ANEXO 9

PREVENÇÃO E CONTROLE DA FRAUDE

1. OBJETIVO

Definir o desenvolvimento de ações coordenadas de prevenção e controle da fraude nas chamadas cursadas nas redes da **TIM** e da **¢OPERADORA¢**.

2. DEFINIÇÕES

Fraude – 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.

Ataque – consiste na origem indiscriminada de ações de acesso a endereços IP de qualquer ponto da rede Internet, com a finalidade de congestionar redes de clientes, provedores ou usuários da Internet, através de sobrecarga aplicada à Infraestrutura ou elemento de rede.

Invasão – Consiste no acesso indevido a Redes IP, de forma não autorizada e indesejada, a fim de coletar ou modificar informações, uso de sistemas ou softwares, implantação de softwares ou informações indesejadas, ações que causem redução de desempenho, restrição de acesso, enfim, qualquer ato ou ação indesejada.

Subscrição – aquisição fraudulenta de serviços através do uso indevido de informação cadastral inexistente, ilegal ou autêntica pertencente a terceiros (seja pessoa física ou jurídica).

Interna – Qualquer tipo de utilização, por parte de um colaborador ou terceiro, através das deficiências técnicas da operadora para realizar a utilização abusiva ou indevida dos serviços e produtos.

Outras – todos os outros tipos de fraudes não definidas neste item.

3. DAS OBRIGAÇÕES DAS PARTES

3.1 As PARTES se comprometem a adotar procedimentos e parâmetros operacionais de prevenção e detecção de Fraudes em suas respectivas redes, objetivando inibir as práticas já conhecidas e as advindas de novos avanços tecnológicos que surgem a cada dia no Setor de Telecomunicações. Dentre alguns tipos de Fraude, pode-se destacar:

3.1.1. **Fraude de Subscrição**: Aquisição fraudulenta de serviços através do uso indevido de informação cadastral inexistente, ilegal ou autêntica pertencente a terceiros (seja pessoa física ou jurídica).

a) Roubo de Identidade: Falsidade ideológica - Suposto cliente (fraudador) utiliza os dados pessoais de terceiros, cuja origem é roubo ou falsificação, para adquirir produtos ou serviços;
b) Aquisição de Terceiros: O titular provém ou vende seus dados pessoais de identificação para o fraudador, para adquirir produtos ou serviços da companhia;
c) Aquisição Própria ou "Auto Fraude**"**: O próprio titular adquire produtos ou serviços da companhia, mas com clara e evidente intenção de não pagar;
d) Aquisição de Longa Distância: Falsidade ideológica de Longa Distância - O mesmo "modus operandi" do "Roubo de Identidade", mas em outras operadoras, utilizando os serviços de longa distância;

e) Aquisição de Serviço de Roaming: Fraudador utiliza os serviços de "roaming out" em outras operadoras que têm acordo com a operadora dona do terminal, mas com clara intenção de não pagar.

3.1.2. Fraude Técnica: Utilização indevida de serviços telefônicos, pertencente a terceiros (usuário ou operadora de telecom).

Invasão de PABX: Acesso não autorizado a PABX com o propósito de gerar tráfego artificial para destinos desconhecidos ou suspeitos, afetando o Cliente proprietário do PABX.

a) Invasão - Gestão Cliente: Por definição contratual, neste caso, a gestão do PABX pertence ao Cliente. Com isto, a responsabilidade por eventuais invasões também é do Cliente;
b) Invasão - Gestão Operadora:Por definição contratual, neste caso, a gestão do PABX pertence a Operadora, que tem responsabilidade efetiva por esta fraude.

Clone: Uso indevido do serviço mediante o registro e ativação de um terminal na rede com os mesmos dados de um terminal legítimo já existente na mesma rede.

a) Equipamento: Ocorre quando a clonagem é realizada em um celular ou seus componentes devido a vulnerabilidade de tecnologia;
b) Smart Card: Ocorre quando a clonagem é realizada em um "smart card" de plataformas de terminais pré-pagos;
c) Calling Card: Ocorre quando a clonagem é realizada em um cartão que não admite recarga, mas tem seu número de PIN, ou mesmo em cartões utilizados em telefones públicos.

