**Unauthorized Port flow**

*Submitted By: NPIF*

*Date Accepted: 07/07/2015*

*Revised: 06/05/2018*

*Revised 08/10/2018*

*Version: 3*

**Version History:**

This Best Practice was created by the LNPA WG (now known as the NPIF – Number Portability Industry Forum) and originally accepted on 07/07/2015 (Version 1). This Best Practice was reviewed on 06/05/2018 where an action item was taken to update the language for this process to be consistent throughout the document (version 2). Additional updates were made as part of the discussion at the 08/10/2018 meeting (version 3).

**Background:**

As porting volumes have significantly increased, a higher volume of attempted unauthorized porting activity is being experienced. It has become increasingly more difficult to determine how to approach a resolution without consistent guidelines about which information can be examined and/or exchanged between providers/carriers. When determining how to address an out of service or unauthorized port, the flow should provide a detailed outline for carriers to follow to resolve customer complaints.

**Documentation Referenced:**

In addition, there are three other Best Practices that address different aspects of returning ported numbers to the original/rightful owner and preventing unauthorized/disputed ports. They are:

* [**BP 037 - Use of Evidence of Authorization v3**](https://workinggroup.numberportability.com/documents/8554/BP_037_-_Use_of_Evidence_of_Authorization_v3.docx)
* **BP 058 – Handling of Disputed Ports**
* [**BP 068 - Stolen Telephone Numbers**](https://workinggroup.numberportability.com/documents/5734/0068__Stolen_Telephone_Numbers.docx)

These Best Practices should also be referenced/followed when addressing the return of a ported number.

**Decisions/Recommendations**

NPAC LNPA WG Best Practice 0073

Unauthorized Port Flow

This best practice addresses three types of Unauthorized Ports\*:

**Disputed Port** – A disputed port is commonly a result of two or more parties each claiming to be the authorized end user. Examples may include: business partner disputes, personal relationship disputes, dissolution of franchises, etc.

**Inadvertent Port** – Any port which occurred because of an error. Errors which result in Inadvertent Ports may include, but are not limited to: incorrect number provided by End User, typographical errors in LSRs, LOAs, etc.

**Fraudulent Port** – A port which occurred as the result of an intentional act of fraud, theft and/or misrepresentation. Examples may include: use of numbers for credit card fraud, vanity number fraud, etc.

\* This Best Practice applies to both completed ports, as well as, ports in process which may be subject to an allegation of Unauthorized Porting activity.

Please Note: This best practice does not address Slamming.

Per FCC, Slamming is the illegal practice of switching a consumer's traditional wireline telephone company for local, local toll, or long distance service without permission. The FCC's slamming liability rules also prohibit unreasonable delays in the execution of an authorized switch by your local telephone company. The rules provide a remedy if you've been slammed, discourage slamming by removing the profit and protect consumers from illegal switches. The Communications Act and FCC rules hold telephone companies responsible for the acts of their agents, including their telemarketers. The FCC's Enforcement Bureau can also take action against slammers.

