ANEXO XI - TRATAMENTO CONJUNTO DE COMBATE E PREVENÇÃO A FRAUDE

1. OBJETIVO

1.1 Desenvolvimento de ações coordenadas de prevenção e controle da fraude nas chamadas cursadas nas redes da **TBRASIL SMP** e da **OPERADORAB**.

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" da "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. 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.

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, 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 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. 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

d."Set-top box/ ou smart-card (TV)": Ocorre quando a clonagem é realizada no set-top box e/ ou smart card que provem do serviço de televisão paga.

3.1.5. 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.

c.Televisão (pirataria): A extensão clandestina é praticada por meio lógico ou físico, geralmente, no cabo, e em grande parte em redes analógicas.

3.1.6. 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 frequências.

c.Televisão: O fraudador adquire um serviço de televisão paga, compartilhando através da rede física ou a retransmissão de sinal.

d.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.

3.1.7. *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.

3.1.8. Desvio de Recursos: 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 (rede CDMA).
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.

3.1.9. Facilidades de Rede (SVAs): Serviços de Valor Agregado são usados com intenção fraudulenta de fazer a conexão telefônica sem a intenção de pagar.
a.Caixa Postal: O serviço de caixa postal, ativado no cliente, é programado de maneira que permite o direcionamento da chamada para um número de destino fraudulento.
b.Transferência de Chamadas (TRF): O serviço "siga-me", ativado no cliente, é programado para um número de destino fraudulento, geralmente um "chat", onde os fraudadores podem efetuar chamadas de maneira simultânea.
c.Roaming Indevido: Pré-pagos fazendo roaming.

3.1.10. Fraude a Clientes (Internet): Fraudes relacionadas com o acesso a conteúdos de internet.
a. Phishing: Refere-se a "pesca" de informação de clientes para cometer fraude, apresenta-se também solicitando a vítima que faça recargas para um número celular em particular.
b. Inadequado acesso aos dados dos Clientes: Uso do site da Vivo para o acesso indevido a conta dos clientes para acessar suas faturas e dados.
c. Smishing: 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.
d. 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.

3.1.11. Fraude Locutórios ou Mobilidade de Locutórios: Presença de mobilidade celular (mais de 11) nas linhas celulares GSM em pontos de venda atacadistas chamados Locutórios.

a. Dentro da Cobertura: Presença de mobilidade dentro da zona permitida de operação do locutório varejista.
b. Fora da Cobertura: Conexão a bases de rádio localizadas fora da base de operação autorizada ao varejista.

3.1.12. Fraude Técnica: Qualquer tipo de utilização, por parte de um terceiro, das deficiências técnicas da operadora para realizar a utilização abusiva ou indevida dos serviços e produtos.

3.1.13. 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

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

3.3 Atuar, quando requisitada pela outra PARTE, nos procedimentos de controle e no desenvolvimento de ações, tão logo venha ocorrer e sejam identificadas situações de fraude relacionadas ao tráfego entre as redes das PARTES.

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 2ª feira a 6a feira, exceto em feriados (municipais, estaduais e federais) e eventuais dias prensados;

GRUPO TELEFÔNICA:

Área:
e-mail:
Telefone:
Contato:

OPERADORAB:

Nome:
e-mail:
Telefone:
Contato:

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 **TBRASIL SMP** e a **OPERADORA B,** antes de serem aplicados, devem ser aprovados pelas Partes, pelos seguintes representantes:

TBRASIL SMP:

Área:
e-mail:
Telefone:
Contato:

OPERADORAB:
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.