • *originated by local Customers (if any) on your network, and/or* • *transited by your toll bypass network (if any)* ***will your network check a Number Portability database** to determine the Ported status of the called number and, if Ported, determine the HOC identifying the Recipient Network (before routing the call to another network)?*	(a) YES – for ALL called mobile network numbers		☐
		(b) YES – for some called mobile network numbers		☐
		(c) NO		☐
		- go to Q7		
7	*For which Customers' number ranges will your network **consult a Number Portability database** to determine porting status and, where Ported, determine the HOC identifying the Recipient Network?* *(A=area code digits 3,4,6,7,9)* *(Please split the number ranges if required to differentiate)*	Not applicable as Q5(c) and Q6(c) both apply. *- go to Q9*		☐
		021	Vodafone mobile range	☐
		027	Spark mobile range	☐
		029	Vodafone mobile range	☐
		02x	Other non-Spark mobile ranges	☐
		0A(2-8)	Spark local ranges ranges	☐
			Your network's own ranges	
		0A9	Other non-Spark local (fixed line) ranges	
			• *Other network's number ranges as appropriate*	
			Other network's number ranges as appropriate	
		- go to Q8		
8	*To which network(s) will you deliver calls to NZ local and mobile network Customers' number ranges whose porting status **has been determined by your network** and found to be either (i) Ported to Recipient Networks identified by 011xn7 HOCs as follows; or (ii) not ported?*			

Q	QUESTION	ANSWER (please ☒ as appropriate)			
	Recipient Network	*HOC*	*Calls will be routed on <u>direct</u> routes to the following Network:*	*Calls will be routed on <u>alternate/overflow</u> routes to the following Network:*	
	For example *Big Bird Networks*	011747	Internally Routed	Not applicable	
	For example • *Spark*	011647	Spark	No overflow routing via other networks	
	2Degrees Mobile	011507			
	Call Plus	011207			
		011227			
		011257			
		011547			
		011577			
		011587			
		011867			
		011997			
	Compass	011217			
	Link Telecom	011517			
	NOW (formerly NOW)	011667			
	Orcon	011677			
	Symbio Networks	011537			
	Spark (local)	011657			
	Spark (mobile)	011647			
		011697			
	Vodafone (TCL) local	0114b7 b=0-9			
	Vodafone (local)	011237			
		011247			
	Vodafone (mobile)	011937			
	Woosh	0112a7 a=6-9			
	WorldxChange	011987			
	……. - *go to Q9*				
9	*How & where will you deliver calls to those NZ fixed and mobile network Customers' number ranges whose porting status **is NOT checked by your network?***				

Q	QUESTION	ANSWER (please ☒ as appropriate)			
		Not applicable as Q5(a) and Q6(a) both apply. *- go to Q10*			☐
		(a) Calls will be routed on direct routes to the following Network(s)…….:	(*please specify network. NB this network will be referred to as Network x in Q 9[c]*)		
		(b)…. with the called party number parameter sent on the direct route in the following format:	either:	0+NN	☐
			or:	011xn8+NN (xn=)	☐
			or:	011xn9+NN (xn=)	☐
			(*please specify xn value if used*)		
		(c) Database lookup will be performed by the following Network(s) delegated to do this on your behalf	(*if 0+NN format is used in 9[b], then this network must be the same as Network x*)		
		(d) What action do you want the delegated network to take if it determines that a number is Ported?	either:	attach 011xn7 HOC to called party number and onward route	☐
			or:	release call with Cause Value 14 (for QOR treatment in your network)	☐
			or:	release call with Cause Value 23 & Redirecting Number (for Redirection treatment in your network)	☐
		- go to Q10			
10	*What action will your network take if it attempts to consult a Number Portability database to determine the Ported status of a called number, but finds that the **database is unavailable**?*	Not applicable as Q5(c) and Q6(c) both apply. *- go to Q13*			☐
		(a) always release the call			☐
		(b) route the call based on the called number (i.e. assume that the called number is not Ported)			☐
		(c) other (*please describe*)			☐
		- go to Q11			
11	*Is your network able to act as a delegated*	(a) NO *- go to Q13*			☐

Q	QUESTION	ANSWER (please ☒ as appropriate)	
	network and consult a Number Portability database on behalf of other networks?	(b) YES *- go to Q12*	☐
12	*Which method(s) of call handling does your network offer when acting as a delegated network, when a called number is found to be Ported?*	(a) will attach 011xn7 HOC to called party number and onward route	☐
		(b) will release call with Cause Value 14 (for QOR treatment in the delegating network)	☐
		(c) will release call with Cause Value 23 & Redirecting Number (for Redirection treatment in the delegating network)	☐
		- go to Q13	
13	*Is your network able to support the sending of the ITU-T ISUP Location Number parameter with calls made by Ported numbers hosted on your network (to identify the geographic location of the Customer to other networks receiving the calls?*	(a) Not Applicable (as Q1(a) applies)	☐
		(b) NO	☐
		(c) YES	☐
		- go to Q14	
14	*Is your network able to receive the ITU-T ISUP Location Number parameter with incoming calls from other networks and use the information contained in the parameter in geographic-origin based call routing (e.g. typically for 0800/0808 & 0900 calls)?*	(a) Not Applicable (as geographic-origin based routing is not used)	☐
		(b) NO	☐
		(c) YES	☐
15	Other Comments:		
	end of questionnaire		

Appendix B. IPMS Management

This section, and the definitions it contains, relate exclusively to the IPMS.

"**Fault**" means the failure, in whole or in part, in the supply of, or a material degradation in the quality of, the IPMS or a failure to provide any data, report or document to TCF or Service Providers or Carriers as required by the IPMS Agreement and the Number Portability Determination;

"**Fault Severity**" means the level of severity of any Fault, as determined by TCF, in accordance with the following:

Severity	Definition
Critical	• IPMS is unavailable to TCF or Service Providers or Carriers; or • severe operational impact degrading the performance or outputs of the IPMS; or • the IPMS (or any output from the IPMS including TCF Data) is affecting the integrity or correct operation of any telecommunications network used by any Service Providers or Carriers.
High	Significant operational impact affecting portions of the IPMS or impacts on the ability of the IPMS to perform effectively.
Medium	Allows the IPMS to continue to operate (possibly with a work-around in place (at no additional cost to TCF, unless agreed otherwise with TCF in writing)) but a minor part of it is unavailable or not working as contemplated under this Agreement.
Low	Non critical to TCF or Service Providers or Carriers.

"Help Desk" means System Administrators Help Desk which is contacted by telephone or email as set out in section 5 of Appendix B, or such alternative phone number or email address as the TCF may, from time to time, advise Service Providers or Carriers in writing;

"IPMS Planned Outage" means the temporary unavailability of the IPMS in order for the System Administrators to carry out any testing, repair or maintenance which is reasonably required in respect of the IPMS;

"Performance Levels" means the performance criteria to which the System Administrator will provide the management services as described in section 4 of Appendix B;

"Resolution Time" means the period from the time a Fault is discovered by the System Administrator or is logged by the TCF or a Service Provider or Carrier (in accordance with this Manual) (whichever is the earlier) until the time that Fault has been Resolved (inclusive);

"**Resolved**" means that a Fault has been rectified and the IPMS has been returned to normal operating conditions as reasonably determined by TCF or a Service Provider or Carrier (and "**Resolution**" shall have a corresponding meaning);

"**Response Time**" means the period from the time a Fault is discovered by the System Administrator or is logged by TCF or a Service Provider or Carrier (in accordance with this Manual) (whichever is the earlier) until the time the System Administrator has advised TCF and Service Providers and Carriers that it has commenced action to diagnose and rectify the Fault (inclusive);

"System Administrator" means the party appointed by the TCF from time to time to maintain and operate the IPMS.

"TCF Coordinator" means the person appointed by TCF and notified to the Service Providers and Carriers from time to time to liaise with the System Administrator and/or Service Providers and Carriers on matters relating to the IPMS;

"TCF Data" means data owned or supplied by TCF or a Service Provider or Carrier to which the System Administrator is supplied access and data which may be generated, compiled, arranged or developed in providing the IPMS;

"TCF Facilitator" means the person appointed by TCF and notified to Service Providers and Carriers from time to time to liaise with the System Administrator and/or Service Providers and Carriers on matters relating to the IPMS for escalation purposes.

2 Support Services

- The following support services shall be available:

The TCF will procure that the System Administrator shall make available the Help Desk to the Service Providers and Carriers on a 24 hour 7 day per week basis, for the purpose of reporting and resolving Faults and operational issues or enquires that arise in relation to the IPMS. The TCF shall notify Service Providers and Carriers in writing of any changes that occur to the relevant telephone or email address of the Help Desk set out in section 5 of Appendix B.

(i)

- The Help Desk will maintain:
  - a reception point for logging Faults and enquires;
  - Fault progress tracking and reporting;
  - IPMS outage tracking;
  - for the duration of any Fault, direct contact, as reasonably required by the relevant Service Provider or Carrier, between the System Administrator and that Service Providers or Carrier's specialist operations groups; and
  - a co-ordination point for the restoration of the IPMS.
- The TCF shall procure that the System Administrator shall, through the Help Desk and after becoming aware of any Fault in respect of Service Providers and Carriers:

- take all action reasonably necessary in order to rectify that Fault, with as little disruption to Service Providers and Carriers as is reasonably possible and in any event in accordance with the Performance Levels;

- advise the TCF Co-ordinator and the relevant Service Providers and Carriers of any actions being taken in order to rectify the Fault;

- provide the TCF Co-ordinator and the relevant Service Providers and Carriers with an estimate of the time required to rectify the Fault;

- provide the TCF Co-ordinator and the relevant Service Providers and Carriers with ongoing progress reports in respect of the actions being taken to rectify the Fault in accordance with the times for the relevant update frequency specified in the Performance Levels as set out in section 4 of Appendix B.

- The Service Providers and Carriers shall be responsible for managing its own staff training in relation to the use of the IPMS and shall not call the Helpdesk for this unless agreed otherwise with the TCF Co-ordinator.

- A breach of the Performance Levels specified in section 4 of Appendix B shall exclude any breach which arises:

  - due to an event of force majeure; or

  - due to a material default by the Service Providers and Carriers of any of its obligations under its Agreement with the TCF; or

  - due to a material default by the TCF of any of its obligations under the agreement with the System Administrator or any other support provider other than the obligation to make payment to those parties; or

  - due to any material default under any IPMS Access Agreement with the Service Provider or Carrier or between the TCF and any other Service Provider or Carrier; or

  - from any act or omission by a the Service Provider or Carrier, their officers, employees, agents, Contractors or consultants or any other person for whom the Service Provider and Carrier is responsible other than any act or omission taken or not taken (as the case may be) at the direction of the TCF, its officers, employees, agents, Contractors, sub-Contractors; or

  - as a direct result of the malfunction of a Service Provider or Carrier connection or equipment or any other connection or equipment which is not under the control of the TCF; or

  - during any Planned Outage.

3 Faults

- Nothing in this Agreement shall require the TCF to provide continuous or fault free access to the IPMS.

- The Service Providers and Carriers shall comply with such specific procedures and obligations in relation to the management of Faults as reasonably required by the TCF.

- The TCF shall procure that the System Administrator shall monitor the IPMS on a 24 hour per day / 7 day per week basis for the purpose of early identification of any Faults, or any circumstances that might reasonably give rise to a Fault.

- On becoming aware of any Fault, Service Providers and Carriers agree that they shall check that the Fault relates to the IPMS prior to notifying the Help Desk. If, after such checking, the Service Provider or Carrier still believes (acting reasonably) that the Fault is with the IPMS System, the Service Providers or Carrier shall notify the Help Desk by phone (at any time) or by email (only recommended during Working Hours) as soon as reasonably practicable. Each such notice shall specify:

  - details of the nature of the Fault; and

  - the Fault Severity of that Fault.

4 Response Time

- Upon becoming aware of any Fault in the IPMS, the TCF shall ensure the System Administrator shall comply with the Response Times and Resolution Times in relation to rectification of that Fault and will use its best endeavours to respond to all Faults within a shorter timeframe.

- Only Faults with Critical or High Fault Severity Level will require a Response outside of Working Hours unless otherwise approved by the TCF Co-ordinator or the TCF.

- The TCF shall procure that the System Administrator will provide an incident report to the Service Providers and Carriers affected by the incident, within 1 Working Day of Resolving a Fault, for all Faults with a Critical or High Fault Severity Level plus any other logged Faults specifically requested.

IPMS Planned Outages

- Subject to sections 3.6 and 3.7 of Appendix B, the TCF shall use its best endeavours to ensure that all IPMS Planned Outages occur between 12.00am and 04:00am on the first Sunday of each month, and that the IPMS Planned Outage does not exceed these hours.

- Subject to sections 3.6, 3.7 and 3.8 of Appendix B, the TCF shall procure that the System Administrator shall give the Service Providers and Carriers and the TCF Co-ordinator a minimum of 2 Business Days prior written notice of any IPMS Planned Outage. Each such notice shall include the following information:

  - the reason for the IPMS Planned Outage;

- the proposed date and time of the IPMS Planned Outage;
- the estimated duration of the IPMS Planned Outage; and
- the name and contact details of the appropriate person whom the Service Providers and Carriers should contact for further information in relation to the IPMS Planned Outage.

