

TATIANA GUMM

FRAUDES NO SEGMENTO DE TELEFONIA MÓVEL NO BRASIL

Monografia apresentada ao Departamento de Contabilidade do setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná, como requisito para obtenção do título de especialista em Gestão de Riscos Corporativos. Professor Orientador: Antonio César Pitela.

CURITIBA

2010

AGRADECIMENTOS

Agradeço pela vida. Em todas as etapas boas e àquelas não tão fáceis, sempre esteve presente junto de mim uma Luz Divina cobrindo-me de bênçãos... Ele está com todos nós.

Agradeço pelo alento familiar. Aos meus pais que tanto fizeram e tanto ainda fazem por mim: o companheirismo incondicional da minha mãe e pelas doces lembranças que guardo do meu pai.

Agradeço ao destino. Aos amigos tão queridos que conquistei, aos professores que atuaram no curso, em especial ao orientador, e ao meu grande amor - meu noivo querido que carinhosamente me acompanha e me incentiva.

RESUMO

Gumm, Tatiana. **Fraudes no Segmento de Telefonia Móvel no Brasil**. 2010. (41 p.) Monografia de Conclusão de Especialização em Gestão de Riscos Corporativos. Universidade Federal do Paraná, Curitiba - 2010.
Orientador: Antônio César Pitela.

A evolução do mercado de telefonia móvel ocorrida recentemente trouxe com os elevados números de novos telefones celulares, um problema que vem sendo tratado cada vez com mais cautela pelos executivos da área, que são as fraudes em habilitações de telefone celular. O tema, não está obrigatoriamente associado à algum avançado subsídio tecnológico ou então uma quadrilha altamente articulada, mas na grande maioria das ocorrências trata-se de golpes e truques bastante antigos que usa principalmente a ingenuidade de suas vítimas ou então a falta de controle das companhias afetadas.

Em diferentes níveis de prejuízo e formas de atuação, essa prática traz para o setor e também para a sociedade vários ônus que interferem na relação prestador de serviço x cliente.

Este estudo mostra qual o contexto de ocorrências de fraudes e alguns pontos de atuação para a mitigação desse risco. Foi estabelecido o conceito de fraude a partir das características e situações em que ocorrem, quais os tipos de fraude presentes no segmento analisado, os principais facilitadores e quais seriam os pontos de controle que auxiliam na prevenção dessa contravenção.

Palavras-chave: fraude, telefonia móvel

ABSTRACT

The current evolution in cellphone market has brought with the high number of new mobiles one problem that has been treated cautiously each time by the management of this area, that is the frauds on cellphone hire. The issue isn't obligatory associated to any advanced technology practice or highly articulated gang, but the most of the time they are old strokes that use mainly the naivety of the victims or the lack of control of the affected companies.

On different levels of damage and acting ways, this practice brings to the section and also for the society much onus that interfere in the relationship between companies vs. customer.

This study shows which fraud context, and any mitigation points about this risk. It was established the fraud concept from the features that occur, which kind of frauds are present in the segment analysed, the main facilitators and the control points that help in prevention of this transgression.

Key words: fraud, mobile phone.

SUMÁRIO

1. INTRODUÇÃO.....	6
2. PROBLEMA.....	8
3.OBJETIVOS.....	8
3.1 OBJETIVO GERAL	8
3.2 OBJETIVO ESPECÍFICO	8
4. JUSTIFICATIVA.....	9
5. METODOLOGIA	10
6. REVISÃO DE LITERATURA.....	12
6.1 FRAUDE – CONCEITO.....	14
6.2 TELEFONIA MÓVEL – CENÁRIO ATUAL.....	16
6.2.1 PORTABILIDADE NUMÉRICA	18
6.3 PROCESSO DE CONCESSÃO DE NOVAS LINHAS x DETECÇÃO DA FRAUDE	19
6.4 DETECÇÃO DE FRAUDE.....	21
6.5 ENGENHARIA SOCIAL.....	23
6.6 TIPOS DE FRAUDE EM TELEFONIA MÓVEL.....	25
6.7 MENSURAÇÃO DAS FRAUDES	27
6.8 RISCOS INTERNOS ÀS ORGANIZAÇÕES	29
6.9 IMPACTOS	32
6.10 FATORES DE MITIGAÇÃO.....	34
7 CONCLUSÃO	37
8. REFERÊNCIAS BIBLIOGRÁFICAS	40

1. INTRODUÇÃO

Nos últimos trinta anos a evolução tecnológica (principalmente com o advento da internet e a popularização de vários meios de comunicação) criou um ambiente propício e atrativo para a obtenção ilícita de bens de consumo e serviços, através de mecanismos fraudulentos.

De fato, o ambiente esteve propício muito antes da criação e ampla divulgação da rede mundial de computadores. A partir da revolução industrial já há registros de desvios, golpes, falsificações e crimes do “colarinho branco” que dependendo da cifra envolvida viraram escândalos internacionais.

Desde os níveis mais primários até as práticas mais elaboradas a fraude tem objetivo único de extorquir, favorecer e ludibriar algo ou alguém para a obtenção de vantagem e benefício para a conquista de algo em benefício de quem cometeu esse ato.

Em diferentes níveis de complexidade, em companhias privadas e instituições públicas, muitos golpes foram e continuam sendo aplicados principalmente quando encontra um ambiente de baixo (ou nulo) controle, ou vítima com perfil ingênuo ou mal instruído que possa facilitar a ação. Recentemente foi divulgado pela mídia o golpe do falso seqüestro, em que o golpista escolhe aleatoriamente números telefônicos e liga para suas vítimas.

Especificamente a última década, em que ocorreu a privatização do extinto Sistema Telebras, a telefonia tornou-se um dos meios mais populares de comunicação, sendo a categoria de telefone móvel um dos nichos mais atraentes para o público em geral, pelas facilidades oferecidas, mas atraem também um problema de proporções cada vez mais expressivo que são as fraudes, e por isso foi elaborado este estudo para explicar acerca do mercado de telefonia móvel, de modo a analisar vários aspectos que culminam com prejuízos estrondosos para as companhias que compõe esse segmento.

Esse tipo de ação, responsável por considerável evasão de receita, será abordado amplamente de modo prático e obviamente preservando a identidade dos representantes desse segmento, por uma questão de sigilo e ética profissional.

Nessa monografia, será feita uma classificação de tipo de risco em que a fraude de Telecom se enquadra para, inclusive associar os meios de controle já existente e aqueles que serão propostos.

À partir de definições previamente formadas, foi elaborado um conceito próprio para qualificar o assunto abordado nesse estudo e então dimensionar quais os fatores que influenciam, afetam e contribuem para que a fraude aconteça.

Para explanar sobre a abrangência dessa ação irregular, foi detalhado o cenário atual de telefonia móvel no Brasil além da evolução das últimas décadas, de modo que seja possível visualizar qual é o ambiente em questão, bem como funciona o processo de comercialização e aquisição de novas linhas telefônicas e as principais fraudes que ocorrem atualmente.

Há também um enfoque sobre às falhas nos processos internos das organizações que podem propiciar a ocorrência de fraude interna.

Por fim, serão explanados quais os impactos, os fatores de mitigação e as observações conclusivas acerca do conteúdo tratado.

2. PROBLEMA

A fragilidade do processo de aquisição de linhas telefônicas móveis diante da larga oferta que a concorrência no setor criou na última década, propicia um ambiente atrativo para a prática de fraudes.

De que modo ocorrem fraudes nas habilitações de novas linhas no mercado de telefonia móvel?

3.OBJETIVOS

3.1 OBJETIVO GERAL

Demonstrar como ocorrem as fraudes no segmento de telefonia móvel em pleno século XXI em que a tecnologia avança a cada instante e qual o reflexo dessas ações para o mercado e a para a sociedade em geral.

