CDSL/OPS/DP/POLCY/2026/517 **July 30, 2026**

VERIFICATION OF MOBILE NUMBER REVOCATION LIST (MNRL) PUBLISHED BY TRAI

DPs are advised to refer Communique no. CDSL/OPS/DP/POLCY/2026/438 dated July 01, 2026, regarding verification of Mobile Number Revocation List (MNRL) published by TRAI.

In view of the above, as per the advisory received from SEBI, for mitigating the potential misuse of mobile numbers, DPs are required to create login credentials on the DoT portal for handling MNRL-related grievances.

DP are advised to refer the Quick Reference Guide for MIIs (Stock exchanges and Depositories) and KRAs refer **Annexure A.** Wherein the information is available to update the Action Taken Reports at DoT Digital Intelligence Platform (DIP)

DPs are advised to take note of the circular and ensure compliance.

Queries regarding this communiqué may be addressed to: CDSL – Helpdesk Emails may be sent **to:** dprtasupport@cdslindia.com and connect through our IVR Number **022-62343333.**

For and on behalf of
Central Depository Services (India) Limited

sd/-

Nilesh Shah
Vice President – Operations

Quick Reference Guide for MIIs (Stock exchanges and Depositories) And KRAs to use the information available and update Action Taken Reports at DoT Digital Intelligence Platform (DIP)

Department of Telecommunications (DoT), Government of India has launched DoT Digital Intelligence Platform (DIP) (https://diu.sancharsaathi.gov.in) which serves as an integrated platform for DoT, Telecom Service Providers, Law Enforcement Agencies (LEAs), Financial Institutions (FIs), Over The Top (OTT) and other stakeholders for bi directional information exchange and coordination for curbing cyber-crime, and financial frauds committed through misuse of telecom resources. More than 1500 organizations including central LEAs, security agencies, State/UT Police, I4C, GSTN, SEBI, NPCI, 1400+ Banks, FIs, TPAPs, PSOs, PPIs, TSPs, NSE, BSE, WhatsApp etc. have been onboarded at DIP. For details refer: https://pib.gov.in/PressReleasePage.aspx?PRID=2011383

2. All the stakeholders onboarded on DIP may update their profile details by following the steps mentioned below:

i. Click on the **Username** tab and select the **User Profile** option

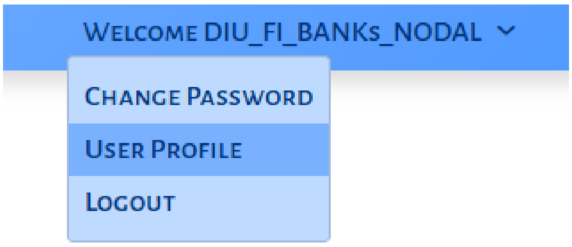
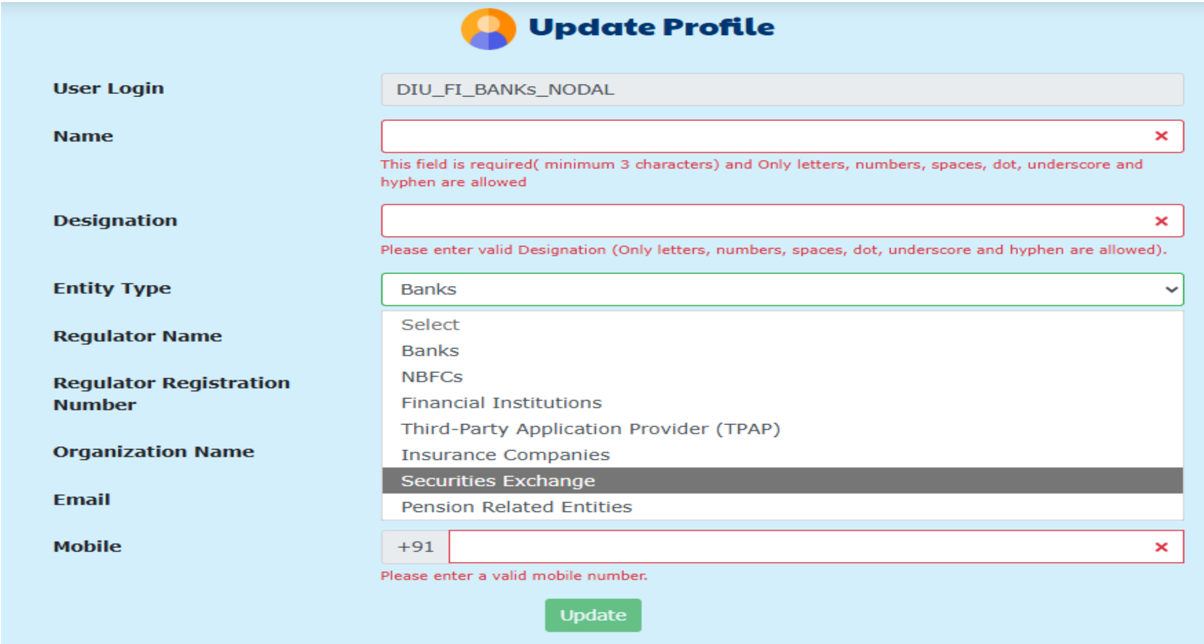


Figure 1 Option to update User Profile

ii. The following additional fields have been incorporated in the Profile section. MIIs and KRAs may update their profile as per the fields available.

a. Name
b. Designation
c. Entity Type
d. Regulator Name
e. Regulator Registration Number
f. Organization Name
g. Email
h. Mobile

Note: The Organisation Name should be the same as the Name in the Registration Certificate and should be in Capital Letters only.



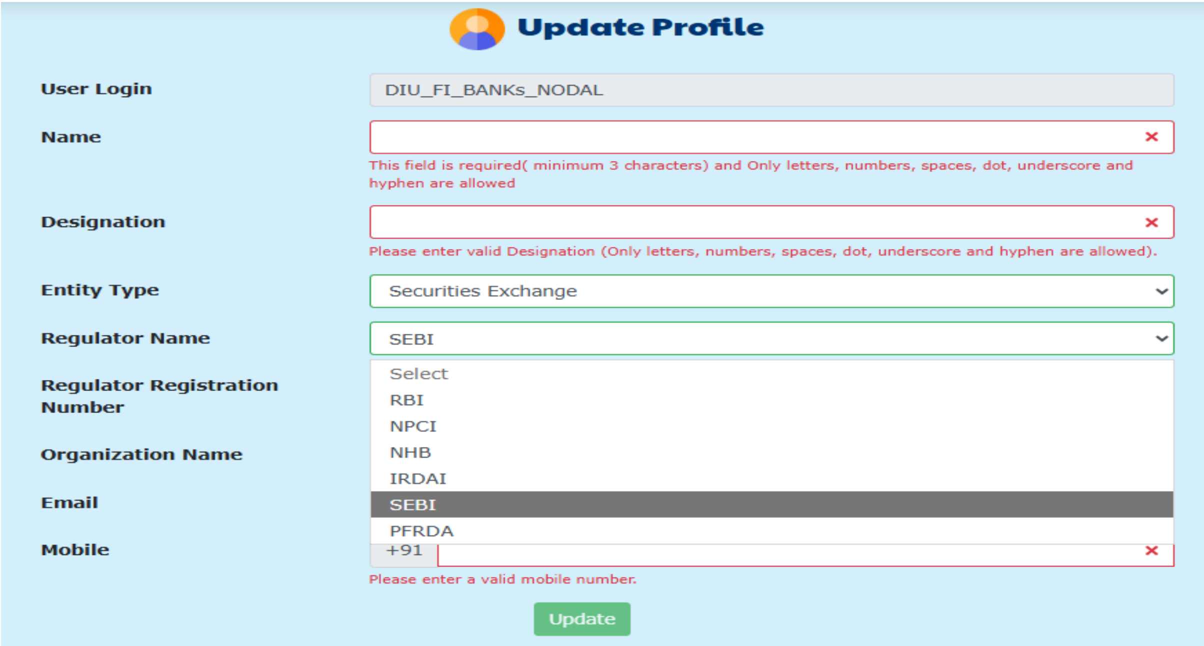


Figure 2 User profile section

3. The DIP offers following facilities to MIIs and KRAs and various stakeholders:

a) Financial Fraud Risk Indicator (FRI) list:

i. The Financial Fraud Risk Indicator (FRI) is a system developed by the Department of Telecommunications (DoT), Government of India to classify mobile numbers based on their potential to be involved in financial fraud. It assigns risk levels (Medium, High, or Very High) to mobile numbers, drawing on data from various sources, including cybercrime reporting portals, telecom data, and information from financial institutions. This allows for real-time, risk-based interventions in banking and UPI transactions to prevent fraud.