- Where the proposed date and time for the IPMS Planned Outage is outside of the timeframe specified in section 3.4 of Appendix B and is:

  - outside Working Hours, the notice period referred to in section 3.5 of Appendix B for the IPMS Planned Outage shall be a minimum of 1 Business Day; or
  - within Working Hours, the notice period referred to in section 3.5 of Appendix B for the IPMS Planned Outage shall be a minimum of 10 Business Days,

  and in either case, the notice to the Service Providers and Carriers shall include the information referred to in section 3.5 of Appendix B and the reason why the IPMS Planned Outage is occurring at that time.

- If the TCF considers (acting reasonably) that any IPMS Planned Outage requires the Service Providers and Carriers to:

  - undertake staff training; or
  - assist with the IPMS Planned Outage,

  then if the date and time of the IPMS Planned Outage is within the timeframe specified in section 3.4, the TCF shall, subject to section 3.8 of Appendix B, procure that the System Administrator gives the Service Providers and Carriers a minimum of 10 Business Days notice or a shorter notice period if agreed by all Service Providers and Carriers.

- Where:

  - the IPMS Planned Outage is as a result of a major enhancement to the IPMS (as reasonably determined by the TCF), then the TCF will endeavour to consult with each Service Provider and Carrier prior to the System Administrator giving notice to agree the length of the notice period, and the TCF shall procure, notwithstanding section 3.7 of Appendix B, that the notice period shall be a minimum of 20 Business Days or such longer period as agreed to by the TCF;
  - the circumstances giving rise to a IPMS Planned Outage are such that an immediate, temporary suspension or restriction of the IPMS is required and the System Administrator is not able to give notice as set out above, the TCF shall procure that the System Administrator shall use its best endeavours to provide the TCF Co-ordinator and the Service Providers and Carriers with such prior notice as is reasonably possible in the circumstances.

5 IPMS Performance Levels

- The TCF shall endeavour to meet the following Performance Levels:
  - Subject to section 1.5 of Appendix B, the TCF shall use reasonable endeavours to ensure the IPMS is available 99% (at all times) per quarter.
- The maximum Response Times and Resolution Times are:

Fault Severity	Response Time	Resolution Time	Update Frequency
Critical	30 minutes	4 hours	Every 45 minutes
High	1 hour	8 hours	Every 2 hours
Medium	10 hours (1 day)	50 hours (5 days)	Every second day
Low	20 hours (2 days)	100 hours (10 days)	Every Week

- For Faults with a Critical Fault Severity Level, the Response and Resolution Times are based on elapsed hours, all other Fault Response and Resolution Times are based on Business Hours.
- Critical and High Fault Severity Response Times and Resolution Times will only be applied to the production environment. The test and training environment is expected to have a lower priority under normal circumstances.

6 IPMS Monitoring

- The TCF shall procure the continual proactive (24 hours per day 7 days per week) monitoring of the IPMS to enable early notification of failures Faults or issues.

Escalation

- If a Fault is unable to be resolved by the System Administrator within a reasonable timeframe then the relevant Service Provider or Carrier may escalate the problem in accordance with the timeframes identified in the Performance Levels to the System Administrator personnel identified in the Table below.

The Service Provider and Carrier /the TCF Interface

- Each Service Provider and Carrier, by written notice to the TCF and the TCF Co-ordinator, shall appoint a user administrator ("User Administrator") and shall maintain the appointment of a User Administrator throughout the term of this Agreement. The relevant Service Provider and Carrier may replace, from time to time, by written notice to the TCF and the TCF Co-ordinator, their User Administrator.
- The principal function of the User Administrator shall be to manage the relationship between the relevant Service Provider and Carrier and the TCF Co-ordinator and the relationship between the relevant Service Provider and Carrier and the System Administrator, in each case, in accordance with this Manual.

IPMS Escalation Roles and Responsibilities

- Level 1 Contact Points:

System Administrator Help Desk

Responsibility: Management of Call Centre, initial logging of events and escalation of issues.

Contact Details: TBA prior to commencement for Management Services

- TCF member contacts

Responsibility: Assistance to System Administrator, Future sourcing as required, and liaison with users.

Escalation/ Level	Role	Responsibility	Contact Details
Vendor			
Level 2	Site/Client Manager	Monthly Reporting Change Control Escalation of issues	TBA prior to commencement for Management Services
Level 3	Manager Managed Services	Escalation of issues	TBA prior to commencement for Management Services
Level 4	NZ Director of Vendor Professional Services	Escalation of Issues	TBA prior to commencement for Management Services
TCF			
Level 2	TCF Coordinator	Escalation of issues	NP Co-ordinator. Refer www.tcf.org.nz for contact details.
Level 3	TCF Facilitator	Escalation of issues not able to be resolved with TCF Coordinator	TCF Forum Administrator. Refer www.tcf.org.nz for contact details.
Parties to the NP Determination			
Representative of each Party to the Number Portability Determination	User Administrators		Refer www.tcf.org.nz for contact details.

- The TCF may add, amend, delete information in section 5.5 and 5.6 of Appendix B, from time to time by notice in writing to the Service Providers and Carriers.

7 Managing the Load on IPMS

The performance of IPMS is impacted primarily by the following factors:

- the polling frequency of API calls;
- the number of Carriers;

- the number of outstanding ports of a given status;
- the amount of time that SOMs spend in-progress; and
- the number of SOMs being processed per month.

As IPMS is solely a reactive system, it cannot control the load and is completely dictated to by the users of the system. The following frequencies were set by HP in the interests of keeping IPMS running smoothly.

Recommended API Polling Frequency (from section 4.5 of the IPMS Technical Specification)

Operation	Conditions	Max Frequency
getRequestedPorts	Filter My SP Action + Date	5 mins for mobile Service Providers 10 mins for local Service Providers
getApprovedPorts	Filter My Carrier Action + statusList + Date	May be called once for each possible Status in the statusList filter within the following periods: 2 mins for mobile Service Providers 10 mins for local Service Providers
getPortProgress	SOM	Once every 5 minutes for each port during activation
getNetworkUpdates	CarrierIdList filter set to null	Once every 10 mins. Set CarrierIdList filter to null to return network updates for all Carriers associated with the user/company.
getApprovedPortChangeRequests	My SP Action	15 mins

APIs called by automated processes can inflict considerable load on the system. Where a Carrier's system is doing more than what is considered safe, they may be asked to reduce the load. Basic methods to do this include:

- slowing down the frequency of calls;
- reducing the frequency of polling for given events after a certain amount of time (eg reduce frequency of getPortProgress after half an hour for a given port and again after four hours); and
- escalating repeated failures (especially security failures, such as 620, PASSWORD_EXPIRED).

Appendix C. Change Request Form

TCF Reference:	
Project Name:	**Reference:**
Module:	**Date:**
Change Title:	
Submitted by:	**Phone:**
Change Type:	Specify one of problem, enhancement or other
Severity:	Specify serious, moderate, minor or cosmetic
Description:	

Appendix D. IPMS Parameter Change Form

IPMS Parameter Change Specification

		Change Number	Cx
Outline	*Note: where work involves change in Donor Carrier, Host Carrier or Service Provider, a Special Project may be required*		
IPMS environments	IPMS Dev	Date of change	N/A
	IPMS Test	Date of change	N/A
	IPMS Prod	Date of change	TBA
	IPMS Train	Date of change	N/A
Proposed by		Date of request	
Company		Telephone No:	
NPUG Status		Internal Status	

Table: Company		**(Technical Specification Reference 3.5.3)**
Action	**Company ID**	**Company Name**
[Create|Delete]		

Table: Service Provider			**(Technical Specification Reference 3.5.4)**
	Record 1	Record 2	Record 3
Action	*[Create|Modify|Delete]*	*[Create|Modify|Delete]*	*[Create|Modify|Delete]*
Service Provider ID			
Service Provider Name			
Company ID			
Min Account Length			
Max Account Length			
Auto-Approve Port Requests within Service Provider			
Auto-Approve Port Requests within Company			
Auto-Accept APC within Service Provider			
Auto-Accept APC within Company			
AccountNumberType			

Table: Carrier			**(Technical Specification Reference 3.5.5)**
	Record 1	Record 2	Record 3
Action	*[Create|Delete]*	*[Create|Delete]*	*[Create|Delete]*
Carrier ID			
Carrier Name			
Company ID			
Carrier Type			
Min Handset Ref Length			
Max Handset Ref Length			
GC Receive Own Ports			
LC Receive Own Ports			
Receive Own RQs			
GC Confirm Port Withdrawal			
LC Confirm Port Withdrawal			
GC Confirm Port Expiry			
LC Confirm Port Expiry			

Table: Carrier-Service Provider			**(Technical Specification Reference 3.5.8)**
Action	Service Provider ID	Carrier ID	Read Only

[Create|Delete]			
[Create|Delete]			

Table: Number Range					**(Technical Specification Reference 3.5.2)**	
Action	IPMS Donor Range	Phone Number Prefix	Donor Name	Donor ID	Description (Local/Mobile)	LICA (See Note i)
[Create|Delete]						
[Create|Delete]						
[Create|Delete]						

Note i: The LICA field is not used by IPMS. It has been included as carriers require this information to set up their network routing tables. Appendix 1 lists valid LICAs.

Table: Queuing By Number Range		**Technical Specification Reference 3.5.15)**				
Action	Carrier ID	Carrier Name	Enabled	Number Range	Network Type	Donor Name
[Create|Delete]						
[Create|Delete]						

Note: This table is used to override the rules for populating the Queuing By Number Range Table specified in Appendix 1.

Table: Queuing By Network Type		**(Technical Specification Reference 3.5.15)**		
Action	Network Type	Network Updates Enabled	Carrier ID	Carrier Name
[Create|Delete]				
[Create|Delete]				

Table: Service Level		**(Technical Specification Reference 3.5.7)**	
	Record 1	Record 2	Record 3
Action	*Modify*	*[Create|Delete]*	*[Create|Delete]*
PORTCATEGORY			
NETWORKTYPE			
ACTIVATIONGRACEMINUTES			
ACTIVATIONWINDOWSIZE			
APCRESPONSEBUSINESSHOURS			
GSPAPPROVALBUSINESSHOURS			
LSPRESPONSEBUSINESSHOURS			
MAXNOTICECALENDARDAYS			
MINNOTICEBUSINESSHOURS			

Table: Parameter	**(Technical Specification Reference 3.5.26)**
Action	*[Create|Delete]*
IPMS API version	
System Identifier	
Max APCs per Port	
Home Page HTML	
Minimum password length	
Maximum Port resubmissions	
Relinquishment quarantine calendar days	
Expiring usiness days	
Expired business days	
Emergency return business days	
Rejected and Cancel appear in getRequestedPorts business days	
Withdrawn Expired and Closed appear in getApprovedPorts business days	
Accepted and Rejected appear in getApprovedPortChangeRequests business days	
Maximum phone numbers per port	
Maximum Errors returned	
Maximum Network Updates returned	

Notes:

1. To modify a record in IPMS, delete the old record and create a new record. This process will make the nature of the change visible.

1 Appendix 1 Queuing By Number Range Rules

When a carrier creates a new number range in the Number Range Table, all other carriers need an entry in the Queuing By Number Range Table for the new number range.

The following default rules should be used by HP to populate the Queuing By Number Range Table for new number ranges. HP should apply these default rules if a carrier has not made an entry in the Queuing By Number Range Table above for the new number range. If there is an entry in the Queuing By Number Range Table on this form, the entry will override the default rules specified below.

Default Rules:

Carrier	
11667	NOW
11227	CALLPLUS01
11217	COMPASS01
11247	IHUG
11517	LINKTEL01
11677	ORCONLOCAL
11417	TCLA100
11657	SPARKLOCAL
11647	SPARKMOBILE
11937	VFNZ01
11267	WOOSH01
11987	WXCLOCAL
11507	NZCL

2 Appendix 2 LICAs

Akaroa	Kurow	Stratford
Alexandra	Lawrence	Taihape
Amberley	Levin	Takaka
Ashburton	Lumsden	Taumarunui
Auckland	Marton	Taupo
Balclutha	Masterton	Tauranga
Blenheim	Matamata	Te Anau
Cheviot	Maungaturoto	Te Awamutu
Christchurch	Milton	Te Kuiti
Cromwell	Mokau	Thames
Culverden	Morrinsville	Timaru
Dannevirke	Motueka	Tokanui
Darfield	Mt Cook	Twizel
Dargaville	Murchison	Waihi
Dunedin	Napier	Waimate
Edendale	Nelson	Waiouru
Fairlie	New Plymouth	Waipukurau
Featherston	Oamaru	Wairoa
Fox Glacier	Ohakune	Waitangi (Chatham Islands)
Franz Josef	Opotiki	Wanaka
Geraldine	Opunake	Wanganui
Gisborne	Otautau	Warkworth
Gore	Otorohanga	Wellington
Great Barrier Island	Paeroa	Westport
Greymouth	Pahiatua	Whakatane
Haast	Palmerston	Whangamata
Hamilton	Palmerston North	Whangarei
Hawera	Paraparaumu	Winton
Helensville	Pukekohe	
Hibiscus Coast	Putaruru	
Hokitika	Queenstown	
Huntly	Ranfurly	
Invercargill	Rangiora	
Kaikohe	Riverton	
Kaikoura	Rotorua	
Kaitaia	Roxburgh	
Kawakawa	Ruatoria	

Appendix E. API Error Messages

Extracted from Tech Spec Section 9 Appendix A

Error Code	Error Text
ACCEPT_STATE	The Approved Port Change cannot be accepted because the Port is not in Approved, Expiring or Failed state.
ACCESS_DUPLICATED	The access value is repeated.
ACCESS_INVALID	The access value is invalid.
ACCOUNT_FORMAT	The account number is not of a valid length.
ACCOUNT_REQUIRED	The account number is required when the Port is not PrePay/PrePaid or the Port is PrePay/PrePaid and all not all numbers are PrePay/PrePaid (not all numbers have a Handset Reference).
ACTION_INVALID	Action must be I for Insert, D for Delete or U for Update.
ACTIVATE_APC	the Port cannot be activated because there is an Approved Port Change in Awaiting APC Approval state.
ACTIVATE_GC	The Port cannot be activated because the user is not of the Gaining Service Provider.
ACTIVATE_STATE	The Port cannot be activated because the Port is not in Approved State.
ALREADY_APC	The Approved Port Change cannot be requested because there is already an Approved Port Change in Awaiting APC Approval state.
ALREADY_CONFIRMED	This Network Update has already been confirmed.
ALREADY_EMERGENCY_RETURNED	The Port has already been Emergency Returned.
APC_ACCEPT_STATE	The Approved Port Change cannot be accepted because there is no Approved Port Change in Awaiting APC Approval state.
APC_EMPTY	Either numbers or a Port start date/time must be specified in an Approved Port Change.
APC_LSP_GSP	The Approved Port Change cannot be accepted because the user is not of the Losing Service Provider or Gaining Service Provider.

