PCC.I/DEC. 234 (XXVII-15)[1]

CLASSIFICATION OF FRAUD AND REGULATORY NON-COMPLIANCE PRACTICES AS REGARDS ICTs

The XXVII Meeting of the Permanent Consultative Committee I: Telecommunications/Information and Communication Technologies (PCC.I),

DECIDES:

1. To request Member States to carry on the Survey attached hereto in the Annex of this Decision, until the XXVIII Meeting of the PCC.I, in order to collect information on classification of frauds and regulatory non-compliance practices.

2. To appoint the Rapporteurship on Fraud Control and Regulatory Non-compliance Practices in Telecommunications to collect the information resulting from the survey; and to submit the results of the survey at the XXIX Meeting of the Committee.

ANNEX I TO DECISION PCC.I/DEC. 234 (XXVII-15)

CLASSIFICATION OF FRAUD AND REGULATORY NON-COMPLIANCE PRACTICES AS REGARDS ICTs

Country/Administration: _____

Name of the person answering the survey: _____
Entity/Organization _____
Contact information:
Telephone_____ e-mail _____

Goal: Survey the current situation in each Member State as regards the 9 most relevant Fraud cases, taking into consideration the first Risk Matrix where were considered the impacts and occurrences of the 34 Fraud Types agreed at the XXV Meeting of the PCC.I.

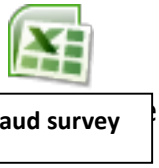
Maneuvers that are more risky and that have major impact:

1. Theft of cell phones
2. Bypass – re-origination
3. Cell phone Cloning
4. SPAM
5. Leak of mobile terminal equipment

[1] CCP.I-TIC/doc. 3688/15

6. IRSF (Third-country fraud)
7. Fraud in service subscription
8. Internal fraud
9. PBX fraud

1. Complete the information on each of the above mentioned maneuvers in the attachment:



2. According to the first version of the Matrix the nine most relevant types of Fraud are those in this consultation, and in that order. In the experience of your country, do these types of fraud coincide?

YES ☐ NO ☐

3. If the previous answer is NO, please mention the types of fraud that are not listed among the 9 most important.

4. Considering risk level 1 - 9, do you agree with the valuation of the first Matrix?

YES ☐ NO ☐

5. If your answer is NO, please order the types according to what actually happens in your country.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____

6. Please explain in detail all you deem necessary on each of the 9 types, as it currently occurs in your country. Take into account impact, detection measures, and mitigation measures.

7. ¿Which would you consider as best practices for each of the types that exist in your country to mitigate fraud?

8. Please, leave a contact email to discuss any questions that may arise out of your answers.

Name: _____
e-mail: _____@_____

ANNEX II TO DECISION PCC.I/DEC. 234 (XXVII-15)

DEFINITIONS OF FRAUDS AND MOST RELEVANT REGULATORY NON-COMPLIANCE PRACTICES

1. **Theft of cell/mobile phones**
   There are gangs engaged in the theft of mobile devices in order to resell them to be used inside and outside the national territory normally with other operators. It is currently a major problem because these devices are re-numbered with other identification numbers that make them appear to the network operator as if they were other devices, thus avoiding monitoring for deactivating stolen terminals in operators' databases.

2. **Bypass - Re-origination**
   The Bypass mode consists of transmitting traffic from the national or international long-distance service through operator networks without a license authorizing them to provide said services. Once the traffic is located at the point of interest of destination, the re-origination takes place, which is to change the origination of the international communication simulating it is a communication between local operators or on the intranet. This modality is applied both to the fixed and mobile services. The fraudster business is profiting from the difference between the international communication price and the local traffic for the fixed service, or for the intranet for the mobile service. In addition, as a rule, these fraudsters are usually not bound to any regulatory obligations, do not pay taxes, and earn their income from abroad. Types of bypass: incoming, outgoing, local, national or international, or mobile re-origination.

3. **Cell phone cloning:**
   Fraudsters intercept the Equipment Serial Number (ESN) using radio reception equipments. These numbers are then reprogrammed into other devices from which they make calls that are billed to the subscriber holding the original ESN.

4. **SPAM**: Unwanted e-mails whereby the spammer tries to bombard lists of users with unsolicited e-mails that, on many occasions, contain self-installing programs that may even damage the contents of computers. Fraudsters often use them as a way to spread viruses, among others.

5. **Leak/drain of mobile terminal equipment:**
   The fraudsters subscribe to mobile telephony plans were devices are subsidized, in order to get the terminal. These terminals are taken by organized crime bands and placed normally in other countries where the price of these devices is much higher, for the purpose of profiting from difference in the price of the equipment.

6. **IRSF International Revenue Share Fraud:**

In this case, after the subscription fraud, long calls are made to international destinations with high cost (generally to nations that are small islands or to numbering ranges that correspond to satellite services). The calls do not reach the corresponding geographical destinations, but are routed by an intermediate operator to a third service provider that has a shared payment service (e.g. audio text). In some cases this routing is done even without the consent of the owner of the numbering block. In this way, the provider of the shared payment service gets the benefit of these calls, while he will not pay the operator with which he has the fraudulent subscription. This type of fraud has been widely documented by GSMA, having drawn up blacklists of suspected or fraudulent number ranges.

7. **Subscriber Fraud:**
   The user provides false documentation, or impersonates another person, to request and subscribe to a telecommunication service generally for the purpose of using it so as not to pay or to clandestinely make other types of fraud.

8. **Corporate or Internal Fraud:**
   This fraud is made by a company's internal staff, with the intent of improperly use company resources for personal or third-party purposes. It involves the privileges and technical know-how of the person committing the fraud, among which are the following:
   1) Appropriation of assets for personal or third-party use.
   2) Sale or use of privileged information for one's own benefit.
   3) Sale of access to goods or services provided by companies for the benefit of third parties.
   4) Access to systems of the service provision chain to change usage information of own or third-party services.
   5) Abuse of services or facilities provided for the internal management of the company for own or third-party benefit.
   6) Access and use of customer network facilities for own or third-party benefit.
   7) Disclosure of information about processes and identified vulnerabilities for the benefit of third parties.
   8) Favoring third parties in bidding processes, selection, and procurement of services, or purchase of company goods and assets for own benefit or the benefit of acquaintances or relatives.

9. **PBX Fraud:**
   This is a facility of PBX exchanges which is normally assigned to executives of companies to allow their remote access with codes to platforms that enable them to use all communication services (local, domestic long distance, international long distance, mobile access, Internet, etc.). Through social engineering or unscrupulously, these access codes are known by third parties who use the service making the company to finally pay the bill for services it has not used for their benefit. This type of fraud is increasing with IP PBX, due to the ease of access that fraudsters have from any part of the world and often because of the little protection of these elements by users.