PCC.I/DEC. 204 (XXV-14) [1]

CLASSIFICATION OF FRAUD AND REGULATORY NON-COMPLIANCE PRACTICES

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

DECIDES:

1. To request Member States to process the survey attached in the Annex herewith, on the basis of PCC.I/RES. 225 (XXIV-14) "STRUCTURE AND TERMS OF REFERENCE OF THE WORKING GROUPS AND RAPPORTEURSHIPS OF PCC.I", for the purpose of gathering information about Fraud in Information and Communication Technologies (ICTs) and Regulatory Non-Compliance Practices.

2. To designate the Rapporteurship on fraud control, regulatory non-compliance practices in telecommunications and regional measures against the theft of mobile terminal devices to gather information on the basis of the survey's results.

3. Instruct the Rapporteurship on on fraud control, regulatory non-compliance practices in telecommunications and regional measures against the theft of mobile terminal devices to present the results of the survey to the XXVI Meeting of PCC.I.

ANNEX 1 TO DECISION PCC.I/DEC. 204 (XXV-14)

CLASSIFICATION OF FRAUD AND REGULATORY NON-COMPLIANCE PRACTICES IN ICTs

Country/Administration:	
Name of person answering the survey:	
Entity/Institution:	
Contact information:	
Phone:	
e-mail:	

Please fill out the following table about frauds and regulatory non-compliance practices in ICTs:

The first part of information is expected for November 28, 2014.
Deadline to provide all the information: March 30, 2015.

Goal: According to the mandate of the Working Group on Policy and Regulation (WGPR) and in order to study and recommend strategies and best practices to detect and reduce fraud in the area of telecommunications/ICT and to identify the principal regulatory non-compliance behaviors currently undermining the normal development of telecommunication/ICT activities, the present survey intends to classify and prioritize which of these behaviors are to be included in the studies of the present Rapporteurship.

[1] CCP.I-TIC/doc. 3337/14 rev.2

Bearing in mind the above, please provide, with respect to each type of fraud or regulatory non-compliance practice, the answer to the following questions:

1. This fraud or practice has been targeted in provisions by the Member State in standards, studies, duties of government institutions, campaigns, programs for its mitigation, etc? YES / NO

2. If the reply to question 1 is YES: Can you provide statistical data about the economic impact, impact on users, or impact on the State that would help to calculate the size of the problem in each Member State. YES (at least 1 of the three data) / NO

Table 1: Classification of frauds and regulatory non-compliance practices

Type of fraud or regulatory non-compliance practices in ICTs (see definitions in Annex 1)	Question 1	Question 2
1. Internal fraud		
2. Fraud in service subscription		
3. Public phone bypass fraud		
4. Third-country fraud		
5. Leak of mobile terminal equipment		
6. PBX fraud		
7. Tampering with network elements		
8. Tampering with information		
9. Theft of phone lines		
10. Theft of PINs from cards or keys of special services to make calls		
11. Use and sale of facilities assigned by the companies for use by third parties		
12. By pass – Reorigination		
13. Callback		
14. Unfair competition		
15. Resale of telecommunication services without due authorization		
16. Slamming		
17. Cell phone cloning		
18. Cramming		
19. Dialers		
20. Theft of cell phones		
21. Automatic subscription to the services of an operator unless the customer expressly refuses them		
22. Adware		
23. Backdoor		
24. Creation and use of own infrastructure without a permit		
25. DIDs		
26. Hacking		
27. Keyloggers		
28. Installing infrastructure to monitor the private information of users		
29. Trickery with messages to draw the attention of persons		
30. Phishing		
31. Clandestine radio and television broadcasting		

32. SCAM		
33. Spyware		
34. SPAM		

ANNEX 2 TO DECISION PCC.I/DEC. 204 (XXV-14)

DEFINITIONS OF FRAUDS AND REGULATORY NON-COMPLIANCE PRACTICES

1. **Corporate or internal fraud:**

It consists of fraud carried out by the company's internal staff, with the intent of improperly using corporate resources for personal or third-party purposes, and involves the privileges and technical know-how of the person committing the fraud, among which the following:

1) Appropriation of assets for personal or third-party use.
2) Sale or use of confidential information for one's own benefit.
3) Sale of access to goods or services provided by the companies for use by third parties.
4) Access to systems of the service provision chain to change information of use 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 vulnerabilities identified for the benefit of third parties.
8) Favoritism for third parties in bidding process, selection and procurement of services or purchase of goods and assets of the company, for own benefit or the benefit of friends or next of kin.

FRAUDS WITH THE INTENT TO NOT PAY AND TO HAVE A THIRD PARTY PAY FOR THE SERVICE

2. **Subscriber fraud:**

The user provides false documentation or impersonates another person to request and subscribe to a telecommunication service for the purpose using it so as not pay or clandestinely carry out other types of fraud.

