syniverse®

MNP 9th Amendment Comments

25 September 2023
Syniverse comments to TRAI's "**Draft Telecommunication Mobile Number Portability (Ninth Amendment) Regulations, 2023**" issued 9th September 2023

syniverse®

Table of Contents

syniverse®

Introduction

Syniverse thanks the Telecom Regulatory Authority of India ("TRAI" or "the Authority") for the opportunity to reply with comments to the proposed 9th amendment as issued by TRAI.

Syniverse has many years of experience in multiple countries dealing with MNP and the growing concern over financial fraud perpetrated by either Subscriber Identity Module ("SIM") swaps or SIM swaps in combination with porting.

Simply put, a SIM swap is not achieved via a port, but usually via social engineering where a person posing as the legitimate user convinces the legitimate subscriber's current operator that they need a new SIM card because current SIM card or mobile device has been lost, stolen or damaged. They may present false (but convincing) information or obtain enough information about the target of the SIM swap to be convincing to the legitimate subscriber's current operator. This information may be obtained by social media, database hacking, insider information or even by social engineering of the subscriber to get personal details. The fraudulent user then makes the claim to the legitimate subscriber's current mobile provider.

Meanwhile, the legitimate user is unaware of the SIM swap until his or her phone stops functioning once the SIM swap is effective. At that point, any calls or messages to the device would go to the new device with the new SIM in possession of the fraudulent user. This allows the fraudulent user to either intercept 2nd factor authentication requests (e.g., one-time passwords required to access another account) or prevents the legitimate user from seeing alerts or warning messages from other accounts. This allows the fraudulent user to log into other accounts of the targeted victim and transfer funds, make purchases, or commit other acts of fraud.

Once detected, a SIM swap can usually be reversed with difficulty by visiting the operator, and assuming they can prove their identity sufficiently, have the phone switched back to their device (undo the SIM swap) but if the number is ported as well then the switch back becomes much harder as now a 3rd party (the recipient operator in the port) is involved. This provides additional time for the fraudulent user to exploit the SIM swap.

Organized crime and hackers have learned that making a SIM swap is a weak point in the system. Making the SIM swap harder to accomplish is the best preventative solution, but stopping a port following a SIM swap is also beneficial to the legitimate subscriber and other stakeholders in that it makes the SIM swap somewhat easier to reverse by preventing (or at least delaying) any port of the phone number for a period of time.

Syniverse looks forward to working with the Authority, the mobile operators of India and other relevant stakeholders to make the porting process safe and efficient for consumers to undertake.

syniverse®

Syniverse Point-by-Point Response

Question 1

Whether it would be appropriate to introduce an additional criterion for rejection of the request for allocation of Unique Porting Code (UPC) in respect of any mobile connection, which has undergone the process of SIM swap/ replacement/ upgradation? Kindly provide a detailed response with justification.

Syniverse Response: Syniverse believes that a ten-day waiting period after a SIM swap is an appropriate and reasonable safeguard to minimize fraudulent ports. We know may there be some legitimate subscribers who lost their phone and who might decide at that time to replace or upgrade their device on a new carrier that would be forced to wait the requisite 10 days before being able to port. However, Syniverse believes the solution proposed by the Authority is reasonable because this limitation can be explained to them as it is for their own good both directly and indirectly. We also believe, this would not be too burdensome on a legitimate subscriber who wants to port after a legitimate SIM swap. A legitimate user should be able to understand this because it can be explained that a simultaneous SIM swap, device swap and carrier switch is often a hallmark of fraudulent activity. It is exactly the kind of activity a fraudulent user might take to make the SIM swap reversal more difficult. While this will at times cause inconvenience to a legitimate user it should protect some users who might be targeted and reduce overall costs for all subscribers and society.

Question 2

If your response to the Q1 is in the affirmative, kindly provide detailed inputs on the draft amendment regulations given above.

Syniverse Response: We understand that the Authority is proposing to change regulation 6 of the principal regulations to insert a new clause (i) that would prohibit a port for a period of ten (10) days from the date of the "replacement of SIM, for any reason". So, for example, if the SIM change takes place on the 1st of the month the next available date for a port for that MSISDN would be after the 11th of the same month to exclude the day of SIM swap while considering 10 days guard.

It may need to be further defined if a port could be set up prior to the 12th to be activated on the 12th, or if the subscriber would need to wait until the 12th to generate the UPC and submit the port. This may be necessary since this section of the regulations is triggered during the UPC request phase when the MCH is trying to determine if a UPC should be issued or not and at that point in the process the MCH does not know the subscriber's intended date of port yet.

We view this added clause as a legitimate and reasonable change.

From the 7th amendment, the MCH will issue a UPC based on the response from the donor operator to seven "yes" or "no" answers. If all seven questions are answered correctly a UPC can be issued, otherwise, the UPC request is rejected with a particular error code.

We view the proposed amendment as adding an eighth "yes" or "no" question. Therefore, the logic of the MCH towards issuing a UPC would need to be modified to allow the 8th answer and store it. We would need to create a new error code and response to send to the subscriber.

Meanwhile operators' MNP gateways receiving the UPC info request would need to be able to respond to that request with the 8th answer in a "yes" or "no" format.

Both operators and MCH will need reasonable and adequate time to plan the changes and align resources to design, develop, test, and deploy the process. We do not believe inter-operator testing is required, but there should be time allowed for each stakeholder to test this process. We believe a minimum of six (6) months should be adequate.

