FRAUDES ELETRÔNICAS: O QUE HÁ DE NOVO?

Paulo Sérgio Siqueira Bastos
Contador da Prefeitura da Cidade do Rio de Janeiro
Pós-graduado em Controladoria e Finanças pela UFF
Mestre em Ciências Contábeis pela Universidade do Estado do Rio de Janeiro.
E-mail: psergios.cgm@pcrj.rj.gov.br

Roberto Miguel Pereira
Contador da Prefeitura da Cidade do Rio de Janeiro
Pós-graduado em Contabilidade e Auditoria pela UFF
Mestre em Ciências Contábeis pela pela Universidade do Estado do Rio de Janeiro
E-mail: rmiguel.cgm@pcrj.rj.gov.br

RESUMO

As fraudes eletrônicas representam atualmente uma grande ameaça tanto às grandes empresas quanto para as pessoas físicas. O crescimento do comércio eletrônico tem gerado facilidade, agilidade e velocidade nas transações comerciais e financeiras cotidianas, mas sua segurança ainda é questionável. Foram levantados neste estudo dados quanto aos tipos de crimes e fraudes em informática, os impactos financeiros atuais, quais os agentes de fraudes e estratégias de defesa, com base em consultas bibliográficas e à *internet*. O objetivo deste estudo é como se proteger contra os mais novos tipos de fraudes em informática, em especial nas que se tem dado pela *internet* e mediante cartões de crédito. Dentre cinco estratégias de defesa destacadas, realizamos detalhamento da pesquisa nas tecnologias criadas recentemente para *prevenir* e *detectar* ilícitos em cartões de crédito.

Palavras-Chave: Fraude eletrônica, Prevenção à fraude, Detecção de Fraude.

ABSTRACT

The electronic frauds currently represent a great threat in such a way to the great companies how much for the natural people. The growth of the electronic commerce has generated easiness, agility and speed in daily the commercial and financial transactions, but its security still is questionable. They had been raised in this study given how much to the types of crimes and frauds in computer science, the current financial impacts, which the agents of frauds and strategies of defense, on the basis of bibliographical consultations and to the Internet. The objective of this study is as if to protect against the new types of frauds in computer science, in special in that if it has given for the Internet and by means of credit cards. Amongst five detached strategies of defense, we carry through detailing of the research in the bred technologies recently to prevent and to detect illicit in credit cards.

Keywords*: Electronic Fraud, Fraud Prevention, Fraud Detection.*

1. INTRODUÇÃO

Numa sociedade globalizada na qual o volume de transações comerciais advindas do ambiente *"e-business"* vêm sendo praticado com forte uso da Tecnologia da Informação (TI), os investimentos em tecnologias de informática e de comunicação de dados é fundamental para a sobrevivência das empresas.

A sobrevivência de uma empresa que opera nesse ambiente depende não só de promover a rentabilidade no relacionamento com seus fornecedores e clientes, mas de minimizar os efeitos das eventuais fraudes, principalmente as chamadas fraudes eletrônicas.

É cada vez mais freqüente notícia de fraudes com cartões de crédito, seja por compra através de telefone, internet ou por fax ou, até mesmo, pelo simples fato de o cliente entregar o cartão ao vendedor e o mesmo levá-lo a lugares fora do seu campo de visão. Também se tornou comum notícia de fraude por e-mail, através do qual se induz os clientes a fornecer dados pessoais, senhas, conta corrente e o número do cartão de crédito.

Pessoas físicas se protegem da forma que podem: rasgando extratos e comprovantes de pagamentos; evitando dar informações pessoais; não emprestando cartão de crédito para compras pela internet; não abrindo e-mails de pessoas desconhecidas e desconfiando de promoções muito vantajosas.

Pessoas jurídicas não podem se valer de igual forma dessas precauções, pois dependem das pessoas que a integram, as quais nem sempre estão comprometidas com a segurança da informação empresarial e, por vezes, até mesmo expõe a organização a ataques externos. Assim, são exigidos investimentos para prevenção, detecção e eliminação de fraudes, os quais embora onerem as empresas, reduzindo suas margens de lucro, as protegem de custos muito mais elevados decorrentes de fraudes informatizadas ou eletrônicas.

2. O CRIME E A FRAUDE EM INFORMÁTICA

A fraude é um tipo de crime previsto pelos códigos penais das nações do mundo todo. Significa dolo, burla, engano, logro ou contrabando (PRIBERAM, Dicionário da Língua Portuguesa On-line, 2005).

