UNIVERSIDADE FEDERAL DO PARANÁ

ANNE DINAURA FRIGO

INSTITUIÇÕES BANCÁRIAS: AS FRAUDES VIA INTERNET BANKING, COM CARTÕES E SUAS MEDIDAS PREVENTIVAS

CURITIBA
2013

ANNE DINAURA FRIGO

INSTITUIÇÕES BANCÁRIAS: AS FRAUDES VIA INTERNET BANKING E COM CARTÕES E SUAS MEDIDAS PREVENTIVAS

Monografia apresentada ao Departamento de Contabilidade, Setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná, como requisito parcial para a obtenção do título de Especialista em Controladoria.

Orientador: Prof. Dr. Ademir Clemente

CURITIBA
2013

TRABABALHO DE CONCLUSÃO DE CURSO

PARECER FINAL

NOME DO (A) ALUNO (A): ANNE DINAURA FRIGO

TÍTULO DO TRABALHO: INSTITUIÇÕES BANCÁRIAS: FRAUDES VIA INTERNET BANKING, COM CARTÕES E SUAS MEDIDAS PREVENTIVAS.

NOME DO PROFESSOR ORIENTADOR: ADEMIR CLEMENTE

PARECER DO PROFESSOR ORIENTADOR:

O trabalho versa sobre tema de interesse à Controladoria. Está bem organizado. A redação poderia ser melhorada —

NOTA: 80 (OITENTA) ASSINATURA: _____

NOME DO PROFESSOR DESIGNADO: JOCKSON CIRO SANDRINI

NOTA: 70 (SETENTA) ASSINATURA: _____

CONCEITO FINAL: _____ ( )

COORDENADOR DO CURSO: PROFESSOR ADEMIR CLEMENTE

ASSINATURA: _____ DATA: 12 / 06 / 2013

AGRADECIMENTOS

Agradeço a Deus, pois sem ele não teria seguido o bom caminho.

Agradeço ao professor e orientador Dr. Ademir Clemente pela compreensão e pelo apoio que me concedeu ao longo da pós-graduação, principalmente na conclusão da mesma.

Agradeço a minha família, que sempre me apoiou de todas as maneiras em minhas decisões.

Agradeço, em especial, a minha amiga e ex-colega de graduação Michelli Gonçalves Stumm pelas conversas e ajuda na organização dos temas e ideias aqui expostos, pois foram fundamentais no início do trabalho.

RESUMO

Discute-se neste trabalho as fraudes bancárias sofridas por clientes de bancos comerciais, tais como clonagem de cartão, golpe da troca de cartão, cartão retido no terminal e fraudes originadas pela utilização do ambiente *internet banking*. Correlaciona-se as fraudes com a teoria da assimetria de informação e do risco operacional, risco este do qual as instituições bancárias estão expostas e no qual as fraudes estão inseridas. Apresenta-se como ocorrem as fraudes, o "*modus operandi*" de cada uma delas, os tipos de invasão de computadores por vírus decorrentes do acesso a páginas falsas ou pela execução de algum arquivo malicioso advindo de *e-mails*. Por último são destacados quais são os métodos preventivos utilizados pelas instituições financeiras para diminuir as ocorrências de fraudes e golpes aplicados em clientes usuários do sistema bancário.

Palavras-chave**:** Bancos Comerciais. Usuários. Fraudes. Golpes. Cartões. Internet. Medidas Preventivas.

SUMÁRIO

1 INTRODUÇÃO

As últimas décadas trouxeram mudanças importantes para o mundo. Dentre elas destacam-se, a globalização da economia, a modernização tecnológica e a rápida proliferação e disseminação da internet. Vemos que a humanidade vive um período de transição de uma sociedade industrial para uma sociedade de informação.

O setor bancário, assim como todos os outros setores da economia, também modernizou seus produtos e serviços oferecendo aos seus clientes muitos facilitadores para a realização das transações bancárias. São os chamados, novos canais de atendimento: internet, telefones, cartões, terminais de autoatendimento etc.

Os novos canais possibilitam, por exemplo, o pagamento de contas e a realização de compras sem que o indivíduo precise sair de sua casa, utilizando apenas seu computador pessoal conectado à internet. Os cartões trouxeram maior segurança e comodidade para o indivíduo a partir do momento em que este não precisou mais circular com grandes valores em espécie.

Nesse panorama encontramos também a modernização das práticas ilícitas e golpes que utilizam dos meios eletrônicos e acabam gerando perdas para as instituições bancárias e para o público em geral. São as conhecidas fraudes bancárias ou fraudes tecnológicas, entendendo-se aqui as fraudes aplicadas em clientes bancários e não na instituição bancária diretamente ou dela proveniente para com o setor financeiro.

De acordo com Lau (2006, p.5) a definição de fraude está relacionada à distorção intencional da verdade ou de um fato, que busca em geral a obtenção de lucro ilícito.

Diante do contexto apresentado, a questão orientativa da presente investigação é a seguinte: Quais os métodos preventivos utilizados pelas instituições financeiras para diminuir as ocorrências de fraudes e golpes aplicados em clientes bancários?

Este trabalho tratará somente das modalidades de fraudes envolvendo cartões e fraudes pela internet, relatando como ocorrem e apresentando quais os

métodos preventivos utilizados pelos bancos comerciais para tentar diminuir as ocorrências citadas.

A proliferação das informações apresentadas neste trabalho contribui para promover a prevenção das ocorrências das fraudes e golpes, na medida em que o melhor entendimento do assunto pelo público em geral fomenta o combate, e principalmente, a prevenção dessas práticas.

Esta monografia está dividida em três capítulos. O primeiro apresenta o referencial teórico concernente ao tema exposto: relação das fraudes com a assimetria de informações e o risco bancário no qual as fraudes estão inseridas. O segundo discute sobre a modernização bancária e a consequente modernização dos serviços disponibilizados pelos diversos canais de atendimento seguido da apresentação das fraudes tratadas nesta monografia. O terceiro apresenta quais são as medidas preventivas utilizadas pelas instituições bancárias para diminuir as fraudes e golpes aplicados nos clientes bancários.

2 ASSIMETRIA DA INFORMAÇÃO E RISCO BANCÁRIO

O objetivo deste capítulo é dar embasamento teórico para o tema fraudes. Esta seção está composta por dois itens. O primeiro trata de como as fraudes estão relacionadas com a assimetria da informação. O segundo trata dos tipos de riscos que as instituições financeiras estão expostas, discutindo primordialmente o risco operacional, no qual as fraudes estão inseridas.

2.1 A Assimetria de Informações e as Fraudes

De acordo com Carmo (2005), a teoria econômica trabalha com modelos simplificadores da realidade que adotam premissas de difícil verificação no mundo real e uma dessas premissas supõe que todos os agentes econômicos têm pleno conhecimento de todas as variáveis, ou seja, conhecem as suas preferências e a dos demais agentes econômicos, presumindo assim, a existência de informações perfeitas.

Carmo (2005) destaca, no entanto, que a realidade mostra que os agentes econômicos na maioria das vezes conhecem apenas as principais características quando da tomada de decisões, além de desconhecerem as preferências dos demais agentes. Na verdade, na maioria das vezes o que encontramos no mundo real são as informações incompletas ou assimétricas, ou seja, o que existe é a assimetria de informações.

Santos (2010) destaca que em economia, a informação assimétrica é um fenômeno que ocorre quando dois ou mais agentes econômicos estabelecem entre si uma relação ou transação econômica em que uma das partes envolvidas detém informações qualitativas ou quantitativas superiores a outra parte.

Em Carvalho (2002) encontramos a informação de que o conceito de assimetria de informações surgiu em um estudo do mercado de automóveis usados, de autoria de George A. Akerlof, publicado em 1970, intitulado “*The market for lemons: quality uncertainty and the market mechanism*”. Carvalho (2002) comenta

que o trabalho mostrava que o vendedor conhece as condições de um automóvel usado melhor que os potenciais compradores, podendo oferecer um carro com boa apresentação, mas em mau estado de conservação, cobrando o preço vigente no mercado para um automóvel em bom estado. Portanto, a existência de assimetria de informações permite que, em uma determinada transação, a parte que detém maior grau de informação consiga benefícios maiores que a outra parte.

Para Carmo (2005) existem duas formas de manifestação de assimetria de informações: a **seleção adversa** e o **risco moral** ou *moral hazard,* sendo a seleção adversa entendida como assimetria de informações *ex-ante*, pois consiste na diferença de conhecimento entre compradores e vendedores antes que as transações se concretizem e risco moral entendido como a assimetria de informações *ex-post*, pois se manifesta após a ocorrência de alguma transação ou ato, quando a ação ou omissão de uma das partes faz com que a outra tenha de arcar com custos desnecessários e/ou imprevistos quando da realização do fato.

