

ALLEGATO 1	PROCEDURA N° PR 01/2010	Pag. 1
Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

Procedura inter-Operatore per il contrasto delle frodi

FINALITÀ	La procedura ha lo scopo di definire il protocollo di comunicazione e le operazioni che le Parti dovranno eseguire per contrastare i tentativi di frode messi in atto, ai danni dei Clienti dei servizi di telecomunicazione e/o degli stessi gestori dei servizi, con metodi e scenari di traffico che richiedono operazioni congiunte e coordinate tra i gestori delle reti coinvolte, per un'efficace repressione.
APPROVAZIONI	<p>Redatto da: Gruppo di Lavoro Monitoraggio Frodi del Tavolo Tecnico ex art. 6 delibera 418/07/CONS</p> <p>Verificato da: Operatori sottoscrittori del Protocollo d'Intesa per il contrasto delle frodi</p> <p>Approvato da: Operatori sottoscrittori del Protocollo d'Intesa</p>
RESPONSABILITÀ	Aggiornato da: Comitato Tecnico Antifrode
STORIA DEL DOCUMENTO	Rev. N° 2.0, del 12 Aprile 2010: la versione 2.0 è adottata per l'avvio della fase a regime, a valle del periodo di sperimentazione.

	Confidential	
--	--------------	--

ALLEGATO 1	PROCEDURA N° PR 01/2010	Pag. 2
Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

ENTI COINVOLTI Tutti gli Operatori sottoscrittori del Protocollo d'Intesa per il contrasto delle frodi

DESTINATARI Contact Point degli Operatori sottoscrittori del Protocollo d'Intesa per il contrasto delle frodi

CLASSIFICA Codice
CTA-FFPR01-I-2.0
•
del <12Aprile 2010>
in vigore dal <data di entrata in vigore>

**RIFERIMENTI
NORMATIVI**

GOLDEN COPY Copia n° 1
Archiviata presso: Contact points degli Operatori sottoscrittori del Protocollo d'Intesa
in Data: <data dell'archiviazione>

**DOCUMENTI DI
RIFERIMENTO** **Verbali delle riunioni del Gruppo di Lavoro per il monitoraggio delle frodi costituito nell'ambito del Tavolo Tecnico** ex art. 6 delibera 418/07/CONS

DEFINIZIONI
NNG: Numerazione Non Geografica
NG: Numerazione Geografica o Numerazione per Servizi di Comunicazione Mobili e Personali
CS: Centro Servizi
SLA: Service Level Agreement
AGCom: Autorità per le Garanzie nelle Comunicazioni
GdL: Gruppo di Lavoro
CTA: Comitato Tecnico Antifrode

	Confidential	
--	--------------	--

ALLEGATO 1	PROCEDURA N° PR 01/2010	Pag. 3
Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

INDICE

1. INTRODUZIONE	4
2. TIPI DI FENOMENI FRAUDOLENTI	4
3. REGOLE E MODALITÀ OPERATIVE DI GESTIONE	6
3.1 Protocollo di Comunicazione	7
3.2 Informativa a supporto della SEGNALAZIONE	8
3.3 Informativa a supporto del RISCONTRO	9
3.5 Criteri di monitoraggio ed esecuzione delle azioni di contrasto	9
3.5.1 Eventi per i quali l'Operatore di accesso si attiva come soggetto segnalante	10
3.5.2 Eventi per i quali l'Operatore titolare della NNG si attiva come soggetto segnalante	12
5. REPORT PERIODICI PER IL MONITORAGGIO DELLA PROCEDURA	13
6. PUNTI DI CONTATTO	13
ANNESSO A: PUNTI DI CONTATTO	14

ALLEGATO 1 Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA N° PR 01/2010	Pag. 4
	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

1. Introduzione

Il presente documento, redatto ai sensi del Protocollo d'Intesa tra gli Operatori per la cooperazione nella prevenzione e contrasto delle frodi, descrive il protocollo di comunicazione e le operazioni da eseguire per la gestione congiunta dei fenomeni fraudolenti.

Nel seguito del documento si definiscono:

- i tipi di fenomeni fraudolenti che rientrano nel campo di applicazione della presente procedura;
- le regole e modalità operative da rispettare per la loro gestione congiunta.