Em breve histórico quanto aos crimes em informática (Furlaneto Neto / Guimarães, 2003, p. 68) cita-se que o surgimento destes remonta à década de 1960, época em que apareceram na imprensa e na literatura científica os primeiros casos de uso do computador para práticas delituosas. Na década seguinte iniciaram-se os primeiros estudos sistemáticos e científicos sobre a matéria, analisando um número limitado de delitos informáticos. Somente a partir de 1980 e, em especial, na década de 1990, o número de crimes em informática teve crescimento acelerado pelas facilidades advindas pelo uso do microcomputador e da *internet.*

Os crimes em informática são classificados em virtuais puros, mistos e comuns (Pinheiro, 2001, p. 18-19). O crime virtual puro seria o ilícito contra o computador (sistema e equipamento). O crime virtual misto seria aquele que o delito transcorre com o uso da informática, mas visa atingir outros bens. Já o crime virtual comum é aquele que já encontra tipificação penal na lei.

Muitas das fraudes ocorridas através da *internet* e meios eletrônicos já encontram tipificação penal na lei. Entretanto, existem outras práticas delituosas que ainda necessitam ser previstas legalmente, visando cumprir um princípio constitucional de que "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal" (Constituição Federal do Brasil, 1988, art. 5º, XXXIX).

A Tecnologia de Informação (TI) tem propiciado facilidades e velocidade na busca de informação, mas também tem colaborado para o desenvolvimento de novas práticas delituosas. A *internet* revolucionou a comunicação mundial, mas também quebrou limites territoriais, os quais têm que ser obedecidos na cominação legal de um crime. Ou seja, na *internet* pode-se ter acesso a páginas do mundo todo, algumas

que incitam o racismo, por exemplo, mas tem a manifestação de pensamento nos meios de comunicação garantida pela lei em algumas nações. Neste ponto tem sido reforçada a importância de um Tribunal Penal Internacional como forma de atuar nos crimes que se dão além dos territórios de uma nação e tipificando os casos delituosos.

Um outro entrave no combate ao crime em informática é o da falta de divulgação. Algumas empresas que sofrem ações criminosas preferem absorver os prejuízos sem torná-los públicos. Os motivos principais são o medo da vulnerabilidade de seus sistemas e de novas investidas de *hackers* ou *crackers* e que a divulgação venha a afetar negativamente sua imagem e reputação no mercado.

Os ilícitos informáticos são diversos. Alguns, como afirmado anteriormente, já encontram previsão em lei. Contudo, de tempo em tempo surgem novos tipos de delitos, os quais talvez por ainda não encontrarem cominação legal, não o podem ser assim chamados, senão como condutas imorais, antiéticas e lesivas. Para citar alguns, independente da previsão em lei, temos: fraudes cometidas mediante manipulação de computadores, falsificações informáticas de dados e documentos, danos ou modificações de programas ou dados computadorizados (vírus, acesso não autorizado de *hackers*, etc.), espionagem industrial, sabotagem de sistemas, pesca ou averiguação de senhas, pornografia infantil, jogos de azar e lavagem de dinheiro (Furlaneto Neto / Guimarães, 2003, p. 70-71).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT) mantém uma estatística dos incidentes que lhe são reportados, divulgando-a periodicamente através de seu *site* na *internet*, a qual pode ser observada através da Tabela 1.

Tabela 1: Incidentes Reportados ao CERT.br

Ano	Incidentes	Worm (%)	Scan (%)	Fraude (%)	Outros (%)
2003	54607	*61*	*34*	*1*	*4*
2004	75722	*55*	*37*	*5*	*3*
2005	68000	*25*	*33*	*40*	*2*
2006	197892	*55*	*23*	*21*	*1*

Fonte: www.cert.br

Nota-se que no ano de 2005 e 2006 houve substancial aumento no número de incidentes reportados tipificados como fraude. Em 2005 o número de incidentes reportados em fraudes foi de 27292 e em 2006, 41776. Isto sem contar os casos de *scan* ou *phishing*, os quais são uma prática de encaminhamento de e-mail oferecendo promoções e vantagens, ou solicitando algum tipo de recadastramento. A isca para "pescar" os usuários são empresas conhecidas, como bancos, editoras de jornais e revistas, e lojas de comércio eletrônico.

Concentramo-nos neste trabalho nas fraudes eletrônicas, naquelas que tem se dado através da *internet,* em especial, pela atenção que têm recebido em todo o mundo.