O economista Levitt (2005) explica que uma das chaves para entender como o mundo funciona nos dias de hoje é observando o poder da informação. Para o autor, dependendo de quem a controla, a informação se torna uma fonte de poder e muitas vezes apenas a suposição de tê-la, mesmo sendo inverídica, dá a aparência de competência:

> A informação é um facho de luz, uma vara, um galho, um freio, dependendo de quem a controla e da maneira como o faz. A informação possui tamanho poder que a suposição de tê-la, ainda que inverídica, já cria a impressão de competência. (Levitt, 2005 p. 65).

Para Levitt (2005) a assimetria de informações foi atingida pela internet, já que a informação se tornou a moeda da internet. Afinal, a internet transfere a informação das mãos de quem a detém para as mãos de quem não a possui. A rede conseguiu diminuir de forma drástica o abismo entre os especialistas e o público em geral. Porém, como destacado na obra, a internet por mais poderosa que seja não conseguiu acabar de vez com a assimetria de informações em todos os aspectos.

Segundo Parodi (2005), a assimetria das informações é uma situação na qual uma parte, normalmente um especialista, detém informações relevantes que a outra parte não tem, usando o especialista as informações para obter vantagens. Para o autor em alguns casos a assimetria de informações é o resultado da simples

sonegação de informações relevantes por parte do detentor da informação. O autor acredita que também pode ser usada para gerar pressão na parte menos informada, normalmente através do uso de várias formas de medo. Para Parodi (2005) na base de boa parte das fraudes existe uma situação de assimetria de informações, onde o fraudador detém informações relevantes que a vítima não tem e se aproveita desta posição de superioridade para aplicar o golpe.

Parodi (2005) afirma que como acontece na maioria dos crimes, as fraudes podem ser explicadas pela coexistência de três fatores primários:

> - **A existência de golpistas motivados**, devido à carência de alternativas para determinadas classes sociais, ineficiência de leis, incerteza de pena, incerteza jurídica, sistema financeiro evoluído, pouca fiscalização, etc.;
> - **A disponibilidade de vítimas adequadas e vulneráveis**, devido à pouca informação e divulgação preventiva, necessária em muitos setores, ignorância e ingenuidade difusas, ganância com valor cultural difuso;
> - **A ausência de "guardas" ou controladores eficazes**, devido à percepção do problema como não prioritário, despreparo e pouco treinamento específico das autoridades de polícia, escassa coordenação em nível nacional, falta de leis específicas e pouca clareza em algumas leis existentes e falta de organismos dedicados à luta contra esses fenômenos. (Parodi, 2005, p.1)

O autor mencionado acima destaca que por incrível que possa parecer o método mais simples, mais usado e, infelizmente, mais eficiente para descobrir informações confidenciais é perguntando.

Para realizar qualquer tipo de fraude, segundo Parodi (2005), os golpistas se aproveitam de alavancas técnicas e psicológicas e de algumas "ferramentas" operacionais específicas, tais como: engenharia social, falsificação de documentos em geral, roubo ou criação de "identidades", "*marketing*" ativo, simulação de situações e fatos, representação "teatral" de apoio, técnicas neurolinguísticas e de persuasão, técnicas de sedução, disfarce, mentira e sonegação de informações, ameaças e medo e uso extensivo da internet para criar "referências".

> A Engenharia Social consiste em um "conjunto de métodos e técnicas que têm como objetivo obter informações sigilosas e importantes através da exploração da confiança das pessoas, de técnicas investigativas, de técnicas psicológicas, de enganação etc.". Existem dois tipos de ataques de engenharia social: 1) Diretos, no qual o atacante entra diretamente em contato com a vítima por e-mail, telefone, ou pessoalmente, ouse já, têm alvo fixo; e 2) Indiretos,

> que não têm alvo fixo ou vítima específica ou definida. (Parodi, 2005, p.5).

Parodi (2005) alerta que estas ferramentas constituem um conjunto poderoso, sobretudo se utilizado em sincronia com alavancas técnicas e psicológicas. Parodi (2005) afirma que é comum os golpistas serem indivíduos com capacidades de sedução e persuasão desenvolvidas, com um bom nível de conhecimentos e uma habilidade na representação teatral. Para que obtenha êxito, o "engenheiro social" pode se passar por outra pessoa, assumir personalidade, vasculhar lixo ou outras fontes de informação, fazer contato com parentes e amigos das vítimas etc.

Assim, para o autor acima mencionado a posse de informações, sem que a outra parte a tenha, está intimamente ligada às ocorrências de fraudes nos dias atuais, pois o especialista ou detentor da informação/conhecimento poderá usá-la em favor próprio e em detrimento da outra parte, subtraindo desta algum tipo de vantagem, principalmente financeira.

2.2 Riscos das Instituições Bancárias

As instituições bancárias estão sujeitas aos mais diversos riscos inerentes à suas atividades. Para Lau (2006) o capital alocado pelas Instituições Financeiras deve cobrir os seguintes riscos:

> - **Risco operacional**: É definido como uma estimativa de perdas resultantes de processos internos pessoais, sistemas inadequados e eventos externos;
> - **Risco de Imagem**: São os riscos referentes à reputação da instituição em situações onde a opinião pública negativa resulta na perda de fundos e clientes. Este processo envolve a exposição do banco junto aos seus clientes e parceiros comerciais;
> - **Risco Legal**: Este item busca minimizar ou eliminar questões de violações e não conformidades das partes envolvidas em uma transação bancária, perante a lei, órgãos regulatórios e práticas adotadas no mercado, e;
> - **Outros riscos**: Há outros riscos relativos às instituições financeiras como risco de crédito, risco de liquidez, risco de mercado entre outros, que influenciam a operação e continuidade de negócio

> do banco perante o sistema financeiro e a sociedade. (Lau, 2006, p.33).

As fraudes em clientes de instituições bancárias estão relacionadas ao risco operacional. As fraudes são um risco previamente assumido pelas instituições bancárias já que resultam de perdas causadas por agentes externos. Para Júnior (2004), o risco operacional pode ser dividido em três grandes áreas:

> - **Risco organizacional**: relacionado com uma organização ineficiente, administração inconsistente e sem objetivos de longo prazo bem definidos, fluxo de informações internas e externas deficientes, responsabilidades mal definidas, fraudes, acesso às informações internas por parte de concorrentes, etc.;
> - **Risco de operações**: relacionada com problemas como overloads (tradução: sobrecargas) de sistemas (telefonia, elétrico, computacional, etc.), processamento e armazenamento de dados passíveis de fraudes e erros, confirmações incorretas ou sem verificação criteriosa, etc.;
> - **Risco de pessoal**: relativo aos problemas com empregados não qualificados e/ou pouco motivados, personalidade fraca, falsa ambição etc. (Júnior, 2004, p.4).

De acordo com LAU (2006) o Comitê da Basiléia divide os riscos operacionais em duas categorias, Risco de segurança e Projeto, criação e manutenção de sistemas.

Os riscos de segurança estão relacionados ao controle de acesso aos sistemas, informações disseminadas pela instituição financeira e parceiros comerciais e adoção de processos contra falsificações. Os riscos relativos a projetos, criação e manutenção dizem respeito à tecnologia empregada para a criação e manutenção dos serviços prestados através de sistemas tecnológicos.

Pôde-se observar neste capítulo que as fraudes e golpes aplicados aos clientes das instituições bancárias relacionam-se com a teoria da assimetria de informação na medida em que as fraudes ocorrem sempre que um dos agentes (o fraudador) possui maiores informações e conhecimento que o agente da outra ponta (o usuário bancário ou público em geral).

Verificou-se também que as instituições bancárias estão expostas aos mais diversos tipos de riscos e que as fraudes e golpes fazem parte do risco operacional a que os bancos estão sujeitos. Nesse sentido, é importante destacar que há grande

interesse por parte do setor financeiro e das instituições que o compõem em minimizar todos os tipos de riscos, inclusive os operacionais.

3 COMO OCORREM AS FRAUDES SOFRIDAS POR CLIENTES BANCÁRIOS

Esta seção está composta por duas partes. A primeira destaca a modernização ocorrida no setor bancário nos últimos anos. A segunda trata das fraudes sofridas por clientes de instituições financeiras que serão abordados neste trabalho por meio de uma subdivisão em duas categorias: 1) fraudes com a utilização física de cartões e 2) fraudes pela internet.

