10-3/2020-AS-IV
Government of India
Department of Telecommunications
(Access Services - IV Section)

Date: 2nd July 2021

Subject: Platform for Digital Intelligence Unit (DIU) at central level and Telecom Analytics for Fraud Management and Consumer Protection (TAFCOP) at LSA field units of DoT - reg.

The approval of Hon'ble Minister of Communications (MoC) is hereby conveyed for creation of Digital Intelligence Unit (DIU) at central level and Telecom Analytics for Fraud Management and Consumer Protection (TAFCOP) at LSA field units of DoT.

2. The functions of DIU and TAFCOP are given in detail at Annexure 'A' and are summarised below:

(i) Coordination with Law Enforcement Agencies (LEAs), financial institutions and other Government agencies in cases involving frauds using telecom resources/services.

(ii) To monitor UCC complaints and to find the associated numbers involved in UCC.

(iii) To identify more than specified connections working against the same set of documents.

(iv) To identify the connections obtained on fake/false documents.

(v) Will provide facility to the consumers to be able to know the number of connections working against their names and to report about the connections not taken by them.

(vi) To detect MNP fraud.

3. Central Telcom Subscriber Database of DIU will collate with TAFCOP and contain information of all subscribers across all telecom service providers in all LSAs.

4. Grievance Redressal System will inter-alia provide a platform for public to register their grievance and monitor its resolution with respect to Unsolicited Commercial Communications (UCC) (Annexure 'B').

5. The platform will also provide DoT, Law Enforcement Agencies (LEAs), Financial Institutions (FIs) and TSPs to seamlessly coordinate in cases of financial frauds committed through misuse of telecom resources.

6. The following will be implemented through DIU and TAFCOP:

i. Central Telecom Subscriber Database system (CTSDS)

ii. Grievance Redressal System named Safe Access of Telecom Resources without Harassment and Infringement (SATHI) system

iii. MNP fraud prevention database system (MFPDS)

iv. Calling line name identification System (CLNIS)

The key details of aforesaid systems are mentioned in Annexure-C.

7. This is for information and further necessary action.

02/07/2021

(Trilok Chandra)
Director (AS-IV)

Encl: Annexure-A, B & C

To,

Director General (Telecom), DoT HQ, New Delhi

Annexure-A

The functions of DIU are as follows:

i. Creation and Maintenance of Central Database system containing information of all telecom subscribers across all telecom service providers of all LSAs.

ii. Assignment of unique ID to the telecom subscribers based on specific parameters.

iii. Analysis of telecom subscriber database to uncover patterns of suspicious telecom connections and suspicious/ restricted telecom activities.

iv. Tracing of fake/ forged PoI/ PoA by specified algorithm and data analytics and disconnections of all SIMs issued on forged documents and make the telecom subscriber database robust and accurate.

v. Using data analytics, enforcing the guidelines of maximum permissible limit of mobile connection (9 connections, 6 connections in case of J&K, North East and Assam).

vi. Creation and maintenance of Grievance Redressal System named Safe Access of Telecom Resources without Harassment and Infringement (SATHI) system.

vii. Data analysis of UCC and financial frauds committed through the utilization of telecom resources, analysis of all associated numbers linked with the suspicious connection.

viii. Coordination with different Law Enforcement Agencies (LEAs), Financial Institutions, and other Government Agencies to support investigations of frauds involving telecom resources/ services.

ix. Creation and Maintenance of MNP fraud prevention database system (MFPDS) and provisioning of service to verify the subscriber details of Mobile Number Portability (MNP) case.

x. Creation and Maintenance of Calling line name identification System (CLNIS) for displaying the name of calling party, submitted in CAF, along with number to the called party (except for the subscribers having CLIR facility) and Record keeping & monitoring of CLIR.

xi. Analysis of IMEI to prevent IMEI duplicity.

xii. Any other activity related to prevention and detection of frauds committed through misuse of telecom resources and strengthening the digital ecosystem in the country.