3.2 OBJETIVO ESPECÍFICO

Apresentar alguns aspectos do mercado de telefonia móvel nacional e a ocorrência de fraude, tais como:

- Operação de vendas e volume de base de clientes;
- Funcionamento das fraudes;
- Quem as executa e em qual ambiente elas ocorrem;
- Quais os impactos desse tipo de ocorrência.

Ou seja, como é denominado por especialistas do meio: o *modus operandi*¹ desse tipo de contravenção.

¹ Tipo de funcionamento, método de atuação.

4. JUSTIFICATIVA

O gradativo aumento do mercado de telefonia proporciona um cenário para ação de fraudadores e golpistas a fim de obter acesso a aparelhos e serviços de maneira irregular, ou seja, aplicando golpes sem que haja a devido pagamento de faturas.

Por isso, a abordagem desse tema apresenta um alerta para a iniciativa privada, os órgãos de fiscalização e para cidadãos que também são afetados à medida que participam involuntariamente dessas contravenções, já que muitas vezes são usados documentos roubados e adulterados no processo de compra de um celular.

5. METODOLOGIA

Toda pesquisa deve basear-se em uma teoria, que serve como ponto de partida para a investigação bem sucedida de um problema. A teoria, sendo instrumento da ciência, é utilizada para conceituar os tipos de dados a serem analisados. Para ser válida, deve apoiar-se em fatos observados e provados, resultantes da pesquisa. A pesquisa dos problemas práticos pode levar a descoberta de princípios básicos e, freqüentemente, fornece conhecimentos que têm aplicação imediata (LAKATOS e MARCONI, 1990 p.17).

O assunto abordado nesse estudo é de divulgação restrita especificamente com referência ao âmbito de telefonia móvel celular, há um reduzido acervo disponível para consulta, entretanto será feita uma pesquisa bibliográfica à alguns títulos relacionados à Administração Financeira, artigos publicados na internet inerentes ao tema, pesquisa *ex post facto*, pois trata-se de um fenômeno já ocorrido.

Esse estudo também possui um enfoque prático propiciado pela experiência profissional da autora e consulta a demais profissionais da área com conhecimento avançado sobre o assunto.

Foi adotada a metodologia exploratória, pois evidenciam de modo objetivo alguns aspectos do funcionamento da fraude, com detalhes técnicos como ambiente em que ocorre como dados estatísticos e pontos de controle e de atenção quanto à fragilidade de processos (algumas ligadas especificamente a experiências empíricas aplicadas pela autora).

Para Mattar (1994), o estudo exploratório visa prover um maior conhecimento ao assunto de pesquisa, permite familiaridade, conhecimento e compreensão do fenômeno que é objeto de estudo, aliados ao conteúdo adquirido através da pesquisa bibliográfica .

Há também a aplicação de metodologia qualitativa em decorrência da apresentação do assunto abordado em que traduz os dados obtidos em formato descritivo, ou seja, dificilmente poderá ser quantificado (principalmente em decorrência à sigilo) e deve ser analisado individualmente de acordo com a interpretação dos fatos estudados. Conforme FONTES (2001, P. 222) a metodologia qualitativa utiliza elementos dissertativos, como análise de texto

e/ou discurso, análise de conteúdo sobre determinado assunto, método fenomenológico de leitura de entrevista e estudos de caso.

6. REVISÃO DE LITERATURA

Independente dos tipos de risco que afetam as organizações, o risco operacional é o mais caro e mais difícil de antecipar. Dentro dessa linha, gestão de risco operacional é fundamental nos processos de obtenção de resultados, gestão do capital e satisfação de clientes. (HARMANTZIS, 2003, p. 1).

Bergamini (2005) afirma que Risco é um fato da vida corporativa em que assumir e gerenciar riscos é parte do que as empresas precisam para obter lucros e criar valor para seus acionistas. Na medida em que todas as atividades empresariais envolvem riscos, o empresário deve avaliar e mensurar os riscos envolvidos em determinada decisão e deve administrá-los com base em sua propensão ou apetite para o risco.

Risco operacional, no mercado de telefonia móvel, pode ser dividido em três grandes áreas:

a) Risco organizacional está relacionado com uma organização ineficiente, administração inconsistente e sem objetivos de longo prazo bem definidos, fluxo de informações internos e externos deficientes, responsabilidades mal definidas, fraudes, acesso a informações internas por parte de concorrentes, etc;

b) Risco de operações está relacionado com problemas como sobrecarga de sistemas (telefonia, elétrico, computacional, etc.), processamento e armazenamento de dados passíveis de fraudes e erros, confirmações incorretas ou sem verificação criteriosa, etc.

c) Risco de pessoal está relacionado com problemas como empregados não-qualificados e/ou pouco motivados, personalidade fraca, falsa ambição, “carreiristas”, etc.

Entre os diversos tipos de riscos que as instituições se encontram expostas, o risco operacional é uma preocupação relativamente recente do mercado empresarial e investidor, decorrente das freqüentes ocorrências de escândalos financeiros em empresas de porte relevante para a contribuição do desenvolvimento econômico de países críticos na ordem econômica mundial. A Lei Sarbanes&Oxley, por exemplo, está levando empresas à implantação de

estruturas de gestão de riscos, com o intuito de mostrar ao mercado investidor a transparência na gestão organizacional e a garantia de controle na condução dos negócios.

De acordo com Tinello (2006, p. 29), aspectos variados influenciam na ocorrência de fraudes, tais como questões comportamentais e cenário atrativo para esse tipo de ocorrência:

“O importante para prevenir a fraude é saber como atua o fraudador: conhecer seu perfil psicológico. No universo dos negócios, os resultados prejudiciais da fraude não se restringem aos valores monetários envolvidos nesse tipo de atividade criminosa. Criou-se a ilusão de que com a informática os problemas de fraude seriam todos resolvidos – apenas porque as operações ficaram mais transparentes. A fraude onera as quinhentas maiores empresas brasileira em seis por cento do faturamento, em média, o que em dólares representa certa de 18 bilhões anuais. Diversos são os fatores que, no aspecto moral e psicológico, podem determinar a incidência da fraude, entre as quais: a insatisfação e a fraqueza de caráter.”

Para Parodi (2008), as fraudes já acontecem há anos, na economia de um modo geral, contemplando tanto o cotidiano das pessoas como das empresas, com a existência de golpistas que praticam um rol variado de fraudes, armadilhas, sistema e esquemas para ludibriar e roubar o próximo.

A fraude no setor de telefonia móvel é um ofensor oriundo de risco operacional em que ocorre devido a falhas diversas no ambiente corporativo (independente do segmento da companhia) e é um ponto crítico em se tratando de elo de relação comercial entre fornecedor x cliente.

O ônus causado por essa ação além do alto dispêndio que há por parte das companhias, também causa outros tipos de prejuízos (que não podem ser valorados através de um indicador financeiro), mas sentido sensivelmente através de um dos ofensores para a formação de base de clientes (similar à *market share*), pois à partir do momento em que alguém é vítima de fraude que gera débito / restrições com determinada operadora, para aquela vítima, o responsável não é um fraudador oculto que se aproveitou de suas informações cadastrais, mas sim a operadora que não teve o cuidado de se certificar da veracidade das informações cedidas para a aquisição indevida de um serviço que lhe tenha gerado danos diversos.