ii. The FRI is shared with stakeholders in real-time through DIP, enabling them to take appropriate action, such as blocking transactions or issuing alerts, warnings, notifications or delaying transactions.
iii. SEBI has issued directions to all the MIIs (Stock exchanges and Depositories) and KRAs for integrating FRI in their ecosystem for strengthening the cyber fraud prevention. (Please refer: SEBI directions dated 18.05.2026)
iv. FRI list contains set of active mobile connections which have been flagged by DoT for re-verification because of their suspected misuse in cyber-crime and financial frauds. These mobile numbers are shared with the stakeholders based on Financial Fraud Risk Indicator (FRI) and highly likely to be disconnected in 70 to 80% cases, due to failing re-verification in telecom domain. The disconnected mobile numbers will move from FRI to Mobile Number Revocation List (MNRL) under the categories – Reported by LEAs Reported cybercrime, Subscriber Verification non-compliant cases, DoT Reported fake or forged cases or TSPs Internal Analysis.
v. Based upon FRI, a pro-active action may be taken by stakeholders by adopting necessary real-time response protocols (alerts, transaction delays, warnings, transaction decline, etc.). The FRI empowers the MIIs and KRAs to save the money at the source itself.
vi. The MIIs (Stock exchanges and Depositories) and KRAs are required to carry out enhanced due diligence (EDD) for finding mule accounts linked to these suspected mobile numbers. Based on the FRI category and their internal risk assessment, REs may undertake enhanced customer verification, increased monitoring of trading and financial transactions, periodic review of customer risk profiles, verification of source of funds where warranted, scrutiny of unusual or suspicious transactions, application of additional internal controls or approvals, and such other risk mitigation measures as may be appropriate in accordance with applicable SEBI regulations and their internal policies.
vii. Please refer PIB Press Release: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2130249
viii. The FRI data is available under the module Financial Fraud Risk Indicator (FRI) List.

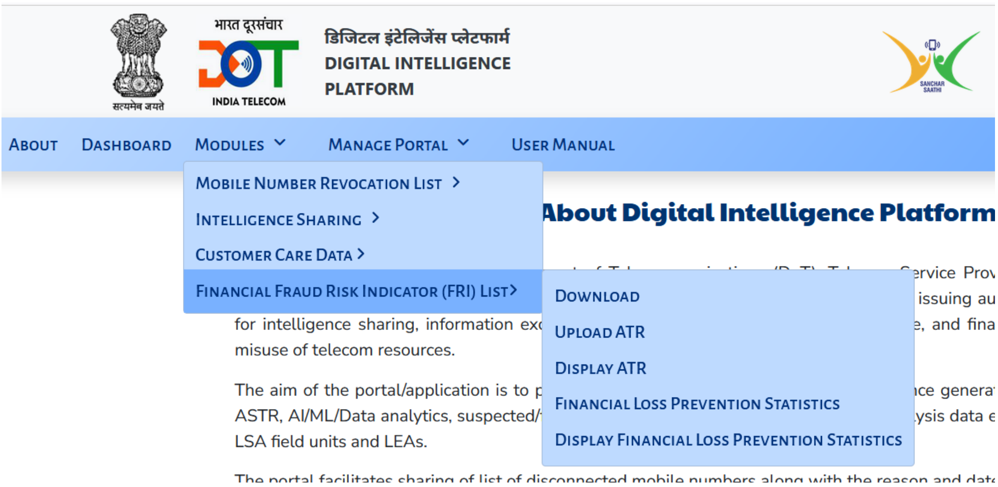


Figure 3: Financial Fraud Risk Indicator (FRI) List at DIP

ix. MIIs and KRAs may download the data on daily basis either through the DIP portal or in real time through the API. The API documentation is available at DIP under the tab User Manual. MIIs and KRAs may scrub these mobile numbers with the list of mobile numbers present in their ecosystem. Based on the matched mobile numbers, actions as advised at Table 1 may be taken by the REs.

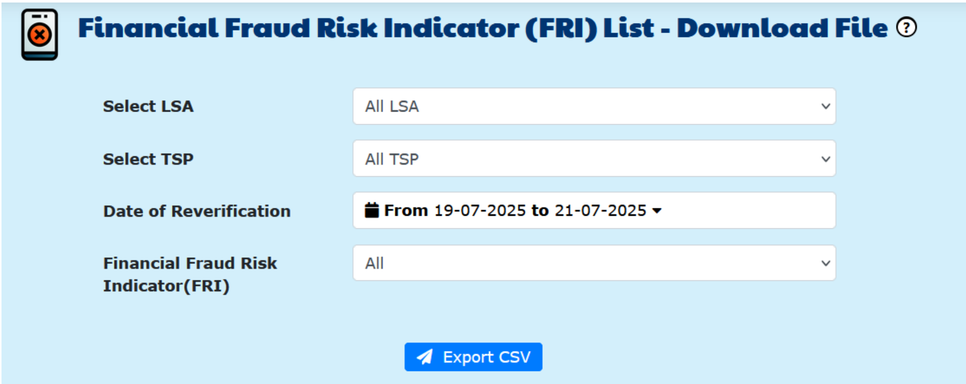
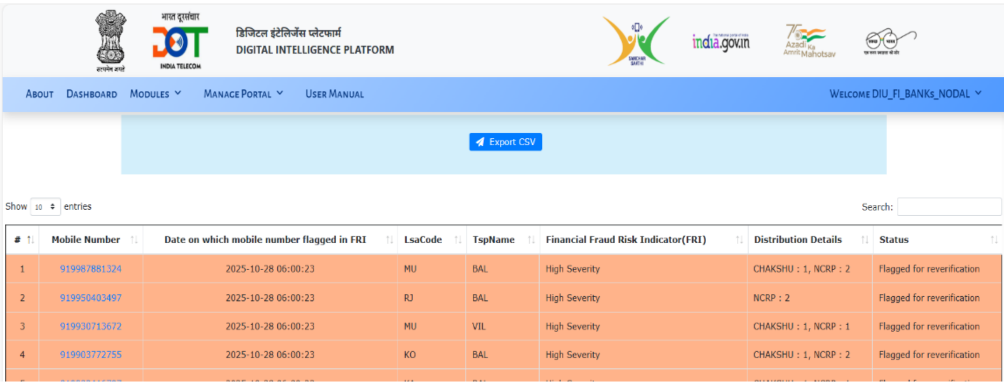


Figure 4: Download Option -Financial Fraud Risk Indicator (FRI) List at DIP

x. The data available in FRI is as shown below:



xi. The data contains details like LSA (State), TSP (Telecom Service Provider), date of Flagging, Status of the number, Distribution details etc. for all suspected numbers under various categories of Medium, High and Very High.

xii. When a number is flagged as suspected, it takes around 15 days for a number to be re-verified and finally either gets compliant or are disconnected. Once the number is flagged for reverification, it is simultaneously sent to stakeholders as part of the FRI list. Everyday new numbers are flagged as part of FRI and some numbers which complete the reverification process are removed from FRI. The complete cycle is defined in the Figure below:

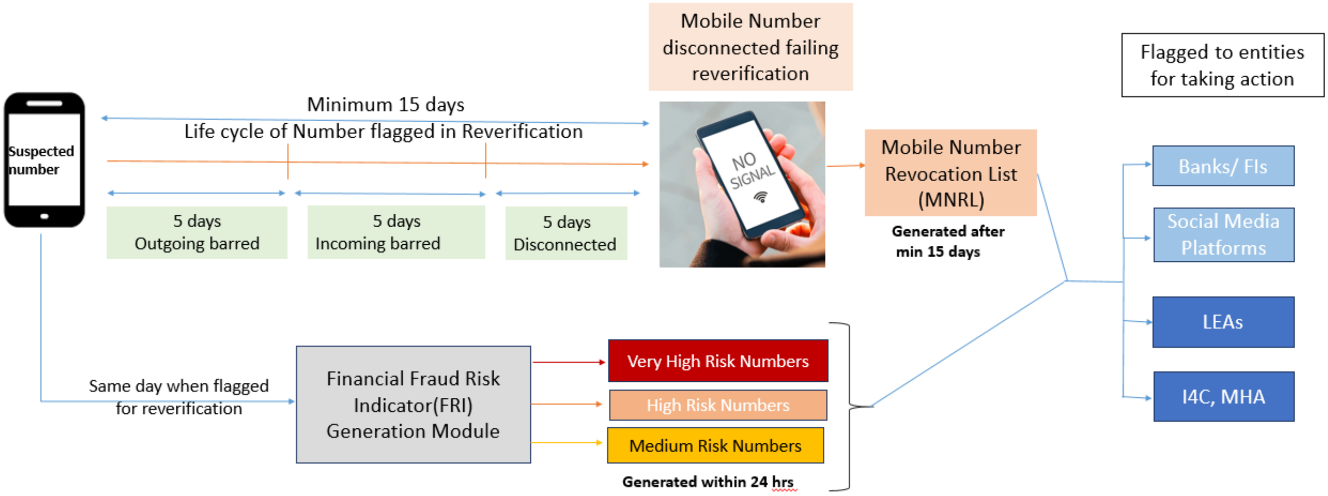


Figure 5: Life cycle of a mobile number flagged as suspected

xiii. Each number which is flagged in FRI will remain in FRI for a minimum duration of 15 days irrespective of its status of reverification.