The functions of TAFCOP are as follows:

i. Handling of Central Database system containing information of telecom subscribers across all telecom service providers at LSA level.

ii. Analysis of telecom subscriber database to uncover patterns of suspicious telecom connections and suspicious/ restricted telecom activities at LSA level.

iii. Using data analytics, enforcing the guidelines of maximum permissible limit of mobile connection (9 connections, 6 connections in case of J&K, North East and Assam) at LSA level.

iv. Tracing of fake/ forged PoI/ PoA by specified algorithm and data analytics and disconnections of all SIMs issued on forged documents and make the telecom subscriber database robust and accurate at LSA level.

v. Analysis of new connection with all the existing connections associated with the same PoI/ PoA used for obtaining the new connection, for timely disconnection of SIM if issued on forged documents.

vi. Monitoring and Handling of Grievance Redressal System named Safe Access of Telecom Resources without Harassment and Infringement (SATHI) system at LSA level.

vii. Data analysis in case of UCC and fraud complaints, analysis of all associated numbers linked with a complaint connection at LSA level.

viii. Coordination with different State Cyber Cells, Financial Institutions, and other Government Agencies to support detection of frauds involving telecom resources/ services at LSA level.

ix. Monitoring of MNP fraud prevention database system (MFPDS) at LSA level.

x. Analysis of IMEI to prevent IMEI duplicity at LSA level.

xi. Analysis of headers, templates and other relevant data associated with Registered Tele-Marketers (RTMs). Sample Audit of Headers, Templates and Content of the SMSs being sent by the telemarketers registered in the LSA unit by the respective LSA field unit on monthly basis.

xii. Any other activity related to prevention and detection of telecom frauds and strengthening the digital ecosystem in the country in coordination with DIU.

Annexure-B

A. In case of UCC by Registered Tele Marketer (RTM), the graded financial penalty as mentioned in below table will be imposed along with disconnection of resources.

Value of "Counts of UCC for particular RTM for one calendar month"	**Penalty to be paid (Month 1 of UCC violations)**	**Penalty to be paid (Month 2 of UCC violations)**	**Penalty to be paid (Month 3 of UCC violations)**
1- 10 valid UCC done by RTM	Rs. 1000 per violation	Rs. 5000 per violation - warning letter to be issued	Rs. 10000 per violation and Disconnection of all resources
For all violations after 10 cases and less than 50 cases	Rs. 5000 per violation- warning letter to be issued	Rs. 10000 per violation - warning letter to be issued	Rs. 10000 per violation and Disconnection of all resources
For all violations after 50 cases	Rs. 10000 per violation- warning letter to be issued	Rs. 10000 per violation and Disconnection of all resources	Rs. 10000 per violation and Disconnection of all resources

Subscribers will have the option to opt out from the promotional SMS by sending SMS, STOP <header name> to 1909.
Eg:

To: 1909
Message: STOP IPAYTM

This will block all the promotional communications from all the headers registered against the said entity (say PAYTM in case of above example) except transactional messages.

The above provisions may require implementation under TCCCPR-2018 in consultation with TRAI.

B. In case of UCC by Unregistered Tele Marketer (UTM), the proposed against defaulter UTM are as follows:

i. After verification of authenticity of complaint, the reported connection will be re-verified. Meanwhile, the reported number would be put under usage cap means 20 calls and 20 sms per day and no data till the re-verification is completed.

ii. The additional details also required to be furnished regarding total number of SIMs with numbers that has already issued on the name of concerned person.