3. **Public phone bypass fraud:**

The public phone line is bypassed to make phone calls with no intention of paying.

4. **Third-country fraud or refile:**

The fraudster obtains one or various phone lines in his/her own country and using the conference call facility or with a small switch makes it possible for users from various countries to communicate between each other, the charges of both calls are invoiced to the phone lines obtained by the fraudster who normally subscribes to these lines with false documents, bypass fraud or unscrupulous technical experts.

5. **Equipment drain:**

The fraudster subscribes to mobile phone plans where devices are subsidized, for the purpose of obtaining the terminal, which are taken by organized crime and place normally in other countries where

the price of these devices are much higher, for the purpose of profiting from the difference in the price of the equipment.

6. **PBX fraud:**
This is a facility of the PBX exchanges, which are normally assigned to executives for remote access with codes to platforms that enable them to communicate with all services (local, national long distance, international long distance, mobile, access to Internet, among others), through social engineering or unscrupulously these access are known by third parties who shall use the service making companies ultimately pay the bill for services not used for their profit. This type of fraud is increasing with PBX-IP, because of the access facility that fraudsters have from any part of the world and oftentimes because of the little protection of these elements by the users.

7. **Tampering with network elements:**
It consists of outsources staff and/or permanent staff of the company intentionally tampering with phone channels to use the service and make sure that it stays on free lines, test line or charges to a customer that has not used this service.

8. **Tampering with information:**
Local access or by hacking the registration, billing and supply platforms to delete and/or alter registrations of use, hired capacity, blocked IMEIs, customer statements and user data in any of the systems of the service provider chain that can alter service payment or release equipment reported stolen and/or lost.

9. **Theft of phone lines**:
Active lines assigned to users whose home address is changed or bypassed for use by a third party without the authorization of the subscriber or the local service provider company.

10. **Theft of PINs of cards or keys of special services to make calls:**
When a user is carrying out a communication using services with PINs such as prepay cards or special services, the fraudster seizes the PINs and general uses the service or sells it on the black market to carry out communications charging them to the card or special service of the customer. They are also obtained by means of SMS with the intention to commit fraud, simulating the awarding of prizes in exchange for a prepay PIN.

11. **Use and sale of facilities assigned by the companies for use by third parties:**
They are processed through telecommunication elements assigned by the companies to their employees to achieve the corporate goals and the latter take advantage of these elements to make them available to third parties, normally in exchange for their own profit.

FRAUD IN THE REGULATORY SYSTEM AND/OR SERVICE PROVISION OF EACH COUNTRY

12. **Bypass – Reorigination:**
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, then that is where the reorigination mode takes place, which consists of changing the origin of the communication, which is international in nature, simulating as if it were between local operators or on the intranet. This modality can be used for landline or mobile phone service. The business of the fraudster consists of profiting from the difference between the international communication price and the local traffic for landlines or intranet for mobile phones. In addition, as a rule, these fraudsters are not bound by any regulatory obligations, do not pay taxes and

earn their income from abroad. Types of bypass: inbound, outbound, local, national or international or mobile reorigination.

13. **Callback:**
This type of fraud consists of inversing the direction of traffic, as a rule international traffic, so that, instead of making a call from the origin to the destination, it appears like a call made from the destination to the origin. Under normal service provision conditions, the subscriber who requires communication (caller user) must make calls originating in his/her country through operators that are there. But in this case a call is dialed to a number abroad to platforms that take the subscriber at the origin, and these platforms then redial from abroad to the original caller and establish the communication as if it were from the destination to the origin. This phenomenon manages to trick payment for the call at origin and as a result incoming calls take place that should have been billed as outgoing calls.

14. **Unfair competition:**
Some companies set up their switchboard equipment to prevent their customers from using other networks, for example national or international long-distance services. They block the competitor operator's identification digits, so that the user believes that the operator is not available and is forced to use the services of the operator to which his/her line is connected. Another way that this kind of fraud takes place is the refusal to interconnect with competitor networks.

15. **Resale of telecommunication services without due authorization:**
This is where persons who intend to reap financial gains acquire services provided with subsidized corporate or residential plans for the purpose of reselling these services without due authorization from the telecommunication service operator.

FRAUDS AGAINST USERS

16. **Slamming:**
It involves the illegal practice of switching the user's operator to another without the consent of the user or using methods that trick the customer.

17. **Cell phone cloning:**
Fraudsters intercept the equipment serial number (ESN) using radio receiver equipment. Once they have these numbers, they reprogram them on other equipment, from which they make calls that are billed to the subscriber holding the original ESN.