Error Code	Error Text
APC_LIMIT	The Approved Port Change cannot be accepted because there have already been too many Approved Port Changes.
APC_NUMBER_MISMATCH	Phone numbers do not match those awaiting approval.
APC_PORT_VERSION	The version specified in the Approved Port Change does not match that of the Port.
APC_REJECT_STATE	The Approved Port Change cannot be rejected because there is no Approved Port Change in Awaiting APC Approval state.
APC_RESPONDER	The user is not of the responding Service Provider for the Approved Port Change.
APC_STATE	The Approved Port Change cannot be requested because the Port is not in Approved, Expiring or Failed state.
APPROVAL_FIELD	The approved field must be the same as that of the Port Request or the same as that of response from the Losing Service Provider.
APPROVAL_GSP	The Port cannot be approved because the user is not of the Gaining Service Provider.
APPROVAL_STATE	The Port cannot be approved because it is not in Awaiting GSP Approval state.
CANCEL_GSP	The Port cannot be cancelled because the user is not of the Gaining Service Provider.
CANCEL_STATE	The Port cannot be cancelled because it is not in Awaiting LSP Response or Request Expired state.
CANNOT_APPROVE	This Port cannot be approved because the Losing Service Provider indicated that: they are not the correct Losing Service Provider or the account number is incorrect.
CANNOT_COMPLETE	The Port cannot be completed because all the numbers failed to port.
CANNOT_CONFIRM	The Network Update cannot be confirmed because there is not such Network Update.
CARRIER_INVALID	The Carrier specified is not a valid Carrier.
CARRIER_RELATIONSHIP	The Gaining Service Provider is not authorized to utilize the specified

Error Code	Error Text
	Gaining Carrier.
CATEGORY_INVALID	The category must be “Simple” or “Complex”.
~~CLIENT_VERSION_INVALID~~ (no longer used)	
COMPANY_INVALID	The specified Company is invalid.
COMPLETE_GSP	The Port cannot be completed because the user is not of the Gaining Service Provider.
COMPLETE_NUMBER	The Port cannot be completed because the number is neither complete nor failed.
COMPLETE_STATE	The Port cannot be completed because it is not in In Progress state.
CONFIRM_CARRIER	The Network Update cannot be confirmed because user is not of the Carrier.
CONFIRM_NETWORKUPDATES_STATE	Can not confirm network update. Network Updates do not apply to the current state of the Port.
CUSTOMER_NAME_REQUIRED	A Customer Name must be entered, unless a Port Request is for prepay/prepaid mobile numbers only.
CURRENT_PASSWORD_INVALID	The password cannot be changed because the old password specified is incorrect.
DETAIL_NOT_ALLOWED	Detailed information is limited to single port requests only.
FAIL_GSP	The Port cannot be failed because the user is not of the Gaining Service Provider.
FAIL_NUMBER	The Port cannot be failed because the number has not failed.
FAIL_STATE	The Port cannot be failed because it is not in In Progress state.
FIELD_REQUIRED	The field is mandatory.
FIELD_LENGTH	String or text field exceeds maximum length.
FILTER_INVALID	The filter value specified is invalid.
FILTER_PROFILE	The filter value specified is not allowed by user’s profile:
GC_NOT_SUPPORTED	Porting from the Network Type of the Losing Carrier to that of the Gaining Carrier is not supported.
GSP_GC_READONLY	The Port cannot be requested because the combination of Gaining Service Provider and Gaining Carrier is set

Error Code	Error Text
	Read-only.
HANDSET_FORMAT	The Handset Reference is not of a valid length.
HANDSET_REFS_NOT_UNIQUE	The Handset Reference for the prePayPrePaid number in the set of ported numbers is not unique.
LOCAL_RFS_FORMAT	For a Local-Local Port, the time part of the Porting Date must be 08:00 or 12:00.
LOGIN_INVALID	The specified combination of user id, company id and password do not represent an active user with an active profile.
LSP_INCORRECT	If you indicate that you are not the Losing Service Provider then no other data may be specified.
LSP_LC_READONLY	This action cannot be performed because the combination of Losing Service Provider and Losing Carrier is set Read-only.
MAX_PHONE_NUMBERS_PER_PORT_EXCEEDED	Maximium number of phone numbers per port exceeded.
MAXIMUM_ERRORS_EXCEEDED	Exceeded maximum number of errors.
NONPORTED_NUMBER_LSP	The Losing Service Provider specified does not have a relationship with the Donor Carrier for the non-Ported number.
NOT_AUTHORISED	You are not permitted to perform this operation.
NUMBER_FORMAT	The number does not have a valid format.
NUMBER_NOT_PORTED	The number cannot be Relinquished because it has not been ported.
NUMBER_PORTING	The number cannot be Ported because it is already involved in an ongoing Port.
NUMBER_RANGE	The number is in a number range unknown to IPMS.
NUMBER_RANGE_DUPLICATED	The number range cannot be inserted because it already exists.
NUMBER_RANGE_IN_USE	The number range cannot be deleted because it is referred to by other records in the IPMS database.
NUMBER_RANGE_INVALID	The number range specified is not a valid number range.
NUMBER_RELINQUISHING	The number cannot be Ported because

Error Code	Error Text
	it is already involved in an ongoing Relinquishment.
NUMBER_REPEATED	This number has been specified more than once.
(obsolete NUMBERS_LC)	(This error code no longer used since change request CR0003)
OVERRIDE_INVALID	You cannot override Losing Service Provider unless IPMS has been shown to contradict the Losing Service Provider specified.
PASSWORD_ALREADY_USED	You cannot use this new password because it is a password that has been recently used.
PASSWORD_EXPIRED	The password has expired and a new password was not specified.
PASSWORD_LENGTH	The new password specified is not of the minimum length.
PORT_RESUBMIT_LIMIT	The Port has already been resubmitted too many times.
PORTED_NUMBER_LSP	The Losing Service Provider specified is invalid for the Ported number.
PREPAYPREPAID _NO_HANDSET	You cannot specify PrePay/PrePaid when no numbers have Handset References.
PROFILE_COMPANY_CHANGE	The Company of a profile may not be changed.
PROFILE_DUPLICATED	The profile cannot be inserted because it already exists.
PROFILE_IN_USE	The profile cannot be deleted because it is referred to by other records in the IPMS database.
PROFILE_INVALID	The user's profile has been made inactive.
PROFILE_IPMS_ADMIN	An IPMS System Administrator can only maintain User Administrator profiles.
PROFILE_NOT_EXISTS	The Profile specified is not a valid Profile.
PROFILE_USER_ADMIN	An User Administrator can only maintain profiles for their Company that are not IPMS System Administrator profiles or User Administrator profiles.
PROGRESS_GC_LC_GSP	The user cannot get Port progress information because they are not of the Gaining Service Provider, Gaining Carrier or Losing Carrier.
PROGRESS_GC_LC	The user cannot set Port progress

Error Code	Error Text
	information because they are not of the Gaining Carrier or Losing Carrier.
PROGRESS_NUMBER	You cannot specify Port progress information for a number that is not part of the Port.
PROGRESS_STATE	You cannot get or set Port progress information because the Port is not in In Progress state.
PROGRESS_STATUSES	The progress update specified is not valid for the current state of the number.
PROGRESS_VERSION	The progress update cannot be completed for the number because another user has changed the data since it was read. Re-read the data and try again.
REJECT_GSP	The Port cannot be rejected because the user is not of the Gaining Service Provider.
REJECT_STATE	The Port cannot be rejected because it is not in Awaiting GSP Approval state.
RELINQUISHMENT_LC	The relinquishment cannot be requested because the user is not current Carrier for ported number.
REPORT_NOT_FOUND	Report not found.
RESPONSE_LSP	The Port cannot be responded to because the user is not of the Losing Service Provider.
RESPONSE_STATE	The Port cannot be responded to because it is not in Awaiting LSP Response state.
RETURN_GSP	The Emergency Return cannot be requested because the user is not of the Gaining Service Provider.
RETURN_NUMBERS	The Emergency Return cannot be requested because the number (including Handset Reference) is not a completed number in the original Port.
RETURN_SOM	The Emergency Return cannot be requested because the Port was made GC and LC Complete too long ago.
RFS_NOTICE_PERIOD	The Port Date/Time specified is not within the minimum and maximum notice periods.
RFS_WINDOW	The Port cannot be activated outside the Ready For Service DateTime window (grace period taken into account).

Error Code	Error Text
SERVICE_PROVIDER_ACCESS	The user is not of the specified Gaining Service Provider.
SERVICE_PROVIDER_INVALID	The specified Service Provider is invalid.
SESSION_INVALID	The specified session is invalid or has expired.
SOM_INVALID	No such SOM exists.
SOM_NOT_ZERO	If a SOM is specified, it must be the SOM of an Invalid port or a valid port resubmission.
STATUS_INVALID	The status specified is not valid.
STATUS_PROFILE	The status is not allowed by the user's profile:
UPDATES_CARRIER	The user is not of the Carrier specified by the supplied Carrier id.
USER_COMPANY_CHANGE	The Company of a user may not be changed.
USER_DUPLICATED	The user cannot be inserted because it already exists.
USER_IN_USE	The user cannot be deleted because it is referred to by other records in the IPMS database.
USER_INVALID	The user has been made inactive.
USER_IPMS_ADMIN	An IPMS System Administrator can only maintain User Administrator users.
USER_NOT_EXISTS	The User specified is not a valid User.
USER_USER_ADMIN	An User Administrator can only maintain users for their Company that are not IPMS System Administrator users or User Administrator users.
VALUE_INVALID	The value specified is invalid.
WITHDRAWAL_STATE	The Port cannot be withdrawn because it is not Approved, Expiring or Failed state.
WITHDRAWAL_GSP	The Port cannot be withdrawn because the user is not of the Gaining Service Provider.

