

Anexo 8

TRATAMENTO CONJUNTO DE COMBATE E PREVENÇÃO A FRAUDE

1 OBJETIVO

- 1.1 Reduzir o volume de fraude nas chamadas originadas a partir das redes das PARTES, por meio de ações conjuntas entre as empresas. Será premissa para essa redução a identificação de todos os terminais classificados como fraude, conforme definições abaixo, bem como definir procedimentos para a identificação de tráfego fraudulento, seja esse de origem ou destino.

2 DEFINIÇÕES

2.1 Definição da Fraude:

Conceito Objetivo:

Subterfúgio para alcançar um fim ilícito, ou ainda, o engano dolosamente provocado, o malicioso induzimento em erro ou aproveitamento de pré-existente erro alheio, para o fim de enriquecimento ilícito.

Conceito Subjetivo:

Obtenção ou uso de um produto/serviço de Telecomunicações com a pré-disposição de não realizar o pagamento integral do produto/serviço utilizado ou ainda gerar cobrança indevida a terceiros.

A fraude pode objetivar o benefício do anonimato, ganho financeiro ou apenas economia para o usuário.

A fraude se distingue da inadimplência.

2.2 Tipos de Fraude:

Subscrição

- Aquisição fraudulenta de serviços pelo uso indevido de informação cadastral inexistente, ilegal ou autêntica pertencente a terceiros (seja pessoa física ou jurídica).

Técnica

- Utilização indevida de serviços telefônicos, pertencentes a terceiros (usuário ou prestadora de serviços de telecomunicações).

Interna

- É a fraude decorrente de prática criminosa por parte de empregados da Empresa.

Abuso de Informações

- Obtenção de informações para exploração fraudulenta do serviço de telecomunicações.

Fraude de Subsídio

- Aproveitamento irregular ou fraudulento do subsídio do aparelho.

Engenharia Social

- Obtenção de informações sensíveis pela utilização de subterfúgios para engano provocado ou malicioso.

2.3 Termos usados na fraude :

Clip-on (Gato) - Conexão física irregular realizada em linhas fixas (STFC)

Clone - Cópia dos códigos ESN/MIN em um 2º aparelho (SMP)

Invasão de PABX – Acesso remoto ao equipamento (Cx Postal ou DISA)

Provedor - Tráfego artificial gerado de forma involuntária

TUP – Utilização de Telefones de Uso Públicos sem o devido consumo de créditos

Vírus de Aparelhos – Violação das configurações dos aparelhos ocasionando originação não autorizada de chamadas ou SMS.

Alteração de IMEI – Prática que permite a reutilização de aparelhos bloqueados por roubo ou furto devidamente incluídos na Lista Negra.

Lista Negra – É a lista de terminais que estão sofrendo ação de bloqueio pelas áreas de Anti-Fraude. É composta de terminais fraudadores, fraudados ou fora do padrão de numeração.

3 OBRIGAÇÕES DAS PARTES

3.1 Monitoramento de tráfego fraudulento

- 1.1.1 As prestadoras do STFC na modalidade local, do SMP ou do SME deverão monitorar o tráfego de todos os seus assinantes, conforme modalidade de prestação do serviço, inclusive o tráfego de Longa Distância, independentemente do CSP escolhido. As prestadoras do STFC na modalidade Longa Distância deverão monitorar o tráfego dos usuários que escolherem o CSP de sua outorga.
- 3.1.1.1 Esse monitoramento de uso deverá contemplar limites de utilização em todos os cenários de chamadas no STFC modalidade Local, no SMP ou no SME e ou no STFC LD, sempre que houver risco de fraude e ou não pagamento.

3.2 Troca de Informações operacionais para combate a fraude

- 1.2.1 As PARTES deverão disponibilizar a base de seus terminais ou de outras prestadoras, designados para assinantes ou vagos, gerando chamadas fraudulentas locais ou de LD, e que estão, no momento, recebendo tratamento anti-fraude. Serão encaminhados terminais com suspeita ou fraude confirmada.
- 3.2.1.1 As PARTES deverão enviar diariamente, de 2ª feira a 6ª feira, exceto feriados (municipais, estaduais e federais) e eventuais dias prensados, os terminais realizando chamadas fraudulentas ou suspeitas, incluídos ou detectados no dia anterior, por meio de e-mail, para os destinatários definidos no item 5 deste Anexo.
- 3.2.1.1.1 As informações referidas no item 3.2.1.1 acima deverão ser dispostas e formatadas em padrão de arquivo, conforme definido no Apêndice I a este Anexo.
- 3.2.1.1.2 No arquivo a ser gerado conforme item 3.2.1.1.1 acima, serão incluídos, a título de Vago (tipo de fraude A), além dos códigos de acesso válidos e não designados, os códigos de acesso fora do padrão e não atribuídos a assinantes, porém que estão gerando chamadas. Ex: 11111111
- 2.2.2 As PARTES deverão enviar diariamente, de 2ª feira a 6ª feira, exceto feriados (municipais, estaduais e federais) e eventuais dias prensados, os terminais removidos da base de terminais fraudulentos (suspeitos não confirmados) de dias anteriores, e que foram enviados anteriormente, por meio de e-mail para os destinatários definidos no item 5 deste Anexo.
- 3.2.2.1 As informações referidas no item 3.2.2 acima deverão ser dispostas e formatadas em padrão de arquivo, conforme definido no Apêndice II a este Anexo.
- 3.2.3 Cada uma das PARTES deverá analisar e tratar as informações sobre terminais suspeitos informados pela outra PARTE, de acordo com os procedimentos e parâmetros operacionais previstos no item 4 deste Anexo, em até 2 (dois) dias úteis a partir do horário do envio do e-mail.
- 3.2.3.1 Cada PARTE deverá atender por telefone às solicitações emergenciais da outra PARTE, no horário das 8:00h às 20:00hs, de 2ª feira a 6ª feira, exceto em feriados (municipais, estaduais e federais) e eventuais dias prensados.