18. **Cramming:**
They are services that are installed and/or billed to the customers although the latter have not requested, received, authorized or used these services.

19. **Dialers:**
Dialers are programs which, when used for wrongdoing, can redirect connections made on the switched network while the user is browsing on the Internet. Their purpose is to halt the phone connection that the Internet user is using at that time in order to establish another by dialing either a phone number with a premium rate or a number of an international ISP.

20. **Theft of mobile phones:**
There are gangs who steal mobile devices for the purpose of reselling them so that they can used inside or outside the national territory normally with other operators. It is currently a major problem because these devices are rebranded 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 the bases of the operators.

21. **Automatic subscription to services of an operator unless the customer specifically refuses these services**:

This type of subscriber fraud is committed by adding services that agreed upon in the contract. These services are, at first, free of charge and the, without the express authorization of the user, they start being charged by the operators.

USE OF ICT PLATFORMS AND INFRASTRUCTURE TO PERPETRATE OTHER TYPES OF FRAUD

22. **Adware**: Unwanted advertisement. Banners of products or services are introduced without the user's consent, which slows down the network and impedes browsing. Oftentimes they are used by free programs to drawn the attention of users and they can often induce users to commit other types of fraud such as phishing.

23. **Backdoor*:*** It is a program that is inserted into the computer and is apparently inoffensive. But once installed, it provides a "backdoor" whereby it is possible to control the target computer. This makes it possible for the fraudster to carry out actions in this computer that compromise the user's privacy or have it viewed in the Internet as a hostile computer or impede its working with others.

24. **Creation and use of own infrastructure without a license:** This type of fraud is normally used by the fraudster to conceal his/her true activities. The best way to do this is for the fraudster to have his/her own infrastructure with a private clandestine network with which he/she can commit crimes such as trafficking in persons, drug trafficking, contraband, extortion, among others.

25. **DIDs:** This type of service, as a rule, is not regulated in our countries. Therefore local lines can be found ringing in third countries towards which there is a different long-distance rate as if it were a local rate and vice-versa. For example, phone lines in Buenos Aires ringing in the USA and lines in the USA ringing in Buenos Aires. This type of service is provided to avoid monitoring by authorities, because while in the operator systems the subscriber has been assigned a service for local use, the latter is really located in another country, which makes it almost impossible to monitor it in case a crime has been committed, which makes its use attractive for extortion, drug trafficking, trafficking in persons.

26. **Hacking**: In this case, the fraudster manages, by fraud, to have access to the computer systems of companies to so they can carry out operations on the company's data for his/her own benefit or for third parties. An example of this type is the illegal access to telecommunication platforms to resell services or the access to bank customer databases to release or transfer money to third parties or to pay third-party services with the money of account holders whose information has been stolen.

27. **Keyloggers**: Through this system, the fraudster manages to seize information keyboarded by a user. Oftentimes this modality is used on public Internet services for the purpose of seizing data, which are afterwards sold on the black market or using the information obtained for the fraudster's own benefit. Examples of this are the seizure of bank passwords and payment of third parties using the money of account holders whose information has been stolen.

28. **Establishing infrastructure to monitoring the private information of users:** The lawbreaker tries to secure information for his/her own profit, for example, by installed automatic teller

machines (ATM) to discover user passwords or cloning the cards of the users. In this kind of offense, the spammer tries to obtain confidential information with a remote monitor to then withdraw money, using technologies such as SMS, Wifi, among others.

29. **Trickery using messages to draw the attention of persons:** In this type of fraud, the lawbreaker makes a profit from his activities and builds a telecommunication infrastructure to draw the attention of ingenuous, oftentimes unemployed, persons who see an opportunity to improve their situation, as a result of messages about work abroad, as a model or earning high income. These messages are published in newspapers, web pages, e-mails, among others. Once the person is lured into this, he/she is used for altogether different activities.

30. **Phishing**: In this type of fraud, the fraudster manages to obtain a user's confidential bank information by cloning web pages or using the e-mails themselves through phone calls. Once they obtain the information, they empty the user's accounts.

31. **Clandestine radio and television broadcasting** for various purposes. For example it can be used to broadcasting information to train groups who operate outside the law, etc.

32. **SCAM:** Fraudsters use scams to try to secure middlemen for international transactions so they can launder money.

33. **Spyware**: All kinds of malignant software that surreptitiously uses a user's Internet connection to extract data or information on the contents of the computer or its behavior without the consent of the user. This method makes it possible to obtain confidential information about the user to be used for various purposes.

34. **SPAM**: Unwanted e-mails, whereby the spammer tries to bombard lists of users with unsolicited e-mails, oftentimes containing programs that are self-installed and can even damage the content of the computers. Fraudsters oftentimes use them as a way to spread viruses, among others.