Error Code Descriptions

Code	IPMS Error Mnemonic	Description
0	SUCCESS	
10	ACCEPT_STATE	"The Approved Port Change cannot be accepted because the Port is not in Approved Expiring or Failed state."
20	ACCESS_DUPLICATED	"The access value is repeated."
30	ACCESS_INVALID	"The access value is invalid."
40	ACCOUNT_FORMAT	"The account number is not of a valid length."
50	ACCOUNT_REQUIRED	"The account number is required when the Port is not prepay/prepaid or the Port is prepay/prepaid and not all numbers are prepay/prepaid (not all numbers have a handset reference)."
60	ACTION_INVALID	"Action must be I for Insert D for Delete or U for Update."
70	ACTIVATE_APC	"The Port cannot be activated because there is an Approved Port Change in Awaiting APC Approval state."
80	ACTIVATE_GSP	"The Port cannot be activated because the user is not of the Gaining Service Provider."
85	ACTIVATE_STATE	"The Port cannot be activated because the Port is not in Approved state."
90	ALREADY_APC	"The Approved Port Change cannot be accepted because there is already an Approved Port Change in Awaiting APC Approval state."
100	ALREADY_CONFIRMED	"This Network Update has already been confirmed."
110	APC_ACCEPT_STATE	"The Approved Port Change cannot be accepted because there is no Approved Port Change in Awaiting APC Approval state."
120	APC_EMPTY	"Either numbers or a Port start date/time must be specified in an Approved Port Change."
130	APC_LIMIT	"The Approved Port Change cannot be accepted because there have already been too many Approved Port Changes."
140	APC_LSP_GSP	"The Approved Port Change cannot be accepted because the user is not of the Losing Service Provider or Gaining Service Provider."
150	APC_PORT_VERSION	"The version specified in the Approved Port Change does not

		match that of the Port."
160	APC_REJECT_STATE	"The Approved Port Change cannot be rejected because there is no Approved Port Change in Awaiting APC Approval state."
170	APC_RESPONDER	"The user is not of the responding Service Provider for the Approved Port Change."
180	APC_STATE	"The Approved Port Change cannot be requested because the Port is not in Approved Expiring or Failed state."
190	APPROVAL_FIELD	"The approved field must be the same as that of the Port request or the same as that of response from the Losing Service Provider." NOTE: Could be the 50 character customer name problem.
200	APPROVAL_GSP	"The Port cannot be approved because the user is not of the Gaining Service Provider."
210	APPROVAL_STATE	"The Port cannot be approved because it is not in Awaiting GSP Approval state."
220	CANCEL_GSP	"The Port cannot be cancelled because the user is not of the Gaining Service Provider."
230	CANCEL_STATE	"The Port cannot be cancelled because it is not in Awaiting LSP Response or Request Expired state."
240	CANNOT_APPROVE	"This Port cannot be approved because the Losing Service Provider indicated that: they are not the correct Losing Service Provider or the account number is incorrect."
250	CANNOT_COMPLETE	"The Port cannot be completed because all the numbers failed to port."
260	CANNOT_CONFIRM	"The Network Update cannot be confirmed because there is no such Network Update."
270	CARRIER_INVALID	"The Carrier specified is not a valid Carrier."
280	CARRIER_RELATIONSHIP	"The Gaining Service Provider is not authorised to utilize the specified Gaining Carrier."
290	CATEGORY_INVALID	"The category must be Simple or Complex."
310	COMPANY_INVALID	"The specified company is invalid."
320	COMPLETE_GSP	"The Port cannot be completed because the user is not of the Gaining Service Provider."
330	COMPLETE_NUMBER	"The Port cannot be completed because the number is neither

		complete nor failed."
340	COMPLETE_STATE	"The Port cannot be completed because it is not in In Progress state."
350	CONFIRM_CARRIER	"The Network Update cannot be confirmed because user is not of the Carrier."
360	CURRENT_PASSWORD_INVALID	"The password cannot be changed because the old password specified is incorrect."
365	CUSTOMER_NAME_REQUIRED	"A customer name must be entered unless a Port request is for prepay/prepaid mobile numbers only."
370	FAIL_GSP	"The Port cannot be failed because the user is not of the Gaining Service Provider."
380	FAIL_NUMBER	"The Port cannot be failed because the number has not failed."
390	FAIL_STATE	"The Port cannot be failed because it is not in In Progress state."
395	FIELD_LENGTH	"String or text field exceeds maximum length."
400	FIELD_REQUIRED	"The field is mandatory."
410	FILTER_INVALID	"The filter value specified is invalid."
420	FILTER_PROFILE	"The filter value specified is not allowed by user's profile:"
425	GC_NOT_SUPPORTED	"Porting from the network type of the Losing Carrier to that of the Gaining Carrier is not supported."
430	GSP_GC_READONLY	"The Port cannot be requested because the combination of Gaining Service Provider and Gaining Carrier is set read-only."
440	HANDSET_FORMAT	"The handset reference is not of a valid length."
445	IMPERSONATE_USER	"The user to be impersonated is not a user in the same company as the requesting user."
450	LOCAL_RFS_FORMAT	"For a Local-Local Port the time part of the porting date must be 08:00 or 12:00."
460	LOGIN_INVALID	"The specified combination of user id company id and password do not represent an active user with an active profile."
470	LSP_INCORRECT	"If you indicate that you are not the Losing Service Provider then no other data may be specified."
480	LSP_LC_READONLY	"This action cannot be performed because the combination of Losing Service Provider and Losing Carrier is set read-only."

490	NONPORTED_NUMBER_LSP	"The Losing Service Provider specified does not have a relationship with the Donor Carrier for the non-ported number."
500	NOT_AUTHORISED	"You are not permitted to perform this operation."
510	NUMBER_FORMAT	"The number does not have a valid format."
520	NUMBER_PORTING	"The number cannot be ported because it is already involved in an ongoing Port."
530	NUMBER_RANGE	"The number is in a number range unknown to IPMS."
540	NUMBER_RANGE_DUPLICATED	"The number range cannot be inserted because it already exists."
550	NUMBER_RANGE_IN_USE	"The number range cannot be deleted because it is referred to by other records in the IPMS database."
560	NUMBER_RANGE_INVALID	"The number range specified is not a valid number range."
570	NUMBER_RELINQUISHING	"The number cannot be ported because it is already involved in an ongoing Relinquishment."
575	NUMBER_NOT_PORTED	"The number cannot be Relinquished because it has not been ported."
580	NUMBER_REPEATED	"This number has been specified more than once."
600	OVERRIDE_INVALID	"You cannot override Losing Service Provider unless IPMS has been shown to contradict the Losing Service Provider specified."
610	PASSWORD_ALREADY_USED	"You cannot use this new password because it is a password that has been recently used."
620	PASSWORD_EXPIRED	"The password has expired and a new password was not specified."
630	PASSWORD_LENGTH	"The new password specified is not of the minimum length."
635	PORT_RESUBMIT_LIMIT	"The Port has already been resubmitted too many times."
640	PORTED_NUMBER_LSP	"The Losing Service Provider specified is invalid for the ported number."
650	PREPAYPREPAID_NO_HANDSET	"You cannot specify prepay/prepaid when no numbers have handset references."
655	PROFILE_COMPANY_CHANGE	"The company of a profile may not be changed."
660	PROFILE_DUPLICATED	"The profile cannot be inserted because it already exists."
670	PROFILE_IN_USE	"The profile cannot be deleted because it is referred to by other records in the IPMS database."
680	PROFILE_INVALID	"The user's profile has been made

		inactive."
690	PROFILE_IPMS_ADMIN	"An IPMS system administrator can only maintain user administrator profiles."
700	PROFILE_NOT_EXISTS	"The profile specified is not a valid profile."
710	PROFILE_USER_ADMIN	"A user administrator can only maintain profiles for their company that are not IPMS system administrator profiles or user administrator profiles."
715	PROGRESS_GC_LC	"The user cannot set Port Progress information because they are not the Gaining Carrier or Losing Carrier."
720	PROGRESS_GC_LC_GSP	"The user cannot get Port Progress information because they are not the Gaining Service Provider Gaining Carrier or Losing Carrier."
730	PROGRESS_NUMBER	"You cannot specify Port Progress information for a number that is not part of the Port."
740	PROGRESS_STATE	"You cannot get or set Port Progress information because the Port is not in In Progress state."
760	PROGRESS_STATUSES	"The progress update specified is not valid for the current state of the number."
765	PROGRESS_VERSION	"The progress update cannot be completed for the number because another user has changed the data since it was read. Re-read the data and try again."
770	REJECT_GSP	"The Port cannot be rejected because the user is not of the Gaining Service Provider."
780	REJECT_STATE	"The Port cannot be rejected because it is not in Awaiting GSP Approval state."
790	RELINQUISHMENT_LC	"The Relinquishment cannot be requested because the user is not the current Carrier for ported number or number is not ported."
800	RESPONSE_LSP	"The Port cannot be responded to because the user is not of the Losing Service Provider."
810	RESPONSE_STATE	"The Port cannot be responded to because it is not in Awaiting LSP Response state."
820	RETURN_GSP	"The Emergency Return cannot be requested because the user is not of the Gaining Service Provider."
830	RETURN_NUMBERS	"The Emergency Return cannot be requested because the number

		(including handset reference) is not a completed number in the original Port."
840	RETURN_SOM	"The Emergency Return cannot be requested because the Port was made GC and LC Complete too long ago."
850	RFS_NOTICE_PERIOD	"The Port date/time specified is not within the minimum and maximum notice periods."
860	RFS_WINDOW	"The Port cannot be activated outside the ready for service dateTime window (grace period taken into account)."
870	SERVICE_PROVIDER_ACCESS	"The user is not of the specified Gaining Service Provider."
880	SERVICE_PROVIDER_INVALID	"The specified Service Provider is invalid."
890	SESSION_INVALID	"The specified session is invalid or has expired."
900	SOM_INVALID	"No such SOM exists."
910	SOM_NOT_ZERO	"If a SOM is specified it must be the SOM of an Invalid Port or a valid Port resubmission."
920	STATUS_INVALID	"The status specified is not valid."
930	STATUS_PROFILE	"The status is not allowed by the user's profile:"
940	UPDATES_CARRIER	"The user is not of the Carrier specified by the supplied Carrier id."
945	USER_COMPANY_CHANGE	"The company of a user may not be changed."
950	USER_DUPLICATED	"The user cannot be inserted because it already exists."
960	USER_IN_USE	"The user cannot be deleted because it is referred to by other records in the IPMS database."
970	USER_INVALID	"The user has been made inactive."
980	USER_IPMS_ADMIN	"An IPMS system administrator can only maintain user administrator users."
990	USER_NOT_EXISTS	"The user specified is not a valid user."
1000	USER_USER_ADMIN	"A user administrator can only maintain users for their company that are not IPMS system administrator users or user administrator users."
1010	VALUE_INVALID	"The value specified is invalid."
1020	WITHDRAWAL_STATE	"The Port cannot be withdrawn because it is not Approved Expiring or Failed state."
1030	WITHDRAWAL_GSP	"The Port cannot be withdrawn because the user is not of the Gaining Service Provider."

1140	DETAIL_NOT_ALLOWED	"Detailed information is limited to single port requests only"
1150	MAX_PHONE_NUMBERS_PER_PORT_EXCEEDED	"Maximum number of phone numbers per port exceeded."
1160	APC_NUMBER_MISMATCH	"Phone numbers do not match those awaiting approval."
1170	MAXIMUM_ERRORS_EXCEEDED	"Exceeded maximum number of errors."
1220	CONFIRM_NETWORKUPDATES_STATE	"Can not confirm Network Update. Network Updates do not apply to the current state of the Port."
1300	REPORT_NOT_FOUND	"Report not found"
10000	IPMS_SERVER_ERROR	"Unexpected error on IPMS server. Error diagnostic information has been logged on the IPMS server."

API Calls

changePassword
getCurrentUserData
getCompanies
getServiceProviders
getCarriers
getAccess
requestPort
getRequestedPorts
submitPortResponse
approvePort
rejectPort
cancelPort
getApprovedPorts
activatePort
getPortProgress
updatePortProgress
completePort
failPort
getNetworkUpdates
confirmNetworkUpdates
requestApprovedPortChange
getApprovedPortChangeRequests
acceptApprovedPortChange
rejectApprovedPortChange
withdrawPort
requestEmergencyReturn
requestRelinquishment
numberEnquiry
SOMEnquiry
getUsers
maintainUsers
getProfiles
maintainProfiles
getNumberRanges
maintainNumberRanges

Appendix F. Service Level Explanatory Notes

Table 1: Simple Mobile Port Service Levels

Nr	Phase	Event	Service Level to apply	Total time elapsed	Earliest start	IPMS status after event	Comment
1	Request	Customer requests Port	N/A	N/A	N/A	N/A	The Customer contacts the GSP and request the number Port.
2		GSP submits Port in IPMS	N/A	0 – "the clock starts now"	N/A	Awaiting LSP Response	The start of the Port process is captured in IPMS. A proposed RFS is set. This step should be completed within 30 days of Customer authorisation.
3		LSP responds to Port request	Within 30 minutes of step 2 *(Terms)*	Up to 30 minutes	Immediately after step 2	Awaiting GSP Approval	The 30 minutes applies to the status in IPMS changing from 'Awaiting LSP response' to 'Awaiting GSP Approval', and includes any IPMS processing time and time intervals for polling the queue.
4		GSP responds and updates status	Within 30 minutes of completion of step 3 *(Terms)*	Up to 60 minutes	Immediately after step 3	Approved	Once approved, the Port is scheduled to start Port Activation on RFS date. If step 3 completes in less than 30 minutes, step 4 can still only take up to 30 minutes.
5	Approved - wait	RFS date arrives	N/A – wait until RFS arrives	Between 60 minutes and up to 30 days	60 minutes after step 2	Approved	RFS is interpreted here as the start of Port Activation. The minimum notice period is 60 minutes from step 2 for a Simple mobile Port.
6	Port Activation	GC signals intention to start Port Activation to IPMS	Within 10 minutes of the RFS *(IPMS measured)*	RFS date (minimum 60 minutes) plus up to 10 minutes	Immediately following step 5	In Progress	The GC updates IPMS to indicate that they will start to Activate the number on their network.

Nr	Phase	Event	Service Level to apply	Total time elapsed	Earliest start	IPMS status after event	Comment
7		GC advises IPMS of GC Port Activation	Within 10 minutes of step 6 *(Manual: proposed)*	RFS date (minimum 60 minutes) plus up to 20 minutes	Immediately following step 6	In Progress	GC has Activated: trigger for LC to change Routing Anywhere between steps 6 and 7, the Customer will start to receive service from their new SP (the GSP).
8		LC advises IPMS of routing update	Within 10 minutes of step 7 *(Manual: proposed)*	RFS date (minimum 60 minutes) plus up to 30 minutes	Immediately following step 7	In Progress	When the LC completes the re-routing, the LSP handset stops working. From a Customer point of view, Porting is complete.
9		GC confirms Port "line by line"	Within 10 minutes of step 8 *(Manual: proposed)*	RFS date (minimum 60 minutes) plus up to 40 minutes	Immediately following step 7	GC and LC Complete	Once the status changes to 'Complete', the Port is put on the IPMS queue for third parties to update their networks. Any IPMS processing time is included in the Service Level. Unless the Port is 'undone', the Customer will not notice this step.
10	**Closing**	Other Carriers confirm routing update	Within 1 hour of step 9 *(Manual: proposed on a best endeavours basis)*	RFS date (minimum 60 minutes) plus up to 1 hour and 40 minutes.	Immediately following step 9	Closed	The Port is closed – the number can now be part of a new Port Request.