Extensão Clandestina: Uso indevido de um serviço ou produto ativo na operadora, objeto de furto através de uma extensão clandestina, feita de maneira física ou lógica. Caracteriza-se por um roubo de serviço.
a) Física - Clip-on: Uso não autorizado da linha fixa, mediante uma derivação irregular, não conhecida pelo cliente;
b) Banda Larga: A extensão clandestina é realizada por meio lógico ou meio físico, por exemplo: através do rastreamento do sinal "wireless" do "Router" do Cliente.

3.1.3. Operadoras: Operadoras que, através de métodos não ortodoxos, geralmente não regulamentados em seu País, ou inclusão de uma fraude, geram tráfego para obtenção de tarifas de interconexão.

a) "PRS (premium rate service)": Os provedores de serviços "PRS" oferecem vantagens ou ganhos para os Clientes que ligam para seus números. Geralmente estes provedores têm acordos com outras operadoras;
b) Refiling: Operadoras de longa distância manipulam o tráfego de interconexão e seus CDR's, mudando este tráfego para uma classe tarifária mais barata, com clara intenção de pagar menos interconexão;
c) Cobilling: Operadoras locais, no momento em que tem que validar os CDR's de Tráfego de longa distância de outras operadoras, procede com impugnações indevidas;
d) Manipulação SS7: Operadoras, no momento em que ocorrem as chamadas, fazem a programação incorreta de suas centrais, informando SS7 incorretamente.

3.1.4. Revenda de Serviços: Caracteriza-se pela prestação de serviços de telecomunicações por pessoas físicas ou jurídicas que não tem autorização para prestar estes tipos de serviços. Geralmente os fraudadores contratam os serviços básicos da empresa e fazem a revenda dos mesmos, de forma compartilhada.

a) By Pass : Sainte ou entrante. O fraudador adquire serviços telefônicos, e/ou infraestrutura de links, transforma a voz em dados e envia o tráfego para outros destinos, geralmente internacionais;
b) Banda Larga: O fraudador adquire um serviço de banda larga de alta velocidade e compartilha o serviço através da rede física, wireless, ou rádio freqüências;
c) Arbitragem: "Tipos de Arbitragem nas telecomunicações:

1. Callback (Landing ilegal): O originador de uma chamada faz um serviço em resposta, imediatamente é desconectado e chamado de volta: A empresa que faz a chamada geralmente utiliza telefonia IP no trecho internacional com terminação na telefonia regular do país correspondente a preço de chamada local (ou também está localizada no país de alguma operadora, possivelmente atacadista, que oferecem chamadas internacionais baratas).

2. Refilling: Técnica para a substituição da CLI (Call Line Identify), em um ponto da rota de uma chamada, para tirar proveito de melhores taxas de acordos tarifários entre os Países.

3.1.5. Dealer: Trata-se das fraudes cometidas pelos "Dealers", empresas ou empregados de terceiros que trabalham direta ou indiretamente para a Operadora.

a) Venda Indevida: Vendas não solicitadas pelos clientes ou aquisição de equipamento em nome do cliente são realizadas pelos dealers, geralmente com a intenção de ganhos de comissões ou também motivado por estelionato;
b) Comissões Indevidas: Acesso indevido e manipulação dos sistemas de gestão de comissões, atribuindo comissões indevidas, sem correlação com as vendas;
c) Reciclagem: Sem nenhuma solicitação ou autorização do cliente, o dealer da baixa e alta em um terminal, obtendo ganho de comissão, de forma indevida.

3.1.6. Fraude Interna: Delitos praticados por empregados ou terceiros que trabalham para a companhia, que se aproveitam das vulnerabilidades dos sistemas de gestão de clientes, sistemas de faturamento, de rede, e outros.