2. Tipi di fenomeni fraudolenti

I principali tipi di fenomeni fraudolenti, che rientrano nel campo di applicazione della presente procedura sono i seguenti (la lista è da considerarsi esemplificativa e non esaustiva):

1. **I fenomeni fraudolenti dovuti ad intromissione di terzi su utenze di clienti ignari:** sono quelli, generalmente perpetrate su utenze di rete fissa di clienti aventi contratti in abbonamento, attuate con diverse tecniche e schemi, finalizzate a generare chiamate verso direttrici a rischio (es. NNG, internazionali, numerazioni mobili con opzioni di autoricarica, ecc.), con addebito a carico dei singoli ignari clienti e conseguente generazione di contestazioni nei confronti dell'Operatore di accesso, il quale, spesso, è reputato dal cliente responsabile del danno o dell'addebito del traffico. Per questa categoria, lo schema di frode è caratterizzato dalle seguenti modalità di perpetrazione:
 - I. manipolazione di cavi telefonici all'esterno della proprietà del cliente (ad es. parallelismo su doppino nell'armadio ripartilinea, in chiostrina od altri elementi dell'infrastruttura di Rete);
 - II. intromissione di terzi su centralini aziendali (ad es. dial in/dial out);
 - III. intromissione logica su infrastrutture o apparati di telecomunicazione o informatici allo scopo di produrre attività fraudolente (ad es. SMS Spoofing, dialer autoattivanti, trojan horse, ecc.).

L'accertamento delle suddette modalità di perpetrazione a volte può essere dedotto, con ragionevole fondatezza, anche dalla semplice analisi delle caratteristiche del traffico originato dall'utenza e/o dalle verifiche fatte direttamente col cliente titolare della stessa.

	Confidential	
--	--------------	--

ALLEGATO 1 Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA N° PR 01/2010	Pag. 5
	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

2. **I fenomeni fraudolenti da sottoscrizione:** ovvero casi di traffico generato da utenze, attivate con dati falsi oppure reali, ma appartenenti ad ignare persone (furto d'identità), al solo scopo di perpetrare frodi o di generare traffico per uso personale con la preordinata intenzione di non pagarne il controvalore.

L'accertamento di tali tipi di frode in genere può essere dedotto "con ragionevole consequenzialità" dalla compresenza di uno o più dei seguenti elementi (la lista è da considerarsi esemplificativa e non esaustiva):

- I. non rintracciabilità o irreperibilità dell'intestatario dell'utenza telefonica;
- II. dati dell'intestatario incoerenti con l'identità dell'utilizzatore (furto di identità, dati/documenti contraffatti/rubati, dati inesistenti, ecc.);
- III. dati di sedi o domicili "fantasma" di persone giuridiche o privati (anche mediante informazioni commerciali effettuate da ditte di fiducia ed autorizzate alle investigazioni);
- IV. mancata corrispondenza delle caratteristiche dell'ubicazione dell'impianto rispetto all'attività dichiarata;
- V. corrispondenza inesitata (welcome letters, telegrammi di contatto, fatture);
- VI. utilizzo di coordinate bancarie/carte di credito false, incongruenti o rubate.

3. **Fenomeni fraudolenti con utilizzo di prodotti ricaricabili** con credito ottenuto attraverso attività fraudolente.
4. **Fenomeni fraudolenti da servizi ingannevoli** (ad es. SMS ingannevoli con inviti a chiamare NNG o altre numerazioni associate a servizi fittizi, wangiri, servizi premium con profili di scarsa trasparenza, ecc.) .
5. **Frodi deducibili dalla presenza di caratteristiche anomale nel traffico.** Si tratta di casi di traffico, generalmente diretti verso specifiche direttrici (ad es. NNG, numerazioni mobili con profilo di autoricarica, numerazioni internazionali ad alto costo, ecc.) ovvero originate da specifiche numerazioni (ad es. decade 4) ed aventi profili d'uso del servizio che risultano anomali per le caratteristiche delle chiamate e/o di utilizzo dei servizi (quantità, durata, orario, frequenza, località d'origine, servizi supplementari di rete utilizzati, numeri chiamati, ecc.) .