3.1 A Modernização Bancária e os Canais de Atendimento

As inovações tecnológicas surgidas nas últimas décadas não estão restritas somente à área de informática e das telecomunicações, mas sim na sociedade como um todo. As pessoas aumentaram sua expectativa etária e estão cada vez mais buscando uma melhor qualidade de vida. O mundo passou de uma sociedade industrial para uma sociedade informacional.

A disseminação da internet e a proliferação dos computadores pessoais revolucionaram o cotidiano das pessoas. A comodidade, facilidade e conveniência de se obter produtos, realizar transações bancárias, conversar com pessoas sem sair de casa trouxe e ainda trás cada vez mais adeptos ao mundo cibernético globalizado da internet.

A globalização trouxe para as empresas uma pressão para que oferecessem diferencial no mercado. No setor bancário não foi diferente, e ocorreu através da automação crescente e contínua dos processos, com a implementação de novos sistemas e a integração dos clientes aos novos serviços oferecidos.

Nos últimos anos, no Brasil, houve um estreitamento do mercado bancário com privatizações e aquisições de bancos nacionais por bancos estrangeiros. A necessidade de se manter competitivo, a crescente demanda por serviços facilitadores, mais eficazes e a custos menores conduziu os bancos naturalmente à automação bancária.

Os bancos que atuam no país hoje disponibilizam, primordialmente, quatro canais básicos de atendimento ao cliente: 1) através de suas agências bancárias, 2) pelos terminais de autoatendimento, 3) pela internet e 4) pelos telefones.

O conceito de autoatendimento (quando o próprio cliente realiza faz o seu atendimento nos canais disponíveis) cresceu muito no setor bancário. Para o setor financeiro a mão-de-obra é gratuita, já que o atendimento é realizado pelo próprio cliente e substitui o funcionário tradicional no atendimento. A economia de custos com novos canais de atendimento é significativa na estrutura financeira dos bancos. Por esse motivo os bancos lançam frequentemente várias campanhas de *marketing* e publicidade para incentivar os mais conservadores a mudarem seus hábitos nas transações bancárias e utilizarem os novos canais de atendimento, principalmente a internet.

Segundo Lau (2006) o maior motivador para a implementação do serviço através da internet é o custo para a realização de cada transação bancária. A tabela abaixo retirada do trabalho de Lau (2006) mostra o custo das transações bancárias nos diversos canais de atendimento:

Canal de Distribuição	Custo por transação (em US$)
Agências	1,07
Telefone	0,54
Autoatendimento	0,27
Home Banking	0,02
Internet Banking	0,01

Fonte: LAU 2010

A internet que se mostra o canal com o menor custo por transação bancária revolucionou os serviços bancários. A área bancária brasileira, segundo Lira (2007) está muito bem posicionada no mercado mundial. Segundo a autora o setor é o que melhor explora os recursos de internet, com uma das melhores atuações no atendimento on-line. Para ela pode-se notar o potencial brasileiro quando comparado com os dados dos Estados Unidos, pois o número de instituições bancárias nos EUA é 43 vezes maior com adesão de apenas 11,3%, enquanto que no Brasil 50% dos 201 bancos em atividade oferecem serviços pela internet.

3.2 As Fraudes Sofridas por Clientes das Instituições Bancárias com a Utilização de Cartões e pela Internet

A evolução histórica da eletrônica e da informática trouxe consigo o aumento da sofisticação dos golpes e fraudes, os quais historicamente crescem proporcionalmente aos recursos modernos disponíveis. Nos dias atuais os fraudadores/golpistas são freqüentemente bem informados, flexíveis e adaptáveis a novas situações, mostrando que as fraudes, assim como a maioria dos fenômenos econômicos, também se globalizaram.

O art. 171 do Código Penal conceitua fraude ou estelionato como a obtenção, para si ou para outrem, de vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

As fraudes cometidas contra usuários bancários podem ocorrer de várias maneiras: desde uma compra com cartão de crédito pela internet, transação por telefone ou até mesmo pelo simples fato de o cliente entregar seu cartão nas mãos de um vendedor para que este o leve a algum lugar fora do campo de visão do cliente para que seja clonado.

Este trabalho tratará somente das modalidades de fraudes envolvendo cartões e fraudes pela internet.

3.2.1 As Fraudes Bancárias por meio de Cartões

As fraudes que envolvem cartões podem ser divididas em duas categorias: transações com a utilização física do cartão, tais como clonagem de cartão, retenção de cartão em terminal de autoatendimento e troca de cartão; e transações realizadas com cartão de crédito pela internet, utilizando-se o número do cartão e o código de verificação. Esta última será tratada na próxima seção que envolve operações pela internet, pois a obtenção da informação normalmente ocorre por meio eletrônico.

3.2.1.1 Clonagem de Cartão

A clonagem de cartão ocorre por meio da utilização de equipamento espúrio, conhecido como “chupa cabra”, no qual são clonados os dados dos cartões e copiadas as informações contidas na tarja magnética. A clonagem é feita ao passar o cartão em uma máquina como se fosse uma máquina eletrônica de autenticação de pagamento.

Os equipamentos espúrios são, segundo Parodi (2005), encontrados frequentemente em postos de gasolina e outros estabelecimentos de grande rotação. Para Parodi (2005) a clonagem pode acontecer com o consentimento, participação ou auxílio de algum funcionário do estabelecimento comercial que passa o cartão para a clonagem longe da visão do dono do cartão. Em outras, pode acontecer de os donos ou funcionários dos estabelecimentos serem enganados por falsos técnicos de manutenção dos aparelhos utilizados para compras com cartão.

Em ambos os casos os aparelhos são adulterados para estocar os dados das tarjas magnéticas dos cartões, além de executar o processo formal de autenticação da compra.

O desenvolvimento dos cartões de crédito com CHIP[1] pode ser considerado uma mudança fundamental na indústria mundial dos sistemas de pagamentos.

Até pouco tempo atrás o principal sistema de armazenamento de dados de cartões de crédito e débito era a banda ou tarja magnética[2], um sistema, segundo Parodi (2005), desenvolvido há aproximadamente 30 anos atrás e utilizado por todos os circuitos. Para o autor esta tecnologia não é mais adequada às necessidades de segurança e favorecia o fenômeno das fraudes.

De acordo com o site Empresas e Finanças, consultado em 16/03/2013 as compras a utilização de cartões funcionam por terminais de captura de dados eletrônicos (EDC) no qual se passam os cartões. Depois que se passa o cartão pelo

[1] É um dispositivo microeletrônico que consiste de muitos transístores e outros componentes interligados capazes de desempenhar muitas funções. Suas dimensões são extremamente reduzidas, os componentes são formados em pastilhas de material semicondutor. Informação obtida no site <http://www.dicionarioinformal.com.br/chip/> em 15/01/2013, ou “*smart cards*” - tradução: cartões inteligentes.

[2] É feita de um filme plástico frágil com base de partículas magnetizadas à base de ferro. Informação obtida no site < http://empresasefinancas.hsw.uol.com.br/cartoes-de-credito-nos-eua1.htm> em 15/01/2013.

leitor, o terminal do *software* EDC do ponto de venda (POS) disca um número previamente armazenado com a utilização de um modem para se comunicar com um *acquirer*, que é, segundo o mesmo site, uma organização que coleta solicitações de autenticações de cartões dos estabelecimentos e as fornece como uma garantia de pagamento.

Segundo o site Empresas e Finanças, consultado em 16/03/2013, quando o *acquirer* recebe um pedido de autenticação ele verifica a validade da transação e o registro da traja magnética quanto ao ID do estabelecimento, a validade do número do cartão, a data de vencimento, o limite do cartão, se estiver sendo utilizado na função crédito e a utilização do cartão. O portador do cartão insere um número de identificação pessoal (PIN) usando o teclado do aparelho de compra e a compra é autorizada.

Ainda segundo o site acima mencionado, diferentemente, os cartões que possuem tecnologia com chip têm capacidade de armazenar dados de forma segura (criptografados), com uma maior capacidade de memória e, graças à presença de um microprocessador interno, podem ser utilizados por múltiplas funções, sendo que no mesmo cartão podem ser armazenados dados de vários serviços diferentes. Além disso, os cartões com chip não podem ser clonados, pelo menos por meio simples.