Um conceito preliminar de fraude consta da Resolução CFC 820/97, a qual aprovou a NBC-T-11 que instituiu Normas de Auditoria Independente das Demonstrações Contábeis. A Norma dispõe que fraude é o ato intencional de omissão ou manipulação de transações, adulteração de documentos, registros e demonstrações contábeis. Em um ambiente informatizado, poderíamos presumir que tal ato é resultado de procedimentos e informações de pessoa jurídica ou física, que tem como finalidade alcançar benefício ou satisfação psicológica, financeira e material apropriada indevidamente de outra pessoa física ou jurídica, através de software e bancos de dados (Gil, 1999, p. 15).

Na proteção dos trabalhos de auditoria independente, a Norma ressalta que a descoberta de fraudes não constitui função do Auditor, embora deva planejar seus trabalhos com base nos riscos e possibilidade de sua ocorrência. Assim, detectar eventos fraudulentos é conseqüência dos exames.

3. OS AGENTES DA FRAUDE

As fraudes podem ser executadas por pessoas de fora da organização, que invadem um sistema ou por pessoas de dentro da organização, autorizadas a usar o sistema, porém fazendo mau uso dessa autorização (Turban; Mc Lean; Wetherbe, 2004, p. 543). As pessoas de fora que invadem um sistema podem também estar agindo através de conluio com outro pertencente à organização, o que potencializa a possibilidade de sucesso de um ataque fraudulento. Já quando a pessoa de fora da organização age sozinha, é necessário que tenha um forte conhecimento técnico de informática e da estrutura de montagem dos controles lógicos de determinada plataforma de informática. A ocorrência de fraudes em nível elevado afeta a qualidade organizacional, particularmente quando atingem consumidores dos produtos ou serviços da empresa.

Gil (1999, p.18-20) classifica as fraudes informatizadas quanto à sua formação:

- Fraudes de funcionários – É a de mais fácil detecção, de maior quantidade de ocorrências;
- Fraudes por quadrilha – É de difícil identificação e de ocorrência mais rara, geralmente causam grandes impactos na empresa;
- Fraudes de chefias – Geralmente acompanha o dolo praticado por executivos empresariais, causam elevados prejuízos às empresas e essas freqüentemente não punem os agentes fraudadores. Essas chefias sentem-se no direito de justificar seus atos ilícitos alegando desvios concretizados pelas organizações por ocasião de seus negócios.

4. O IMPACTO DA FRAUDE NO SETOR FINANCEIRO

Segundo Camargo (2004, p. 02) a auditoria de sistemas em "*e-business"* e fraudes eletrônicas é um dos maiores desafios da fiscalização do sistema financeiro. O aumento substancial das negociações via internet, conforme destacado pela pesquisa da Federação Brasileira dos Bancos (FEBRABAN), segundo a qual as transações por "*internet banking P.F.*" cresceram 450% entre 2000 e 2004, é a maior causa do crescimento deste tipo de auditoria. A instantaneidade dessas negociações via cartão de crédito impacta em maiores riscos de fraudes, pois muitas das vezes tais negociações são autorizadas sem a efetiva participação, ou seja, presença do cliente.

Investimentos em sistemas de controle para as áreas de auditoria interna, controle interno e gestão de riscos trarão soluções baseadas em regras e em análise do comportamento do cliente, seja pessoa física ou estabelecimento comercial conveniado e dos empregados da instituição financeira. A tecnologia deverá suportar sistemas não só para detecção de erros internos, mas também de riscos operacionais. Deverá também delinear padrões de operações suspeitas, ou seja cada incidente deverá ser investigado, denunciado e documentado em banco de dados.

Segundo pesquisas da FEBRABAN, em 2003 e 2004 foram investidos R$ 8,411 bilhões em Tecnologia da Informação pelas instituições financeiras. O valor investido é prova da importância que está sendo dada à segurança dos sistemas e transações eletrônicas como forma de minimizar o número de fraudes. Contudo, tal montante certamente não é tão expressivo se comparado às perdas prováveis que ocorreriam com ataques aos sistemas bancários desprotegidos e fraudes.

Em apenas um incidente em 1994, um *hacker* russo invadiu o sistema de transferência eletrônica de fundos do Citibank e furtou mais de 10 milhões de dólares, transferindo-os para várias contas espalhadas pelo mundo (Turban; Mc Lean; Wetherbe, 2004, p. 541). Considerando que o Citibank movimenta cerca de um trilhão de dólares por dia, pode-se imaginar como os prejuízos poderiam ter sido maiores caso não fossem tomadas medidas de segurança.