Notes

1. 'IPMS status after event' column reflects the status during a successful Port.
2. The column 'Service Level to apply' indicates the source of the Service Level
    a. The Terms – the (maximum) duration of the Activity is prescribed in the Terms.
    b. IPMS – the (maximum) duration of the Activity is measured by IPMS – in addition to Service Levels specified in the Terms
    c. Manual: proposes – the Business Process workstream has identified that in order to guarantee a satisfactory Customer experience, the duration of the Activity should be subject to a Service Level.

Key messages

1. The minimum notice period for a simple mobile Port is one hour and the activation window is up to 30 minutes. Therefore, a Customer who wants to Port 'as soon as possible' should be given an expectation for completion of the Port (i.e. new phone works and old phone stops working) between 60 and 90 minutes, to allow for steps 6, 7 and 8 in the table above.
2. If a Customer wants to Port at a specified time in the future, for example next Friday at 4pm, then the GSP representative has to set a RFS date (for IPMS) working backwards from that time – so for Simple Mobile, set the RFS at 3.30pm. The rep also should inform the Customer that their Port will be completed between 3.40pm and 4pm.
3. The RFS used in IPMS should NOT be communicated to the Customer. Rather, the Customer should instead be given an expectation of when step 7-8 will take place. The suggestion is to call this "Cut-over" date/time.
4. During the time elapsed between steps 7 and 8, the Customer will have (partial) service on both handsets: both handsets can be used for outbound calling/SMS, and depending on where the incoming call originates from, may receive calls on both handsets.
    a. Note: this scenario assumes a Port between Spark and Vodafone.
5. During the time elapsed between steps 8 and 10, the Customer may not receive calls originated from third party networks, unless the two Carriers involved in Porting have an arrangement in place for Carrier re-routing.

Appendix G. Extract from TCF Customer Transfer Code

J. APPROPRIATE CUSTOMER CONTACT AND ACCESS TO AND USE OF INFORMATION

38. The objective of this section is to facilitate best practice in terms of Service Provider etiquette and how Customer information is accessed and used.

39. Privacy and Use of Information (this is covered section 4.1.4 of the LMNP Terms)

39.1 Information relating to Customer Transfer will be kept confidential at all times by the parties to the Code except as set out in this clause or as required by law. Information provided as part of the Transfer process can only be used or disclosed for the purpose of Customer Transfers, in association with the delivery of Telecommunications Services, and for Customer and network fault management and complaint handling. Information provided in the Transfer Process must not be used for any other purpose (including winback and marketing purposes).

39.2 A Service Provider or the Carrier to whose network an access line is directly connected and over which services are supplied ("ASD"), which receives any type of information relating to the Transfer of a Customer, may only use or disclose such information in accordance with Privacy Act 1993, the Telecommunications Information Privacy Code 2003, and any Bilateral Agreement in place between the parties.

39.3 If there is any inconsistency between this Code, the Privacy Act 1993, and the Telecommunications Information Privacy Code 2003, the Privacy Act and the Telecommunications Information Privacy Code prevail.

40. Contact with the Customer

40.1 No Party to this Code will undertake telemarketing, direct mail marketing, face to face marketing or other marketing activities specifically targeted at the relevant Customer where those activities are based on, and are in direct response to, the LSP receiving a Validation Request or the ASD receiving a Transfer Request.

40.2 The ASD may contact the Customer about any processing/technical issues but may not use this opportunity to attempt to win the Customer back or refer the Customer to any other personnel within the ASD that engages in retail sales activity.

40.3 For the avoidance of doubt nothing in clause 40.1 will prevent the LSP from undertaking marketing activities, which are based on or utilise retail billing or Customer information generated within the LSP.

40.4 For the avoidance of doubt, the GSP may contact the Customer at any time.

41. Customer Initiated contact

41.1 If the Customer contacts the GSP or the LSP, there are no restrictions on the Communication that either Service Provider can have with the Customer. However, if the Customer has a complaint, then the Service Provider must comply with the provisions of the Telecommunications Carriers' Forum Consumer Complaints Code.

41.2 If the Customer contacts the ASD about the Transfer, and the ASD is not the GSP, then the ASD must refer the Customer to the GSP.

42. Conduct of Parties to this Code

When interacting with any Customer:

42.1 All Parties and their representatives will act in a professional and courteous manner;

42.2 No Party may make any comment or statement about any other Party that would or may be likely to bring the other Party's reputation into disrepute, particularly where that Party does not know the complete facts to the situation (for instance when there has been an Invalid Transfer);

42.3 Parties must ensure that their representatives, if referring to another Party's Telecommunications Service(s):

i. Do not mislead Customers in any form or manner or engage in any conduct that is likely to mislead;

ii. Refer only to comparisons that are relevant to the Transfer being made or attempted.

42.4 Parties must ensure that their representatives do not:

42.4.1 Harass or coerce a Customer; or

42.4.2 Engage in unconscionable conduct.

Appendix H. LMNP - New Entrants and Potential New Entrant Guidelines

1. Introduction

The Commerce Commission and the TCF wish to encourage New Entrants and Potential New Entrants to participate in Local and Mobile Number Portability (LMNP). The purpose of this document is to outline the procedures and steps that New Entrants and Potential New Entrants will need to undertake in order to begin Porting.

New Entrants are required to participate in Number Portability and comply with the Number Portability Determination. New entrant and existing Carrier responsibilities are covered in the Network Terms Section 20, New Entrant Procedures.

2. Definitions

"Agreed Business Test Scenarios" means a suite of tests designed to test the compliance of Local and Mobile Number Portability functions with the LMNP Terms

"Carrier" as defined in the LMNP and Network Terms means an entity that operates a public switched telephone network (or a functionally equivalent system) that originates, transits or terminates voice calls or short messages. The same person may be both a Carrier and a Service Provider.

"Common Costs" means the New Entrant's share of the Capital Cost Payment and the Operational Cost Payment, as specified in the Number Portability Determination.

"End-to-End Testing" means a suite of tests designed to prove the integrity of intercompany LMNP business and networking functions.

"IPMS or Industry Portability Management System" as defined in the LMNP and Network Terms means the software, hardware and other shared facilities used to give effect to the LMNP Terms.

"Network" as defined in the LMNP and Network Terms means a system comprising telecommunications links to permit telecommunications.

''New Entrant'' means the Carrier or Service Provider whom the Commerce Commission has recently determined to be an Access Seeker or Access Provider in relation to Local Numbers or Mobile Numbers or both, who wishes to connect to the IPMS to Port Numbers. This includes Carriers or Service Providers who had previously been determined by the Commerce Commission to be an Access Provider or Access Provider under the Determination for Local Numbers or Mobile Numbers (but not both) and who have recently been determined by the Commerce Commission to be an Access Seeker or Access Provider in relation to Mobile Numbers or Local Numbers (as the case requires) and they wish to Port those Numbers using IPMS.

"NP Co-ordinator" means the party appointed by the by TCF to liaise with the System Administrator and is to be the primary contact point for any queries in respect of matters relating to the IPMS The name and contact details of the NP co-ordinator are available on the TCF website.

"Number Portability Determination" means the Commerce Commission's Determination on the multi-party application for determination of 'local telephone number portability service' and 'cellular telephone number portability service' designated multinetwork services Decision 554, dated 31 August 2005, including any amendments and subsidiary determinations. For the avoidance of doubt, unless otherwise specified, this includes the Operational and Support Manual for LMNP.

"Operations and Support Manual for LMNP" means a multilateral agreement between Carriers that covers operational issues that are not dealt with by the LMNP Terms or the Network Terms.

''Potential New Entrant'' means the Carrier or Service Provider who wishes to participate in LMNP and who has not currently been determined by the Commerce Commission to be an Access Seeker or Access Provider in relation to either Local Numbers or Mobile Numbers or both Local and Mobile Numbers.

"Service Provider" as defined in the LMNP and Network Terms means any person providing a local service or mobile service to a Customer

"System Administrator" means the party appointed by the TCF from time to time to maintain and operate the IPMS.

"TCF Forum Administrator" means the party appointed by the by TCF to provide all analytical, secretariat, communications, accounting services and website support to the TCF. The name and contact details of the NP co-ordinator are available on the TCF website.

"Technical Specification" means and can be obtained from the NP Co-ordinator.

"TCF" means the Telecommunications Carriers' Forum. For further information contact the TCF Forum Administrator.

3 Current Participants

- The parties defined by the Commerce Commission as Access Seekers and Access Providers are listed on the TCF Website.

- The definitions of Access Seeker and Access Provider are defined in Commission Decision 554, and subsequently clarified by Decision 579, which for convenience are provided below:

  - An **Access Provider** means every person who operates-

    - a PSTN to which numbers have been allocated; and
    - a telephone service that relates to that number portability service

  - **Access Seeker** means any person who-

    - operates a PSTN to which numbers have been allocated; and
    - operates a telephone service that relates to that number portability service; and
    - seeks access to that number portability service

4 Pre-Requisites

In order to begin discussions with the existing parties to the Determination (whether is a Carrier and/ or Service Provider) the following pre-requisites must be in place to facilitate participation into Portability:

The pre-requisites are:

- **Application to the Commerce Commission**

  - All Potential New Entrants must have applied to the Commission to become party to the Determination. Upon acceptance by the Commission, that party will be deemed a New Entrant.

    On 22 June 2007 the Commerce Commission signed off decision 605 which was a further clarification to the NP Determination. The clarification stated that the new entrant implementation timeframe was defined as a 3 month window from the qualifying date. The qualifying date is defined as the date a party is declared eligible as an access provider or the date of the decision whatever is the later.

    The Commerce Commission considers that new parties must have physically interconnected with at least one other Determination party, have tested that interconnection to the satisfaction of both interconnecting parties, and must be afforded an opportunity to implement and test their systems before being required to port local or mobile numbers in accordance with the Determination.

  - On receipt of the Commission's acceptance, the TCF Forum Administrator will:
    - Ensure the New Entrant executes the IPMS Access Agreement;
    - Outline the New Entrant's obligations in respect of the Number Portability cost allocation relating to Common Costs.
    - Inform the NP Co-ordinator that a New Entrant will be applying to participate in LMNP; and
    - Advise the other parties to the Determination of the existence of the New Entrant .

- **Understanding of Number Portability**

  - It is the responsibility of the Potential New Entrant and/or the New Entrant to ensure it or its agents have read and, where necessary, sought appropriate advice on the following:
    - LMNP Terms;
    - Network Terms;
    - Operations and Support Manual;

- IPMS Technical Specification;
- ipms-reportDownloadClient-src.zip;
- TCF_IPMS_Technical_Manual_1_2.doc;
- Number Portability - IPMS report download web servicev2.1.doc;
- TCF_IPMS_User_Guide_1_0.doc; and
- IPMS_Reporting_Web_Service_User_Guide_1_1.doc.

- The above documents can be obtained from the NP Co-ordinator. All obligations specified in the documents for Potential New Entrants and New Entrants must be complied with.
- If the New Entrant or Potential New Entrant requires clarification of any terms in the above documents, it should contact the NP Co-ordinator in the first instance.

5 Bi Lateral Agreements

- All Potential New Entrants and New Entrants must contact any proposed Carrier(s) and/or Service Provider partners to ensure that the following have been documented and agreed where appropriate :
  - Technical Inter Connect Agreements; and
  - Bi Lateral LMNP Operational Agreements, as appropriate.
- Bi-Lateral Testing –
  - The New Entrant must successfully complete bi-lateral testing of the following 'Agreed Business Test Scenarios' below in order to move to the formal Inter Carrier testing:

1	Processing a Simple Successful Port;
2	Rejecting a Simple Port;
3	Processing an Approved Port Change Request (Approved);
4	Withdrawing a Port (Approved);
5	Cancelling a Port (Awaiting LSP Response);
6	Failing a Port;
7	Emergency Return;
8	Relinquishment;
9	Activate port that which has an outstanding port change request;
10	Try to Fail a Port where Carriers have passed some of the numbers; and
11	Third party Network Updates Process.

  - If the New Entrant is a Carrier, it must also undertake the successful testing of its Network in order to move to formal End-to-End Testing. These test scenarios need to be formally agreed and documented with the Carrier (s).

- Testing of any bilaterally agreed porting processes, for example after hours porting, is to be done at the discretion of those bilateral partners. In any case, the provisions of the LMNP Terms and the Network Terms are not to be compromised.

- Inter-Carrier Testing
  - After successful bi-lateral testing has been completed the New Entrant will need to co-ordinate an appropriate test date/schedule with the NP Co-ordinator to complete an agreed set of End-to-End Tests with the other Carriers who are parties to the Determination. Testing should be carried out on an as required basis. It is not necessary for all tests to be carried out with all Carriers however every test should be carried out with at least one Carrier. Testing should be done by agreement with the Carrier they will be testing with to ensure that porting will work with all impacted participants (End-to-End Inter-Carrier Test Plan).