6.1 FRAUDE – CONCEITO

No Brasil (mas também se aplica a outros países, inclusive do primeiro mundo) as características da fraude se caracterizam por diversos fatores, principalmente em função das seguintes condições:

a. Existência de golpistas especializados: carência de alternativas para determinadas classes sociais, ineficiência das leis e do sistema penitenciário, incerteza da pena, existência de inúmeras oportunidades para obtenção de bens ou serviços adquiridos por meios ilícitos, fiscalização irregular, não cumprimento das leis encarado como comportamento comum (inclusive em função dos exemplos em nível de governo).

b. Vítimas adequadas e vulneráveis: pouca informação e divulgação preventivas, ignorância e ingenuidade da população.

c. Ausência de regras ou órgãos fiscalizadores eficazes: percepção do problema como não prioritário, despreparo e pouco treinamento, falta de leis específicas para aplicação nas situações de fraude ou golpes, falta de organismos dedicados à luta contra esses fenômenos.

Com o ambiente descrito acima, é extenso o campo de atuação dos fraudadores, pois na maioria das vezes o delito fica impune e estimula cada vez mais a aquisição de dinheiro, bens e serviços de modo indevido. Essa acaba sendo uma questão até mesmo de cunho social, sendo que o sistema judiciário estipulou uma penalidade de certo modo branda para esse tipo de contravenção, que se enquadra da seguinte forma no Código Penal:

Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.
§ 1º. Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.

Na esfera do Direito Civil, para Pereira (1999, pag. 378) a descrição de fraude está relacionada à “consonância com as idéias mais certas, a manobra engendrada com o feito de prejudicar terceiro, e tendo se insere no ato

unilateral (caso em que macula o negócio jurídico ainda que dela não participe outra pessoa) como se inscui no ato bilateral (caso em que a maquinação é concentrada entre as partes)".

Embora as definições e punições legais para esse tipo de contravenção tenham sido citadas na legislação vigente, o freqüente acontecimento de fraudes desse tipo acaba sendo banalizado em função da facilidade que o fraudador tem de atuar e da falta de repreensão pela autoridade policial para delitos como esse.

Nos mais variados segmentos de mercado, serão relacionados os métodos mais recorrentes no que tange a fraude, especialmente as ações que atingem o segmento de telefonia móvel:

- Documentos de identificação adulterados ou comprovantes de residência falsos;
- Utilização de dados cadastrais roubadas de titulares idôneos e reais (seja pessoa física ou jurídica);
- Intenção premeditada de não pagar pelo uso dos serviços contratados;
 - Quadrilhas simulando empresas fantasma ou desativadas;
 - Abuso nos serviços contratados;
 - Fraude interna na operadora.

Conforme Sá (1982, p.55), a fraude é tanto mais perigosa quanto mais sofisticada for o meio usado para praticá-la e que as modalidades de fraude mais comuns são: falsificação de fatos materiais, ocultação de fatos materiais, suborno, conflito de interesses, furto de dinheiro ou propriedade intelectual, sonegação de impostos e práticas ofensivas às leis vigentes.

Diante dos fatos apontados, uma síntese do conceito de fraude para o assunto principal desse estudo, pode ser expressa da seguinte forma: obtenção ou uso de um produto/serviço de Telecomunicações por meios ilegais, com o objetivo premeditado de não realizar o pagamento pelo serviço/aparelho fornecidos.

6.2 TELEFONIA MÓVEL – CENÁRIO ATUAL

O crescente mercado de telefonia móvel transforma-se gradativamente em alvo cada vez mais cobiçado pela ação de fraudadores, diante do volume de habilitações, relação de serviços com tecnologias avançadas e principalmente da facilidade que o serviço oferece para a solução de vários itens agrupados em um único aparelho (telefone, tv, vídeo mensagem, acesso rápido à internet, etc).

Os últimos anos foram preponderantes para a evolução das telecomunicações como um todo, mas principalmente no ramo de telefonia móvel, que trouxe a partir de 1998 a popularização e comercialização em larga escala de aparelhos celulares, com a privatização da estatal detentora do segmento. A partir de então, a concessão das bandas de frequência de cada estado do país, abriu a comercialização e a concorrência pelo mercado que até então havia sido pouco explorado.

Abaixo segue detalhamento sobre a evolução do mercado de telecomunicações (móvel) e os tipos de fraudes presentes em cada um desses períodos:

Início dos anos 90:

Tecnologia: AMPS, TDMA e CDMA.

Tipo de fraude: Expressivo volume de clonagem (fraude técnica) e início da prática de fraude de subscrição.

Padrão: Chamadas para destinos com conteúdos tarifados (telesexo, por exemplo), ligações de longa distância nacionais e internacionais.

1998 – 2002:

Tecnologia: AMPS, TDMA e CDMA.

Tipo de fraude: Controle efetivo para a prevenção de clonagem e descoberta de vários tipos de fraude de subscrição.

Padrão: Alto volume de chamadas internacionais, SMS, aparição de documentos falsificados na aquisição de linhas móveis.

2003 – 2006:

Tecnologia: TDMA, CDMA e GSM.

Tipo de fraude: Casos isolados de clonagem e crescimento significativo de incidência de fraude de subscrição.

Padrão: Alto volume de ligações de longa distancia nacionais e internacionais, serviços como SMS e MMS, Roaming Internacional.

2006 – 2009:

Tecnologia: TDMA, GSM e 3G – rede convergente (Terceira Geração)

Tipo de fraude: Nesse período já está praticamente extinta a fraude técnica (clone) e fraude de subscrição. Predomínio de fraudes tecnológicas (aproveitamento de falhas de rede)

Padrão: fraude de redirecionamento (conhecido como *by pass*) subscrição em larga escala, utilização de serviços de valor agregado (compra de toques musicais, por exemplo), transmissão de dados.

De acordo com estatísticas, O Brasil fechou o mês de agosto/2009 com 164,5 milhões de celulares e uma densidade de 85,9% de adesão, ou seja, entre linhas pré pagas e pós pagas, em cada dez habitantes, oito possuem uma linha de telefonia móvel.

Das operadoras que atuam nesse segmento, nota-se números cada vez mais expressivos, em se tratando de participação no mercado, faturamento e volume de novas linhas habilitadas. O quadro abaixo mostra o volume de novas linhas celulares habilitadas das operadoras que atuam em todo Brasil (número expresso em milhões):

Operadora	2007	2008	Até Ago/09
A	37.385	44.945	48.334
B	30.228	38.731	41.873
C	31.268	36.416	39.211
D	21.664	29.993	34.508
E	363	454	502
F	73	85	91
G	-	17	20

Fonte: site <http://www.teleco.com.br/ncel.asp>, consulta em 13/06/2009

O cenário é propício para a ação de golpistas, visto que quanto maior a base de clientes de uma operadora, maior é o dispêndio com controles e nesse caso, mesmo as organizações que dispõem de fluxos de controle, também são vitimadas principalmente em situações de fraudadores se passando pelo cliente, portanto dificilmente haverá uma medida que possa eliminar em definitivo o risco de fraude no segmento.

Outro fato que deixa esse segmento suscetível à irregularidades dessa natureza é que trata-se de um mercado relativamente recente, sendo que o período dos últimos dez anos contempla o período propulsor para a expansão de operações de telefonia móvel no Brasil.

Pesquisas revelam que a América Latina está entre as regiões com os mais altos níveis de fraudes, acima dos dez por cento, embora as operadoras de telefonia móvel entrevistadas na região acreditem que esse índice não seja superior aos cinco por cento, conforme pesquisa realizada em 2006 por uma empresa especializada em soluções tecnológicas na prevenção de fraude.

6.2.1 PORTABILIDADE NUMÉRICA

Recentemente, houve a implantação da norma de portabilidade numérica, que é um fator relevante para o assunto em questão, que consiste em possibilitar ao usuário de serviço de telecomunicações manter o número do celular à ele designado, independentemente de prestadora de serviço de telecomunicações, conforme determinado pela Anatel (Agência Nacional de Telecomunicações).