> Entre os cartões com chip se destaca o padrão EMV, criado a partir de 1993 pela colaboração dos principais sistemas de pagamentos mundiais (EUROPAY, MASTERCARD e VISA). O padrão EMV define uma série de regras a padrões no que diz respeito às modalidades de operação dos cartões com chip, às suas características físicas e elétricas, à estrutura dos cartões sob o ponto de vista da segurança, à interoperabilidade dos cartões nos terminais em nível global etc.(Parodi, 2008, p.243)

Segundo Parodi (2008), o padrão EMV define os requisitos mínimos de segurança, mas deixa os circuitos livres para estabelecer parâmetros adicionais de segurança. O autor destaca que isso levou ao desenvolvimento de diferentes sistemas: a VISA desenvolveu o VSDC (VISA *Smart Debit Card*), a MASTERCARD o M/CHIP e que todos esses sistemas são compatíveis com o padrão EMV, mas têm parâmetros adicionais de gestão de risco nas transações.

Parodi (2008) informa que o padrão EMV define quatro elementos básicos de segurança nas aplicações financeiras dos cartões:

> - Autenticação do cartão *offline*, ou seja, o terminal deve identificar o cartão como genuíno sem ter que se conectar ao sistema;
> - Parâmetros de gestão de risco. O cartão grava todas as transações e emite um alarme caso se verifiquem determinadas condições;
> - PIN *offline*. Os cartões com chip podem armazenar dados de forma segura e sigilosa, permitindo que a verificação PIN (número de identificação pessoal ou senha do cartão) possa ser feita internamente sem necessidade de conexão ao sistema;
> - Autenticação *online*. Quando necessário ou de forma casual, pode ser feita uma verificação *online* do cartão através de conexão junto ao sistema. (Parodi, 2008, p.243 e 244)

Para Parodi (2008) os cartões com chip, diferentemente dos com banda magnética (no qual é usado para autenticação, o sistema CVV, que só pode ser verificado *online*), utilizam diferentes técnicas que permitem que a autenticação seja tanto online quanto offline. O autor destaca alguns deles:

> - SDA (*Static Data Authentication*). É a tecnologia mais simples e menos cara. Neste processo o cartão é identificado e autenticado pelo terminal, sempre através do uso dos mesmos dados (assinatura digital) contidos no *chip*;
> - DDA (*Dynamic Data Authentication*). Neste caso o sistema cria uma assinatura digital diferente para cada operação *offline*. Esta tecnologia é mais segura, porém tem um custo 25% maior que a DAS;
> - CDA (*Combined Data Authentication*). Nela o cartão gera um "*Aplication Criptogram*" e uma assinatura digital. O terminal verificando a assinatura digital tem condição de determinar se o *Aplication Criptogram* foi gerado por um cartão genuíno. (Parodi, 2008, p.244)

Ainda segundo Parodi (2008), os objetivos que as grandes redes de cartões pretendem alcançar com a introdução dos cartões com chip, além da redução das fraudes, das falsificações e clonagens de cartões são os seguintes:

> - Possibilidade de gerir um maior número de transações. Os sistemas de pagamentos atuais precisam de uma conexão *online* (via telefone) para autenticação, o que resulta em uma necessidade maior de tempo e maior custo pó transação. Os *smarts cards* podem

> ser autenticados sem conexão agilizando as operações de crédito e débito;
> - Maior interoperabilidade entre bancos e circuitos de pagamentos seja em nível nacional ou internacional;
> - Definição de um único padrão para os cartões, eliminando, entre outros, a necessidade de diferentes terminais para diferentes bandeiras;
> - Possibilidade de desenvolvimento de aplicações seguras para o comércio e os pagamentos via internet. (Parodi, 2008, p.244).

De acordo com Parodi (2005), periodicamente aparecem informações ou boatos de alguém que teria conseguido encontrar falhas de segurança ou quebrar o sistema criptográfico dos *smarts cards*, ou seja, de que seria aberto o caminho para um sistema simples de clonagem de cartões ou de aproveitamento de cartões com chip roubados.

Segundo o autor nada apareceu de forma comprovada em qualquer parte do mundo. Sabe-se que é possível quebrar a segurança dos *smarts cards* através de equipamentos que penetram no *hardware* do chip e observam como está trabalhando e armazenando informações, mas tais equipamentos são muito caros (na casa de 2 milhões de dólares), precisam de pessoas altamente especializadas para serem operados e os laboratórios equipados com eles são muito poucos (perto de 200 no mundo inteiro, sobretudo em universidades, grandes empresas e centros de pesquisas de governos).

Para Parodi (2005), os "*carders*" (criminosos especializados em fraudes com cartões) profissionais, cientes das grandes dificuldades em se conseguir um sistema "econômico" capaz de quebrar a criptografia de *smarts cards* ou de aproveitar falhas de segurança, estão se concentrando em outros pontos do processo de autorização, mais fracos e mais facilmente aproveitáveis.

É consensual que as maiores falhas de segurança são descuidos dos usuários ou dos humanos em geral, e não do sistema em si. Por esta razão, os "*carders*" estão se concentrando em sistemas e técnicas que visam capturar as senhas no momento em que os usuários as digitam ou em sistemas onde estas possam estar armazenadas. Depois disso, é só extraviar, roubar ou trocar o cartão do cliente bancário para usá-lo, como se verá a seguir.

3.2.1.2 O Golpe do Cartão Retido

É importante destacar que este e o próximo subtítulo tem seu conteúdo obtido a partir do conhecimento profissional da autora deste trabalho em um setor que analisa contestações de débitos por fraudes em uma instituição bancária de atuação nacional.

O golpe do cartão retido tem como "*modus operandi*" (Expressão em latim que significa "modo de operação", utilizada para designar uma maneira de agir, operar ou executar uma atividade seguindo sempre os mesmos procedimentos) a inserção de artefato espúrio que retém o cartão do usuário em algum TAA (Terminal de Autoatendimento) quando este é inserido. O TAA pode estar disponível nas agências bancárias ou em estabelecimentos comerciais com TAA cedido pela instituição bancária.

O cliente ao inserir o cartão no equipamento percebe que seu cartão ficou preso/retido na máquina e então procura no ambiente por telefone da central de atendimento do banco para reportar o ocorrido e bloquear o cartão.

Essas ações normalmente ocorrem fora dos dias e horários de atendimento bancário, quando não há funcionários nas agências que podem atender e solucionar dúvidas dos clientes. Faz parte do golpe a fixação de cartazes com falsos números de centrais de atendimento. O cliente liga para o suposto número e é atendido por falsa funcionária/atendente que ouve o ocorrido e informa que o cartão foi bloqueado por medida de segurança e que será enviado um novo cartão para o usuário em alguns dias.

Na conversa com a atendente o cliente é persuadido a confirmar alguns dados, para maior segurança do atendimento. Dentre os dados solicitados incluem-se as senhas, os dados da conta e algumas informações cadastrais do cliente que serão supostamente informadas para um sistema que fará o reconhecimento e confirmação das informações prestadas. A partir desse momento os fraudadores estão de posse do cartão e com as senhas para a realização das mais diversas operações, tais como: saques, compras, contratação de empréstimos, transferências e pagamentos, esvaziando as contas das vítimas.

3.2.1.3 O Golpe da Troca de Cartão

As fraudes de troca de cartão ocorrem quando um falso funcionário da instituição bancária, muitas vezes portando falso crachá de identificação, se oferece para ajudar na realização das transações feitas em terminais de autoatendimento. Assim como o golpe anterior ocorre normalmente fora do horário de atendimento normal das agências.

Geralmente, as pessoas que sofrem este golpe são pessoas com maior dificuldade na utilização dos terminais de autoatendimento, tais como idosos e pessoas não acostumadas com a utilização dos equipamentos. O falsário, de boa aparência, simpático e prestativo ajuda o cliente a efetuar as operações com o cartão, fazendo-o ele mesmo. Quando a vítima vai digitar sua senha o meliante, muitas vezes com o auxílio de outro comparsa, memoriza a senha digitada e ao final do “atendimento” efetua a troca do cartão da vítima por outro semelhante sem que o cliente perceba. Ao final o golpista está de posse do cartão e com as senhas memorizadas para efetuar as mais diversas operações bancárias.

3.2.2 As Fraudes Bancárias pela Internet

O objetivo da oferta pelos bancos de serviços bancários pela internet é a atração de um número maior de usuários deste canal e se justifica pelo fato de que essas operações reduzem expressivamente os custos dos clientes no banco, diminuindo a presença deles nas agências bancárias, e assim, diminuindo a necessidade de pessoas para atendê-los.

Os crimes digitais afetam o mundo inteiro, muitas entidades financeiras e milhares de pessoas sem que o agressor sequer saia de casa. As ameaças antes restritas a especialistas e estudiosos, são muitas vezes disponibilizadas gratuitamente na internet, tais como programas para fraudar senhas, disseminar vírus, monitorar redes, identificar fragilidades e atacar servidores etc.