  - The NP Co-ordinator will have use the following as guidelines for Inter-Carrier Testing:

Entry Criteria

(ii)

- The following entry criteria are required to have been completed / implemented prior to the start of Inter-Carrier Integration Testing:

  - All static data must be set up within IPMS as specified in section 5.3 of the Technical Specification;

  - The IPMS environment in which testing will take place must be available and a test date agreed;

  - The New Entrant must have connectivity to IPMS; and

  - All Carriers testing staff are available and familiar with how to use the IPMS.

Exit Criteria

(iii)

- The following exit criteria must be met before IPMS Inter-Carrier Integration testing can be signed off:

  - All planned tests have been completed;

  - No priority 1 or 2 defects remain outstanding; and

  - A test completion report is created and agreed by the New Entrant and the NP Co-ordinator.

Agreed Business Test Scenarios

(iv)

- As agreed in the End-to-end Inter-Carrier Test Plan, the Carriers/Service Providers must perform the following scenarios where required:

  - Processing a Simple Successful Port;

  - Rejecting a Simple Port;

- Processing an Approved Port Change Request (approved);
- Withdrawing a Port (approved);
- Cancelling a Port (Awaiting LSP Response);
- Failing a Port;
- Emergency Return;
- Relinquishment;
- Activate port that which has an outstanding port change request;
- Try to Fail a Port where Carriers have passed some of the numbers; and
- Third party Network Updates Process.

6 Other

In addition to any Carrier one-off certification of compliance of Equivalent Service, the New Entrant must submit an implementation plan to the TCF for approval. This plan must include key dates (inter carrier testing, bi-lateral agreements etc.) for their transition to IPMS which all parties to the Determination must have agreed on. Once all parties have agreed to the key dates they cannot be changed unless 75% or more of the parties to the Determination agree to it.

- The procedures set out in this document are a guide to New Entrants and Potential New Entrants as to what needs to be completed in order to participate in Number Portability.

  A detailed checklist must be completed by all New Entrants. The checklist includes the following actions:

  - Application to Commerce Commission
  - Understanding of Number Portability through the NP Operations & Support Manual, LMNP Terms, Network Terms, IPMS Technical Spec.
  - Bi-lateral agreements in place
  - Bi-lateral testing (including agreed business test scenarios
  - Inter-Carrier testing
  - Entry criteria
  - Exit criteria

  Parties to the Determination are required to give approval for the New Entrant to go live on IPMS. This approval can be a verbal approval given during the regular Number Portability User Group meeting which will then be recorded in the minutes. Alternatively, written approval must be provided within 3 days. If no

response is received from the approval party, a further 2 days will be given for a response to be forthcoming and if no response is received after this period the party is deemed to have approved.

7 Inter-Carrier Test Plan for Phased Integration of New Entrants into IPMS

- To meet the requirements of New Entrants (hereafter referred to as the entrant) for testing of IPMS usage and inter-Carrier operations, a phased process for testing and integration into the live IPMS environment has been developed. The following document should be completed with appropriate details and distributed to all parties as the basis for new entrant testing.

- Each phase would generally run for 1 – 2 weeks depending on resource scheduling, and would not be deemed completed until all Carriers advise the Forum Administrator that they are happy for the entrant to proceed to the next phase (this would normally be done at an NPUG meeting)

- **Clarifications:**

  1. Carriers/Parties: The terms Carriers and parties are used throughout this document. They are intended to include Carriers and Service Providers as necessary
  2. Dates listed are soft and may change for any reason as required. Examples of such requirement are:
     a. Failure to pass a phase sufficiently by the listed End date
     b. Early completion of a phase where some parties are willing to move tests forward to get underway earlier.
  3. Date ranges are listed giving other Carriers a chance to specify a time within that period that best suits them. The entrant will work with all parties to lessen the operational impact of testing on those parties by working to their schedule as much as possible.

- **Technical Data:**

  While this data may not be of direct use to Carriers for initial testing it is included for all parties who find it of interest or use for any reason.

  - **Number Blocks:**

    Following is a list of number blocks and LCAs that have been appropriately obtained through the NAD that the entrant will be using initially:

Prefix(s)	LCA

  - **Contact Details:**

    BAU and First Contact for faults will be:
    Name:
    Phone:
    Mobile:
    Email:

    Escalation of faults:

Name:
Phone:
Mobile:
Email:

- **Phase 1: IPMS processes testing**

  Summary:
  Phase 1 will be simple testing between the new-entrant and other Carriers to ensure that the new-entrant follow processes with the use of IPMS that matches the expectations and operational understanding of existing Carriers.

  Loading the configuration data for the new entrant in TEST, DEV, and TRAIN is the first step in using IPMS. The new entrant can complete test ports internally by using the Dummy Company as the other party (the NP Co-ordinator can supply user IDs and passwords for Dummy Companies). It can be useful to configure some "private" number ranges in TEST, that don't require 3rd party network updates for all Carriers before the SOM is closed (a good technique can be to use some small ranges visible only to the new entrant and Dummy Company and the new entrant and each of their key interconnect partners).

  Testing at this phase may be as simple as one inbound and one outbound port between the entrant and each Carrier; however if any Carrier wishes or it is deemed necessary by any suitable party the entrant will need to undergo other testing actions (failing/withdrawing/etc) as necessary.

System:	IPMS-TEST
Commencing:	<insert date> (This should be at least 1 to 2 weeks from the date that this plan would be presented to the NPUG to allow time for other Carriers to prepare resources. Individual times will still need to be organized with each party)
Ending:	<insert date>
Outputs:	Acknowledgement from Carriers that they are sufficiently happy that the entrant is making use of the IPMS system in a way that conforms to predefined processes and pre-existing IPMS usage.

- **Phase 2: Dummy Number Testing**

  Summary: Phase 2 will commence following successful completion of Phase 1, and loading of the entrants data into IPMS-PROD and is likely to take around two weeks. It is important to ensure that all Carriers can have the entrants number ranges and Carrier and Service Providers ID's setup ready for this phase as the potential 6 week lead time needed by some Carriers would slow testing down significantly.

  It is important to note that the entrant will be required to commence processing Network Updates generated by the IPMS-PROD environment (failure to process within acceptable timeframes will slow down porting completion for all Carriers and potentially lead to issues at a system level) so the entrant should not be enabled in IPMS-PROD until the entrant advises the Forum Administrator that they are able to handle this task. Feasibly, this will require an automation system to process the potentially high number of updates generated.

During this phase, the entrant will port test numbers to and from other Carriers. These ports will verify not only that correct IPMS procedure is followed, but that end to end routing of ported numbers is being handled correctly for inbound to and outbound from the entrants network.

Testing at this stage may be as simple as one inbound and one outbound port for most Carriers, however to ensure that all processes are operating correctly, it is proposed that the following tests are carried out with at least one Carrier (not all tests would necessary need to be with the same Carriers, reducing the burden on any given Carrier) to meet the End-to-End inter-Carrier test requirements for New entrants.

- Rejecting a simple port
- Processing an approved port change (Approved)
- Withdrawing a port (Approved)
- Canceling a port (Awaiting LSP Response)
- Failing a port
- Emergency Return
- Relinquishment
- Activate a port that has an outstanding APC request
- Try to fail a port where Carriers have passed some of the numbers
- Third party network update process

System:	IPMS-PROD
Commencing:	<insert date> (date phase 2 would be approved complete)
Ending:	<insert date>
Outputs:	Acknowledgement from Carriers that they are sufficiently happy that the entrant is accurately handling routing of ported numbers.

- **Phase 3: Soft Launch**

Summary: Upon successful completion of Phase 2, the entrant will do live ports of some test users. The ports for these will be carried out as soon as possible following Phase 2, and will be used for testing for no less than one week. During this time one of these test numbers will be tied to a phone line at the office, allowing trial phone calls to be made to and from that number if so desired.

System:	IPMS-PROD
Commencing:	<insert date> (date phase 2 would be approved complete)
Ending:	<insert date>
Outputs:	Successful active ports.

- **Phase 4: Live**

Summary: Once Phase 3 has been completed it will be considered that all test scenarios and requirements will have been met allowing full live porting to commence.

System:	IPMS-PROD
Commencing:	<insert date> (date phase 3 would be approved complete)
Ending:	NA
Outputs:	None

8 Appendix 1 – Configuration Data for IPMS

- The items that say "Provided by IPMS" require the use of lookup tables that will be supplied. Entity names may be sufficient but in the case of Carriers the ID is required.

Company

(v)

- The Company entity is used for users and security and any Service Provider or Carrier entities need to refer to this Company in the setup.

Company Information	
Unique numeric identifier for Company	Provided by IPMS
Name of Company, e.g. Spark NZ	

Service Provider

(vi)

- The Service Provider is the entity defined in the LMNP Terms as:

  "any person providing a Local Service or Mobile Service to a Customer and who has the Billing Relationship with the Customer for that service. The same person may be both a Carrier and a Service Provider."

Service Provider Information	
Unique numeric identifier for Service Provider	Provided by IPMS
Name of Service Provider, e.g. Vodafone	
ID of Company that operates this Service Provider	Provided by IPMS
Minimum characters/digits in Customer account number when this Service Provider is the Losing Service Provider in a Port	
Maximum characters/digits in Customer account number when this Service Provider is the Losing Service Provider in a Port	
Auto-Approve Port Requests "N" = No, "S" = Service Provider, "C" = Company (For internal porting style events)	
Auto-Accept APC within Service Provider "Y = Yes, "N" = No. If set to Yes, Approved Port Change requests will automatically go to "Accepted" status if the Port is only a change of Carrier (Service Provider staying the same).	
Auto-Accept APC within Company "Y = Yes, "N" = No. If set to Yes, Approved Port Change requests will automatically go to "Accepted" status if the Port is between Service Providers within the same Company.	

- See Technical Specification Section 3.5.4 for additional information

Carrier

- A Carrier is the entity defined in the LMNP Terms as:

  "an entity that operates a public switched telephone network (or a functionally equivalent system) that originates, transits or terminates calls. The same person may be both a Carrier and a Service Provider. If a party to the LMNP Terms has more than one Network, it can be classified as more than one Carrier."

- However, the Carrier entity in the IPMS is really a Network, as a Carrier may have a PSTN that comprises more than one identifiable element. The Carriers in IPMS may represent different parts of a Carriers PSTN, and may represent different geographical areas, technologies, and or points of interconnect.

Carrier	
Unique numeric identifier for a Carrier. This should be set to the number portability network Hand Off Code (HOC) for the Carrier, e.g. 11647 or 11227, allocated by the NAD with a 7 suffix and without the leading zero. Carrier IDs and Carrier Names will be returned by API functions.	
Name of Carrier, e.g. Spark Mobile	
Unique numeric identifier of the Company that owns this Carrier	Provided by IPMS
One of the possible Carrier Types from the Carrier Type table, e.g. Local, Mobile	
Minimum characters/digits in prepay/prepaid handset reference when this Carrier is the Losing Carrier in a Port	
Maximum characters/digits in prepay/prepaid handset reference when this Carrier is the Losing Carrier in a Port	
GC Receive Own Ports "Y = Yes, "N" = No. For Ports where this Carrier is the Gaining Carrier, should the SOM also be added to this Carrier's network updates queue and require confirmation	
LC Receive Own Ports "Y = Yes, "N" = No. For Ports where this Carrier is the Losing Carrier, should the SOM also be added to this Carrier's network updates queue and require confirmation	
Receive Own RQs "Y = Yes, "N" = No. For relinquishments where this Carrier was the Host Carrier (and not Donor Carrier) for the Numbers, should the relinquishment be added to the network updates queue for the Carrier (will happen 30 days after relinquishment).	
GC Confirm Port Withdrawal "Y = Yes, "N" = No. For Ports that have been Withdrawn, where this Carrier was the Gaining Carrier, should the withdrawal be added to the Carrier's network updates queue and require confirmation	
LC Confirm Port Withdrawal "Y = Yes, "N" = No. For Ports that have been Withdrawn, where this Carrier was the Losing Carrier, should the withdrawal be added to the Carrier's network updates queue and require confirmation	
GC Confirm Port Expiry "Y = Yes, "N" = No. For Ports that have Expired, where this Carrier was the Gaining Carrier, should the expiry be added to the Carrier's network updates queue and require confirmation	

LC Confirm Port Expiry "Y = Yes, "N" = No. For Ports that have been expired, where this Carrier was the Losing Carrier, should the expiry be added to the Carrier's network updates queue and require confirmation	

- See Technical Specification Section 3.5.5 for additional information

Carrier – Service Provider

(vii)

- The IPMS is configurable in terms of the relationships between Carriers and Service Providers. This information allows Service Providers to Port to and from Carrier entities that may or may not be owned by the Company they are a part of (ie some form of resale).

Carrier – Service Provider	
Unique identifier for one of the Service Providers from Service Provider table	
Unique identifier for one of the Carriers from Carrier table	
Read-Only "Y" = Yes, "N" = No.	

- See Technical Specification Section 3.5.8 for additional information

- It is worth noting that Read-Only should be set to No for most relationships. A setting of Y would indicate an Service Provider can only port out from a given Network and might be used during the phasing out of a Network.

9 Additional Data

Number Ranges

(viii)

- The IPMS stores a list of Number Ranges and Donor Carriers. Any new entrant with Number Ranges allocated to them by the NAD must supply details for inclusion to enable Porting in those ranges.