A regulamentação de Portabilidade Numérica trouxe um alerta para o setor, especialmente pelo fato de que nenhuma operadora poderá recusar a migração de um cliente, ou seja, não é possível evitar a recepção de um cadastro “suspeito” de acordo com a regulamentação vigente.

Para tanto, a etapa de prevenção nesse tipo de aquisição de cliente acaba sendo nula pela operadora receptora, logo o foco é na detecção do perfil de utilização suspeito após a conclusão da portabilidade numérica, para então atuar na redução do risco de perda com fraude.

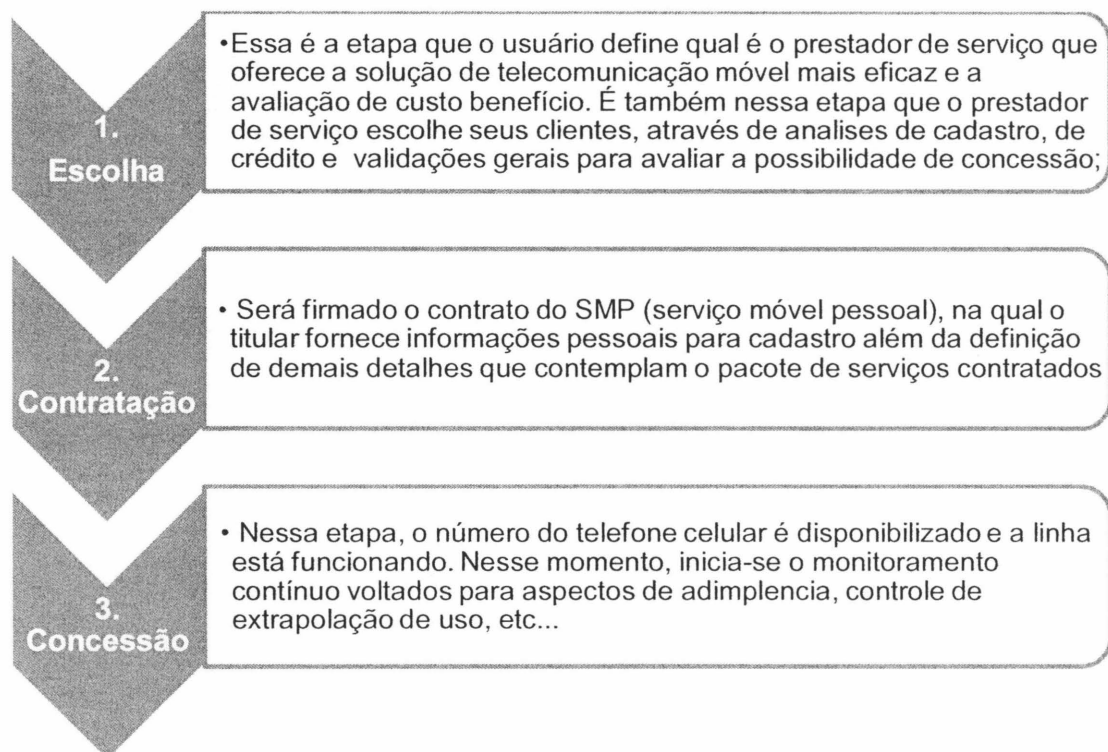
A tabela a seguir demonstra o volume total de solicitações de portabilidade numérica de até junho/2009, com a grande maioria (algo em torno de 2/3 sendo solicitação de migração de operadora de telefonia móvel):

Pedidos de Portabilidade Brasil (Portados)		
Fixa	Móvel	TOTAL
566.011	1.189.049	1.755.060

Fonte: ABR Telecom (consulta em julho 2009)

6.3 PROCESSO DE CONCESSÃO DE NOVAS LINHAS x DETECÇÃO DA FRAUDE

Atualmente, diante das ações mercadológicas agressivas que as companhias vêm oferecendo, cada vez mais tornam simplificado o processo de concessão de uma nova linha celular. O processo de venda segue basicamente as seguintes etapas:



O processo de vendas contempla não apenas a aquisição de um novo cliente, mas é nesse momento que são feitas algumas das principais validações de cadastro através de consultas à órgãos de proteção ao crédito e da confirmação *in loco* da veracidade das informações prestadas pelo titular que deseja adquirir uma linha telefônica. As operadoras móveis sofrem mais com as fraudes, pois precisam oferecer aos usuários um sistema de crédito bastante facilitado em decorrência da penetração de mercado das novas concorrentes, isso acaba gerando algumas brechas em suas redes.

Por isso essa é uma das etapas fundamentais para prevenção de fraudes, já que pode “filtrar” a entrada de cadastros irregulares na base de clientes. O planejamento é voltado para coibir basicamente dois riscos: inadimplência e fraude. Através de estratégias de prevenção de fraude (etapa 1) é possível criar uma espécie de lista negra que impede a concessão de linhas telefônicas pós pagas para determinados perfis considerados suspeitos. Aspectos como faixa etária, situação do CPF junto a listas de inadimplentes, local de residência, entre outros, compõe as variáveis que são analisadas para a venda de um ou mais linhas celulares.

Já no fluxo de venda (etapa 2), simples verificações podem confirmar a legitimidade de documentos cedidos, tais como:

a) Conferencia da similaridade de aparência entre a fotografia do documento de identificação com a de quem está portando, aspectos de nitidez pra checar se não há nenhuma colagem ou substituição da foto do documento;

b) Observar os dados constantes nos documentos que devem conter informações óbvias como data de emissão posterior a data de nascimento (em caso de RG) ou data de emissão anterior a data de vencimento (em caso de comprovante de residência);

c) Em caso de pessoa jurídica, avaliar se a compra condiz com o porte da empresa (relativo a capital social, número de funcionários, ramo de atividade, etc) e se no local de entrega de aparelhos e faturas realmente há atividade comercial (por exemplo loja ou escritório)

d) A assinatura feita no momento da contratação da linha, pelo titular que está adquirindo, deve ser semelhante à assinatura contida no documento de identidade. Importante verificar nesse momento se que está assinando está agindo com naturalidade ou se está titubeando para tentar reproduzir uma assinatura falsificada.

Após habilitado (etapa 3), o telefone móvel será monitorado para que em caso de alto tráfego, inadimplência ou perfil suspeito de utilização, passe por uma nova validação com o objetivo de detectar possíveis irregularidades e assim reduzir ao máximo a possibilidade de perda financeira.

A partir do momento em que apresenta qualquer indício suspeito de fraude, são feitas checagens cadastrais e de perfil de utilização, para confirmação de que o celular foi efetivamente comprado pelo titular dos documentos apresentados no ato da contratação do serviço e também conferir se essa linha não foi repassada para terceiros, cujo usuário não se responsabilizará pelo débito gerado.

6.4 DETECÇÃO DE FRAUDE

Um dos métodos mais utilizados (pela eficácia que apresenta) é a análise de documentos que contempla a técnica da documentoscopia. Consiste em identificar a autenticidade de documentos para validar se o mesmo possui autenticidade garantida, ou seja, é de fato o documento expedido pelo órgão emissor.

A Documentoscopia é a técnica que estuda, analisa e identifica os diversos tipos de falsificações e adulterações em documentos, moedas, selos, cartões de crédito, cheques, contratos, procurações, certidões de nascimento, óbito entre outros documentos. O objetivo dessa análise é confirmar se o documento apresentado no ato da habilitação da linha móvel é do portador que está se apresentando como o titular do documento cedido.

Os documentos mais utilizados em golpes de falsificação são documentos de identificação pessoal (RG, Carteira Nacional de Habilitação, Carteira de Registro em Órgão de Classe, etc) e documentos de comprovação de residência (conta de energia, de cartão de crédito, de telefone fixo, entre outros).