xiv. Each number appears in FRI under three statuses:

a. **Flagged for reverification:** The number is still under reverification cycle in telecom domain.

b. **Disconnected:** The number has failed reverification and has been disconnected. The action taken by MIIs/KRAs on these numbers should continue and additional action on account and delinking of account maybe done based on EDD. Subsequently these numbers move to MNRL.

c. **Compliant:** The number has been successfully reverified and is working with the same person. There are instances where suspects/ fraudsters even after getting compliant in telecom domain continue to commit frauds. Therefore, these numbers appear in medium category of FRI for another 15 days. So, MIIs/KRAs are advised to give nudge to the citizens even after the number gets compliant for another 15 days.

xv. MIIs/KRAs are advised to refresh the entire FRI list on daily basis and use the new list for taking action as per the Table 1 below.

xvi. **Process flow for using FRI**:

- ***Bank Onboarded on DIP: T***
    - *Download complete FRI data and take action of blocking transactions, generating alerts and blocking accounts*
- ***Action on everyday basis: T+1***
    - *Compare data of T and T+1 and extract:*
        - *Common numbers: Replace T with T+1 and take action*
        - *New numbers of T+1: Take action*
        - *Old cases: Check Status:*
            - *Disconnected/ compliant: Carry forward for next 15 days from date of action and then remove*
            - *To be verified: Carry forward action till status updated*

xvii. The proposed action on transactions for FRI list after EDD by MIIs/KRAs is as under:

Table 1: Suggestive action which may be taken by MIIs/KRAs after EDD

FRI	Status	Inference	Account Based Action	Transaction Based Action
Medium	Flagged for reverification	Number is suspicious	EDD on Account	Real-time Response protocol like Alert/ notification/ warning etc.
Medium	Compliant	Compliant in telecom domain	EDD on Account	Real-time Response protocol like Alert/ notification/ warning etc. after EDD
Medium	Disconnected	Number is disconnected	EDD on account and Delinking of number from account	Real-time Response protocol like Alert/ notification/ warning etc.
High	Flagged for reverification	Number is suspicious	EDD on Account	Real-time Response protocol like transaction declines, transaction delays, etc.

High	Disconnected	Number is disconnected	EDD on account and Delinking of number from account	Real-time Response protocol like transaction declines, transaction delays, etc.
Very High	Flagged for reverification	Number is suspicious	EDD on Account	Real-time Response protocol like transaction declines, transaction delays, etc.
Very High	Disconnected	Number is disconnected	EDD on account and Delinking of number from account	Real-time Response protocol like transaction declines, transaction delays, etc.

Note: MIIs and KRAs should carry out the EDD of accounts linked to FRI mobile numbers, even when the mobile number is found compliant in telecom domain, to check its behaviour in financial domain and rule out or detect any mule bank for further action.

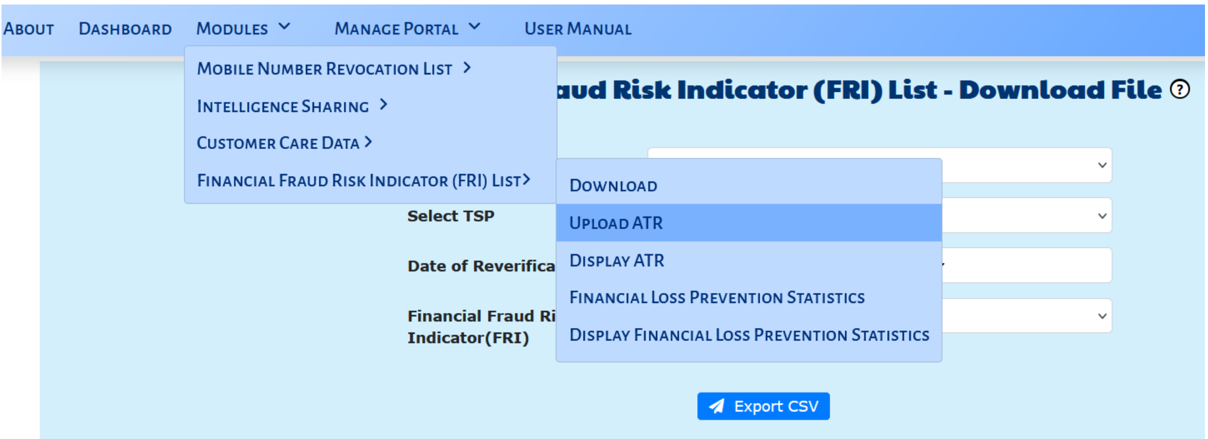


Figure 6: FRI List - Upload Action taken Report (ATR) at DIP

xviii. **Uploading Action taken by MIIs/KRAs:** The MIIs and KRAs may use the above-mentioned tab for uploading the Action taken on the Bank account /profiles linked to the mobile numbers.

xix. Following actions are available:

Type of action	Action Taken
Based on Transactions	Transaction decline
	Transaction Alert / Warning / Notification Generated
Based on EDD	Account not found suspicious after EDD
	User denied service (loan/ insurance/ credit card etc.)

	Account freeze
	Credit and Debit Restriction
	Debit Restriction
	User rejected at the time of onboarding
	User blacklisted

xx. The MIIs and KRAs may use the bulk upload option: Download Sample File, fill the information and use Bulk Upload option or may upload the action taken one by one.

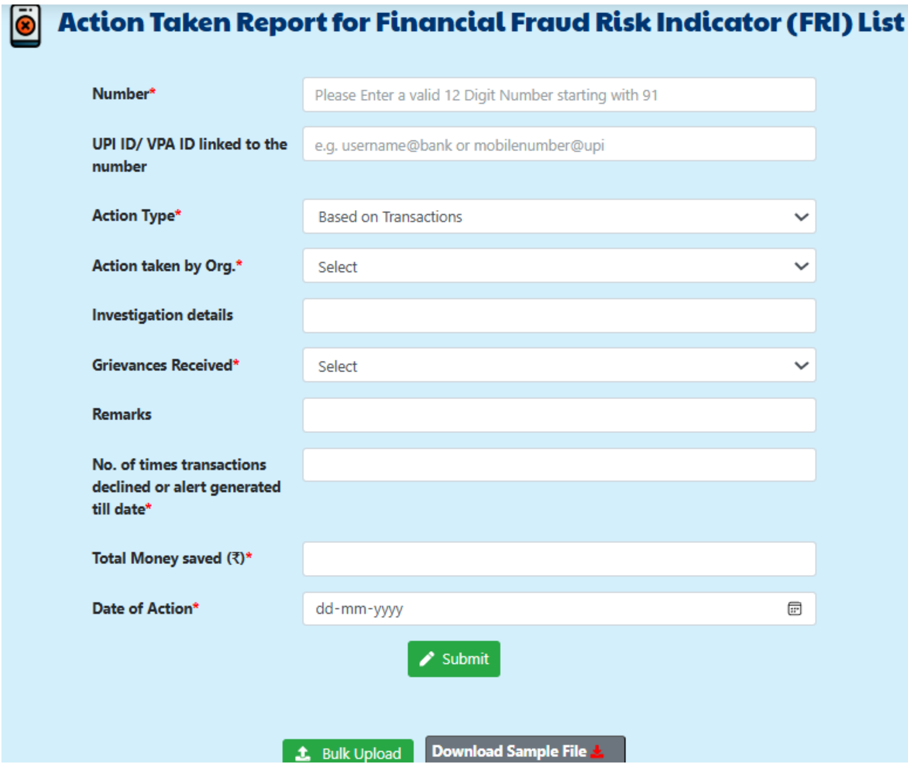


Figure 7: FRI List – Format for Uploading Transactions based ATR at DIP

Figure 8: FRI List – Format for Uploading EDD based ATR at DIP

xxi. The Bank/FIs/TPAP may choose the action type as per the below mentioned tabs:

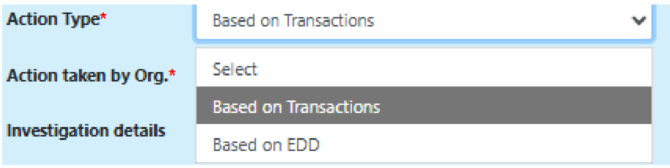


Figure 9 For uploading as per Action Type (Single)

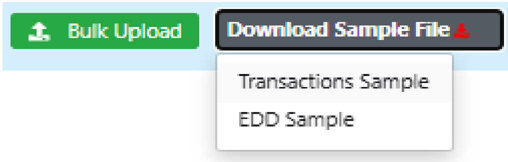


Figure 10: For uploading as per Action Type (Bulk)

xxii. The MIIs and KRAs may see the list of all the mobile connections against which they have been submitted the Action Taken Report.

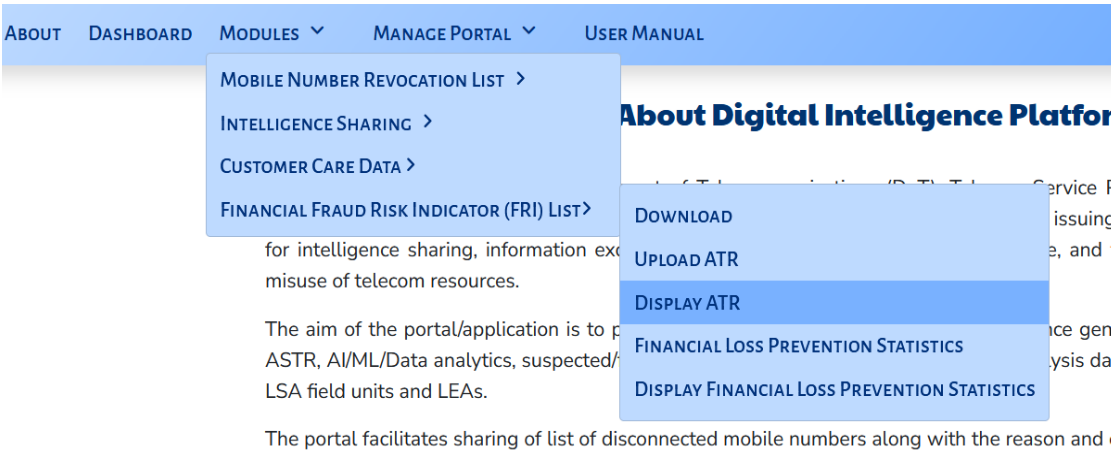


Figure 11: Display Action Taken Report for FRI List

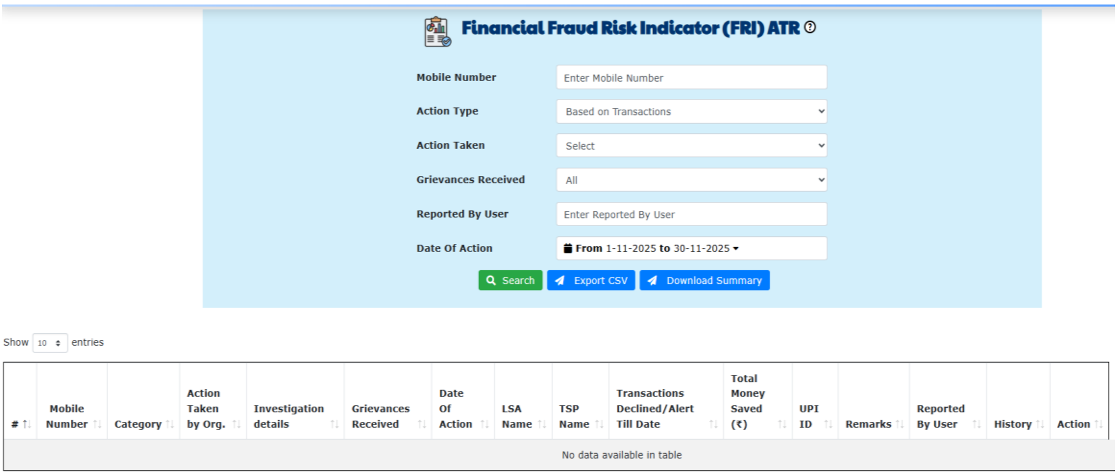


Figure 12: Display Action Taken Report FRI List based on Transactions

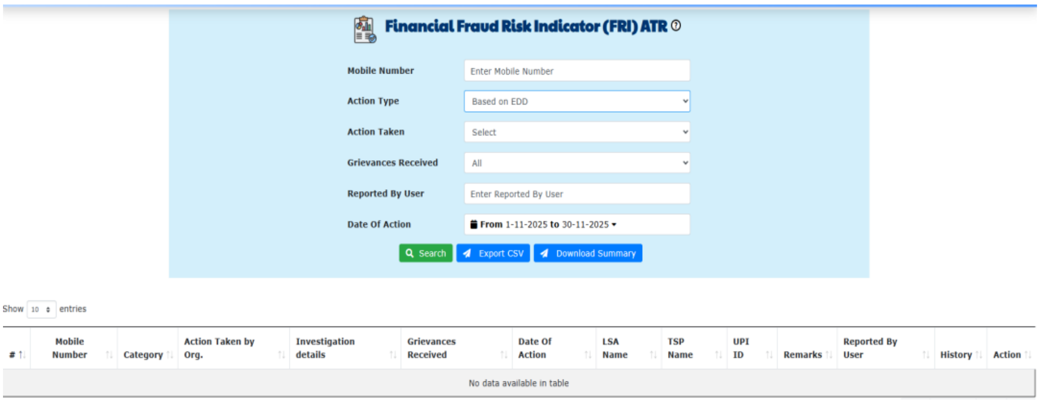


Figure 13: Display Action Taken Report FRI List based on EDD

xxiii. The MIIs and KRAs are also requested to upload the statistics and summary of the **Financial Loss Prevented** using FRI.

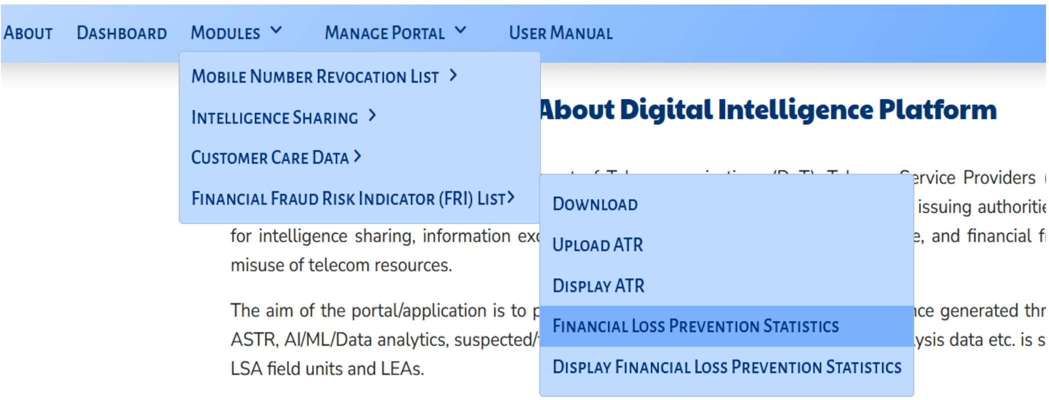


Figure 14: Financial Loss Prevention Statistics to be uploaded by MIIs and KRAs for FRI List

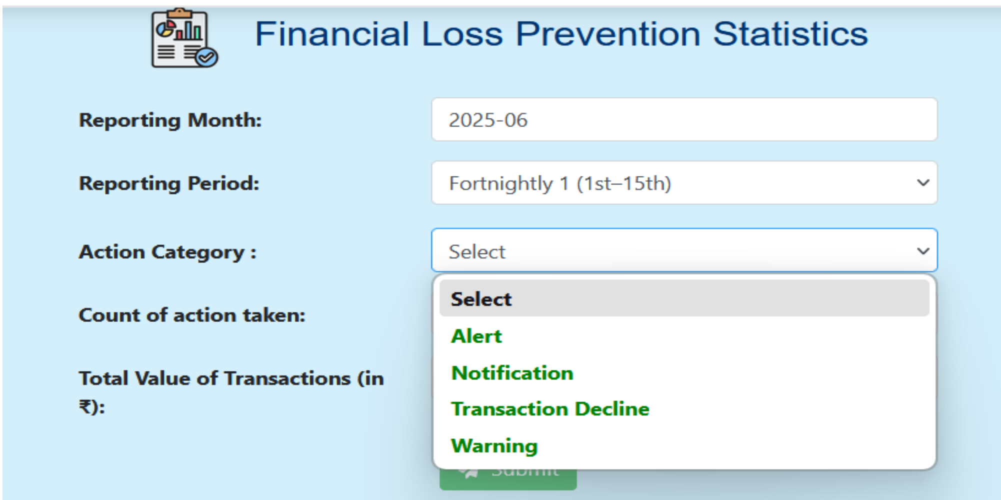


Figure 15: Financial Loss Prevention Statistics to be uploaded by MIIs and KRAs for FRI List

xxiv. The MIIs and KRAs may see the uploaded statistics and summary of the Financial Loss Prevented using FRI.