Destacam-se três conceitos relativos à disponibilização de canais pelos bancos aos seus clientes nos dias atuais:

- *Home Banking*: é um conceito mais amplo que, conforme Lau (2006), precede o conceito de *internet banking*, pois é o serviço disponibilizado a clientes de instituições financeiras que permite a efetivação de transações através da conexão de um equipamento à infraestrutura da instituição financeira por um canal público ou privado, ou seja, engloba além do computador o acesso de outros equipamentos como o telefone;
- *Office Banking*: é o conceito de *home banking* utilizado por empresas; e
- *Internet Banking*: também conhecido como *Web Banking*, é conhecido como o canal de acesso a produtos e serviços bancários exclusivamente pela internet, possibilitando que o cliente realize operações bancárias em qualquer lugar onde haja um computador ou até mesmo celular conectado à internet.

Hoje é possível realizar quase todo tipo de transação bancária pela internet, tais como, contratação de empréstimos com limites pré-aprovados, pagamento de títulos, convênios de luz e água, aquisição de produtos de previdência, investimentos em ações, renovação de seguros, consultas a saldo e extratos, transferências de valores etc.

De acordo com a literatura disponível e destacada em cada item abaixo as fraudes pela internet podem ocorrer de várias maneiras. A seguir destacamos as mais conhecidas:

a) *Spam*

Spam, segundo Lau (2006), são correios eletrônicos (*e-mails*) não solicitados, geralmente enviados para um número significativo de destinatários, não permitindo que os receptores escolham entre receber ou não tais mensagens. Esse tipo de correio eletrônico pode conter programas maliciosos ou mensagens com algum tipo de engenharia social. Os e-mails podem vir com vários intuitos, tais como: participação em promoções, inscrições em programas de televisão, cadastramentos, pendências na Receita Federal e/ou no SCPC e SERASA, anexos com conteúdos chamativos, que dizem conter fotos ou cartões virtuais de admiradores, etc.

Segundo Parodi (2008) o mecanismo conhecido como *AntiSpam* é um sistema que permite identificar e filtrar e-mails classificados como Spam e descarta-los de forma automática, permitindo ao usuário selecionar o que ler e o que não ler.

A maioria dos administradores de *e-mail* já possuem aplicativos que separam automaticamente esse tipo de mensagem em uma pasta chamada de lixo eletrônico ou mesmo de *spam*. Nestas pastas, são feitas limpezas pelo sistema, em curtos períodos de tempo, possibilitando que o usuário tenha a possibilidade de ler as mensagens se for de sua vontade, caso contrário não precisa eliminá-la manualmente, pois o sistema elimina automaticamente.

O objetivo do golpe é fazer com que, ao acessar e abrir arquivos *Spam*, seja instalado no computador um vírus chamado "*trojan*" ou "*worm*", cujas funções são de atrapalhar o funcionamento do computador e também interceptar senhas e dados digitados quando for acessado o banco pela internet ou quando for efetuado algum pagamento com o cartão de crédito.

Segundo Almeida (2008), existem vários tipos de programas maliciosos usados por criminosos virtuais com o objetivo de capturar informações, os quais estão destacados a seguir:

> - *Sniffer*: que significa farejador. O programa é capaz de monitorar e registrar o tráfego de dados de rede. Os dados coletados são usados para obtenção de informações úteis para a solução de problemas em rede, quando utilizado com boas intenções por um administrador do sistema, ou, para ataques ao sistema, quando usado por criminosos para obter usuários, senhas e outras informações confidenciais;
> - *Keylogger*: significa registrador de teclado, é um *software* que, quando instalado em um computador captura e registra tudo aquilo que é digitado no teclado da máquina. Alguns funcionam de forma a salvar os dados capturados em arquivos de texto no próprio computador, esses geralmente são instalados por pais que desejam monitorar as atividades de seus filhos ou por empresas para controlar seus funcionários. Outros tipos enviam os dados através de correio eletrônico até um terceiro que, de posse destes, poderá usá-los de forma ilícita;
> - *Screenlogger*: que significa registrador de tela é um programa que captura imagens da tela do computador do usuário e pode enviá-las por correio eletrônico para outra pessoa. Os programas são especializados para fraudes em *internet banking* e capturam uma imagem a cada clique do cliente no teclado virtual, obtendo assim a sua senha de acesso. Alguns programas chegam a filmar a ação do usuário bancário, incrementando a ação dos fraudadores. (Almeida, 2008, p.45).

b) *Scam*

Segundo Lau (2008), é um tipo de mensagem eletrônica que, assim como o Spam, é enviada sem autorização para vários endereços de e-mails e apresentam natureza fraudulenta. Essa natureza se deve ao fato de a mensagem estar relacionada à tentativa de convencimento do receptor mediante alguma oferta descrita na própria mensagem.

As características das mensagens classificadas como *SCAM*, de acordo com o trabalho de Lau (2006) são:

> - O conteúdo da mensagem pode ou não conter uma marca comercial forjada;
> - Contém endereços *de e-mail* e *links* forjados;
> - Representa uma mensagem que aguça a curiosidade da vítima;
> - O golpe busca atingir a vítima, através da instalação acidental de um programa existente no *link* forjado. A partir da instalação deste agente, dados são coletados no computador infectado. Estes programas são conhecidos como “cavalos de Tróia”;
> - O processo de captura de credenciais pode ser imperceptível à vítima, ou se apresentar na forma de uma tela sobreposta sobre os aplicativos do computador, induzindo a vítima a colaborar involuntariamente com o fornecimento de seus dados pessoais. (Lau, 2008, p.63)

b) Falsos Sites de Bancos ou *Phishing*

Conforme destacado pelo autor Parodi (2005) ocorre, normalmente através de e-mails com componentes gráficos e logomarcas que identifiquem aparentemente como sendo enviado por um banco no qual o cliente é convidado a acessar um falso site da instituição com alguma desculpa (recadastramento de dados, participação em promoções, sorteios, seguros gratuitos, autenticação ou cadastramento de *e-mails*, atualização de configurações de segurança etc.).

O fraudador aguarda o retorno à aceitação do estímulo através do acesso ao *link* existente na mensagem, acesso à página falsa da instituição e a inserção voluntária dos dados solicitados à vítima. Dentre os dados estão o número da conta, da agência e/ou cartão com as respectivas senhas, o suficiente para realizar transações bancárias e gerar uma fraude.

Normalmente os falsos sites de bancos têm endereços plausíveis, frequentemente contêm o nome do banco e alguma palavra atraente do tipo “sorteio” ou “promoção”. Segundo PARODI (2005), raramente possuem URL (*Uniform Resource Locator*), ou seja, endereço de site de internet com terminação “.COM.BR”, mas sim “.COM”. Ao acessar o site, o ambiente gráfico e o conceito são idênticos aos sites verdadeiros. Este golpe é chamado de “*phishing*”, ou seja, pescaria já que são enviados milhares de *e-mails* (iscas) tentando pescar as vítimas (peixes).

Nas fraudes ocorridas pela internet das mais variadas formas mencionadas acima o golpista pode solicitar dentre as informações para acesso à conta do usuário vitimado o número do cartão de crédito e do código de segurança ou código de verificação (É o código de verificação é a composição de três números que ficam no verso do cartão e que não compõem o número do cartão. É utilizado para confirmar a compra como sendo feita com o verdadeiro cartão) disponível no verso do cartão e assim efetuar compras na *web*.

As práticas fraudulentas realizadas com cartão ou pela internet vêm aumentando com o passar do tempo. De acordo com publicação da Revista Eletrônica de Jornalismo Científico Com Ciência na reportagem intitulada “Não mora da Isca”[3] a Federação Brasileira dos Bancos (FEBRABAN) informou que as instituições financeiras investem R$ 1,2 bilhões por ano para atualizar seus mecanismos de combate às fraudes eletrônicas.

Ressalta-se que não existem dados concretos ou estatísticas que possam dar a dimensão das perdas com as fraudes que ocorrem no Brasil, no mundo ou em outros países. A falta de números concretos se justifica pelo fato de as instituições financeiras não disponibilizarem essas informações. A não disponibilidade se dá pelo interesse dos bancos na continuidade e no aumento dos negócios realizados pelos novos canais de atendimento devido ao reduzido custo da realização das transações. Para as instituições é preferível, muitas vezes, ter uma perda com a utilização desses novos canais do que a volta aos altos gastos com funcionalismo se as mesmas operações voltassem a ser efetuadas nas agências com o cliente presente fisicamente e sendo atendido por funcionário.