A fraude nesses documentos, geralmente é produzida através de manipulação digital que reproduz a partir de um documento verdadeiro, cópias falsificadas com dados cadastrais digitados pelo fraudador. Funciona como se fosse uma matriz (documento original), que reproduz várias cópias, alterando as informações, fotografias e assinaturas.

Normalmente, esses documentos são produzidos através de um software apropriado para esse tipo de adulteração, pois contém vários documentos padrões em que basta o usuário inserir seus dados pessoais e imprimir o comprovante, que se parece muito com o original, embora suas informações sejam irreais.

Esse tipo de detecção ocorre somente após a solicitação do serviço, pois o documento foi fornecido no momento da aquisição do serviço, logo é classificado como um meio corretivo de combate à fraude, pois em nenhum momento evitou a ação inicial do golpista.

Outro modo de detecção corretiva compreende o acompanhamento de tráfego suspeito ou também conhecido como tráfego nocivo, em que são analisadas as variações periódicas de tipos de chamadas, duração, destino,

entre outras informações através de sistemas específicos de monitoramento, os chamados FMS (*Fraud Management System*).

6.5 ENGENHARIA SOCIAL

Uma tendência cada vez mais popular nas técnicas para iniciar, estruturar ou executar fraudes, é o uso da chamada "Engenharia Social". Uma definição desse termo é a seguinte: Engenharia social é mecanismo que tem como objetivo obter informações sigilosas e importantes através da exploração da confiança das pessoas, principalmente através de enganação.

Para isso, o contraventor pode se passar por outra pessoa, assumir outra identidade, vasculhar lixo ou outras fontes de informações. Podem também fazer contato com parentes e amigos da vítima para ações de suborno.

Embora haja vários tipos de alertas pelo setor privado e também veiculação de comunicados orientando sobre esse tipo de ação, o golpista que age através da Engenharia Social tem como principal aliado o fato de haver pessoas ingênuas e que facilitam roubos e são lesados pelo simples descuido de liberar informações ou de aceitar algum tipo de ajuda que tem o objetivo específico de usurpar alguma coisa.

O método mais simples para descobrir informações confidenciais é semelhante ao que era chamado como o "golpe do baú", ou seja, um indivíduo com atuação persuasiva e envolvente, com habilidades na comunicação, reação rápida e pleno domínio de técnicas psicológicas. Nesse contexto, o sucesso do golpe está diretamente relacionado com a ingenuidade da vítima.

Existem dois tipos de ataques de engenharia social - os ataques diretos e indiretos:

- **Diretos:** são aqueles em que o golpista entra diretamente em contato com a vítima por e-mail, telefone ou pessoalmente. Os ataques diretos têm alvo fixo, ou seja, o contraventor conhece o perfil da vítima, optando por aquelas que apresentam características mais vulneráveis, como por exemplo, idosos ou pessoas com baixa ou nenhuma escolaridade.

Talvez esse seja o meio menos vantajoso por assim dizer, para o golpista, já que de alguma forma ele terá que se expor e isso pode facilitar a desarticulação de seu esquema ilícito e assim ser denunciado.

Esse modo de operação é comum e freqüente para detentos, pois praticamente não há risco uma vez que já estão presos e então não há nenhuma outra pena adicional ou prejuízo maior.

- **Indiretos:** são aqueles que não têm um alvo específico, ou seja, está em busca de uma vítima não estabelecida previamente e que por um ato de falta de atenção, despreparo ou então simples ignorância não se atenta para a possibilidade de ser vítima. Um exemplo para demonstrar é a inocência de determinados usuários de caixa automático de bancos. Esses são alvos fáceis, visto que há meliantes especialistas em se passar por um mero cliente do mesmo banco que felizmente está no local para fornecer auxílio numa transação desse tipo de auto-atendimento, sem que a vítima note que teve sua senha copiada e então é fácil movimentar indevidamente a conta bancária de um computador, por exemplo.

No ramo de telefonia móvel, a inocência das vítimas também é uma das principais causas desse tipo de problema.

Outro exemplo de fraude associada à Engenharia Social, são os golpes de desvio de chamadas em que o fraudador se passa por um funcionário da operadora de telefonia, liga para a vítima (a seleção do número da vítima é escolhida de forma aleatória) solicita à ela que digite uma combinação numérica em seu aparelho celular e a partir desse momento, as chamadas do cliente são transferidas para outro terminal de acordo com a combinação de dígitos que foi programado pelo dono do aparelho.

A vantagem desse tipo de golpe, é que a partir do momento em que o celular está com programação de desvio, pode receber chamadas à cobrar que são atendidas pelo terminal que participa da fraude, ou seja, o dono do celular que irá receber a fatura, com chamadas que não são de sua autoria.

Esse golpe é muito comum na região Sudeste, principalmente em São Paulo e no Rio de Janeiro, em que a fraude de Engenharia Social “alimenta” e está diretamente relacionada com a comunicação de quadrilhas e chefes de tráfico de drogas.

Nesse aspecto, há um contexto social para o assunto abordado. A grande variação de renda e as condições precárias de subsistência da classe pobre estimulam a iniciação muito prematura de fraudadores e golpistas em função do baixo risco de punição e altíssima margem de lucro. Obviamente essa é uma seara delicada e extensa para se abordar, mas é notório que esse fator importante em especial as Telecoms, que sofrem constantes ataques de fraude.

Diante dos fatos, Parodi comenta sobre Engenharia Social: "...Sabe-se que o ser humano tende a acreditar no que gosta ou gostaria, mas nem sempre o que gosta é o certo ou possível. Pense sempre se o que está sendo proposto tem sentido à luz da racionalidade, sem levar em consideração condições "milagrosas" eventualmente apresentadas. Lembre-se que ninguém dá nada de graça ou assume riscos inúteis (ou sem um adequado lucro ou garantia). Se estiver na dúvida, fique longe porque há uma chance grande de ser uma fraude!"

6.6 TIPOS DE FRAUDE EM TELEFONIA MÓVEL

Fraudes ocorrem pelo simples fato de haver falhas no processo, que permitem que haja condições de utilização indevida de algo.

Para o segmento em questão, a fragilidade de rede, de sistemas e de processos, possibilita a ação de contraventores para a prática de alguns desses tipos de fraude:

a) Subscrição: normalmente associado com técnicas de engenharia social que usa adulterações de documentos e de informações para a aquisição de um bem (por exemplo um aparelho celular de última geração) ou serviço (linha móvel);

b) Auto fraude: essa é uma espécie de aquisição com intenção premeditada de contestar a habilitação, ou seja, o titular compra uma linha celular apresentando seus próprios documentos e informações cadastrais, só que no ato da assinatura do contrato de prestação de serviço, adultera sua

própria assinatura, para que no futuro possa alegar que não tem conhecimento nem responsabilidade sobre aquele celular;

c) Clone: captura e cópia de códigos que originam chamadas telefônicas. A partir dessa cópia é possível originar chamadas como se fosse uma réplica do terminal clonado mesmo não tendo acesso físico ao aparelho que foi clonado;

d) Alteração de código IMEI: através desse tipo de fraude, é possível reutilizar um aparelho celular mesmo após ter sido bloqueado. Normalmente, quando ocorre a perda ou furto de aparelho, a operadora executa um bloqueio no aparelho celular, para evitar que seja utilizado indevidamente, entretanto com a alteração do código IMEI, é possível efetuar o desbloqueio do aparelho para futura reutilização;

e) Fraude de redirecionamento: Atualmente, os celulares (tanto o aparelho, quanto a linha telefônica) possuem um serviço chamado siga-me. O objetivo é redirecionar chamada de um terminal A para terminal B, bastante utilizado em caso de indisponibilidade do aparelho de A, ou algo do gênero. Esse tipo de fraude acontece normalmente quando o golpista liga para um celular, se passando por funcionário de operadora de Telecom e solicita uma programação com o argumento de que se trata de teste. Sem saber, o dono do celular está programando as chamadas para serem direcionadas para um número B que está com o comparsa do fraudador. Com isso, é possível que ambos fraudadores possam se comunicar a partir de chamadas à cobrar;