Acronym list

**CMRS –** Commercial Mobile Radio Service (aka cellular)

**CPNI -** Customer Proprietary Network Information

**CSR -** Customer Service Record

**EU -** End User and/or Assignee of a TN(s) or an Authorized User

**FCC -** Federal Communications Commission

**FOC -** Firm Order Confirmation

**LSR -** Local Service Request

**MVNO –** Mobile Virtual Network Operator (aka CMRS Resellers)

**NNSP –** New Network Service Provider

**NPAC – N**umber Portability Administration Center

**NSP -** New Service Provider (may be reseller or otherwise is the same as NNSP)

**ONSP –** Old Network Service Provider

**OSP -** Old Service Provider(may be reseller or otherwise is the same as ONSP)

**PUC -** Public Utility Commission

**TN -** Telephone Number

**WPR -** Wireless Port Request

Unauthorized Port Flow

| Flow Step | **Description** |
| --- | --- |
| 1. START: OSP is notified about an out of service or porting issue | * The process begins with an EU advising their carrier that they are experiencing an out of service or porting issue * If the EU that lost their number is with a reseller, the reseller may contact their underlying network provider(s) to address the dispute * OSP will investigate if a port did occur * If Yes, go to Step 2 * If No, OSP will follow their internal processes to investigate the out of service condition |
| 1. OSP investigates | * OSP may investigate one or more of the following (as may be available): * Review porting LSR/WPR/FOC/NPAC transactions * Compare LSR to CSR if applicable * Review recent porting activity and length of time TN(s) was on an active account * Review TN(s) account (i.e. copy of bill) * Billing Record Name and Authorizing Name vs. LSR * Confirm current provider of TN(s) in NPAC * Ask EU if they inquired about a new service with a different service provider * Ask EU if they know who ported their number * Review incident and/or police report details if provided (official document showing case number or other verification that the matter was reported or attempted to be reported to law enforcement by reporting end user is acceptable) |
| 1. OSP will define priority level | * Based on the data found in Step 2, the OSP will identify priority as a Level 1 or Level 2 * Level 1 is an Unauthorized Port that has a heightened severity of impact. Examples may include: FCC/PUC/Attorney General complaint; court order; military institution; medical facility; business lines (i.e. national organization, main published line); emergency services; medical support services; or otherwise documented as properly reported to law enforcement. * Level 2 is all Unauthorized Ports that do not qualify as a Level 1 |
| 1. OSP will review and attempt to determine the type of Unauthorized Port and contact NSP | * OSP will contact NSP, or reseller if applicable, and share any relevant information without violating CPNI rules which may include: * Information collected in Step 2 * Prioritization level in Step 3 * If determined, the OSP will communicate the type of Unauthorized Port * Inadvertent Port * Disputed Port * Fraud/Vanity Port |
| 1. NSP acknowledges and researches | * Recommended response time frames for the NSP to acknowledge OSP inquiry is within four NSP business hours * NSP should make best effort to prioritize Level 1 issues * NSP may investigate one or more of the following (as may be available):   + Review original and any subsequent porting LSR/WPR/FOC/NPAC transactions   + Review current and prior TN(s) history   + Review CSR or CSR mismatch report (if applicable)   + Review Letter of Authorization (LOA), Wireless Resellers (MVNO) authorization or other form of authorization   + Call history, internal notes and billing activity on new account   + Compare names on NSP account versus the OSP account if applicable or available   + Porting history   + Considerations if new account is wireless prepaid and/or MVNO   + Calling patterns of new user (i.e. calls to financial institutions)   + Contact EU/account holder as appropriate for validation and/or additional documentation (i.e. bill copy [partially redacted acceptable], screen-print, etc.)   + Review police and/or incident report details (if forwarded from OSP) |
| 1. NSP status/resolution response to OSP | * All Unauthorized Ports carry a heightened sense of urgency and should be handled expeditiously * NSP investigation time frames are as follows:   + Level 1 status update(s) as available --- Resolution provided within 1 NSP business day   + Level 2 status update(s) as available --- Resolution provided within 1-2 NSP business days   *NOTE: The complexity of Unauthorized Ports may cause these recommended timeframes to be exceeded.*  *NOTE: Above timeframes also apply to resellers and MVNOs, best effort should be used to resolve issue as quickly as possible.*  *NOTE: If early resolution determination is for NNSP to release the TN(s) to OSP then both providers should coordinate timing (i.e. NNSP will advise when to send LSR or WPR; OSP should not send LSR or WPR until instructed to do so).*  *NOTE: Regardless of the number of carriers involved in an Unauthorized Port, all carriers will work collaboratively to determine the appropriate carrier to regain the number.* |
| 1. OSP and NSP reach conclusion | * Does the NSP agree to release the TN(s)?   + If Yes, go to Step 8   + If No, go to Step 10 |
| 1. NSP agrees to release TN(s) to OSP | * NSP and OSP coordinate release of TN(s) in accordance with industry processes which may include but are not limited to:   + NSP may exchange CSR info to submit an LSR/WPR or alternatively TN(s) may be released at the NPAC level   + OSP sends port request and NSP provides FOC on TN(s)   + NSP notifies OSP that TN(s) has been released   + If reseller does not have NPAC access, go to step 9 * Once TN(s) is activated by OSP, dispute is resolved, go to step 11 |
| 1. NSP Reseller without NPAC access | * Reseller communicates to NNSP that TN(s) is approved for release and/or NSP determines that TN(s) should be released * NNSP releases TN(s) to OSP in NPAC * Reseller communicates to OSP that the TN(s) has been released * Dispute is resolved, go to step 11 |
| 1. NSP does not agree to release TN(s) to OSP | * Will EU of OSP accept number change to close dispute?   + If Yes, the dispute is closed, go to step 11   + If No, then the OSP’s EU/account holder may elect to take any action they deem appropriate |
| 1. End |  |