a) Descontos Indevidos: Descontos em produtos ou serviços são atribuídos a clientes de maneira indevida. Acesso indevido a plataforma de gestão de pré-pagos, fazendo recargas indevidas nos terminais;
b) Vagos: Terminais vagos (sem clientes) são ativados, programados e liberados para utilização fraudulenta;
c) Isenção de Tarifas: Isenção de tarifas dos clientes que são praticadas de maneira indevida;
d) Habilitação Indevida: Habilitação no sistema de provisionamento (HLR), sem a inserção correspondente nos sistemas de faturamento;
e) Recargas Indevidas: A alocação de saldos indevidos através do sistema comercial para os produtos pré-pago e controle;
f) Alteração de Dados do Cliente: A fraude por transações indevidas realizadas por usuários com acesso ao sistema, tanto interno como externo, alteração de equipamento, aumento de limite de consumo. Alteração de nome, alteração de assinatura, alterações no cadastro do cliente, ajustes indevidos e acessos a serviços de valor agregado;
g) Sincronismo de Sistema: Fraudes identificadas através do monitoramento de recargas virtuais, como por exemplo: estornos indevidos que se realizam para fazer compras durante o tempo que demora a execução do estorno. Fraude gerada por produto que compartilha seu saldo, onde o cliente compra, estorna e logo compartilha o saldo no tempo que dura o estorno;
h) Rede: Exclusão de informação da plataforma de voz e dados. Ativação de redes/ serviços, dados de baixa;
i) Fuga de Terminais: Fraudador adquire o aparelho móvel com desconto da operadora e ativa e utiliza os serviços em outra operadora. O aparelho móvel é roubado e tem a ativação indevida do IMEI em outras operadoras ou em outros países.

3.1.7. Engenharia Social: Obtenção de informações sensíveis através da utilização de subterfúgios através do engano provocado em legítimo cliente e posterior uso do serviço.

a) Programação de Serviços: induzir o cliente de boa-fé a disponibilizar “facilidades” para fins fraudulentos (siga-me, conferência e chamadas a cobrar);

b) Phishing: Refere-se a "pesca" de informação de clientes através de SMS para cometer fraude, apresenta-se também solicitando a vítima que faça recargas para um número celular em particular;

c) Degradação de Imagem – Extorsão: Fraudes que são cometidas usando a rede da operadora para fraudar os usuários finais da empresa, muitas vezes o fraudador se passa por funcionário da operadora. - Fraude cometida por grupos criminosos através de extorsão aos usuários finais da rede da operadora, seja por SMS ou Voz;

d) Alteração Cadastral: Prática realizada pelo fraudador que de posse dos dados do cliente legítimo, através dos canais de atendimento das prestadoras passa a ter a posse do serviço. Podem ser:

1. Mudança de Endereço: Fraudador entra em contato com o atendimento e solicita a mudança de endereço da prestação do serviço e a linha é instalada na casa do fraudador. O cliente legítimo tem sua linha cortada.
2. Mudança da Data de Vencimento: Prática realizada para que o cliente legítimo não perceba cobrança que ele não reconheça a origem. Esta prática esconde uma fraude de gato por exemplo.

3.1.8. Tráfego Artificial: Geração de tráfego, sem que haja a real utilização dos serviços pelo usuário ou que mantém a chamada ativa com objetivo de entretenimento, ou simplesmente utilização do canal (voz, dados e sms), visando desbalanceamento entre a receita de público e os valores de remuneração, com a finalidade contrária à transmissão de voz e de outros sinais destinadas a comunicação entre pontos fixos e móveis determinados, utilizando processos de telefonia, caracterizando assim, o uso inadequado do STFC, SMP e SME.

3.1.8.1 São evidências de tráfego artificial as seguintes situações: Ausência de mobilidade quando do serviço móvel; Chamadas automatizadas (rediscagem, desvio, siga-me, conferencia,; chamadas massivas; chamadas nacionais com identificação de chamadas internacionais; Desbalanceamento acentuado de trafego entrante e sainte comparado com usuário médio do serviço; Longa duração de chamadas; chamadas com ausência de conversação entre pessoas ou seja, maquina para maquina (M2M); Comportamento de trafego não humano.. Estas evidências podem ser obtidas na análise dos CDR expectativa ou através dos CDR da outra Parte.

3.2 As Partes devem manter pessoal técnico capacitado para interagir na detecção, localização e isolamento de Fraudes, Ataques e ações prejudiciais à segurança das redes.

3.3 Quando uma das Partes requisitar a outra Partes se compromete em adotar procedimentos de controle, desenvolver e implementar ações de forma a identificar situações de fraude relacionadas ao tráfego entre as redes das PARTES

3.4 Quando identificado o uso suspeito do CSP, através do monitoramento por qualquer uma das partes, a operadora detentora do assinante deverá fornecer imediatamente ou se solicitada, o cadastro completo do(s) cliente(s) originador(es) das chamadas suspeitas, contendo as seguintes informações: Nome completo, CPF, endereço e dados de contato. Após o fornecimento destes dados a prestadora de longa distância deverá entrar em contato com o(s) cliente(s) e analisar possíveis fraudes por meio de checagem do(s) cadastro(s) com os dados fornecidos pelo(s) cliente(s) no(s) contato(s) de monitoração.