f) Golpe do Falso Sorteio: essa é uma prática essencialmente oriunda de engenharia social, ou seja, o fraudador se aproveita da ingenuidade de suas vítimas para ludibriá-los com argumento de que foi sorteado em uma promoção que não existe, mas que o prêmio só poderá ser entregue mediante à doação de créditos para celular pré pago. Normalmente o golpista é presidiário;

g) Fraude em Roaming Internacional: esse tipo de fraude consiste em exportar chips em branco para efetuar a habilitação da linha quando estiver no exterior. A característica principal é possuir conivência com o funcionário da Telecom vítima do golpe ou então acesso remoto aos sistemas da operadora para executar ilicitamente a ativação da linha. A partir do momento em que a linha é disponibilizada, inicia a utilização indevida e só finda quando a operadora detectar a fraude. Essa modalidade apresenta um risco ainda maior devido ao alto custo de chamadas em roaming internacional (originada fora da rede da operadora local).

Além das modalidades listadas acima, há um novo modelo de fraude que também pode ser considerada como técnica, tendo em vista que é sucedida em âmbito virtual, ou seja, com a criação da rede convergente (utilização de dados via celular, por exemplo), é possível realizar uma série de ações ilícitas, visto que está acessando a rede mundial de computadores – Internet – através de um aparelho celular. Com isso, é possível multiplicar spams e vírus, romper a segurança de sites, burlar e copiar informações sigilosas disponíveis na rede, entre outras ações.

6.7 MENSURAÇÃO DAS FRAUDES

Medir é preciso. A afirmativa vem seguida de certo grau de desconforto entre os executivos que atuam em Telecons, uma vez que são identificados e os dados quantitativos que envolvem perdas de fraude, entretanto são informações que são tratadas com o mais absoluto sigilo mediante ao mercado e principalmente aos concorrentes.

Medir a extensão do fenômeno das fraudes, nos vários setores econômicos, sempre foi um assunto de certo interesse e de grande dificuldade prática. O montante de perdas provenientes de fraudes contra empresas (de vários setores) no acumulado de janeiro a agosto de 2009 foi de R\$ 72 milhões, aproximadamente 41,2% menor do que os R\$ 122,53 milhões registrados no mesmo período do ano passado. “Esses números revelam que as empresas têm conseguido ser mais ágeis e eficientes na identificação de

inconsistências de dados e informações que representam riscos e podem resultar em perdas mercantis, tanto no momento da venda a prazo quanto na aceitação de novos clientes”, afirma Laércio de Oliveira, Presidente da unidade de negócios da Serasa.

No segmento analisado, há outro fator que dificulta o correto apontamento do montante financeiro envolvido com perdas, em função do equívoco que há entre perdas de fraude e perdas de inadimplência. A diferença básica da origem da perda é identificar se o titular ou proprietário poderá recusar sua responsabilidade na aquisição e/ou contratação do bem ou serviço que ocasionou no débito, haja vista que um fraudador sempre será inadimplente (é uma questão premeditada), porém um inadimplente nem sempre será um fraudador.

As perdas financeiras oriundas de fraudes e golpes, com cifras cada vez mais expressivas, é assunto tratado com o mais absoluto sigilo entre as concorrentes de um mesmo segmento, de modo que evitem a exposição de suas imagens perante a sociedade e principalmente para seus clientes, por isso preferem manter essas ocorrências camufladas para evitar qualquer tipo de escândalo envolvendo seu nome e marca, e na maioria das vezes optam por não exigir a punição dos infratores, em função do volume de ocorrências.

Outro fator que pode impactar na correta sinalização do percentual de cadastros irregulares são os casos que nem chegam a ser detectados e por isso não podem ser relevados nas estatísticas. Isso reduz ainda mais a exatidão do nível de fraudes tanto no que tange ao volume de ocorrências quanto aos valores.

A tabela abaixo demonstra o volume de fraudes no segmento móvel de telefonia, com dados referentes ao segundo semestre de 2009, das quatro maiores companhias que atuam no setor em nosso país:

Operadora	Volume de Fraude
A	494.454
B	235.391
C	61.205
D	47.312

Fonte: Site da ABR Telecom (consulta dez/2009)

Algumas organizações adotaram a criação de um departamento especializado na detecção e análise de cadastros suspeitos, são os chamados departamentos de anti-fraude, o qual se destina a criar processos de prevenção, detecção e monitoramento das perdas oriundas de fraude. Esse departamento geralmente está ligado à diretoria financeira ou comercial, de modo que interage com outras gerencias, como a de faturamento, segurança da informação, tecnologia da informação.

Os métodos mais utilizados para identificar o nível do problema é comparar o valor do prejuízo mensal ao montante do total faturado (em termos quantitativos) e confrontar qual é o volume de contratos fraudados com o volume de novos contratos no período em análise.

O patamar considerável aceitável entre os especialistas do ramo, para a perda financeira com fraude é de até 1% do total faturado no período, acima disso já é considerado sinal de alerta. Frequentemente o aumento desse percentual está diretamente ligado à ações mercadológicas que visam o aumento de contratação num determinado período, como por exemplo ações de alavancagem de vendas na época do Natal.

É possível citar as datas comemorativas consideradas ofensoras como dia das mães e dias dos namorados, que na área de telecomunicações, impulsionam as vendas em torno de 30% na média, com isso, aumenta o nível de incidência de fraudes.

6.8 RISCOS INTERNOS ÀS ORGANIZAÇÕES

Há inúmeros casos de empresas que detectaram irregularidades na rotina de seus funcionários, em áreas diversas e valores que variam de acordo com o intelecto do funcionário e a fragilidade dos controles internos.

Para Parodi (2008, p. 365), pode haver funcionários que se aproveitam de falhas para elaborar fraudes, estimulados por impulsos de dificuldades financeiras ou então aspectos emocionais, com interferências de um comportamento diferenciado, como por exemplo:

- Viver além dos próprios meios;
- Dívida pessoal elevada ou crédito restrito;

- Perdas financeiras;
- Jogo, drogas, bebidas ou relações instáveis;
- Pressão familiar por sucesso financeiro;
- Crise de meia-idade;
- Avidéz;
- Vingança contra a empresa ou contra superiores e outros funcionários;
- Desafio de se mostrar mais esperto do que o sistema;
- Insatisfação com o trabalho;
- Falta de reconhecimento profissional;

As organizações estão constantemente expostas e dentre os principais focos de atenção para mitigação dessas ocorrências estão a gestão efetiva dos recursos e resultados (isso vale para resultados operacionais, custo e orçamento), a presença constante de auditoria com esforços voltados para revisões do controle financeiro / contábil e dos processos de cada área, e por fim, uma ação simples, mas muito não menos importante que é a qualidade do processo de seleção dos funcionários, com padrões definidos e eficientes de avaliação e recrutamento.

O fato de existir um controle fiscalizador, seja ele qual for, é um ponto de segurança para reduzir o risco de fraude dentro da organização, independente de como ele é exercido.

Referente ao tema abordado, por exemplo, em se tratando de um alto volume de habilitações de linhas de celular pós pago, as operadoras devem manter rigorosos pontos de controle (com revisão periódica) para evitar que através de um funcionário mal intencionado haja desvios ou habilitações indevidas, sendo que ele possui conhecimento suficiente e acessos sistêmicos necessários para cometer infrações.

Em paralelo, se esse funcionário tem conhecimento dos controles internos que são mantidos pela Empresa, ele automaticamente é desmotivado à práticas ilegais, sabendo que ele pode ser descoberto à qualquer momento.

