From: pparag@yahoo.com
To: "Akhilesh Kumar Trivedi" <advmn@trai.gov.in>, "Akhilesh Kumar Trivedi" <advmn@trai.gov.in>
Sent: Tuesday, October 10, 2023 11:50:07 AM
Subject: Response to Draft Telecommunication Mobile Number Portability (Ninth Amendment) Regulations, 2023

To,
Shri Akhilesh Kumar Trivedi,
Advisor (Networks, Spectrum and Licensing),
Telecom Regulatory Authority of India

Dear Sir,

This refers to the Consultation Paper on Ninth Amendment on MNP dated 27/9/2023.

I have enclosed my detailed response on the same (PDF format).
I hope that my submission will merit your kind consideration and support.

Sincerely,

Parag Palsapure
Navi Mumbai
pparag@yahoo.com | +91-9322662040

P.S.: Would highly appreciate if you could acknowledge the receipt of my email. Thanks

Response to TRAI's Draft Telecommunication Mobile Number Portability (Ninth Amendment) Regulations, 2023

Date: Oct 10, 2023

To,
Shri Akhilesh Kumar Trivedi,
Advisor (Networks, Spectrum and Licensing),
Telecom Regulatory Authority of India

Dear Sir,

This refers to the Consultation Paper on Ninth Amendment on MNP dated 27/9/2023. I would like to submit my response on the same.

As widely recognized, citizens are increasingly (and many, mandatorily) being linked, identified and authenticated by their mobile numbers by various institutions to deliver financial and non-financial services. These include, but not limited to, registration of movable and immovable property, tax assessment, educational/health plus many other e-governance services, authentication by UIDAI/Aadhar, targeted benefits, transport, utility, securities trading etc. Mobile numbers are also linked to social media accounts, email/messaging, e-commerce accounts, e-wallets etc.

A fraudster, with a SIM/phone of another citizen, even for a short duration, can easily impersonate that citizen, steal / manipulate data, carry out fraudulent financial and non-financial transactions – e.g. fraudulently transfer movable and immovable assets, reset passwords, access computers, email and social media accounts, cloud storage, carry out illegal / fraudulent shopping, plant malware, trade/mine crypto currencies, distribute illegal or copyrighted content (e.g. hidden torrent), robotic telemarketing and so on. Criminals can also potentially create fake trail of data implicating an honest telecom subscriber in offences or crime that he/she never committed, damage his career and reputation, virtually destroy the victim's life.

Fraudulently obtained SIM can also lead to denial of critical services to genuine telecom subscribers or are made to pay for services they never used intentionally.

Unauthorized SIM swap can be considered violation of fundamental rights granted by articles 12 to 35 under the Part III of the Constitution of India. Abuse of telecom service by unauthorized users can pose serious danger to the National Security.

Therefore, I strongly believe, multiple measures / amendments are required in the telecom regulations, licensing conditions and extend some beyond the telecom domain to:

1. Minimize the chances operators issuing replacement SIMs in non-genuine cases
2. Prevent the issued replacement SIMs to fall in the wrong hands
3. Mitigate risks - limiting the damage even if the replacement SIM or stolen phone has fallen in the wrong hands, through direct and indirect alerts, giving sufficient time for citizen to respond

As a citizen of India, I highly appreciate the TRAI's initiative to address this important issue and taking proactive steps to prevent misuse of telecom services. I hope TRAI will also coordinate

with various agencies/ministries that link citizen's identity with a mobile number to ensure interests of genuine users are protected.

I hope that my submission will merit your kind consideration and support.

With best regards,

Parag Palsapure
Navi Mumbai
pparag@yahoo.com | +91-9322662040

Response / Explanations:

Q4: 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.

Response for Q4:

Significantly improved protection from frauds that use SIM swap techniques is required (especially) for Senior citizens, citizens who travel frequently, citizens with medical conditions or are under treatment, and people from smaller towns/villages who are less alert or not aware of the potential impact of SIM swap.

Therefore, it is necessary to also add additional criteria for rejection of MNP requests and make additional procedural amendments in order to protect genuine telecom subscribers and innocent citizens from any SIM swap frauds.

While the new procedures can potentially add delay for activation of services after porting the telecom service to another service provider or obtaining replacement SIMs, the benefits of the added preventive measures far outweigh the disadvantages. Further, ways are suggested below that could minimize delays and reduce cost of transactions while still mitigating the risks.