[3] Acessada em 05/02/2013 no endereço <http://comciencia.br/comciencia/?section=8&edicao=20&id=218>

O que se pode concluir é que, se as perdas com as fraudes bancárias forem menores que os ganhos da instituição com redução de custos decorrentes da utilização dos novos canais hoje disponíveis, ainda valerá o risco a que a instituição está exposta. Se em algum momento as perdas forem maiores que os lucros ganhos com a economia de custos não compensaria a continuidade do uso dos novos canais.

Apesar de existir essa análise custo/benefício por parte das instituições bancárias os clientes já estão habituados e facilidades no atendimento bancário. Seria muito difícil que as pessoas deixassem de fazer compras com cartões em estabelecimentos comerciais ou pela internet, que voltassem a frequentar as agências bancárias para pagar suas contas. Os investimentos em segurança e Tecnologia de Informação cresceram nos últimos anos no setor bancário para proteger a instituição e também os clientes que ela atende.

Além dos altos investimentos em segurança as instituições passaram a atacar o problema por outro lado, aparentemente mais eficaz: orientando o cliente para que o mesmo tome cuidados básicos de segurança, tema abordado no próximo capítulo.

4 MEDIDAS PREVENTIVAS UTILIZADAS PELOS BANCOS NA MITIGAÇÃO DAS FRAUDES

Esta seção se propõe a destacar quais são as medidas preventivas utilizadas pelas instituições financeiras para a prevenção e mitigação das ocorrências de fraudes com cartões e pela internet.

4.1 Medidas de Mitigação das Fraudes com Cartões

As mudanças ocorridas nas últimas décadas, como a globalização e a rápida proliferação da internet, trouxeram também a modernização do crime organizado, assim como o surgimento de tratados internacionais de lavagem de dinheiro provocando grandes alterações na visão de governos e corporações em todo o mundo sobre o tema segurança.

No ambiente corporativo a segurança passou a ser vista como uma área de abrangência multidisciplinar que deve se basear em equipes de excelência, tecnologias de ponta e inteligência estratégica, considerando que a eficácia do processo de segurança depende do envolvimento de todas as pessoas.

4.1.1 Substituição dos Cartões com Tarja Magnética pelos *Smart Cards*

Segundo PARODI (2005) o principal sistema de armazenamento de dados de cartões de crédito e débito era a banda magnética, desenvolvida há aproximadamente 30 anos atrás e utilizada por todos os circuitos. Essa tecnologia não é mais adequada às necessidades de segurança atualmente.

Os cartões com tarja magnética ainda estão em uso, mas o número foi reduzido a patamares mínimos, sendo então substituídos por cartões inteligentes ou cartões com *CHIP*.

O desenvolvimento dos cartões com *CHIP*, conhecidos como “*smart cards*” trouxe uma mudança fundamental na indústria mundial dos sistemas de pagamentos. As instituições bancárias juntamente com as operadoras de cartões do mundo inteiro estão difundindo os cartões com *CHIP*, pois estes possuem capacidade de armazenar dados de forma segura (criptografados), com maior capacidade de memória e, graças à presença de um microprocessador interno, podem ser utilizados por múltiplas funções, além do armazenamento dos dados.

Os cartões com chip não podem ser clonados, pelo menos por meio simples. De acordo com PARODI (2005), é possível quebrar a segurança dos *smart cards* através de equipamentos que penetram no *hardware* do *chip*, porém esses equipamentos são muito caros, por volta de dois milhões de dólares cada e precisam de pessoas altamente especializadas para operar as máquinas.

4.1.2 Orientações de Segurança aos Usuários de Cartões

As fraudes ou golpes realizados nas salas de autoatendimento têm sido combatidos através do repasse de informações e recomendações de segurança no manuseio dos cartões. O repasse dessas recomendações vem sendo feito quando da abertura de conta bancária com a entrega de uma cartilha de segurança, pela internet geralmente em um *link* intitulado “Recomendações de Segurança” e também na tela inicial dos terminais de autoatendimento.

Através de pesquisa realizada nos sites dos nos bancos de maior relevância atuantes no país, mostramos a seguir a compilação das recomendações mais utilizadas pelas instituições quanto ao manuseio de cartões:

- Nunca se afaste do terminal de autoatendimento sem concluir sua operação. Na dúvida clique na tecla cancelar;
- Nunca inicie qualquer operação ou passe/insira seu cartão a pedido de terceiros;
- Não digite sua senha ou código de acesso caso seu cartão fique retido no terminal, pois esse procedimento não vai liberá-lo;

- Nunca entregue seu cartão a terceiros e tenha cuidado com esbarrões propositais;
- Sempre verifique se está de posse do seu cartão, caso contrário comunique imediatamente a central de autoatendimento;
- Não ligue para números que se encontrem afixados na máquina ou sugeridos por terceiros;
- Somente aceite ajuda de funcionários nos horários de expediente bancário e que estejam devidamente identificados;
- A senha é pessoal e intransferível, portanto, não deve ser divulgada a ninguém, nem mesmo pessoa de confiança;
- Ao criar sua senha não utilize números que tenham relação com dados pessoais como R.G., C.P.F., telefones, datas de nascimentos etc. ou números sequenciais ou repetitivos;
- Troque a senha caso ela possa ser descoberta facilmente ou haja desconfiança de quebra de sigilo da mesma;
- Memorize suas senhas, evite anotá-las;
- Altere regularmente suas senhas;
- Nunca digite suas senhas quando pessoas estranhas estiverem observando;
- Após compra com cartão, não se esqueça de confirmar se o cartão devolvido pelo atendente é o seu catão;
- Caso o cartão seja roubado, perdido ou extraviado comunicar imediatamente o fato à Central de Atendimento;
- No telefone somente digite suas senhas quando a ligação não for iniciada por terceiros;
- Nunca aceite celular de desconhecidos para se comunicar com o banco, pois o aparelho pode estar preparado para gravar os dados de sua conta;
- Certifique-se de que está ligando para o número de telefone correto da Central de Atendimento do seu banco;
- Nunca informe sua senha por telefone ao atendente. A Central de Atendimento só é solicitada a partir de mensagens de voz pré-gravadas e, nesse caso, deverá ser teclada no aparelho de telefone;

- Mantenha seu cadastro no banco sempre atualizado, pois o banco solicita informações para a identificação positiva;
- Procure um lugar discreto para que ninguém ouça o que está sendo falado durante a ligação, principalmente se for informar dados cadastrais.

4.2 Medidas de Mitigação das Fraudes Ocorridas pela Internet

As medidas preventivas utilizadas pelas instituições financeiras na mitigação das ocorrências de fraudes via internet consistem na busca através de sistema próprio da instituição da realização de transações na conta do cliente que fogem ao seu perfil, e disponibilização no site das instituições de recomendações de segurança no uso da internet como canal de movimentação financeira.

De acordo com LAU, (2006) a FEBRABAN (Federação Brasileira de Bancos) informa aos clientes bancários que os bancos mantêm fortes sistemas de segurança em seus computadores e programas de acesso à internet mencionando, porém, que a instituição não pode garantir a segurança no computador de cada cliente que utiliza o canal. Assim, a FEBRABAN faz algumas recomendações para a prevenção à ocorrência de fraudes, recomendações estas que norteiam as recomendações de segurança repassadas pelas instituições financeiras aos seus clientes.

Abaixo são listados os meios mais utilizados para garantir a segurança das transações bancárias realizadas pela internet:

4.2.1 Autenticação

Para Lau (2006), a autenticação permite a identificação positiva do usuário, ou seja, itens adicionais de identificação introduzidos pelos bancos, além da senha, como por exemplo, confirmação de algum dado pessoal, que está associada às credenciais que permitem o reconhecimento do cliente no sistema *Internet Banking*.

De acordo com LAU (2006) há três fatores de autenticação utilizados em sistemas e a combinação de dois destes três fatores é considerada uma autenticação forte. Os três fatores destacados pelo autor são os seguintes:

> - Algo que o usuário conhece: são os dados que identificam o usuário no sistema e sua respectiva senha;
> - Algo que o usuário possui: são objetos que pertencem ao usuário e o auxiliam na identificação. O cartão magnético de um banco, certificados digitais e dispositivos geradores de senhas dinâmicas estão baseados neste fator de autenticação; e,
> - Algo que constitui o usuário: Características pessoas como a íris, voz e impressão digital podem ser utilizadas para autenticação em sistemas. (Lau, 2006, p. 25 e 26)

Atualmente, segundo Lau (2006), os sistemas de *internet banking* utilizam os dois primeiros fatores de autenticação, representando uma autenticação forte segundo os princípios de segurança da informação.

Apesar de a autenticação ser considerada forte na utilização dos dois primeiros fatores, muitas vezes, não há como a instituição bancária garantir que determinada transação bancária está sendo realizada pelo cliente ou não já que os meliantes acabam de algum modo conseguindo os dados de identificação e as senhas do cliente.