A participação de funcionários de empresas de telefonia vem sendo amplamente divulgada pela mídia que cada vez mais afetam o resultado de

seus empregadores, movidos principalmente pelo comissionamento na venda de uma linha com destino ilícito, ou seja, o funcionário facilita a venda (mesmo diante da desconfiança de se tratar de um fraudador), pois seu interesse é volume de vendas e não examinar a qualidade do comprador.

Mais um meio relevante de facilitação para ativação de linhas telefônicas é venda de senha de sistemas internos para acesso remoto via *web*, de modo que facilite a participação de *hakers* que são especializados em burlar sistemas de informação de fora da empresa com a finalidade de criar linhas telefônicas, alterar cadastro de clientes idôneos entre outras operações criminosas que dificultam a ação das autoridades fiscalizadoras (Polícia Federal) e principalmente da organização que está sendo vítima do ataque.

O uso dos sistemas de informação das organizações, suas permissões de acesso e perfis de usuários são fatores determinantes para resguardar a base de informações e impedir que um funcionário que atue como atendente em um call center, por exemplo, efetue um lançamento de venda de aparelho celular, obviamente se esse não for seu foco de atuação.

Há dois fatores que determinam se um fluxo ou processo, independente do segmento de mercado, apresenta risco ou é seguro:

1) Utilização falha ou indevida de usuários:

Esse assunto está relacionado com o fator quase que predominantemente vinculado com qualquer tipo de irregularidade desencadeada da fraude – o recurso humano.

Atualmente a terceirização de algumas atividades é um processo natural e rentável, entretanto a partir do momento que é delegado a um prestador de serviço uma etapa de determinado processo é inevitável a abertura do acesso aos sistemas internos e conseqüentemente várias pessoas poderão ter acesso a informações confidenciais, ativações de serviços, permissão de pagamentos ou descontos dentre outras funções.

De acordo com recente pesquisa divulgada pelo Sindicato dos Funcionários de Atendimento (Call Center), o nível de *turn over*² em empresas terceirizadas pode chegar até a 30% por mês. Essa alta rotatividade pode trazer riscos, como por exemplo a situação de um funcionário desligado, além

² Refere-se ao nível de rotatividade do quadro de funcionários.

de conhecer os acessos e os processos internos, em algumas situações conseguem acessar o sistema do antigo empregador, utilizando todo o perfil de acesso remoto para a obtenção de favorecimento próprio (desconto em faturas, alteração de dados cadastrais, habilitações indevidas), pelo simples fato de que ao ser demitido não efetuaram o cancelamento de seus logins de sistema.

2) Gestão de perfil de acessos:

A evolução da matriz de alçadas deve aumentar de modo escalonado, sendo que os níveis situados no primeiro patamar devem deter acesso para as atividades mais simples e nas necessidades de liberação de alguma funcionalidade que represente algum risco em caso de uso fraudulento, é aplicado ponto de controle (auditorias e conferências) periódico, para examinar amostras das ações executadas se houve algum tipo de irregularidade.

Em 2009, foi veiculado na imprensa, o caso da funcionária de uma empresa de telefonia na grande São Paulo que realizava ativação de linhas fixas de telefone para a utilização dentro dos presídios do Estado, mediante à pagamento em sua própria conta corrente por habilitação efetuada. Esse caso foi descoberto pela equipe de segurança de informação da empresa contratada, pois identificaram que para o nível hierárquico da funcionária envolvida, não estava na relação de acessos permitidos funcionalidades como ativação de linhas, nesse caso, uma falha no processo ocasionou a ação irregular.

6.9 IMPACTOS

Temerosas de se expor e prejudicar a sua imagem quando fraudadas, as empresas optam por manter sigilo absoluto sobre o ocorrido e a punição na grande maioria dos casos termina com a demissão de funcionários fraudadores (Tinello 2006).

Avaliar e mensurar os danos causados por fraude é uma questão abrangente. O mercado de telefonia móvel vem crescendo vertiginosamente e a concorrência impulsiona à qualidade na prestação de serviço para cima, ou

seja, nessa “selva” sobrevive a companhia que está mais reparada para atender as demandas, combater os riscos e que gerar maior rentabilidade.

Inicialmente é possível indicar o maior impacto presente nesse assunto: a perda financeira. As organizações estão vulneráveis à três tipos básicos de prejuízo financeiro:

1) Não irá receber a receita oriunda da prestação do serviço, já que o golpe prevê a intenção premeditada de não honrar o débito gerado;

2) Terá que arcar com despesa fiscal sobre aquela utilização indevida, já que está alocada no segmento de prestação de serviço e se houver faturamento, logo haverá incidência de imposto;

3) Há um custo embutido na tarifa de celular que corresponde à interconexão, ou seja, se um celular da operadora A origina uma chamada para outro celular da operadora B, ao completar a ligação, a operadora que emitiu a chamada terá que pagar uma tarifa para a operadora que recebeu, com isso, há esse valor adicional para contabilizar no ônus causado pela fraude.

A partir da identificação da perda financeira, fica visível o tamanho do problema e considera-se um fator mais propício de analisar, visto que há um dado real para contemplar e com isso é possível estabelecer metas, ações de redução de perda, porém o próximo impacto tem um destaque relevante, pois é imensurável.

Trata-se do impacto na imagem da companhia que sofre esse tipo de ataque, no qual torna vulnerável o relacionamento com seus clientes. Essa é uma das questões mais delicadas, já que não é possível medir qual é o tamanho do prejuízo causado, inclusive porque há um detalhe ofensor, é o conhecido “boca a boca” – se um cliente é vítima de fraude, conseqüentemente ele irá espalhar para seu círculo de familiares e amigos sobre tal fato e logo, todas essas pessoas certamente irão evitar qualquer relacionamento com aquele prestador de serviço, uma vez que já possui referências negativas.

Além de comprometer à imagem perante aos clientes, também é um impacto diante do mercado, pois um segmento tão concorrido é extremamente relevante esse tipo de problema, além de acionistas, fornecedores, funcionários, etc.

Por fim, será citado um dos prejuízos mais onerosos desse tipo de ocorrência, visto que há valores agregados que se somam às perdas indicadas anteriormente, que são as ações judiciais e multas aplicadas por órgão de defesa ao consumidor e de regulamentação, decorrentes de ação de fraudadores.

Esse é sem dúvida um dos problemas mais delicados do assunto abordado, visto que além de toda a despesa gerada pelo fraudador, o imposto que a Companhia terá que arcar, ainda há ônus com ações de danos morais e materiais que podem elevar o prejuízo à um patamar muito elevado de acordo com a alegação da vítima e a determinação do juiz.

Esses são alguns dos impactos previstos diante do cenário atual do ramo de telefonia móvel, porém no futuro, com o avanço tecnológico que se especula pelo mercado, há uma tendência de aparecimento de novos tipos de fraude, que vão requerer técnicas mais evoluídas de detecção. Segundo Edmo Lopes³, executivo da área, novas modalidades de fraude aparecerão, tais como fraudes com transações concluídas via celular para pagamentos com cartão de crédito, golpes via internet com dificuldade em rastrear a identificação do computador que originou e fraudes crescentes com vítimas oriundas de redes sociais.

6.10 FATORES DE MITIGAÇÃO

Atualmente há uma retaguarda avançada para o combate dessas ocorrências em diversos segmentos do mercado, como por exemplo, administradoras de cartão de crédito, área bancária, companhias de seguro e telefonia. São as áreas especializadas que atuam na mitigação e prevenção de fraude, que dispõe de softwares específicos para monitoramento e detecção de perfil suspeito de utilização.