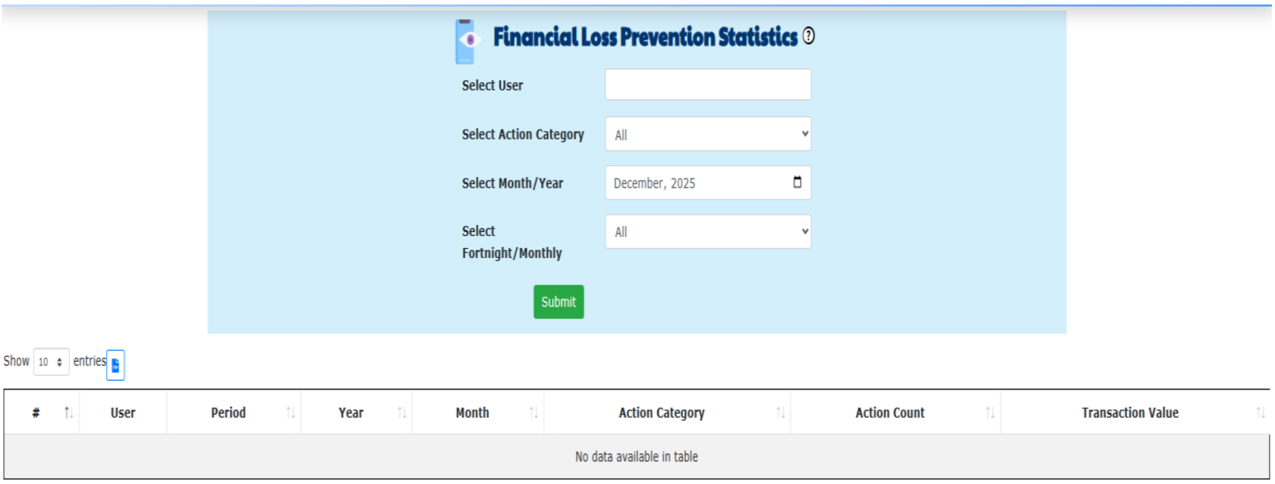


Figure 16: Display Option to see Financial Loss Prevention Statistics uploaded by MIIs and KRAs for FRI List

b) Mobile Number Revocation List (MNRL)

i. MNRL contains a list of all the disconnected mobile numbers along with reasons and date of their disconnections on near real time basis. MIIs (Stock exchanges and Depositories) and KRAs are requested to carry out enhanced due diligence (EDD) for the cases being shared. Further, a pro-active alert may be given to any citizen who is making payment to any account linked to any mobile number being shared in this list.

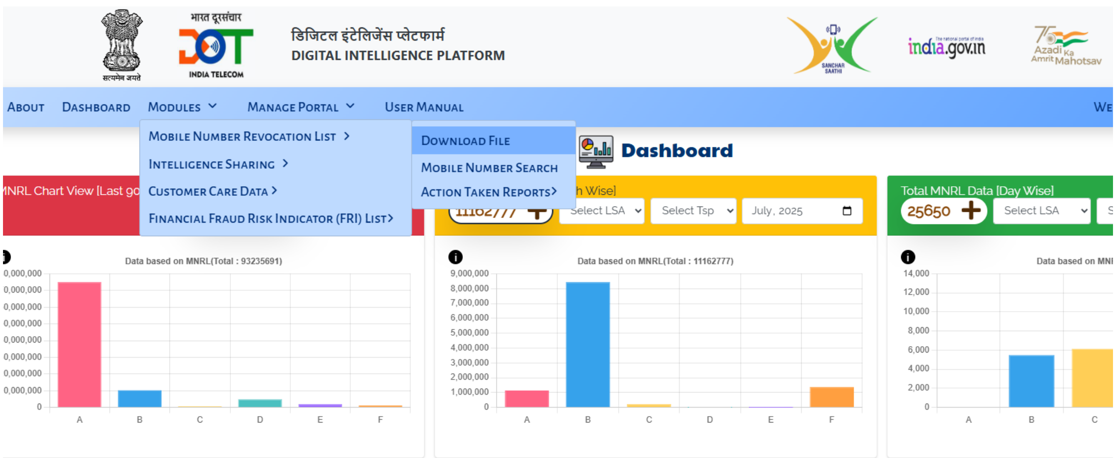


Figure 17: MNRL module: Mobile Number Revocation List

ii. The data may be downloaded LSA wise (India has been divided into 22 telecom license service areas – LSAs), TSP (Telecom Service Provider) wise and with reasons. The option to download the data of a period is also available. A number remains dormant for a period of 90 days after it is disconnected. Therefore, the data remains in MNRL at max for a period of 90 days after date of disconnection.

After 90 days the number may get allotted to a new subscriber therefore, it is removed from MNRL as well.

iii. MIIs and KRAs may download the data on daily basis either through DIP or in real time through the API facility. The API documentation is available at DIP under the tab User Manual. MIIs and KRAs may scrub these mobile numbers with the list of mobile numbers present in their ecosystem. Based on the matched mobile numbers, actions as advised at Table 1 may be taken. (Please refer: SEBI directions dated 18.05.2026)

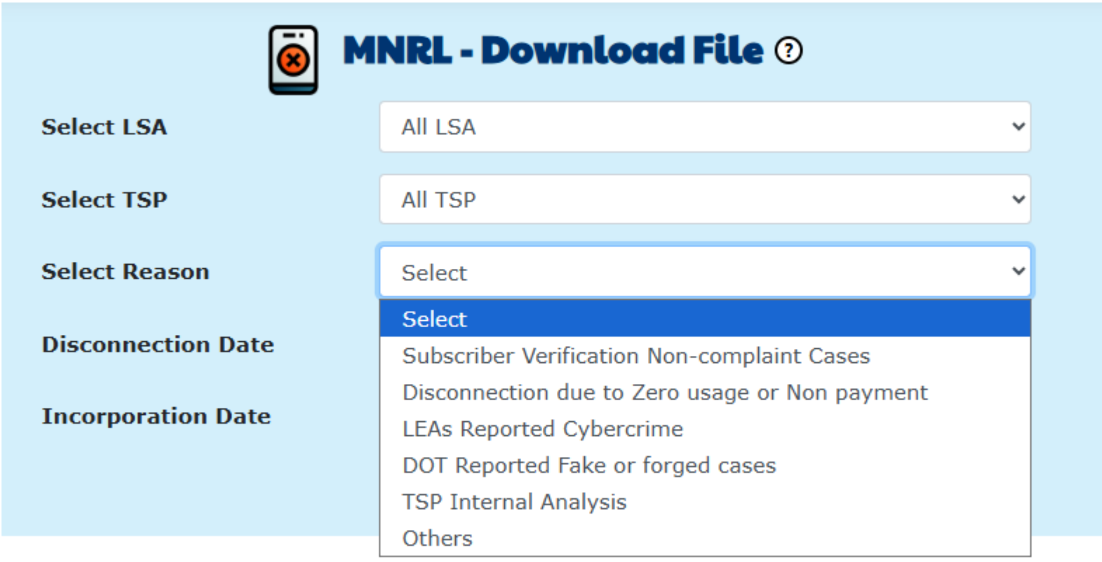


Figure 18: Categories / Reason- Mobile Number Revocation List

iv. Following set of actions may be taken by MIIs and KRAs for the MNRL data.