3.4.1.1 Caso a prestadora do SME, detentora do cliente não forneça os dados supracitados, ela estará sujeita as sanções previstas da Cláusula 5.2, deste Anexo.

4. PROCEDIMENTOS A SEREM ADOTADOS

4.1 Manter Sistema de Controle de Ataques e Fraudes na sua rede, investigando e/ou tratando os incidentes de forma pragmática;

4.2 A comunicação entre as PARTES deverá ser efetuada por telefone, no horário das 9:00h às

17:00h, de 2 a feira a 6a feira, exceto em feriados (municipais, estaduais e federais) e eventuais dias prensados;

4.3 Os procedimentos adotados podem ser revistos a qualquer momento pelas Partes, desde que acordados mutuamente;

4.4 Quaisquer alterações dos procedimentos adotados, definidos neste acordo operacional entre a **TIM** e a **¢OPERADORA¢**, antes de serem aplicados, devem ser aprovados pelas Partes, pelos seguintes representantes:

TIM:

Nome: Gerência de Risco
E-mail: prevencaoafraude@timbrasil.com.br
Telefone: 21 4009-4216
Contato: Sandra Gomes

¢OPERADORA¢ :

Nome:
E-mail:
Telefone:
Contato:

4.5 As alterações indicadas neste item devem ser formalizadas por meio de aditivo a este Contrato.

4.6 Manter Sistema de Controle de Ataques e Fraudes na sua rede, investigando ou tratando os incidentes de forma pragmática, comunicando às respectivas PARTES cujas redes estão envolvidas

4.7 Caso evidencie-se a prática de geração de tráfego artificial, conforme descrito no item 3.1.8.1, as Partes desde já acordam em reduzir o dimensionamento de suas interconexões (quantidade de E1), de forma a comportar somente o tráfego sem evidências de que seja artificial. Esta medida visa evitar riscos à estrutura e equipamentos destinados à interconexão, garantindo a continuidade operacional e função social da interconexão das redes de telecomunicações.

5. CRITÉRIOS PARA REMUNERAÇÃO DE REDES E ACERTO DE CONTAS

5.1 O pagamento das remunerações de redes será sempre devido pela prestadora detentora da receita de público, independentemente da ocorrência de fraudes, sobre quais as Partes buscarão sua redução.

5.2 Excluem-se do item acima as situações em que haja evidências de geração de tráfego artificial e do mau uso da interconexão de redes em que se configure a geração de chamadas fraudulentas, caracterizando a geração da fraude pela própria Operadora. Nestes casos, serão adotados os seguintes procedimentos:

1. Uma das Partes deverá notificar a Anatel sobre essa grave infração, prevista no Artigo 17 da na Resolução 588, de 7 de maio de 2012, Regulamento de Remuneração pelo Uso de Redes de Prestadoras do Serviço Telefônico Fixo Comutado – STFC e solicitar a abertura de um procedimento Administrativo para sua apuração e aplicação das sanções cabíveis, sem prejuízo das medidas judiciais e criminais cabíveis.

2. O pagamento da remuneração de redes, para a operadora geradora desse tráfego, estará automaticamente suspenso, sendo que no caso de chamadas de Longa Distância

Internacional, a Operadora geradora do tráfego fraudulento também deverá ressarcir o pagamento da remuneração de redes das prestadoras internacionais, efetuado pela prestadora de Longa Distância.

2.1 O valor devido pela Prestadora fraudadora será corrigido monetariamente de acordo com as Cláusulas 11.1.1, 11.1.2 e 11.1.3 do Contrato e deverá ser pago em até 15 (quinze) dias da apresentação da cobrança.

3. Envio de uma comunicação à Parte geradora do tráfego artificial e/ou das chamadas fraudulentas, para que essa prática seja interrompida em até 2 (dois) dias corridos;

5.3 Caso a Operadora que recebeu a comunicação não cesse a geração de chamadas fraudulentas no prazo supracitado, a interconexão de redes poderá ser bloqueada até que haja um parecer da Anatel sobre o procedimento Administrativo.

5.4 O acerto de contas se dará de acordo com o disposto no “Anexo 2 - Apresentação e Forma de Acerto de Contas entre as Partes”, e demais cláusulas pertinentes previstas neste Contrato.