Number Range, e.g. 099596	
Unique identifier for one of the Carriers from Carrier table, e.g. 11647	

Users and User Profiles

(ix)

- A super user for the new Company will be added. The new Company can then add User Profiles and Users as appropriate. User Profiles must have Carriers and/or Service Providers selected for Users to be able to perform the relevant functions.

- See Technical Specification Sections 3.5.18 and 3.5.20 for additional information.

Queuing by Number Range

(x)

- The Carrier can manage what updates it receives for 3rd Party Network Updates, and can manage this through the Queuing by Number Range table. It is more relevant to Companies with multiple Carrier entities in the IPMS or those using a CSD model.

- See Technical Specification Section 3.5.15 for additional information.

Queuing by Carrier Type

(xi)

- The Carrier can manage separately whether it receives Network Updates for Local and Mobile Ports.

- See Technical Specification Section 3.5.16 for additional information.

Appendix I. Special Projects Upload File Structure

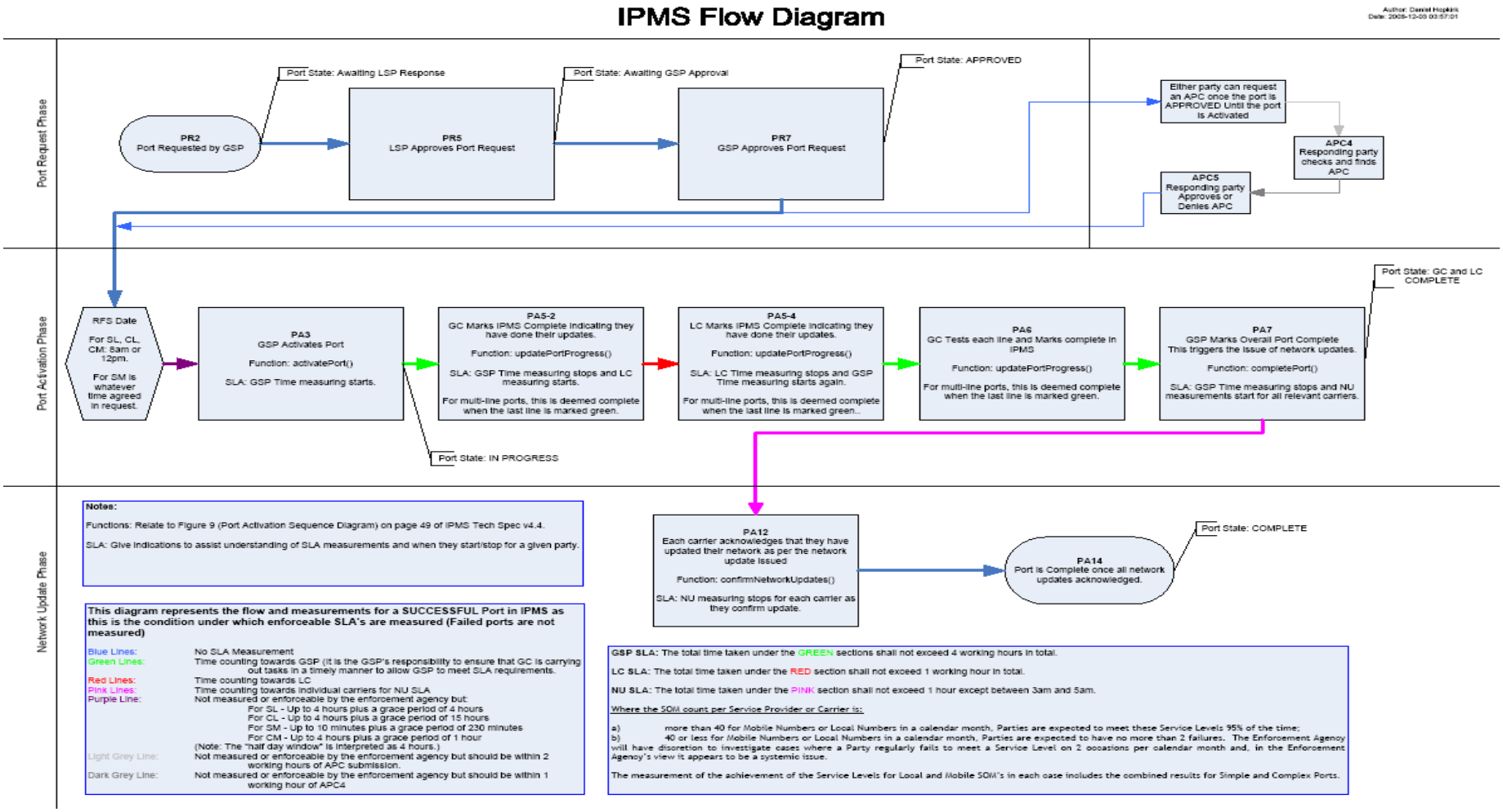
Header record

Field name	Data Type	Description
Company Name	One String – VarChar(50)	Company name as defined in IPMS database, e.g. ”Vodafone NZ Ltd”
File Date and Time	DateTime – DDMMMYYYY HH:MM:SS	Date and time when file was created, e.g. 31NOV2005 23:59:59

Detail record

Field name	Data Type	Description
Number	VarChar(11)	String of up to 11 numeric digits, including area code or prefix with leading zero, e.g. 0271234567 for Mobile, or 097654321 for Local Numbers
Carrier Name	Integer	ID of one of the Carriers defined in IPMS database, e.g. 11407
Service Provider Name	One String – VarChar(50)	Name of one of the Service Providers defined in IPMS database, e.g. “Vodafone, “Woosh”

Appendix J. IPMS Flow Diagram



Appendix K. Table 2: Service Levels

The table below sets out the Service Level for given steps in the Porting Processes as detailed in the LMNP Terms. The 3 columns to the right have been added to clarify which Service Levels are currently measured and/or monitored by the Enforcement Agent and have been included for information purposes only.

Action	Party	Process	Local		Mobile		Measured by IPMS	Monitored by the Enforcement Agent (EA)	Comments
			Simple	Complex	Simple Pre-Pay or Post-Pay	Complex Post-Pay			
Responds to Port Request (PR4 to PR6)	LSP	Port Request	Within one Business Day	Within two Business Days	Within 30 Working Minutes	Within two Business Days	Can be although not currently measured	No	Not currently measured in IPMS or monitored by the EA as it is not customer impacting.
Reviews LSP response and Approves/ Rejects (PR6 to PR8)	GSP	Port Request	Within one Business Day	Within two Business Days	Within 30 Working Minutes	Within two Business Days	Can be although not currently measured	No	Not currently measured in IPMS or monitored by the EA as it is not customer impacting.
Port as GSP/GC (PA3 to PA5.2 and PA5.4 to PA7)	GSP	Port Activation	At agreed time[2]	At agreed time[2]	N/A[1]	At agreed time[2]	Yes	Yes	Currently measured and enforced as this is customer impacting.
Port as Losing Carrier (PA5-3 to PA5-4)	Losing Carrier	Port Activation	Within one Working Hour[3]	Within Four Working Hours[3]	Within ten Working Minutes[3]	Within Four Working Hours[3]	Yes	Yes	Currently measured and enforced as this is customer impacting.
Port as 3rd party	Donor	Port	Within one	Within	Within one	Within	Yes	Yes	Currently

Action	Party	Process	Local		Mobile		Measured by IPMS	Monitored by the Enforcement Agent (EA)	Comments
			Simple	Complex	Simple Pre-Pay or Post-Pay	Complex Post-Pay			
and Donor Carrier (PA8 to PA12)	Carrier	Activation	Working Hour except between the hours of 03:00 am and 05:00 am[3]	one Working Hour except between the hours of 03:00 am and 05:00 am[3]	Working Hour except between the hours of 03:00 am and 05:00 am[3]	one Working Hour except between the hours of 03:00 am and 05:00 am[3]			measured and enforced as this is customer impacting.
APC Response to request (APC3 to APC5)	Responding Party (GSP or LSP)	Approved Port Change	Within two Working Hours	Within four Working Hours	Within two Working Hours	Within four Working Hours	Can be although not currently measured	No	Not currently measured in IPMS or monitored by the EA as it is not customer impacting.
APC update service orders from APC changes (APC7 and APC8)	Gaining Carrier and Losing Carrier	Approved Port Change	Every Working Hour	Every two Working Hours	Every Working Hour	Every two Working Hours	Can be although not currently measured	No	Not currently measured in IPMS or monitored by the EA as it is not customer impacting.
Relinquishment of Ported Number (NR2)	Host Carrier	Ported Number Relinquishment	Within five Business Days	Within five Business Days	Within five Business Days	Within five Business Days	No	No	Not able to be measured by IPMS
Relinquishment as 3rd party and Donor Carrier (if required) (NR2 to NR4)	Other Carrier and Donor Carrier	Ported Number Relinquishment	Within one hour except between the hours of	Within one hour except between the hours of	Within one hour except between the hours of 03:00am and	Within one hour except between the hours of	Can be although not currently measured	No	Not currently measured in IPMS or monitored by the EA as it is not customer impacting.

Action	Party	Process	Local		Mobile		Measured by IPMS	Monitored by the Enforcement Agent (EA)	Comments
			Simple	Complex	Simple Pre-Pay or Post-Pay	Complex Post-Pay			
			03:00am and 05:00am[3]	03:00am and 05:00am[3]	05:00am[3]	03:00am and 05:00am[3]			
Confirmation of service order deletion for Port Expiry (PE5 to PE8)	Gaining Carrier and Losing Carrier	Port Expiry	Within four Working Hours	Within four Working Hours	Within four Working Hours	Within four Working Hours	Can be although not currently measured	No	Not required to be measured in IPMS (stated in LMNP Terms)
Port Withdrawal (entire process)	GSP	Port Withdrawal	Within four Working Hours	Within four Working Hours	Within four Working Hours	Within four Working Hours	Can be although not currently measured	No	Not required to be measured in IPMS (stated in LMNP Terms)
Confirming Port Withdrawal (PW3 to PW5)	Losing Carrier	Port Withdrawal	Within two Working Hours	Within two Working Hours	Within two Working Hours	Within two Working Hours	Can be although not currently measured	No	Not required to be measured in IPMS (stated in LMNP Terms)

[1] The Gaining Carrier activates as soon as they wish to.

[2] Agreed between both the GSP and LSP, being within the prescribed working hours for Local and Complex Mobile.

[3] This Service Level comes into effect the first full calendar month after this Clarification Application is approved by the Commerce Commission. Prior to this amended Service Level coming into effect, the existing Service Level shall apply.

Where the SOM count per Service Provider or Carrier is:

a) more than 40 for Mobile Numbers or Local Numbers in a calendar month, Parties are expected to meet these Service Levels 95% of the time.
b) 40 or less for Mobile Numbers or Local Numbers in a calendar month, Parties are expected to have no more than 2 failures. The Enforcement Agency will have discretion to investigate cases where a Party regularly fails to meet a

Service Level on 2 occasions per calendar month and, in the Enforcement Agency's view it appears to be a systemic issue.

The measurement of the achievement of the Service Levels for Local and Mobile SOM's in each case includes the combined results for Simple and Complex Ports.

Appendix L. Account Number Lengths and Type

NAME	MIN LENGTH	MAX LENGTH	ACCOUNT NUMBER TYPE
2Degrees	2	12	Alpha
2Degrees Local	8	10	Alpha
2Talk Local	8	8	Numeric
NOW	10	10	Numeric (starting 31337)
B+W Local	10	10	Numeric
B+W Mobile	10	10	Numeric
CallPlus	4	8	Alpha
CallPlus Mobile	4	8	Alpha
CallPlus Reseller	1	40	Numeric
Compass Local	6	7	Numeric
Compass Mobile	6	7	Numeric
Digital Island Local	5	5	Numeric
Digital Island Mobile	5	5	Numeric
iHug	4	16	Numeric
Link Telecom	5	14	Alpha
M2 Local	10	10	Numeric
M2 Mobile	10	10	Numeric
Megatel Mobile	12	14	Alpha
MyNetFoneAust	6	14	Numeric
Orcon	8	8	Numeric
Orcon Mobile	8	8	Numeric
Skype	1	150	Alpha
Snap Mobile	6	7	Numeric
Symbio Wholesale	6	14	Numeric
TelcoInABox Mobile	4	10	Numeric
Teletraders Local	8	32	Alpha
Vodafone (TCL) Local	1	30	Numeric
Vodafone (TCL) Mobile	1	30	Numeric
Spark Local	8	12	Numeric
Spark Mobile	8	17	Numeric
Vodafone NZ Local	6	12	Numeric
Vodafone NZ Mobile	6	12	Numeric
Woosh	4	16	Numeric
WorldxChange Local	7	12	Numeric
WorldxChange Reseller	1	40	Alpha
Zintel Cogent Mobile	3	12	Alpha

Prepay/Postpay Mobile Account Lengths

Service Provider	Prepay/Postpay	Account#	SIM ID
2Degrees	Both	6 digits	18 digits
B+W	Postpay	10 digits	NA
Compass	Postpay	6 digits	NA
M2	Postpay	10 digits	NA
Orcon	Postpay	8 digits	NA
Spark	Both	9 digits	17 digits
Vodafone (TCL)	Postpay	4-8 digits	NA
Vodafone	Both	9 digits (starting 3 or 0)	Last 12 digits only (remove 6401 or STK Vx.x.x)
CallPlus	Postpay	8 digits	NA
Digital Island	Postpay	5 digits	NA
Megatel	Postpay	12 digits	NA
Snap Internet Mobile	Postpay	6 digits	NA
TelcoInaBox	Postpay	6 digits	NA
Zintel Cogent	Postpay	10 digits	NA