Diante disso, algumas instituições fornecem a seus clientes usuários da internet o que é chamado de *token* e o cadastramento de computadores.

Segundo informações disponíveis no site da Tecmundo[4], os *tokens* são dispositivos que geram senhas para confirmação de operações pela internet aleatórias a cada pequeno intervalo de tempo. Esse mecanismo coloca algo físico, que pode ser um cartão ou um aparelho, que não pode ser obtido pelo meio virtual, na tentativa de garantir maior segurança ao ambiente *internet banking*. O mecanismo pode ser considerado seguro, porém não 100% seguro já que em muitos golpes os meliantes fazem o usuário acreditar que está na página do banco, enquanto informa operações para uma página falsa. O indivíduo que recebe as informações verdadeiras repassadas na página falsa vai realizando as transações fraudulentas no site verdadeiro da instituição bancária.

O cadastramento de computadores é o mecanismo onde o cliente irá cadastrar os computadores que utiliza na realização das operações bancárias. É

[4] <http://www.tecmundo.com.br/senha/3077-o-que-e-token-.htm> acessado em 05/03/2013

uma forma de vincular o IP (endereço que cada máquina possui) de cada computador como o cliente. O sistema de cadastramento pode ser considerado seguro, mas a exemplo do *token*, também pode ser burlado já que existem alguns vírus que conseguem simular outras máquinas, parecendo ser a transação verdadeira e do computador do cliente.

4.2.2 Criptografia

Lau (2006) informa que a criptografia é uma tecnologia que garante a confidencialidade e privacidade dos dados. O autor relata que há duas utilizações possíveis da criptografia no ambiente *internet banking*: a proteção de dados armazenados em bancos de dados e o sigilo das informações que trafegam no ambiente internet.

Ainda conforme o autor, a segunda forma citada é adotada pelas instituições financeiras, pois a comunicação entre o cliente do serviço e o banco poderia ser monitorada, permitindo a exposição de dados confidenciais como os dados de autenticação no sistema.

4.2.3 Detecção de Intrusos

Para Lau (2006), a implementação de sistemas capazes de detectar intrusos nas redes das instituições financeiras é uma medida essencial de segurança que busca invasores, tanto de origem interna quanto externa. A detecção ocorre a partir de equipamentos chamados, de sensores, os quais podem ser classificados em dois grupos:

- *Networks IDS*: sensores que buscam características de tráfego na rede que se assemelham a ataques registrados no sistema; e,

> - *Host IDS*: são agentes instalados em servidores contendo aplicações que buscam por atividades inesperadas ao perfil normal de um usuário. (Lau, 2006, p.29)

A busca de atividades que fogem ao perfil do cliente pode ser muito útil já que as características dos ataques são as mesmas na maioria dos casos. Quando um meliante consegue todos os dados necessários para o acesso à conta de um cliente bancário ele normalmente faz empréstimos na conta até o limite disponível pela instituição àquele cliente e utiliza todo o valor disponível na conta, inclusive o limite de cheque especial.

Vale lembrar que as instituições bancárias estabelecem um limite de valor ou quantidade de transações bancárias que cada usuário pode fazer em determinado período de tempo, normalmente um dia, na tentativa de minimizar as perdas com atos ilícitos. São exemplos, o limite de valor para compras no débito, limite diário de saque, limite de transferências etc.

Com a utilização pela instituição de sistemas que buscam atividades que fogem ao perfil do cliente e sabendo-se que o fraudador irá utilizar totalmente os recursos disponíveis é possível que a instituição tome medidas que bloqueiem a continuidade das transações fraudulentas, como o bloqueio provisório de senhas até que se confirme com o cliente a autenticidade das operações.

4.2.4 Recomendações do Comitê de Basiléia

O Comitê de Basiléia faz algumas recomendações de segurança a serem seguidas pelas instituições financeiras para controle de riscos de segurança, destacadas abaixo, obtidas do trabalho de LAU (2006):

> - **Autenticação de clientes**: as instituições devem adotar meios para permitir a autenticidade de uma identidade e prover autorização ao cliente para utilização do internet banking;
> - **Não repúdio e contabilidade das transações**: as instituições devem utilizar métodos transacionais de autenticação que possibilitem confirmar a veracidade das operações e rastreamento da sequência de transações efetuadas;

> - **Medidas que asseguram segregação de funções**: as instituições devem possuir normas que obriguem a segregação de funções de seus funcionários envolvidos em sistemas, bancos de dados e aplicações do ambiente internet banking;
> - **Controles apropriados de autorização em sistemas, bancos de dados e aplicações**: as instituições devem assegurar que controles de autorização e privilégios de acesso estão definidos de acordo com a função de seus funcionários, de acordo com perfis de acesso a sistemas e bancos de dados;
> - **Integridade dos registros, informações transacionais**: as instituições financeiras devem adotar medidas que garantam a proteção da integridade dos dados em ambiente internet banking, como registros, informações e transações;
> - **Estabelecimento do rastreamento transparente em transações**: as instituições financeiras devem se assegurar da existência de processos transparentes que permitam o rastreio de todas as transações efetuadas sobre o sistema internet banking;
> - **Confidencialidade em informações bancárias essenciais**: as instituições financeiras devem prover mecanismos que garantam a confidencialidade de informações sigilosas, sejam eles dados transmitidos através de meios eletrônicos, ou armazenados em mídias magnéticas. (Lau, 2006, p.37 e 38)

Segundo LAU (2006) há diversas linhas para a mitigação das fraudes no canal internet banking. O modelo que o autor apresenta deve atingir três segmentos distintos: usuários finais, provedores e fraudadores, conforme abaixo:

> - Ações junto a usuários finais: o autor sustenta que os usuários necessitam de maiores esclarecimentos sobre esse tipo de ameaça. O autor destaca que infelizmente as informações existentes sobre a efetivação das fraudes e recomendações hoje oferecidas aos clientes são escassas, disponíveis em sites especializados de segurança de informação que nem sempre estão acessíveis aos clientes do *internet banking*;
> - As ações junto aos provedores são consideradas necessárias, pois os mesmos são responsáveis pelo fornecimento de serviços junto aos clientes e em muitos casos os serviços que fornecem podem ser considerados de imprudência técnica, pois não foram tomadas as medidas de segurança cabíveis. LAU destaca que, em geral, apenas o provedor financeiro (a instituição bancária) é acionado para reparar o dano causado ao cliente e recomenda que se deva avaliar a extensão do dano e envolver todos os fornecedores diretos através da argumentação da corresponsabilidade;
> - LAU (2006) sinaliza a necessidade de ações junto aos fraudadores no sentido de aumentar a repressão aos crimes de informática. Destaca que os responsáveis por este tipo de crime são enquadrados em estelionato, formação de quadrilha, furto qualificado, quebra de sigilo bancário e lavagem de dinheiro que somados levam a pena máxima de dezoito anos prisão, mas que na prática se limitam de quatro a seis anos de reclusão. O autor recomenda que se deva aprovar leis específicas que tipifiquem as

> ações, pois os magistrados associam o crime de fraudes de internet com os códigos civis e criminais vigentes, que já não condizem com a realidade dos dias atuais.

A FEBRABAN (Federação Brasileira dos Bancos) disponibilizou uma cartilha na internet com recomendações de segurança para que os clientes das instituições bancárias possam compreender melhor as medidas de segurança adotadas pelas instituições financeiras e tomar ciência dos cuidados no uso dos serviços bancários pela *web*.

A cartilha da FEBRABAN foi feita pelo CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil). Na cartilha foi divulgada uma lista contendo os temas de e-mails mais comuns utilizados nas mensagens eletrônicas maliciosas. A tabela pode ser obtida na página da CERT, endereço <http://cartilha.cert.br/golpes/>.