Table 2: Categories of MNRL

Sl.No.	MNRL Category / Reason	Description
1	LEAs Reported Cybercrime	Mobile numbers which were found to be misused in cyber-crime or financial frauds and got disconnected as per inputs from Law Enforcement Agencies, States/UT Police.
2	Subscriber Verification Non-Complaint Cases	The mobile numbers detected by DoT using AI/ML based tools using data like KYC details, roaming patterns, handsets used, misuse etc. The suspected cases were sent for re-verification and failed in re-verification and thus got disconnected.
3	DOT Reported Fake or forged cases	Based on face recognition and AI, the cases detected by DoT wherein one face has been misused for taking mobile connections with different KYC details and fake/forged documents. The suspected cases were sent for re-verification and

		failed in re-verification and thus got disconnected.
4	TSP Internal Analysis	Mobile numbers detected by Telecom operator's internal fraud management system which were found to be doing suspicious activities and disconnected by them.
5	Discontinuation due to Zero usage or non-payment	The mobile numbers which have been disconnected by the TSPs due to no recharge or which have been surrendered by the citizens.
6	Others	Cases related to surrender of connection in case of deceased person. May be treated as normally zero usage cases.

Table 3: Action advised for MIIs and KRAs etc. for different Categories / Reason of Mobile Number Revocation List (MNRL)

Sl. No.	Category of disconnected mobile number in MNRL	Action advised
1	LEAs Reported Cybercrime	Enhanced Due Diligence
2	DoT reported fake or forged cases	Enhanced Due Diligence
3	Subscriber Verification non-compliant cases	Enhanced Due Diligence
4	TSP Internal analysis	Enhanced Due Diligence
5	Disconnection due to zero usage or non-payment	Enhanced Due Diligence
6	Others	Due Diligence

v. The MIIs (Stock exchanges and Depositories) and KRAs are required to carry out enhanced due diligence (EDD) for finding mule accounts linked to these disconnected mobile numbers. Based on the MNRL category and their internal risk assessment, REs may undertake enhanced customer verification, increased monitoring of trading and financial transactions, periodic review of customer risk profiles, verification of source of funds where warranted, scrutiny of unusual or suspicious transactions, application of additional internal controls or approvals, and such other risk mitigation measures as may be appropriate in accordance with applicable SEBI regulations and their internal policies.

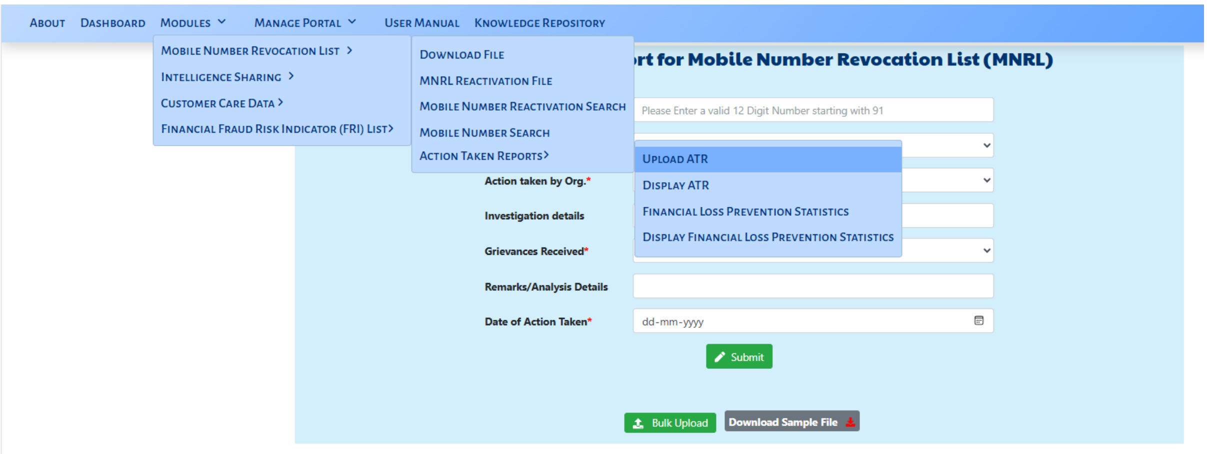


Figure 19: Uploading ATR option - Mobile Number Revocation List

vi. The MIIs and KRAs may use the above-mentioned tab for uploading the Action taken on the account /profiles linked to the mobile numbers. The MIIs and KRAs may use the bulk upload option: Download Sample File, fill the information and use Bulk Upload option or may upload the action taken one by one.

vii. Based on the EDD, MIIs/KRAs can take following actions on the accounts linked to mobile numbers flagged in Effective MNRL.

Sr. No.	Action Taken
1	Account freeze
2	Credit and Debit Restriction
3	Debit Restriction
4	Account not found suspicious after EDD
5	Mobile Number Delinked from account
6	Services of user restricted (loan/ insurance/ credit card etc.)
7	User Blacklisted

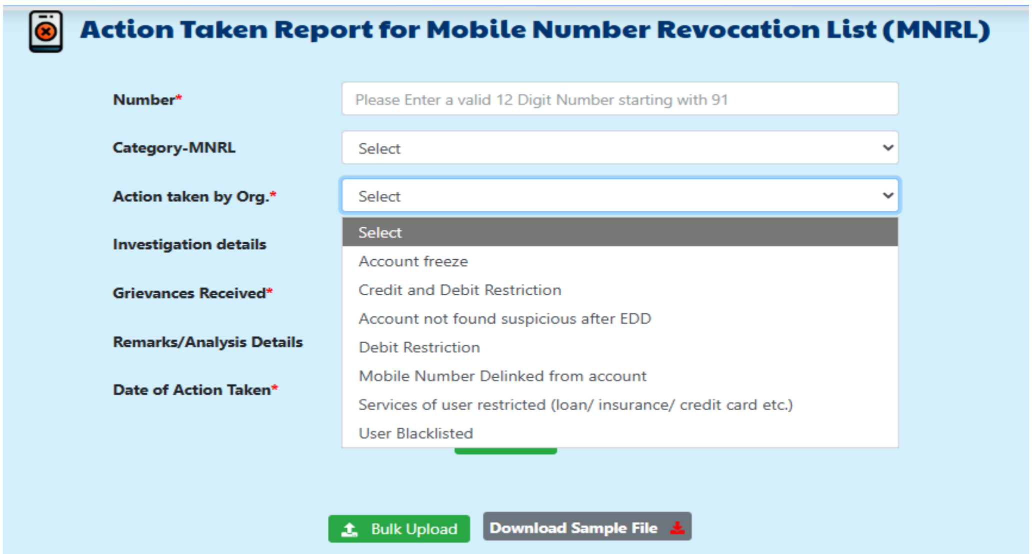


Figure 20: Action Taken Report for Mobile Number Revocation List (MNRL)

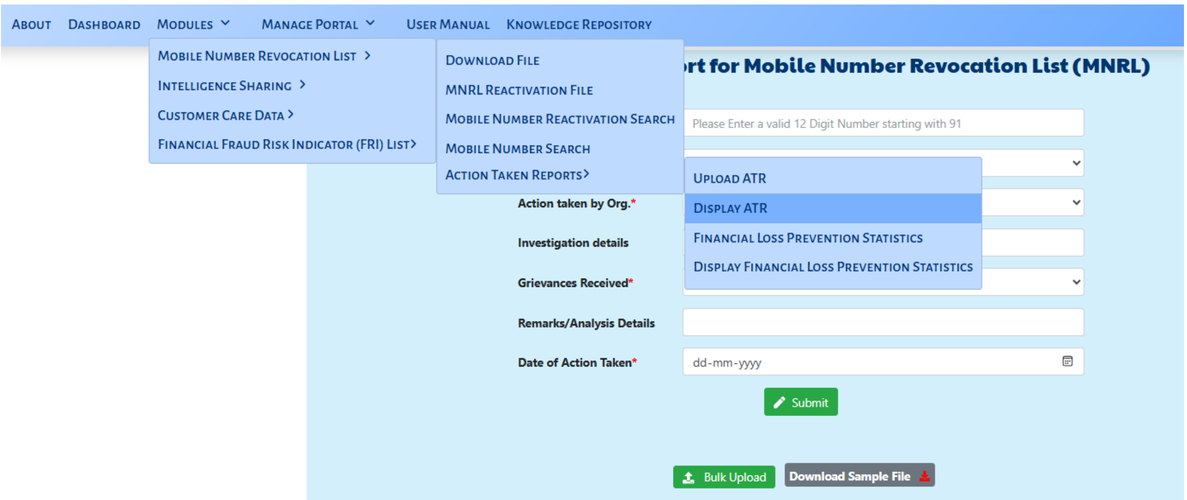


Figure 21: Display Action Taken Report for Mobile Number Revocation List (MNRL)

viii. In addition to the MNRL, the MNRL reactivation data is also provided to the REs for purging out cases which are reconnected before 90 days to the same person due to some reason by the TSP. MIIs/KRAs are required to remove such numbers from the EDD/ action.