L'accertamento di tali ipotesi di frode può essere dedotto dal rilevamento, nelle caratteristiche del traffico, di uno o più dei seguenti elementi (l'elenco è da intendere esemplificativo e non esaustivo):

	Confidential	
--	--------------	--

ALLEGATO 1	PROCEDURA N° PR 01/2010	Pag. 6
Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

- I. raggiungimento di volumi di traffico telefonico insolitamente elevati rispetto ai consumi storici del cliente (anche solo in relazione a specifiche numerazioni o direttrici geografiche e non geografiche, comprese quelle in decade 4);
- II. raggiungimento di volumi di traffico terminati su una singola NNG, o su un insieme di NNG afferenti allo stesso CS ovvero originati da una numerazione in decade 4 assimilabile, insolitamente elevati rispetto al profilo storico del traffico oppure anomali per le caratteristiche del traffico;
- III. traffico proveniente da singola numerazione in decade 4 insolitamente elevato rispetto ai volumi storici della numerazione;
- IV. anomala ripetitività del traffico da cui si può dedurre la carenza di volontà del cliente di usufruire del servizio fornito dal CS oppure l'incoerenza con un normale utilizzo del servizio (es. collegamenti per diverse ore senza soluzione di continuità, ecc.);
- V. utilizzo abnorme della linea telefonica attivata (è il caso delle frodi finalizzate a rivendita di traffico);
- VI. utilizzo di servizi di call conference per terminare traffico su NNG, SIM con autoricarica, numerazioni internazionali, ecc.;
- VII. generazione di alti volumi di traffico per finalità di frode con SIM prepagate usate con modalità che eludono i processi di billing;
- VIII. singole chiamate (anche di durata anomala) distribuite su interi archi di numerazione chiamanti;
- IX. traffico da/verso direttrici di traffico a valore aggiunto (es. 4X, 709, 89x), numerazioni mobili con profilo di autoricarica o internazionali mediante l'ausilio di strumenti automatici;
- X. utilizzo massiccio di schede SIM al fine di favorire l'interruzione, totale o parziale, o l'alterazione del funzionamento di apparati di rete o sistemi di controllo.

3. Regole e modalità operative di gestione

Gli Operatori si impegnano a predisporre, ove applicabile, quanto necessario per rilevare gli scenari di frode descritti nel capitolo precedente ed a gestirli secondo le modalità operative descritte nel seguito.

La tempestività e l'adeguatezza dell'informativa con cui si segnala il caso di sospetta frode costituiscono fattori determinanti per l'efficacia della presente procedura.

	Confidential	
--	--------------	--

ALLEGATO 1	PROCEDURA N° PR 01/2010	Pag. 7
Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

Di seguito si descrive il protocollo di comunicazione da osservare (fermi restando gli obblighi in capo a Telecom Italia di cui all' art. 4, commi 12, 13 e 14 della Delibera AGCom n. 27/08/CIR) per la gestione end to end dei casi di presunta frode, il contenuto ed il formato delle informative previste nelle diverse fasi operative ed i criteri di gestione da rispettare per quanto concerne la responsabilità del monitoraggio e delle azioni cautelative da eseguire per i diversi tipi di frode.

3.1 Protocollo di Comunicazione

Qualora le analisi sul traffico e gli accertamenti tecnici e/o gestionali rilevino la presenza di elementi che inducano a ritenere che sia in atto un possibile fenomeno fraudolento riconducibile ad uno dei tipi descritti nel paragrafo precedente, l'Operatore che rileva l'evento ne dà tempestiva comunicazione ai punti di contatto degli altri Operatori interessati/coINVOLTI (ivi inclusi laddove esistenti gli Operatori di transito e gli Operatori ospitanti) mediante l'invio di un'informativa (di seguito "**Segnalazione**"). Per i dettagli di tale informativa si rimanda al paragrafo 3.2; per la lista dei punti di contatto si rimanda all'Annesso A della presente procedura.