3.3 Troca de informações gerenciais de tráfego fraudulento

- 3.3.1 Mensalmente, cada PARTE deverá disponibilizar a relação de terminais que tiveram fraude confirmada com base nos 3 (três) últimos meses de tráfego.
- 3.3.1.1 Deverão ser encaminhados como fraude, todos os terminais identificados por ambas as PARTES, sejam eles terminais próprios ou de outras prestadoras e informados por meio do arquivo descrito no Apêndice I de forma consolidada.
- 3.3.1.2 Deverá ser disponibilizado mensalmente, por cada PARTE, relatório de tráfego, com finalidade informativa, somente referente a chamadas originadas e terminadas em terminais com fraude confirmada, por meio de arquivo no mesmo formato utilizado pelas PARTES no processo de conciliação de DETRAF.

4 PROCEDIMENTOS E PARÂMETROS OPERACIONAIS

- 4.1 As PARTES se comprometem a adotar os procedimentos e parâmetros operacionais acordados ou que vierem a ser acordados entre as prestadoras participantes do Grupo Executivo de Anti-fraude, incluindo:
 - 4.1.1 Tratamento a ser dado aos terminais identificados pela outra PARTE como fraudulentos ou suspeitos, inclusive quanto a compromisso de bloqueio
 - 4.1.2 Parâmetros utilizados para identificação de terminais fraudulentos.

5 COMUNICAÇÃO ENTRE AS PARTES

- 5.1** Todas as notificações, relatórios e outros comunicados relacionados a este Documento e seus Anexos, deverão ser efetuados por e-mail, ou, na indisponibilidade deste, por telefone, ou por fax, entre os pontos de contato da área de fraude das PARTES, a serem indicados em até 15 (quinze) dias contados da assinatura deste Contrato.
- 5.1.1** Deverão constar dos comunicados mencionados no item acima, as seguintes informações dos destinatários: nome, departamento, e-mail e telefone.

Apêndice A

INCLUSÃO DE TERMINAIS COM CHAMADAS FRAUDULENTAS OU SUSPEITAS

1 MODELO DE E-MAIL

De: e-mail da operadora que detectou a fraude

Para : e-mail da operadora recebedora da informação

Subject: Inclusão - dd.mm.aa

Os números do arquivo anexo foram inseridos na Lista Negra na data de hoje.

2 PADRÃO DE ARQUIVO

Arquivo CSV com os seguintes campos e informações:

Tipo de Arquivo preenchido com o valor I, referente a inclusão:

Número do terminal no formato XYABCDMCDU onde:

XY é o código de área, variando de 11 a 99;

ABC ou ABCD é o prefixo;

MCDU é a Milhar, Centena, Dezena e Unidade do terminal.

Data do bloqueio ou da detecção, no formato DD/MM/AAAA onde:

DD é o dia com 2 dígitos

MM é o mês com 2 dígitos

AAAA é o ano com 4 dígitos

Nos tipos de fraude A a D o campo refere-se a data de bloqueio

Nos tipos de fraude E e F o campo refere-se a data da detecção

Motivo do bloqueio (BL de A, BL de B, PRS,...)

Tipo de Fraude onde:

A – Vago;

B - Fraude de Subscrição;

C - Fraude de Subscrição com uso CSP DA OPERADORA;

D - Fraude com uso CSP da XXXXX

E – Suspeita de fraude

CPF / CNPJ onde: (Nos tipos de fraude A e D o campo estará vazio)

Nome: (Nos tipos de fraude A e D o campo estará vazio)

Endereço: (Nos tipos de fraude A e D o campo estará vazio)

Localidade: (Nos tipos de fraude A e D o campo estará vazio)

Outras Linhas do Assinante: (Nos tipos de fraude A e D o campo estará vazio); Os terminais adicionais estarão no formato especificado e separados por “/”

Situação: (O campo estará vazio)

Bloqueado: (O campo estará vazio)

Data de Habilitação: (O campo somente será preenchido no tipo de fraude E)

Apêndice B EXCLUSÃO DE TERMINAIS COM CHAMADAS FRAUDULENTAS OU SUSPEITAS

1 MODELO DE E-MAIL

De: e-mail da operadora que detectou a fraude
Para : e-mail da operadora recebedora da informação
Subject: Exclusão - dd.mm.aa
Os números do arquivo anexo foram retirados da Lista Negra na data de hoje.

2 PADRÃO DE ARQUIVO

Arquivo CSV com os seguintes campos e informações:

Tipo de Arquivo preenchido com o valor E, referente a exclusão:

Número do terminal no formato XYABCDMCDU onde:

XY é o código de área, variando de 11 a 99;

ABC ou ABCD é o prefixo;

MCDU é a Milhar, Centena, Dezena e Unidade do terminal.

Data do desbloqueio no formato DD/MM/AAAA onde:

DD é o dia com 2 dígitos

MM é o mês com 2 dígitos

AAAA é o ano com 4 dígitos

Motivo do desbloqueio (Fraude não confirmada, ANATEL, PROCON)

Tipo de Fraude: (O campo estará vazio)

CPF / CNPJ onde: (O campo estará vazio)

Nome: (O campo estará vazio)

Endereço: (O campo estará vazio)

Localidade: (O campo estará vazio)

Outras Linhas do Assinante: (O campo estará vazio)

Situação: (O campo estará vazio)

Bloqueado: (O campo estará vazio)

Data de Habilitação no formato DD/MM/AAAA: (O campo estará vazio)