Um dos principais objetivos dessas equipes é evitar que após de adquirido, o produto ou serviço represente perdas significativas, ou seja, atuam na identificação rápida para que uma aquisição fraudulenta incida no menor prejuízo possível.

³ Declaração dada em no Evento "*Revenue Assurance & Fraud Management*" que aconteceu em 09/2009 - Rio de Janeiro, Brasil.

No âmbito de telefonia móvel, essa é uma ação reativa, já que foi permitida a venda irregular para terceiros se passando pelo titular portador da documentação apresentada na aquisição do serviço. Entretanto para a adoção de uma medida preventiva mais eficiente, propõe-se através desse estudo, a análise de viabilidade para o desenvolvimento e implantação de um software específico que teria como objetivo principal cruzar informações de documentos com a leitura da impressão digital do suposto portados do documento para confrontar a veracidade da titularidade.

Trata-se de um software que teria a capacidade de leitura precisa da impressão digital do portador (com leitor de impressões digitais do tipo "finger") e através da digitalização do documento de identidade fornecida pela pessoa que deseja adquirir o serviço, possa codificar e dar a resposta se as impressões digitais são da mesma pessoa. Com isso, seria praticamente impossível utilizar a documentação de uma pessoa para a habilitação de linha celular sem sua ciência e obviamente, este não teria condições de alegar desconhecimento do débito gerado pela prestação de serviço, portanto se houver alguma perda, poderá ser convertida em inadimplência e não fraude. Importante frisar que não há no mercado essa solução com todas as características acima descritas, por isso, essa seria uma das propostas de fator de mitigação para que fosse analisada e implantada no segmento para ação de combate à fraude.

Atualmente, há no mercado disponível para medidas preventivas (em variados segmentos) algumas soluções para coibir ou eliminar o risco de fraude, sendo que alguns dos que estão citados no quadro abaixo, poderiam ser adaptados para a Telefonia móvel:

Tecnologia	Precisão	Falhas em Operação	Melhor Uso	Probabilidade de Falsificação
Veias da palma da mão	Ótima	Baixa	Massivo	Praticamente nula
Iris	Ótima	Baixa	Massivo	Praticamente nula
Impressão Digital	Boa	Média	Pessoal	Média
Geometria da Face	Boa	Baixa	Massivo	Média
Dinâmica da Assinatura	Boa	Média	Massivo/Pessoal	Média
Voz	Regular	Média	Massivo/Pessoal	Média

Fonte: Manual das Fraudes

7 CONCLUSÃO

A estrutura das organizações de telefonia móvel demanda e demandará cada vez mais controles rigorosos relativos à mitigação do risco operacional, em específico o risco de evasão de receitas provinda de fraudes.

No assunto abordado nessa monografia, destacaram-se as ocorrências de fraude no segmento de telefonia móvel no Brasil, a qual oferece maior probabilidade desse tipo de infração, visto que possui o maior volume de habilitações e em paralelo um mercado aquecido comercialmente e em constante evolução tecnológica.

O fato de haver um mercado extremamente aberto esse tipo de produto (refere-se ao serviço e aos aparelhos comercializados) que está fundamentado em uma concorrência consideravelmente equilibrada em determinadas localidades e na regulamentação dos órgãos responsáveis, possibilita a atuação de contraventores com objetivo de obter benefícios próprios ou à terceiros, com intenção premeditada de não efetuar os pagamentos correspondentes por determinado serviço.

A falta de dados estatísticos centralizada prejudica a atuação mais efetiva, pois, conseguindo mensurar a extensão do fenômeno, pode-se calibrar as ações de combate e prevenção e, gradativamente, verificar sua eficácia. Além disso, medir de modo assertivo o problema é um fator determinante para chamar a atenção de todos os envolvidos (sociedade, autoridades competentes, mercado, acionistas) para então ter uma noção quantitativa.

A condição de se obterem dados razoavelmente indicativos na mensuração de fraudes, independente do segmento é através de pesquisas e ações conjuntas da categoria, em que os operadores de uma determinada categoria forneçam estatísticas que podem ser comparados e analisados com referências de mercado e com médias de outros setores ou de outros países, para efetuar estimativas e/ou ajustar eventuais distorções.

De acordo com as observações efetuadas, o controle contínuo é fundamental para gerir o risco de perdas de fraude no segmento de telefonia móvel com processo de monitoramento, prevenção e detecção, para assegurar

a manutenção da rentabilidade e saúde financeira das organizações que participam desse nicho.

No que tange a poder público, uma das opções para mitigar esse tipo de risco, seria a implantação de um sistema nacional de identificação, através de leitura digital do titular do documento, que seja possível confrontar com as bases da Secretaria de Segurança Pública de cada estado, para confirmar a autenticidade do portador e de seus documentos. Esse certamente seria um meio de coibir uma série de ações criminosas que tem por objetivo principal mascarar a real identidade do usuário de documentos adulterados.

Para o setor privado, especialmente as operadoras que compõe esse segmento, a recomendação seria a expansão dos departamentos de anti fraude, que além da função de prevenir e detectar, também somaria a função de estudar o fenômeno fraude com maior riqueza em detalhes, de modo que abranja os dados estatísticos referentes à fraude no mercado como um todo, para a implantação de regras mais assertivas para a mitigação desse tipo de perda que vêm onerando consideravelmente a receita das companhias.

Outro fator de extrema importância seria a implantação de processos de controle de qualidade na etapa de venda de linhas telefônicas. É uma equação lógica que motiva a provável facilitação por parte de revendedores: quanto mais se vende, mais se ganha, logo a implantação de controles de qualidade seria de suma importância para evitar essas ocorrências.

Referente aos cidadãos que involuntariamente participam das fraudes através do uso não autorizado de seus dados cadastrais, a orientação é que adote medidas básicas de segurança, se resguardando de possíveis golpes que normalmente são dados com o objetivo de extorquir dados cadastrais para posterior uso para fins ilícitos. Outra forma de prevenir esse tipo de contravenção é o registro de boletim de ocorrência nas situações de perda, furto ou roubo de documentos pessoais. Obviamente que essa ação não irá impedir o uso indevido de documentos alheios, entretanto poderá auxiliar na comprovação de que o verdadeiro titular foi vítima de fraude.

Por fim, com os apontamentos contidos nesse estudo, a expectativa é ter elucidado a assunto de modo prático, a fim de prover meios de identificação e redução (se não for possível eliminar definitivamente), com a tentativa de alertar os interessados no assunto sobre essas ocorrências, o prejuízo que

pode ser envolvido nesse ato e como articular meios de combater fraudes na telefonia móvel.

8. REFERÊNCIAS BIBLIOGRÁFICAS

Ambito Jurídico. Disponível em: <http://www.ambitojuridico.com.br/site/index>, Acesso em 17 de fevereiro de 2009.

BANDEIRA, José R. Rocha. **Documentoscopia forense a arte de desvendar fraudes**. Âmbito Jurídico. Rio Grande do Sul, 2006

Documentoscopia. Disponível em:

<http://www.cinelli.com.br/nono-comite.htm>. Acesso em 17 de fevereiro de 2009

MATTAR, Fauze Najib. **Pesquisa de Marketing**. Vol. 1. 2^a. Ed. São Paulo: Atlas, 1994.

PEREIRA, Caio Mario da Silva. **Instituições de Direito Civil**. Editora Forense. Rio de Janeiro. 1999

PARODI, Lorenzo. **Manual das Fraudes** 2^a. Ed. Editora Brasport. Rio de Janeiro, 208.

SÁ, Antonio Lopes. **Fraudes Contábeis**. Editora Tecnoprint. Rio de Janeiro, 1982.

TINELLO, Maurício Ricardo. **A arte da fraude. Quando nada é o que parece**. Editora Sicurezza, São Paulo, 2006.