Recommendations:

a. In normal circumstances there must be a cooling period of at least 10 days before a new SIM can be issued and activated after earlier SIM replacement, especially in cases of lost / damaged SIM replacement and MNP. If telecom providers agree, their customer portal may be enhanced to include a provision to customize cooling period from 10 days to 30+ days, so that subscribers who are frequently traveling may have better protection.

b. In case of MNP, the Donor Operator must pass the demographics details along with the address of the telecom subscriber seeking MNP to the Recipient Operator. The Recipient Operator shall verify for demographics+address match. In case of any mismatch, the MNP request shall be rejected and telecom subscriber shall be asked to

update the details with the Donor Operator before MNP can be re-initiated. This ensures that telecom operators have more updated records for every subscriber, which is important from the national security perspective too.

c. All telecom operators shall maintain a common database of subscriber numbers violating the usage terms, such as unsolicited telemarketing/UCC, or reported for carrying out phishing or frauds, or are used in criminal activities etc. MNP shall be refused for such numbers for atleast 3 years from last reported violation. This can potentially reduce the menace of telemarketing, phishing etc using telecom services provided in India. Further, such numbers, if deactivated, should not be re-allocated for atleast 6 years to any new subscriber in order to protect the interests of the new subscribers, who may otherwise face the wrath of victims of the criminal (previous subscriber).

d. In case of MNP and SIM replacements (e.g. reported lost/damaged SIM), spot delivery of SIMs at Operator's outlets SHALL BE COMPLETELY BANNED.

    i. Mobile Subscriber shall be required to personally visit the telecom operator's service centers to make an application. In case the subscriber has valid disability/old age/medical reasons and unable to visit the operator's service center, telecom operator's representative shall visit the subscriber on request.
    ii. On successful completion of data verification, **new SIM shall be couriered to the address available in the records (as received from the Donor Operator in cases of MNP and re-verified).**
    iii. Only after confirmation of receipt of delivery of the SIM, activation of the SIM shall be carried out to mitigate risks where SIMs are stolen in transit.
    iv. Measures such as activation code (provided at the service center post receipt of SIM, sent on alternate number / nominee's number or sent via separate letter) can be considered depending upon risk levels.
    v. Fees for courier / speed post of the SIM may be recovered with MNP / SIM replacement charges as necessary.

e. In order to protect all genuine telecom subscriber from frauds, TRAI may prescribe a new procedure that mandates the telecom service provider to issue notification of the SIM replacement to the following key entities which may include:

    i. **UIDAI**: To lock biometrics and temporarily disable certain transactions through OTP (such as real estate registrations, authentication for opening or closure of any bank accounts, withdrawal of EPF, vehicle registrations, Aadhar updates etc), to minimize the chances of fraudulent transactions during cooling period.
    ii. **Employee Provident Fund Organization** (EPFO): To temporarily block fund withdrawal requests, closure of EPF account or any subscriber data updation of the EPF linked account to the subscriber's mobile number.
    iii. **Banking regulator/association:** To temporarily suspend third party electronic funds transfer beyond certain threshold, OTP based authentication for debit or credit card transactions, large withdrawals, changes in account holder details linked to the mobile, change in nominee, bank locker, and outbound transfers from linked demat account.
    iv. **Department of Posts**: to suspend large transactions/updates in Post Office linked bank account, saving schemes etc as above.
    v. **SEBI**: To temporarily suspend electronic funds transfer beyond a threshold and OTP based authentication, changes in account holder details linked to the mobile, suspend large securities transactions etc.
    vi. **Property registrar and RTO/Vahan portal:** In future, various registration departments in future related to registration of transfer of movable and immovable assets (vehicles, real estate etc) to temporarily suspend the

transactions with a cooling period, or to trigger extra precautions during a cooling period.

TRAI may initiate process with above and other identified departments / reputed institutions / authorized agencies to integrate such alerts / databases to protect their clients from frauds. The method of sharing data on SIM swap may be worked out with those agencies separately.