This additional information may be helpful to avoid unnecessary disturbance by doing again re-verification of remaining numbers that are matched with same POI and POA.

iii. If the suspected number produces fake/ forged documents/ new documents which were not used earlier during the procurement of the connection, then the re-verification will not be processed successfully and the number will be disconnected.

iv. With the help of central database, all the associated numbers will be identified and a system generated message will be forwarded to suspected numbers for verification at any nearest POS location.

v. In case of non re-verification, all the numbers will be disconnected and associated IMEIs will be put under suspected list. No calls/ sms/ data will be allowed for the IMEIs in suspected list for a period of 30 days.

vi. Whenever a new connection will be attached with the IMEIs in suspected list, the connection will be promoted for re-verification. And if this connection gets attached with the new IMEI, then that IMEI will also be put in suspected list and the above process will keep on repeating itself.

vii. In case same number after re-verification is again found to be involved in UCC activity second time, then usage cap (20 calls and 20 sms per day and no data) will be put for a period of six months and in case of third violation, disconnection of all the resources along with blocking of PoI/ PoA for a period of 2 year.

viii. In case of fake complaints by the complainant, action could be initiated against the complainant as well. The suspected numbers would also have the option to raise grievance, if they feel that the action taken against them is not justified. For all these purposes an appellate level may be created.

The provisions related to usage cap are required to be implemented in consultation with TRAI.

Annexure-C

A. Central Telecom Subscriber Database System (CTSDS)

i. Creation of Central Telecom Subscriber Database System (CTSDS) - containing information of telecom subscribers across all telecom service providers of all LSAs.

ii. Integration of CTSDS and Telecom Service Providers' (TSPs) subscriber database system.

iii. Due to security and privacy of data, connectivity between CTSDS and TSP database is planned only on secure MPLS link. MPLS connectivity between CTSDS and TSPs database system will be provided by TSPs. After submission of initial data, incremental data will be updated periodically (24 hours) through MPLS connectivity.

iv. Access of CTSDS to LSAs' will be provided through MPLS connectivity. LSAs will have visibility of telecom subscriber database of their respective LSAs.

v. Assignment of unique ID to all the telecom subscribers after filtration of all the forged connections.

vi. Development and deployment of data analytics tool in CTSDS for finding the forged and suspected mobile connections.

B. Safe Access of Telecom Resources without Harassment and Infringement (SATHI) System

i. Development and deployment of web based system named SATHI for integration of all stakeholders for prevention and detection of frauds committed through utilization of telecom resources. The stakeholders are as follows: -
DIU, TAFCOPs, TSPs, LEAs, Cyber Cells, all Financial organization/Institutes/entities, etc.

ii. Creation of profiles of all stakeholders on SATHI portal as per their roles and rights.

iii. Development and deployment of web and mobile application APP based platform to receive UCC complaints (RTM/UTM).

iv. Development and deployment of web, mobile application APP and SMS based platform to handle the following requests from the telecom subscribers: -
   a) enquiry about no. of SIMs registered against any particular ID
   b) disconnection of unauthorized mobile connections.

v. Integration of the whole platform with SATHI system and creation of user friendly dashboard for all stakeholders to enable fast and smooth handling of all the complaints and requests.

C. <u>MNP fraud prevention database system (MFPDS)</u>

i. Creation of MNP fraud prevention database system (MFPDS).

ii. Integration of MFPDS with MNP service providers' database system and DIU server through MPLS link.

iii. Creation of a mobile based application APP named MNP fraud prevention database platform (MFPDP) and integration of it with TSPs system for providing visibility of subscribers details to activation officers of TSPs.

iv. The access of subscriber details (name, father name, date of birth, photograph), available with Donor TSPs will be extended to Recipient TSPs, for verification purpose, before activation of MNP connections.

D. <u>Calling line name identification System (CLNIS)</u>

i. Explore the mechanism for displaying the calling party name along with the number to the called party.

ii. Integration of TSPs network with calling line name identification database (CLNID) which consist of telecom subscriber's names (as per customer acquisition form) along with the mobile numbers.

iii. To prevent the fraud using identity hide, the calling party name along with the number will be provided by service provider to the called party in the call log of called party through CNAM facility without internet.