Figure 22: MNRL Reactivation File

ix. The MNRL Reactivation Data appears as follows:

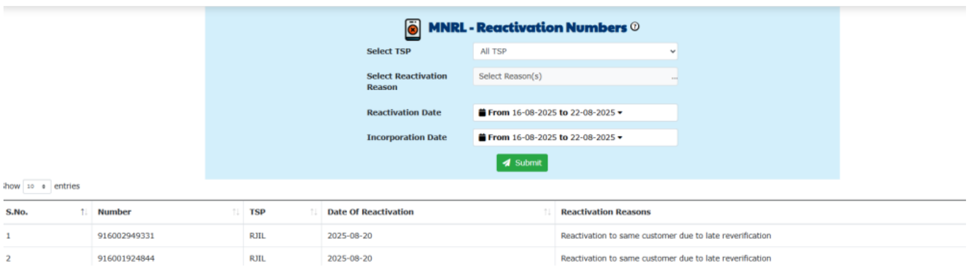


Figure 23: MNRL Reactivation List

x. MIIs/KRAs are required to download MNRL reactivation list along with MNRL list and remove these numbers from MNRL before performing EDD on the same.

xi. Further, in case bank receives any grievance and after EDD bank finds the account holder as genuine, the grievance can be informed to DoT through the ATR being uploaded.

xii. The MIIs and KRAs may see the list of all the mobile connections against which they have been submitted the Action Taken Report.

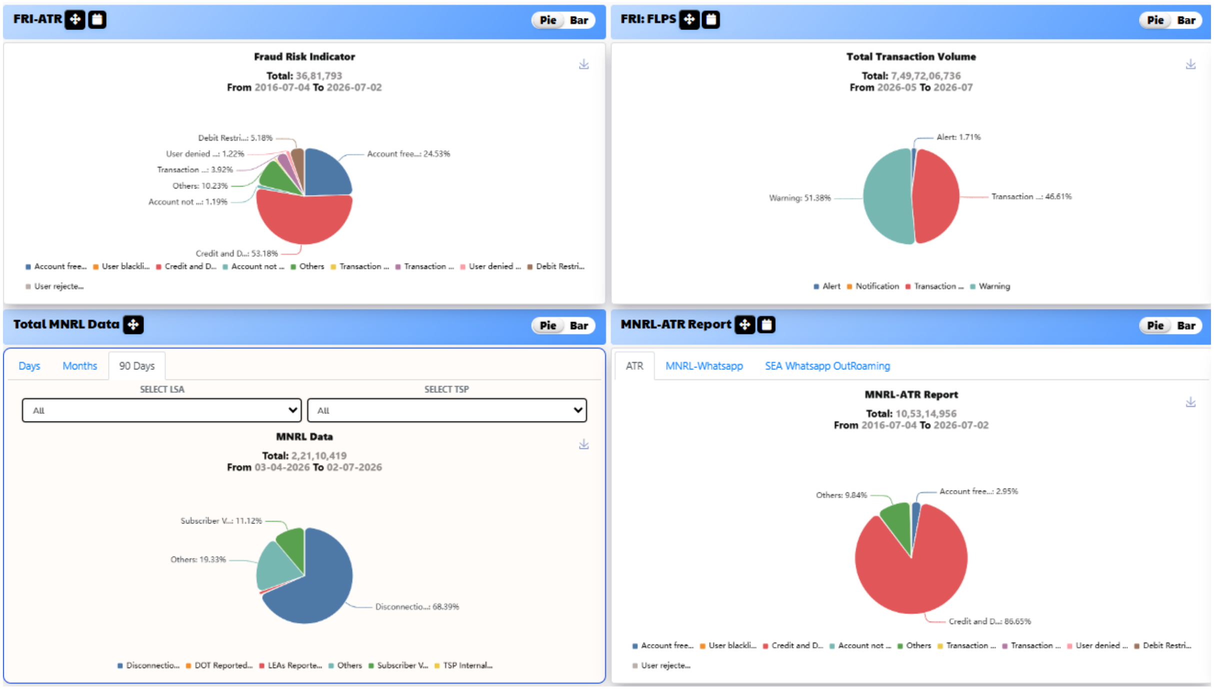


Figure 24: Dashboards at DoT Digital Intelligence Platform (DIP)

xiii. For better visualization, dashboards have been created for the MIIs and KRAs.

Note: Effective MNRL = MNRL – MNRL Reactivation

xiv. Best Practices for ATR updation:

a. **No Modification of action on accounts**: This gives wrong feedback; therefore, REs should upload action on accounts only after EDD.

b. **Modification of action on accounts** option available only for few grievance related cases.

c) Intelligence Sharing:

i. The MIIs (Stock exchanges and Depositories) and KRAs may keep on sharing list of suspected mobile numbers based on their internal analysis related to investment/ loan related scams, complaints received by them etc. DoT will carry out re-verification of such flagged mobile numbers. Data from MNRL's

Intelligence sharing module will be automatically available in DOT Intelligence sharing module for re-verification of such suspected mobile numbers. The action taken report is also made visible to the respective users.

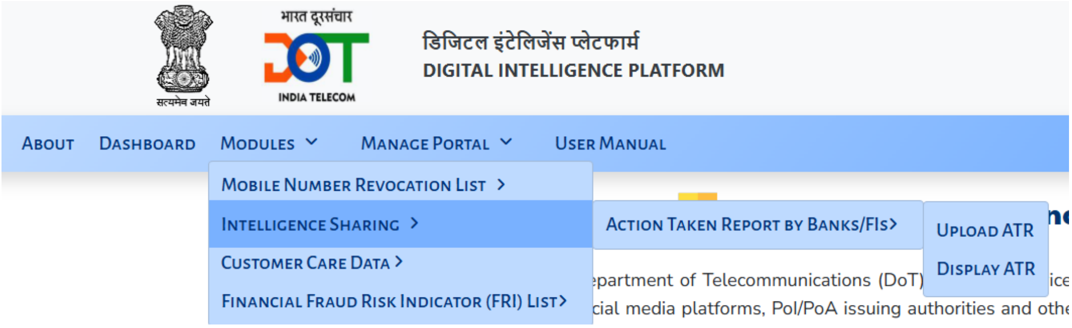


Figure 25:. Intelligence Sharing by stakeholders at DIP

ii. The MIIs and KRAs may use the above-mentioned tab for uploading the list of suspected landline or mobile numbers. The MIIs and KRAs may may use the bulk upload option: Download Sample File, fill the information and use Bulk Upload option or may upload the landline or mobile number one by one.

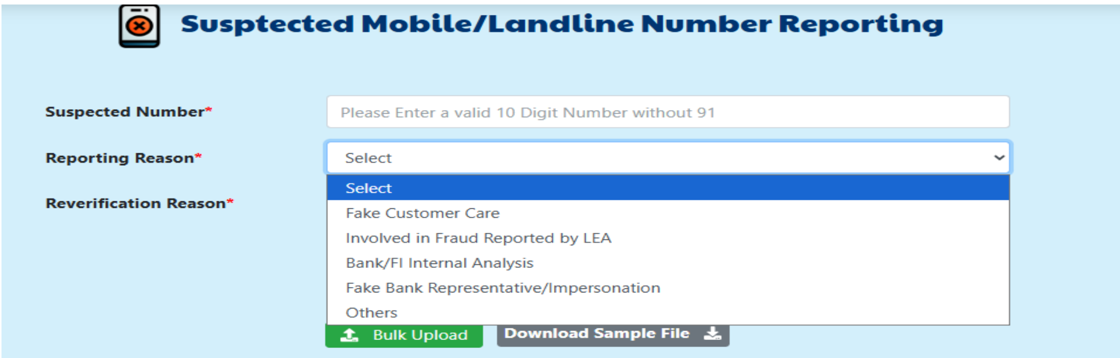


Figure 26: Intelligence Sharing by MIIs/KRAs – Bulk Upload or one by one reporting

iii. The MIIs and KRAs may see the list of all the landline or mobile connections uploaded by them as part of Intelligence Sharing.