The remainder of the proposed changes regarding SIM swap are technical substitutions to the enumeration of the requirements (e.g., replacing clause "(b) to (g)" with "(b) to (h)"), while important these alterations do not change the flow or logic of the porting process. Syniverse views these only as necessary corrections to make the document logically correct.

Question 3

Stakeholders are requested to provide detailed inputs with justification on the DoT's proposal that – (a) after the generation of UPC code, at an appropriate stage, the demographic details of the subscriber such as Name, Gender, Date of Birth and Photograph, etc., or scanned copy of Customer Application Form (CAF)/ Digital CAF may be transferred from Donor Operator to Recipient Operator. To avoid time delays, such transfers may preferably be done through electronic means; and (b) the recipient operator should match the demographic details of the subscriber with those details received from Donor Operator. If the subscriber's demographic details match, then only further steps in MNP process may be allowed otherwise, the porting process may be terminated.

Syniverse Response: Today, by intentional design, very little personal subscriber data is processed by or stored by the MNP Service Providers. This helps prevent identify theft and is consistent with modern principles for safeguarding subscriber privacy. These added data elements will change that fact. We would suggest that the Authority make the MNP Service Providers a pass-through channel only and not store this information in its database. This information is used by the Recipient Operator to validate that the information from the Donor Operator is consistent with the information stated by the subscriber. The MNPSP has no role in this authentication other than being the reasonable and efficient method of transfer of the information. Therefore, Syniverse proposes that the MNPSP hold this information only for a brief period. Upon receipt from the donor operator in a new API call, the MNPSP would immediately transmit the information to the Recipient Operator and then upon acknowledgment of the message receipt from the Recipient remove the data from its temporary cache. Thus, there would be no persistent store of information at the MNPSP database. However, we believe that the MNPSP database should keep a record of the successful (or failed) transmission from the DO to the MNPSP and from the MNPSP to the RO. The exception may be that the MNPSP should retain the information if the RO does not acknowledge the transmission of this information. This would enable the MNPSP to re-transmit it until either the RO acknowledges the transmission, or all re-tries have been extinguished and the UPC expires.

Syniverse also has doubts about the usefulness of scanned images of CAF forms or ID cards, passports, driver's licenses with pictures of the subscriber. Specifically, our doubts concern the quality of these scans and the process for verifying the data. While optical character scans have been around for many years now, they are still not 100% reliable and accurate and this may cause false rejections in many cases which could unnecessarily delay or prevent ports from occurring. We also find that in practice scans can

be of very poor quality often rendering them next to useless. Additionally, these scans consume huge amounts of data. Also scans of facial images are not always clear proof of identity. It is not clear who at the Recipient Operator would determine that the blurry picture taken years ago at the Donor Operator is the same person now. Particularly for teenagers who may look very different at 16 vs. 26 or men who grew or removed facial hair, people who previously wore glasses but now do not. While certain attributes such as inter-pupil differences do not change, and facial recognition has improved much in recent years, it is still far from infallible.

For these reasons, we would recommend that the Authority require the Donor Operator to make this exchange of information in electronic text information via a new porting message rather than a scan of information. We believe that this is already in effect from 1st Oct 2023 as per DOT instructions dated 24 July 2023.

In cases, where this information is exchanged from Donor to Recipient and the Recipient determines the subscriber attempting the port is not legitimate then we would recommend that the port be cancelled leading to unsuccessful porting. Further the Authority may want to recommend that the Recipient inform the donor that the port has been cancelled/unsuccessful so the Donor may notify the legitimate subscriber of the attempt. In addition, it may be worthwhile to consider having the port blocked for an additional period to prevent a fraudulent user from attempting the port again with a different recipient network that may not cancel the port.

Also, the authority should impose a tight time period measured in minutes on the donor providing this information to the Recipient so that the port is not unduly delayed by the donor. Failure to specify a tight time period would result in an effective roll back of the improvements in porting process realized in the 7th amendment implementation. We propose that the MNPSP should send a CAF information request to the Donor operator upon receipt of a valid port request from a Recipient Operator. Sending the subscriber CAF information prior to this point in the porting flow means the information cannot be delivered to the Recipient Operator in timely manner because the Recipient is not yet known. This would require the MNPSP to store information that might never be needed for a much longer period.

Question 4

Are there any suggestions /comments on any other issues for improving the process of porting of mobile numbers? Please provide a detailed explanation and justification for any such concerns or suggestions.

Syniverse Response: In furtherance of amendments/addendum to the existing instruction issued by DOT for adequate verification of customers before enrolling them as subscribers and other subscriber related matters dated 31 Aug 2023, specifically para 4 and 5, to further make the process more efficient and effective, the MNPSP activity may be enhanced to add verification of the digital information submitted by the RO with the central DB of AI & DIU Unit/TAFCOP of DOT with API call.

This would reduce dependency on the DO and would enhance process to check that the subscriber is legitimate. In cases where the subscriber info from RO is not matching with the central DB of AI & DIU Unit/TAFCOP of DOT the MNPSP cold block the mobile number under porting process after comparing other credentials on record.

syniverse®

About Syniverse

Syniverse is the world's most connected company. We seamlessly connect the world's networks, devices, and people, so the world can unlock the full power of communications.

Our secure, global technology powers the world's leading carriers, top Forbes Global 2000 companies, and billions of people, devices, and transactions every day. Our engagement platform delivers better, smarter experiences that strengthen relationships between businesses, customers, and employees.

For over 30 years, we have accelerated important advances in communications technology. Today we are an essential driver of the world's adoption of intelligent connectivity, from 5G and CPaaS to IoT and beyond. Find out more www.syniverse.com.