5. ESTRATÉGIAS DE DEFESA: COMO SE PROTEGER?

As estratégias de defesa são basicamente cinco: prevenção e detenção, detecção, limitação, recuperação e correção (Turban; Mc Lean; Wetherbe, 2004, p. 545-546).

A prevenção visa impedir os ataques de criminosos ao sistema. Ganha maior importância onde o potencial de dano é muito alto.

A detecção objetiva encontrar um dano causado por crimes o mais próximo de sua ocorrência, visando que seja logo combatido e os prejuízos menores.

A limitação é uma estratégia de redução de perdas tão logo ocorram problemas com o sistema, incluindo-se provisoriamente um sistema de tolerância às falhas até que tenha sido recuperado o sistema e sanada a falha de segurança.

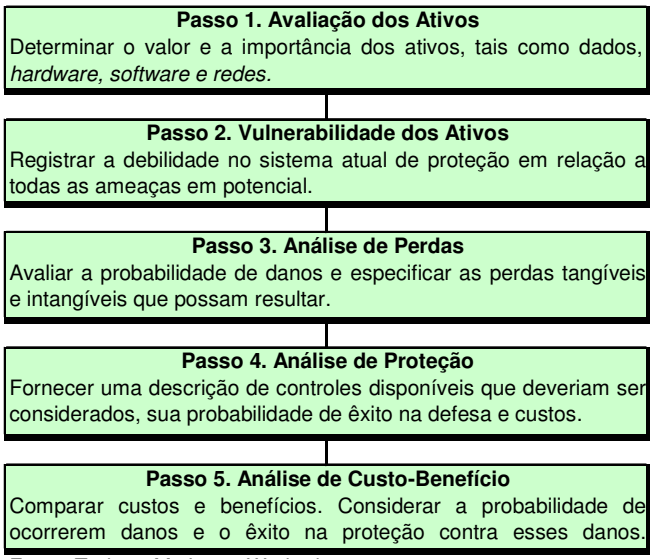
A recuperação visa à manutenção corretiva de um sistema de informação danificado, o mais rápido possível, e a correção, sanar as causas dos danos no sistema pela raiz do problema.

As estratégias de defesa não são excludentes entre si, ou seja, o uso de uma não descarta a possibilidade de uso de outra. Ao contrário, na maioria das vezes, grandes empresas investem concomitantemente em todos esses tipos de estratégias. Neste estudo focamos as duas primeiras estratégias mencionadas: prevenção e detecção.

6. A PREVENÇÃO DE FRAUDES

O processo de prevenção de fraudes está intrinsecamente relacionado ao risco de perdas. Uma análise de custo-benefício mensurando a probabilidade de danos e perdas prováveis que poderiam ser combatidas com a implantação de um sistema de prevenção de fraudes deve ser considerada. Na figura 1 apresentamos um resumo do processo de gerenciamento de risco para definição de investir-se em sistemas de prevenção de fraudes.

Figura 1: O Processo de Gerenciamento de Risco



Fonte: Turban; Mc Lean; Wetherbe, 2004, p. 555

Tomando o exemplo do sistema de prevenção de fraudes em cartões crédito, após observar que as fraudes vinham tomando maior vulto, os custos e prejuízos aumentavam, os usuários começavam a preferir deixar de usar o cartão de crédito por insegurança e medo e a imagem das organizações empresariais envolvidas ficavam desgastadas perante o público, muitas instituições passaram a desenvolver sistemas de prevenção de fraudes como forma de coibir danos.

Uma das ações tomadas pelas administradoras de cartão de crédito e que se encontra atualmente em uso, é a verificação, mediante autorização eletrônica, se o cartão é válido e possui fundos suficientes para que seja efetivada uma compra. Nesse processo avalia-se também se não há registros do cartão ter sido roubado ou "clonado".

Recentemente, no Reino Unido, foi desenvolvida uma tecnologia que utiliza *microchips* e *PIN (Personal Identification Number).* O *microchip* visa assegurar a validade do cartão e o *PIN* substitui a assinatura no ponto de venda. Esses procedimentos requereram instalação de equipamentos específicos nos pontos comerciais, mas ofereceram maior segurança contra fraudes.