Appendix M. QBNR Entries in TEST and DEV

No QBNR Entries:

PHONENUMBERPREFIX	DONOR	CODE	DESCRIPTION
0201	VFNZ01	11937	Mobile
021	VFNZ01	11937	Mobile
0210	VFNZ01	11937	Mobile
021029	VFNZ01	11937	Mobile
02110	VFNZ01	11937	Mobile
021189	VFNZ01	11937	Mobile
02120	FBNTCLMob	99877	Mobile
0213	VFTEST1	99967	Mobile
02130	FBNSparkMob	99897	Mobile
0214	VFNZ01	11937	Mobile
0218	VFNZ01	11937	Mobile
021917	VFNZ01	11937	Mobile
022	2degrees	11507	Mobile
0229361	VFNZ01	11937	Mobile
0229362	FBNVodafoneMob	99917	Mobile
0229367	SPARKMOBILE	11647	Mobile

Ranges with Limited QBNR Entries:

RANGE	TYPE	DONOR	Carrier ID	Carrier Name
0201	Mobile	VFNZ01	11677	ORCONLOCAL
0201	Mobile	VFNZ01	11937	VFNZ01
02130	Mobile	FBNSparkMob	11647	SPARKMOBILE
02130	Mobile	FBNSparkMob	99897	FBNSparkMob
02130	Mobile	FBNSparkMob	99899	SPARKMOBILE1
0229361	Mobile	VFNZ01	11507	2degrees
0229361	Mobile	VFNZ01	11677	ORCONLOCAL
0229362	Mobile	FBNVodafoneMob	11507	2degrees
0229362	Mobile	FBNVodafoneMob	11677	ORCONLOCAL
0229367	Mobile	SPARKMOBILE	11507	2degrees
0229367	Mobile	SPARKMOBILE	11677	ORCONLOCAL
0229368	Mobile	FBNSparkMob	11507	2degrees
0229368	Mobile	FBNSparkMob	11677	ORCONLOCAL
0240123	Mobile	DummyMobile	11507	2degrees
0245	Local	WOOSH01	11507	2degrees
0245	Local	WOOSH01	11677	ORCONLOCAL
024901	Mobile	2degrees	11507	2degrees
024901	Mobile	2degrees	11647	SPARKMOBILE
024902	Mobile	2degrees	11507	2degrees
024902	Mobile	2degrees	11937	VFNZ01
02709	Mobile	FBNVodafoneMob	11937	VFNZ01
02709	Mobile	FBNVodafoneMob	99917	FBNVodafoneMob
027099	Mobile	FBNVFMob2	11937	VFNZ01

027099	Mobile	FBNVFMob2	99917	FBNVodafoneMob
0272	Mobile	SPARKMOBILE	11647	SPARKMOBILE
0272	Mobile	SPARKMOBILE	99897	FBNSparkMob
0272	Mobile	SPARKMOBILE	99899	SPARKMOBILE1
0273	Mobile	SPARKMOBILE	11647	SPARKMOBILE
0273	Mobile	SPARKMOBILE	99899	SPARKMOBILE1
0274	Mobile	SPARKMOBILE	11647	SPARKMOBILE
0274	Mobile	SPARKMOBILE	99897	FBNSparkMob
0274	Mobile	SPARKMOBILE	99899	SPARKMOBILE1
0274011	Mobile	FBNVodafoneMob	11417	TCLA100
0274011	Mobile	FBNVodafoneMob	11937	VFNZ01
0274011	Mobile	FBNVodafoneMob	99917	FBNVodafoneMob
0274012	Mobile	FBNVodafoneMob	11417	TCLA100
0274012	Mobile	FBNVodafoneMob	11937	VFNZ01
0274012	Mobile	FBNVodafoneMob	99917	FBNVodafoneMob
0274013	Mobile	FBNVodafoneMob	11417	TCLA100
0274013	Mobile	FBNVodafoneMob	11937	VFNZ01
0274013	Mobile	FBNVodafoneMob	99917	FBNVodafoneMob
0274014	Mobile	FBNVodafoneMob	11417	TCLA100
0274014	Mobile	FBNVodafoneMob	11937	VFNZ01
0274014	Mobile	FBNVodafoneMob	99917	FBNVodafoneMob
0274015	Mobile	FBNVodafoneMob	11417	TCLA100
0274015	Mobile	FBNVodafoneMob	11937	VFNZ01
0274015	Mobile	FBNVodafoneMob	99917	FBNVodafoneMob
0275	Mobile	SPARKMOBILE1	11647	SPARKMOBILE
0275	Mobile	SPARKMOBILE1	99899	SPARKMOBILE1
0276	Mobile	SPARKMOBILE	11647	SPARKMOBILE
0276	Mobile	SPARKMOBILE	99899	SPARKMOBILE1
0277	Mobile	SPARKMOBILE	11507	2degrees
0277	Mobile	SPARKMOBILE	11677	ORCONLOCAL
0279	Mobile	SPARKMOBILE	99887	FBNSparkLoc
02824	Mobile	VFNZ01	11937	VFNZ01
028258	Mobile	VFNZ01	11937	VFNZ01
02910	Mobile	TCLH01	11937	VFNZ01
02910	Mobile	TCLH01	99907	FBNVodafoneLoc
02910	Mobile	TCLH01	99917	FBNVodafoneMob
0298	Mobile	VFNZ01	11417	TCLA100
0298	Mobile	VFNZ01	99867	FBNTCLLoc
029997	Mobile	FBNSparkMob	11647	SPARKMOBILE
029997	Mobile	FBNSparkMob	99897	FBNSparkMob
029997	Mobile	FBNSparkMob	99899	SPARKMOBILE1
0421000	Local	VFNZ02	11237	VFNZ02
0421000	Local	VFNZ02	11937	VFNZ01
0421000	Local	VFNZ02	99907	FBNVodafoneLoc
04239	Local	SPARKLOCAL	11507	2degrees
04239	Local	SPARKLOCAL	11657	SPARKLOCAL
04239	Local	SPARKLOCAL	99887	FBNSparkLoc
04810	Local	SPARKLOCAL1	11507	2degrees
092500	Local	SPARKLOCAL	11417	TCLA100
092500	Local	SPARKLOCAL	11657	SPARKLOCAL

092500	Local	SPARKLOCAL	99867	FBNTCLLoc
09660	Local	SPARKLOCAL1	11507	2degrees
098811	Local	LINKTEL01	11517	LINKTEL01
09908	Local	TCLA101	11417	TCLA100
09908	Local	TCLA101	11657	SPARKLOCAL
09908	Local	TCLA101	99867	FBNTCLLoc
099375	Local	FBNSparkLoc	11507	2degrees
099375	Local	FBNSparkLoc	11677	ORCONLOCAL
099375	Local	FBNSparkLoc	99889	SPARKLOCAL1
0994900	Local	VFNZ02	11237	VFNZ02
0994900	Local	VFNZ02	11937	VFNZ01
0994900	Local	VFNZ02	99907	FBNVodafoneLoc
0994901	Local	VFNZ02	11237	VFNZ02
0994901	Local	VFNZ02	11937	VFNZ01
0994901	Local	VFNZ02	99907	FBNVodafoneLoc
0994902	Local	VFNZ02	11237	VFNZ02
0994902	Local	VFNZ02	11937	VFNZ01
0994902	Local	VFNZ02	99907	FBNVodafoneLoc
0994903	Local	VFNZ02	11237	VFNZ02
0994903	Local	VFNZ02	11937	VFNZ01
0994903	Local	VFNZ02	99907	FBNVodafoneLoc
0994904	Local	VFNZ02	11237	VFNZ02
0994904	Local	VFNZ02	11937	VFNZ01
0994904	Local	VFNZ02	99907	FBNVodafoneLoc
0994905	Local	VFNZ02	11237	VFNZ02
0994905	Local	VFNZ02	11937	VFNZ01
0994905	Local	VFNZ02	99907	FBNVodafoneLoc
0994906	Local	VFNZ02	11237	VFNZ02
0994906	Local	VFNZ02	11937	VFNZ01
0994906	Local	VFNZ02	99907	FBNVodafoneLoc
0994907	Local	FBNVodafoneLoc	11237	VFNZ02
0994907	Local	FBNVodafoneLoc	11937	VFNZ01
0994907	Local	FBNVodafoneLoc	99907	FBNVodafoneLoc
0994908	Local	VFNZ02	11237	VFNZ02
0994908	Local	VFNZ02	11937	VFNZ01
0994908	Local	VFNZ02	99907	FBNVodafoneLoc
099495	Local	VFNZ02	11237	VFNZ02
099495	Local	VFNZ02	11937	VFNZ01
099495	Local	VFNZ02	99907	FBNVodafoneLoc
09984	Local	FBNSparkLoc	11657	SPARKLOCAL
09984	Local	FBNSparkLoc	99887	FBNSparkLoc
09984	Local	FBNSparkLoc	99889	SPARKLOCAL1

Appendix N. Security Policies for IPMS

Since IPMS went live in April 2007, the TCF has granted access to the system to Parties to the Determination and Third Parties (including Resellers as well as SMS providers, emergency services operators and other Ministries and interested parties).

Security requirements for individual access to IPMS have been left primarily to the companies that execute an access agreement with the TCF, providing that the company itself remains liable for any misuse by their "Authorised Users". There have also existed a number of unwritten policies and procedures to ensure the ongoing security of the IPMS system.

Following the recommendations of the Voco Report dated March 2014, the policies for access to IPMS are set out below

General Policies and Procedures

Given the critical nature of the IPMS system, the TCF recognises the importance in having oversight of who uses the system and ensuring that Parties to the Determination and other authorised entities that use IPMS adhere to good security practices.

The following items list the good security practices the TCF requires:

- The admin account (ipmsadmin) used by the NP co-ordinator must have the password changed every 90 days. The co-ordinator is not able to change this timeframe, it is the same policy used for application support personnel.

- No user, including the ipmsadmin user can see user passwords; they are obscured in a hashing algorithm. Passwords can and should be changed when required by this policy.

- Individual users should have individual user accounts. The use of admin-class accounts should be limited to managers and key personnel only. There should be a minimum of 2 admin-class accounts per company to ensure redundancy if one account is locked out or the staff member leaves the organisation. Admin-class accounts should not be used for automated systems.

- IPMS does not allow the ipmsadmin account to perform account maintenance on non-admin accounts. It is the responsibility of the admin class account users to maintain their own individual users. Admin-class account users should regularly, at least twice a year, review the needs and requirements of their individual users and ensure that they have the level of access appropriate to their role. Similarly, the ipmsadmin should review the needs of admin-class account users at least twice a year to ensure that all policies and requirements of IPMS are being met (such as password expiry length and the number of admin-class accounts).

- Because the logs and archive requires user accounts to remain in place even when they have become inactive, user accounts can never be deleted. User

accounts should be made inactive as soon as practicable after an admin-class account user becomes aware that the individual user no longer requires access to IPMS. The ipmsadmin can and should make accounts inactive if he becomes aware that an individual user has left an organisation or no longer requires access and this has not been done by the admin-class account user within a reasonable time.

- In some cases, the NP Co-ordinator may have a company specific admin account (RCAdmin) within a carrier. This is created only with permission from the carrier concerned and is used only for carrier account administration where there is urgent need. Some carriers choose to disable this account when not required.

- Automation (API) accounts may have a long password expiry (9999 days) because it can be expensive and difficult to change passwords in automation, especially if poor design means that the password is stored in multiple locations. The disabling of automation accounts can cause widespread inconvenience to the industry. To minimise the risk of potential breach, API accounts should have long passwords of at least 10 made up of randomised letters, numbers and/or symbols.

- Individual users and admin-class account users should have the passwords changed no less frequently than every 90 days.

- Weekly reports are sent to the NP Co-ordinator on expired and expiring passwords. The NP Coordinator will review and note these. If an API account is involved, the NP Coordinator should take immediate action along with the carrier to reset this password. If individual admin accounts are noted, the NP Coordinator is to log these and raise them with the carrier if they appear in the following week's list of expired passwords.

- Error logs are sent to the NP Co-ordinator weekly, these are logged and graphed. Any spikes or trends are closely examined and relevant carriers are contacted about their processes, and asked to explain. Advice can be given on possible solutions and improvements.

- API activity is logged daily, tabled and graphed weekly, and reviewed by the NP Co-ordinator. Spikes or unusual activity are investigated and followed up with Application Support or the carrier concerned.

Escalation

Any highly abnormal activity or activity which would indicate that a user's account has been compromised or used contrary to this security policy should be raised by the NP Coordinator with the carrier concerned and the Forum Administrator immediately. Any such activity must be investigated thoroughly to rule out any instance of a malicious use of IPMS. The account may be made inactive during this time to rule out third party involvement.

The Forum Administrator and the NP Coordinator will inform the TCF CEO of the relevant event and the work in progress to identify or resolve the event as soon as practicable. The TCF CEO will be responsible for informing the TCF Board of the matter in due course.