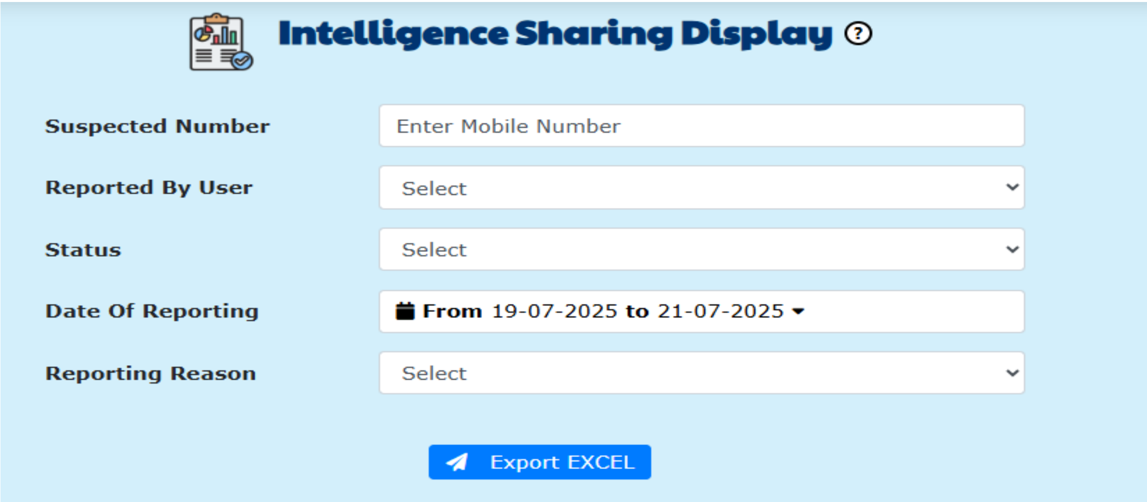


Figure 27: Intelligence Sharing by Stakeholders – Display Uploaded list

iv. Best practices for Sharing Intelligence:

a. **Financial Sector Sources:** Numbers reported from other sources like MuleHunter, Impersonation, citizens, stakeholders' internal fraud risk analysis should be reported on **immediate basis.**

b. **NCRP/ LEA sources:** Numbers reported from NCRP/I4C should not be directly flagged on DIP. Should be **flagged after bank's due diligence.**

c. Reporting time should be within 30 days. Very old complaints maybe ignored.

d. Frequency of reporting should be at least once every week.

e. API based solution for instant reporting.

f. Automating EDD processes of MIIs/KRAs to reduce delay in reporting.

g. **Careful handling of data** being shared at DIP – not to be shared further

d) Customer Care Data:

i. A module named "**Customer Care Data Upload**" has been added through which information may be updated by the MIIs/KRAs regarding their official customer care / toll free numbers, their websites so that whitelisted data may be created for citizens.

a. Official numbers of MIIs/KRAs: These are the numbers through which financial sector entities reach out to customers. As per the guidelines of TRAI, REs can reach out to customers either through 140 series for promotional calls and 1600 series for service and transactional calls. Calling from 10 digit mobile or landline numbers is not allowed. Therefore, only 140/1600 series numbers are to be provided in this.

b. Tollfree number: Series of 1800 numbers are to be provided in this. Using this number customers can reach out to customer care of MIIs/KRAs.

c. Other Customer care numbers: Any other number using which customer care can reach out to MIIs/KRAs for queries are to be given in this.

The data will be displayed to citizens through Sanchar Saathi portal and Mobile App.

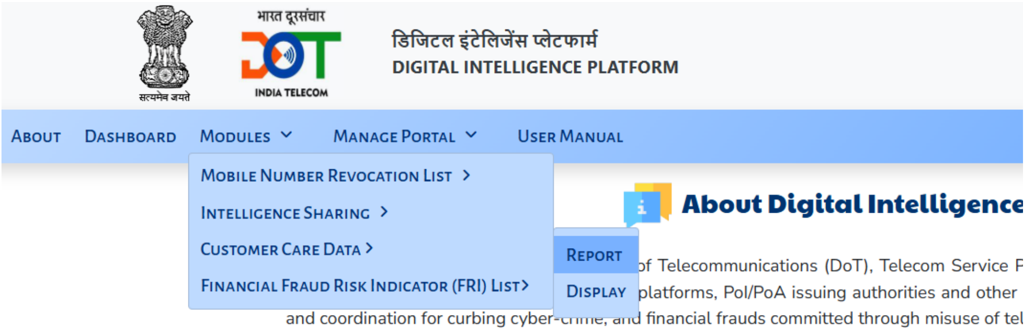


Figure 28: Customer Care Data – to be uploaded by MIIs/KRAs at DIP

ii. The MIIs and KRAs may use the below-mentioned tab for uploading the list of their official customer care / toll free numbers, their websites. The MIIs and KRAs may may use the bulk upload option: Download Sample File, fill the information and use Bulk Upload option or may upload one by one.

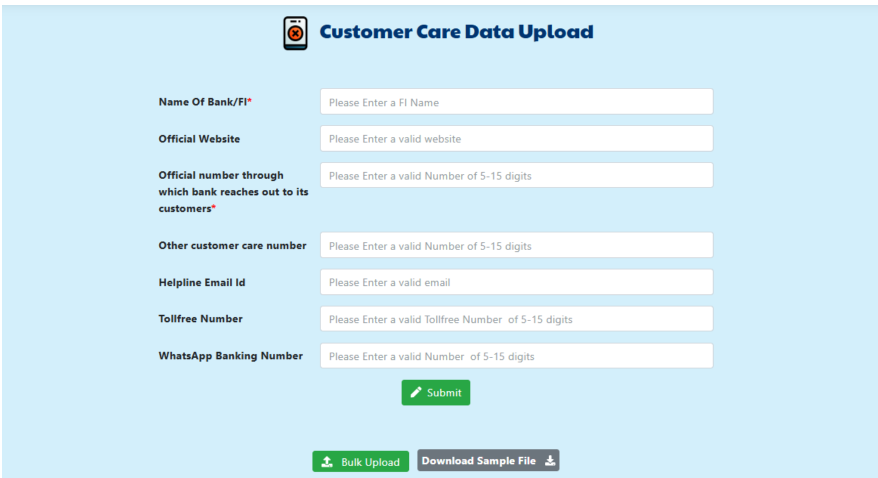


Figure 29: Facility to upload Customer Care Data by MIIs/KRAs at DIP

iii. The MIIs and KRAs may see the list of all the official customer care / toll free numbers, their websites uploaded by them as part of Customer Care Data.

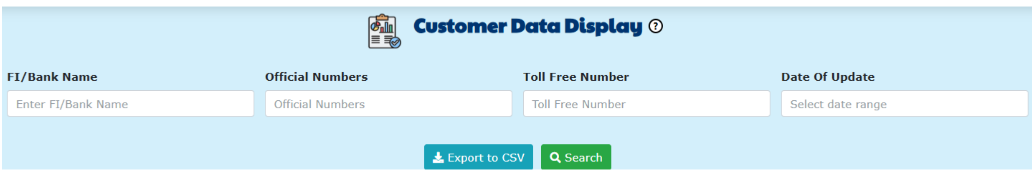


Figure 30: Facility to display Customer Care Data uploaded by MIIs/KRAs at DIP

e) Grievance Handling: Grievances broadly fall into the following **three** categories:

1) **Numbers in MNRL that have been reactivated, but accounts/profiles remain frozen:**

a. **Solution**: MIIs/KRAs are advised to download MNRL Reactivation data along with MNRL and use the effective MNRL i.e. MNRL – MNRL Reactivation data and then take action.

b. **Keep in Mind:** Numbers may be reactivated with some delay as well. So complete reactivation data of 90 days from the date of disconnection of the number to be considered.

c. For numbers belonging to BSNL, MIIs/KRAs are advised to carry out EDD and verify the status and possession of the number through OTP-based authentication and then take action.

2) **Action by MIIs/KRAs on numbers in old MNRL:**

a. **Solution**: MIIs/KRAs are advised to take action only on active database in the effective MNRL.

3) **Compliant cases**: A number which was present in FRI before but found Compliant in telecom domain.

b. **Solution:** Based on EDD conducted by MIIs/KRAs, any action taken earlier may be reviewed and revoked in such cases after the cool-off period.