Per la gestione della Segnalazione le Parti coinvolte dovranno osservare le seguenti regole generali:

1. La segnalazione da parte dell'Operatore che rileva l'evento dovrà essere sempre tempestiva rispetto alla data di rilevazione della sospetta frode ed in ogni caso dovrà avvenire al massimo entro 30 (trenta) giorni solari dall'evento, fatto salvo quanto previsto al successivo paragrafo 3.5.
2. Gli Operatori che ricevono la Segnalazione dovranno, in base a quanto comunicato, eseguire le relative verifiche del caso, determinare se trattasi di possibile frode o solo di improvvisa concentrazione di traffico lecito e volontario e ove necessario, compiere tutte le azioni di propria competenza allo scopo di impedire il protrarsi della frode e/o il conseguimento dell'illecito profitto, comunicando quindi all'Operatore segnalante l'esito delle verifiche nonché le azioni eseguite (per la descrizione delle azioni in funzione dei diversi scenari si rimanda al successivo paragrafo 3.6).
3. La risposta (di seguito "**Riscontro**") dell'Operatore destinatario della Segnalazione, per comunicare l'esito delle verifiche e delle eventuali azioni eseguite, dovrà essere sempre tempestiva rispetto alla Segnalazione ed in ogni caso dovrà essere fornita al massimo entro 30 (trenta) giorni solari dalla data di ricevimento della Segnalazione.

	Confidential	
--	--------------	--

ALLEGATO 1 Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA N° PR 01/2010	Pag. 8
	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

Le comunicazioni di cui ai punti precedenti avverranno, ove non sia espressamente stabilita una diversa modalità, mediante scambio di e-mail tra i punti di contatto operativi di cui all'Annesso A alla presente procedura. Le Parti potranno concordare l'impiego di metodi di protezione dei dati scambiati.

3.2 Informativa a supporto della SEGNALAZIONE

In questo paragrafo vengono elencate le informazioni minime da inviare a supporto della Segnalazione. Tali informazioni potranno essere anche maggiormente dettagliate in funzione della tipologia di evento fraudolento segnalato.

Oggetto della Segnalazione: da indicare nell'oggetto della mail tramite il codice "Operatore_X_AAMMGG_progressivo", dove:

- "Operatore" assume la ragione sociale dell'Operatore segnalante;
- "X" può assumere i valori:
 - I (in caso di intromissione);
 - S (in caso di sottoscrizione);
 - SI (in caso di servizi ingannevoli);
 - FSR (frodi da utilizzo di servizi ricaricabili), con credito ottenuto attraverso attività fraudolenta;
 - TA (traffico anomalo);
- AAMMGG indica la data della segnalazione;
- il progressivo è il codice univoco su base Operatore segnalante assegnato all'evento e che servirà per il prosieguo delle comunicazioni.

Breve descrizione del fenomeno: è necessario indicare tutte le informazioni utili alla comprensione del fenomeno segnalato e alle successive analisi del fenomeno segnalato.

Dati di traffico: da inserire in apposito file excel in allegato alla mail:

- numerazioni (CLI) di destinazione del traffico sospetto (in chiaro), ovvero anche di origine per le numerazioni in decade 4 e per ognuna di queste:
 - numerazioni di origine del traffico sospetto (CLI), con le ultime tre cifre oscurate (nel caso di frodi originate da rete fissa che interessano un'elevata numerosità di clienti chiamanti, il CLI sarà sostituito dal distretto geografico di origine del traffico);
 - numero di chiamanti diversi (da indicare obbligatoriamente quando l'origine del traffico è espressa mediante distretto telefonico);
 - per ogni numerazione di origine (numero o distretto):
 - tipologia di eventi (chiamate, SMS, MMS, ecc.);
 - numero di eventi per singola numerazione di destinazione;

	Confidential	
--	--------------	--

ALLEGATO 1 Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA N° PR 01/2010	Pag. 9
	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

- durata complessiva delle conversazioni (in minuti) e, ove applicabile possibile, anche dettagliata per singola numerazione;
- importo complessivo del traffico (iva esclusa) sospetto e, ove disponibile possibile, anche suddivisa per singola numerazione.
- periodo di generazione del traffico sospetto.