De acordo com o trabalho de LAU (2006) e pesquisa realizada nos sites dos bancos de maior relevância no país destacamos a seguir quais as recomendações mais utilizadas pelas instituições quanto à utilização da internet como canal de operações bancárias:

- Manter programas antivírus atualizados instalados nos computadores utilizados para o acesso aos serviços bancários;
- Trocar a senha de acesso ao *internet banking* periodicamente;
- Não executar aplicações ou abrir arquivos de origem desconhecida, pois podem conter vírus e outros procedimentos prejudiciais, que ficam ocultos para o usuário e permitem a ação de fraudadores a partir de informações capturadas após a digitação no teclado;
- Usar somente provedores confiáveis. A escolha de um provedor deve levar em conta mecanismos, políticas de segurança e confiabilidade da empresa;
- Tome cuidado com e-mails não solicitados ou de procedência desconhecida, especialmente se tiverem arquivos anexados;
- Evitar sites arriscados. Só faça transferência de arquivos (*download*) para o seu computador de sites confiáveis;
- Quando for efetuar pagamentos ou realizar operações financeiras certificar-se de que está no site desejado clicando sobre o cadeado e/ou chave de segurança que aparece quando se entra na área de segurança do site. O certificado

de habilitação do site, concedido por uma certificadora autorizada que aparecerá na tela, confirmando sua autenticidade, juntamente com informações sobre o nível de criptografia utilizada naquela área pelo responsável pelo site;

- Acompanhar os lançamentos de sua conta corrente;
- Evite atalhos para acessar o site da instituição bancária, especialmente os obtidos em sites de pesquisa. Digite sempre no campo do endereço;
- Evite realizar operações em equipamentos de uso público, eles podem estar com programas antivírus desatualizados ou preparados para capturar os dados digitados;
- Certifique-se de que as demais pessoas que utilizam seu computador tenham conhecimento e sigam as orientações de segurança;
- Saiba que as instituições financeiras não enviam mensagens de correio eletrônico a seus clientes, nem autoriza qualquer parceiro comercial a fazê-lo;
- Nunca informe o número do seu cartão ao utilizar o *internet banking*.

O que se pode perceber diante das medidas de mitigação das fraudes é que essas ocorrências vão ser efetivamente combatidas quando as medidas ações de prevenção vierem em várias frentes participantes do processo, pelas instituições financeiras, pela orientação e conscientização dos usuários, dos provedores de serviços de internet e no combate ao crime propriamente dito. As dicas que as instituições repassam aos usuários são eficientes, porém não são amplamente divulgadas, talvez pelo temor de expor que esses riscos existem e possam prejudicar a imagem das instituições. Sem a ampla divulgação, normalmente quem toma conhecimento das recomendações são as pessoas que as procuram.

5 CONCLUSÃO

As mudanças ocorridas nos últimos anos trouxeram benefícios e mazelas à sociedade atual. Vemos que com a globalização muitos crimes também se difundiram internacionalmente. Com a inovação tecnológica surgiram as facilidades no cotidiano das pessoas, com a proliferação da internet, se difundiram também os crimes tecnológicos ou virtuais, antes restritos somente ao contato físico.

Dentre os facilitadores da vida moderna encontram-se os cartões de débito para movimentação de conta bancária e cartões de crédito com limites atrativos, oferecendo prazos para pagamentos de compras, parcelamento, além de outras vantagens como a segurança de não se andar com grandes valores em espécie, e sim somente com um plástico vinculado à sua conta corrente e acessado através de uma senha pessoal.

A internet conseguiu conectar o mundo, difundir informações, ligar pessoas, culturas, aproximar o que a distância da vida real separou.

As instituições financeiras utilizaram a tecnologia da informática para melhorar seus sistemas internos de comunicabilidade e também para aproximar seus clientes por mais distantes que possam estar. O negócio bancário evoluiu a tal ponto que a concorrência entre as instituições as obrigou a oferecerem cada vez mais facilidades e melhores serviços para seus clientes, diversificando seus canais de atendimento ao consumidor pela internet, pelo telefone etc.

Dentro da proliferação e difusão das facilidades trazidas pelas novas tecnologias surgiram também os crimes tecnológicos, chamados de fraudes tecnológicas, ou seja, delitos em que um especialista tecnológico consegue obter de outrem, com menor conhecimento, vantagens normalmente expressas em valores através da clonagem de cartões, de uso da engenharia social e da invasão de computadores através de vírus que infectam computadores e repassam informações confidenciais de transações bancárias.

A dificuldade de estatísticas sobre a quantidade ou o montante envolvido nesse tipo de crime pode ser explicada no risco de imagem das instituições que não querem afugentar a clientela que é incentivada a utilizar os novos canais, mais baratos para as instituições. O benefício na economia de gastos com funcionalismo parece ser maior que as perdas oriundas da disponibilização dos novos canais de

atendimento, os chamados autoatendimentos, já que neles os próprios clientes se autoatendem, gerando uma economia para o setor bancário.

As medidas mitigatórias das ocorrências de fraudes e golpes são tomadas pelas instituições financeiras quanto à segurança de seus sistemas e dos sistemas que as ligam a seus clientes, porém o que se vê normalmente, não são falhas diretas das instituições, e sim falhas na difusão e conscientização dos usuários na utilização dos canais de autoatendimento. As fraudes geralmente são oriundas de descuidos ou desconhecimento dos usuários por falta de informação.

O presente trabalho apresentou como ocorrem as fraudes bancárias, como são efetivamente controladas e reduzidas pelas instituições e identificou que, normalmente, as ocorrências poderiam ser combatidas com a difusão de informações e recomendações de segurança. Recomenda-se que as informações de segurança cheguem a todos os usuários e não somente estar disponível para quem as procura. A difusão deveria ser repassada para todos os que venham a utilizar dos canais de autoatendimento bancário através de cursos ou cartilhas quando da abertura de conta na instituição financeira, já que como foi visto, as recomendações se repetem e sendo as mesmas seguidas pelos usuários as fraudes poderão ser efetivamente combatidas.

6 REFERÊNCIAS

ALMEIDA, Paula Carneiro de. **Segurança da Informação Bancária: Aplicação de *Internet Banking***. Universidade do Vale do Sapucaí. Porto Alegre, 2008;

CARMO, Claudio Roberto da Silva, (2005) **O problema da assimetria de informações nas atividades da Receita Federal do Brasil.** Disponível em: < http://www.esaf.fazenda.gov.br/esafsite/premios/schontag/Monografias_premiadas_arquivos/monografia/monografias%204%C2%BA/1%20lugar%20CLAUDIO%20ROBERTO%20DA%20SILVA%20CARMO.pdf > Acesso em 27/08/2012;

CARVALHO, Fernando J. Cardim de; SOUZA, Francisco Eduardo Pires de; SICSÚ, João, PAULA, Luiz Fernando Rodrigues de; SUDART, Rogério. **Economia Monetária e Financeira.** Rio de Janeiro, 2002. Editora Campus;

JÚNIOR, Antônio Marcos Duarte. **Risco: Definições, Tipos, Medição e Recomendações para seu Gerenciamento.** Disponível em: < http://www.risktech.com.br/PDFs/RISCO.pdf > Acesso em 01/10/2010;

LAU, Marcelo. **Análise das fraudes aplicadas sobre o ambiente *Internet Banking*.** Dissertação apresentada à Escola Politécnica de São Paulo, 2006;

LEVITT, Steven D., DUBNER, Stephen J. ***Freaknomics*: o lado oculto e inesperado de tudo que nos afeta.** Editora Campus. 7ª Edição. 2005;

LIRA, Waleska Silveira, CÂNDIDO, Gesinaldo Ataíde. **Fatores determinantes do uso dos serviços bancários via internet segundo o método de avaliação SERVQUAL**. Revista Negócios e Tecnologia de Informação. Vol. II, nº 1 (2007). FESP-PR. Disponível em: < http://publica.fesppr.br/index.php/rnti/article/viewArticle/v2n1ART9 > em 15/04/2011;

PAULA, Luiz Fernando de, FARIA, João Adelino de (2008). **Reestruturação Bancária e Eficiência dos Bancos por Segmento: uma avaliação recente**. Artigo

apresentado à UFRJ. Disponível em: < http://www.ie.ufrj.br/datacenterie/pdfs/seminarios/pesquisa/texto2711.pdf > Acesso em 02/03/2013.

PARODI, Lorenzo. **Manual das fraudes**. Editora Brasport. 2005;

PARODI, Lorenzo. **Manual das fraudes**. Editora Brasport. 2008;

SANTOS, Sérgio Luiz dos Santos. (2010) **Contribuição ao estudo do papel da controladoria nos processos de demandas informacionais: problemas de comunicação e assimetria informacional**. Dissertação apresentada à Faculdade de Ciências Econômicas da UFRGS. Disponível em: < http://www.lume.ufrgs.br/bitstream/handle/10183/25783/000741315.pdf?sequence=1 > Acesso em 30/08/2012.

Site: <http://empresasefinancas.hsw.uol.com.br/cartoes-de-credito-nos-eua1.htm> Consultado em 12/05/2011;

Site: <http://www.dicionarioinformal.com.br/chip/>**.** Consultado em 12/05/2011;

Site: < http://comciencia.br/comciencia/?section=8&edicao=20&id=218>. Consultado em 05/02/2013;

Site: <http://www.tecmundo.com.br/senha/3077-o-que-e-token-.htm>**.** Consultado em 05/03/2013.