Initially, I suggest a simple provision to be built on TRAI / Operator's portals for query where authorized agencies can enter target MDN to find "**SIM Replacement Status"** (i.e. whether SIM was replaced or number ported during the last 30 days) with simple response as "**YES**" or "**NO**". This will enable various agencies to stop, delay or take additional precautions when authorizing or registering any large or suspicious transactions linked to that mobile.

f. When applying for SIM replacement, subscriber shall be asked to give an undertaking of not using the mobile connection for any unsolicited telemarketing activities, phishing, fraud or any other illegal activity. The same shall also be informed to the subscriber at the telecom operator's service center.

g. In case of SIM upgrades / migration to eSIM or physical SIM, the operator may check the working status of the old SIM and provide new SIM to the telecom subscriber on visiting the operator's service center personally, AFTER verification of ID, address proof and on receipt of the replacement verification code (sent via SMS). Re-KYC shall be required in case of mismatch of demographics/address.

The operator shall ensure that the old working SIM (as applicable) is surrendered by the subscriber before the activation of new SIM/e-SIM. For atleast one week, the new SIM shall be locked to work only with the Mobile handset/device with Electronic Serial Number (ESN) or a Mobile Equipment Identifier (MEID) used by the old SIM. This may prevent cloning and abuse of the process.

h. In order to provide expedited services, in future, Telecom operators may be maintaining a database of verified 'alternate mobile number', 'verified email', and 'nominee' of the subscribers. Only sufficiently aged records shall be used for this process to minimize chances of fraudulent changes in the details before SIM swap.

During Re-KYC or demographics check, the operator may optionally collect verify alternate number / nominee's number and email address. Alerts related to application for MNP, SIM replacement and upgrades shall be sent to alternate/nominee's number, email in addition to subscriber number (as applicable). Shorter activation time may be permitted where alternate number / nominee number is provided, has the same address as subscriber, and through verification using OTPs received on the nominee/alternate number, provided a cooling period of 5 days is completed. Please note that once a fraudster has access to subscriber's mobile handset or computer, the fraudster can also access emails also fraudulently. **Therefore standalone use or overdependence on email/app based OTP verification MUST BE AVOIDED.**

i. **TATKAL MNP / SIM replacement:** A premium service may also be considered where the telecom operator may issue a SIM card (ideally temporary, and with certain

restrictions on services) at the customer service outlet under certain conditions including, but not limited to:

a. Subscriber making application personally and submit following documents
    i. Police complaint/FIR on lost SIM/Phone / copy of FIR along with certificate of verification of applicant's identity and address
    ii. Original Proof of Identity (PoI) documents (operator to verify details, keep a photocopy)
    iii. Original Proof of Address (PoA) documents (operator to verify details, keep a photocopy)
    iv. Photograph + photographed by the operator's service center as part of application.
    v. Affidavit on stamp paper in prescribed format (justification for new SIM, declaration of genuine need, confirmation of authorization, no fraud declaration, Also indicate if there is a mismatch in address in operator record vs new valid proof of address)
    vi. Additional documents - ID and signature verification certificate from a recognized bank (dated after the lost SIM date) along with the original passbook if there is a mismatch in address on records or was recently updated
    vii. Two witnesses and their verified IDs/contacts/addresses in case of address mismatch or if address was recently updated
    viii. Magistrate's / Court's order – as alternative to police certificate
b. In case of MNP: UPC code, CAF in addition to above documents. Police verification for tatkal MNP should be mandatory.
c. Additional premium service fees (TRAI may prescribe after consultation with operators)

Operator may also consider to deactivate this temporary SIM card, replaced with a new SIM card sent via courier at the registered address depending upon risk assessment of individuals, age of customer data, type (replacement SIM vs MNP) validity dates of documents provided and other such factors prescribed by TRAI.

As far as possible, the issuance of replacement SIM should be treated in similar way as issuance of passport from security perspective. **A swapped SIM has potentially higher financial and non-financial risks for the telecom subscriber than a lost Passport.**

j. By default, after MNP, the subscriber shall be automatically enrolled for Do Not Disturb facility to protect from telemarketers. The subscriber may opt-in to marketing as necessary. For SIM replacement and upgrade cases, the DND registration shall be maintained as prior to the SIM replacement.

k. After MNP, the recipient operator shall monitor the call and SMS patterns of the subscriber whether the subscriber is carrying out any telemarketing / phishing or any other fraudulent activity. Appropriate measures shall be taken to curb the menace proactively.