Eventuali azioni intraprese come ad es. lo sbarramento temporaneo dell'accesso alla numerazione interessata dal fenomeno fraudolento o la sospensione delle utenze da cui ha origine il traffico fraudolento. Ove tali azioni non vengano esplicitate sarà sottinteso che nessuna azione è stata intrapresa dall'operatore segnalante.

Richieste particolari: eventuali richieste di azioni/informazioni che il segnalante ritiene necessarie al fine di reprimere il fenomeno, come:

- informazione sul Centro Servizi assegnatario (in caso di NNG);
- sbarramento del traffico dei propri clienti verso una specifica numerazione;

3.3 Informativa a supporto del RISCONTRO

L'operatore destinatario di una Segnalazione, effettuate le verifiche del caso, risponderà all'Operatore segnalante fornendo le informazioni relative all'esito delle verifiche ed alle eventuali azioni eseguite, nei termini indicati nel seguito.

Oggetto della risposta: facendo un mero reply alla prima segnalazione.

Breve descrizione dell'esito delle analisi del fenomeno: sarà fornita una descrizione complessiva della situazione riscontrata con l'indicazione di tutti i dettagli utili al congiunto accertamenti dei fatti, ivi inclusa l'indicazione di elementi oggettivi volti a qualificare il fenomeno come lecito.

Azioni effettuate: dovranno essere sempre fornite le informazioni di sintesi sulle azioni intraprese.

3.5 Criteri di monitoraggio ed esecuzione delle azioni di contrasto

Il monitoraggio e la segnalazione degli eventi di sospetta frode saranno assicurati da tutti gli attori responsabili del servizio di trasporto delle chiamate: l'Operatore di accesso, l'Operatore di transito e l'Operatore di terminazione/titolare della NNG.

	Confidential	
--	--------------	--

ALLEGATO 1 Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA N° PR 01/2010	Pag. 10
	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

Ciascuna Parte agirà come soggetto segnalante per quelle manifestazioni di sospette frodi per cui risulta più efficiente un suo impegno in “prima battuta” (tipicamente, perché ha maggiore visibilità dei fenomeni rivelatori della specifica tipologia di frode).

Più precisamente, con riferimento a tutti gli scenari di frode definiti nel capitolo 2, la ripartizione dei compiti tra le Parti per la gestione end to end dei casi di sospetta frode seguirà le regole seguenti.

3.5.1 Eventi per i quali l'Operatore di accesso si attiva come soggetto segnalante

L'Operatore di accesso è tenuto a segnalare eventi potenzialmente fraudolenti per quanto previsto dalle casistiche di cui ai punti 1, 2, 3, 4, 5 (escluso il punto 5.II) del cap. 2 della presente procedura, entro un termine di 30 (trenta) giorni dall'evento (mediante la prima Segnalazione di cui al paragrafo 3.1).

I criteri di rilevamento dei suddetti scenari fraudolenti saranno definiti autonomamente da ciascun Operatore.

Naturalmente l'Operatore di accesso, a fronte della Segnalazione, avrà facoltà sulla propria rete di porre in essere tutte le azioni cautelative ritenute idonee a tutelare i propri interessi e quelli dei propri clienti finali.

In particolare, **nel caso in cui il traffico presumibilmente fraudolento sia diretto verso NNG**, ovvero nel caso in cui sia originato da numerazioni in decade 4 o altre con servizi analoghi, tali azioni potranno essere, ad es.:

- inibizione parziale o totale dell'accesso alla/e NNG interessata/e dalla propria rete (anche nel caso trattasi di numerazione in decade 4 ed assimilabile);
- sospensione cautelativa dei pagamenti, ove previsto;
- deposizione di esposto/denuncia;
- ecc.

Gli Operatori destinatari di tali Segnalazioni, saranno tenuti nel più breve tempo possibile, ove applicabile e tecnicamente fattibile, a cooperare nel seguente modo:

- eseguire le verifiche del caso sulle numerazioni di transito/terminazione o segnalate e gli eventuali servizi associati;
- eseguire, in caso di riscontri che confermano ragionevolmente la fondatezza dell'evento segnalato, le azioni cautelative applicabili sulla propria rete e/o nei confronti dell'eventuale CS interessato, per impedire il perpetrarsi/ripetersi della frode e/o dell'abuso rilevato;

	Confidential	
--	--------------	--

ALLEGATO 1	PROCEDURA N° PR 01/2010	Pag. 11
Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

- fornire il Riscontro all'Operatore d'accesso segnalante, secondo le modalità descritte nel precedente paragrafo 3.1;
- inviare, all'occorrenza, una Segnalazione di avviso ad eventuali altri Operatori di accesso interessati al fenomeno anomalo rilevato, per permettere loro di effettuare le verifiche del caso.

Le azioni cautelative a carico degli Operatori destinatari delle Segnalazioni sono definite in funzione del tipo di frode.

In particolare si distinguono i seguenti due casi:

- a) Segnalazioni caratterizzate da traffico terminante su NNG oppure originato da numerazioni in decade 4 o con servizi assimilabili;
- b) Segnalazioni caratterizzate da traffico terminante su SIM prepagate, finalizzato all'autoricarica fraudolenta.

Nel primo caso le azioni minime, ove tecnicamente applicabili, dovranno essere:

- sospensione del pagamento della reverse a favore del CS per il traffico presumibilmente fraudolento o abusivo o eventuale richiesta di ripetizione delle somme nel caso in cui il pagamento fosse già avvenuto (ove applicabile);
- richiesta al CS di rimuovere, entro un lasso di tempo ristretto, le eventuali irregolarità rilevate sul servizio, pena la risoluzione del relativo contratto o la chiusura della NNG o del gruppo di NNG interessate;
- chiusura della/e NNG e, nei casi più gravi, disdetta del contratto col CS, ove applicabile (es. in caso di servizi fittizi o con evidenti profili ingannevoli/finalità ingannevoli).

Nel secondo caso le azioni minime, ove applicabile, dovranno essere:

- sospensione cautelativa della SIM destinataria del traffico presumibilmente fraudolento o, almeno, blocco dell'eventuale credito residuo derivante da frode, se tecnicamente fattibile;
- eventuale inibizione del traffico verso NNG se tecnicamente fattibile (limitatamente ai casi in cui la SIM destinataria del traffico fraudolento "scarichi" il credito ottenuto fraudolentemente verso NNG oppure funga da collettore di traffico fraudolento originato da numerazioni in decade 4 o assimilabili)
- invio, seguendo le modalità di cui al par. 3.5, di una Segnalazione all'Operatore titolare della NNG nei casi in cui si rilevasse un fenomeno di "scarico" del credito illecito verso NNG e, se tecnicamente fattibile, blocco cautelativo del pagamento della reverse per gli importi di traffico derivanti dallo scarico;
- invio, seguendo le modalità di cui al par. 3.5, di una Segnalazione all'Operatore mobile interessato nei casi in cui si rilevasse un fenomeno di autoricarica a catena, ossia di "scarico" del credito illecito verso SIM di altri operatori per presumibili finalità di autoricarica, seguendo le modalità di cui al par. 3.5.

	Confidential	
--	--------------	--

ALLEGATO 1 Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA N° PR 01/2010	Pag. 12
	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

Infine si precisa che, per gli eventi presumibilmente fraudolenti di cui l'Operatore di accesso può avere notizia direttamente dal cliente finale, tipicamente afferenti alle casistiche di frode indicate al punto 4 dell'elenco riportato nel cap. 2 (casi di Spamming effettuati con metodi vari) oppure a casi di scarsa trasparenza o potenziale ingannevolezza del messaggio introduttivo del servizio offerto su una NNG, qualora il cliente finale ne dia notizia all'Operatore di accesso, quest'ultimo, una volta riscontrata la fondatezza della segnalazione del cliente, provvederà a darne Segnalazione all'Operatore di terminazione/titolare della NNG nel più breve tempo possibile dal ricevimento della notizia, riservandosi la facoltà di sbarrare cautelativamente l'accesso alla NNG interessata in attesa di ricevere il Riscontro da parte di quest'ultimo.

L'Operatore di terminazione/titolare della NNG, in questi casi specifici, sarà tenuto, nel più breve tempo possibile, ad inviare apposita comunicazione al CS con richiesta di rimuovere, entro un ristretto lasso di tempo, le eventuali irregolarità rilevate sul servizio, pena la risoluzione del relativo contratto o la chiusura della NNG o del gruppo di NNG interessate.

3.5.2 Eventi per i quali l'Operatore titolare della NNG si attiva come soggetto segnalante

Gli Operatori titolari di NNG si impegnano a:

- monitorare il corretto utilizzo delle NNG a loro assegnate al fine di verificare che essi rispettino la normativa vigente;
- monitorare il traffico terminato su una singola NNG, o su un insieme di NNG afferenti allo stesso CS, oppure originato da numerazioni in decade 4 o assimilabili al fine di verificare la presenza di variazioni anomale presumibilmente fraudolente, quali (a titolo esemplificativo e non esaustivo) quelle di cui al punto 5.II delle casistiche di frode riportate nel cap. 2.

I criteri di rilevamento dei possibili eventi di natura fraudolenta saranno definiti autonomamente da ciascun Operatore.

Le eventuali anomalie rilevate con riferimento ai due punti suddetti dovranno essere segnalate agli Operatori interessati in accordo al protocollo di comunicazione precedentemente descritto.

Nel caso in cui l'anomalia segnalata dall'Operatore titolare della NNG evidenziasse il non corretto utilizzo della numerazione assegnata e/o sancito dalla normativa vigente, esso è tenuto a:

	Confidential	
--	--------------	--

ALLEGATO 1	PROCEDURA N° PR 01/2010	Pag. 13
Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

- richiedere al Centro Servizi, entro un lasso di tempo ristretto, l'adeguamento ed il ripristino del corretto utilizzo, pena la risoluzione del relativo contratto;
- sbarrare temporaneamente la NNG interessata sulla propria rete, in funzione della gravità del caso.

Gli Operatori di accesso destinatari della Segnalazione si impegnano ad effettuare le verifiche nei tempi tecnici oggettivamente necessari (non superiori a 30 giorni dalla Segnalazione ricevuta) e dando riscontro all'Operatore titolare della NNG, riservandosi, all'occorrenza, la facoltà di inibire l'accesso alla NNG interessata dalla propria rete, qualora le condizioni che hanno determinato l'esistenza del rischio di frode non siano state rimosse e le eventuali azioni risolutive a carico dell'Operatore di terminazione/titolare della NNG non siano state espletate

5. Report periodici per il monitoraggio della procedura

Ogni Operatore sottoscrittore del Protocollo d'Intesa per il contrasto delle frodi, al fine di supportare il Comitato Tecnico Antifrode, nell'attività di monitoraggio ed adeguamento della procedura antifrode, si impegnerà a fornire, via e-mail, con cadenza trimestrale, entro il primo mese successivo al trimestre di riferimento, alla casella di posta indicata dal CTA, i report conformi alla seguente struttura:

Report Statistico sul Traffico Anom.	Report Sulle TOP 20 Numerazioni Ci
---	---------------------------------------

6. Punti di contatto

Per l'avvio della fase operativa è necessario che le Parti comunichino i rispettivi punti di contatto secondo lo schema seguente:

	Confidential	
--	--------------	--

ALLEGATO 1 Protocollo d'Intesa per il contrasto delle frodi	PROCEDURA N° PR 01/2010	Pag. 14
	PROCEDURA INTER-OPERATORE PER IL CONTRASTO DELLE FRODI	Versione 2.0

Operatore XXXX 1° Livello (operativo) Numero telefono (possibilmente della sala operativa frodi) Orari operativi Mailbox condivisa: segnalazione_frodi_altri_Op@dominio.it 2° Livello (manageriale) Fraud Manager (o delegato) Numero telefono (mobile) Indirizzo e-mail

Ogni Parte assicurerà che, durante le ore di ufficio, sia disponibile un referente al quale, all'occorrenza si potrà chiedere eventuali chiarimenti sulle segnalazioni scambiate.

La lista dei punti di contatto forniti da ciascun Operatore è disponibile in Annesso A alla presente procedura.

Annesso A: Punti di contatto



Contact Point List.xls