Uma questão também enfrentada pelas administradoras de cartão de crédito foi quanto às transações realizadas pela *internet*, as quais encontravam-se desprovidas da segurança dos *microchips* e *PIN*, somente implantadas em pontos comerciais em que a pessoa está presente, de posse do cartão e o apresenta para concretizar a compra.

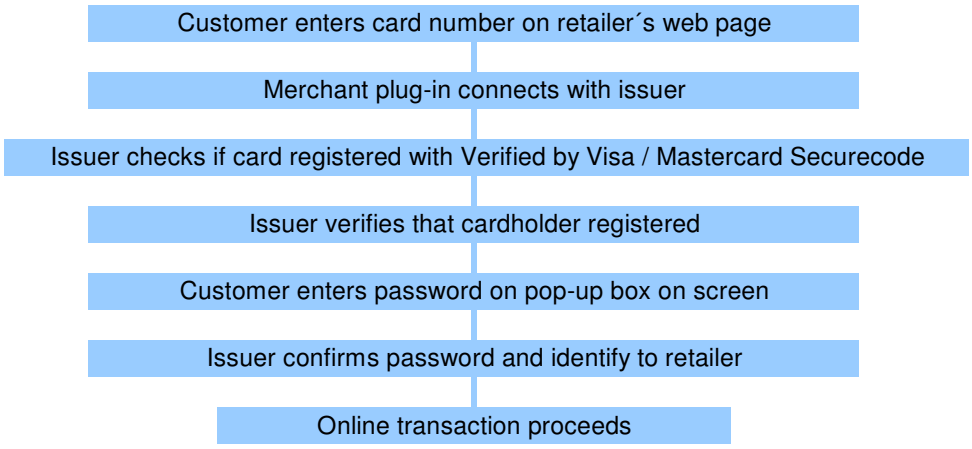
O Reino Unido e os EUA desenvolveram duas estratégias adicionais de prevenção a fraudes na *internet,* com parceria de instituições financeiras e administradoras de cartão de crédito: "*an adress verification service (AVS)"* e *"a card verification number (CVN)"*.

O AVS é um serviço de verificação de dados cadastrais dos portadores de cartões de crédito oferecido aos estabelecimentos comerciais. O AVS permite a verificação do endereço de entrega da fatura e do número do CPF do titular informados pela *internet* mediante uma verificação cruzada com os registros da administradora do cartão de crédito.

O CVN consiste em três ou quatro dígitos impressos no verso dos cartões de crédito. Estes dígitos têm sido solicitados em grande parte das compras pela internet como forma de confirmação de que a pessoa está em posse do cartão, evitando assim as fraudes ocorridas em que se conseguia um número de cartão de crédito através de salas de bate-papo, extratos, comprovantes de compra, etc.

Outra forma de prevenção a fraudes adotada pela Visa e Mastercard na Austrália foi "Verified by Visa" e "Mastercard Securecode". Essas estratégias aumentaram a segurança das transações comerciais virtuais quando permitiram à empresa vendedora realizar uma confirmação de dados do cliente diretamente a Visa ou Mastercard. A administradora do cartão de crédito é a que libera efetivamente a compra ao confirmar os dados do cliente em seus sistemas. A empresa vendedora apenas conclui o processo da venda. Na figura 2 apresentamos um resumo dos procedimentos.

Figura 2: Procedure of transactions involving Verified by Visa or Mastercard Securecode



Fonte: Visa (2004); Westpac (2003). In Charton / Taylor, 2004, p.15.

A Visa acredita que 80% dos custos com reembolsos aos vendedores virtuais por motivo de fraude hão de ser eliminados através desse sistema de verificação.

7. A DETECÇÃO DE FRAUDES

A estratégia de detecção de fraude se dá após a ocorrência do fato. O principal objetivo das empresas que investem nesse tipo de estratégia é estreitar o *gap* entre a ocorrência e a detecção da fraude, ou seja, reduzir o tempo de constatação da fraude, combatendo e corrigindo as falhas de controle e expurgando a possibilidade de novos prejuízos.

Em geral o sistema de detecção de fraudes busca acompanhar perfis de uso de determinado produto ou serviço, verificando aqueles que se afastam da normalidade.

Por exemplo, o uso de energia elétrica de determinado consumidor tende a manter um histórico padrão com pequenas variações. Variações excessivas indicam a possibilidade de fraude. A ocorrência de sinistro logo após a contratação de um seguro de alto valor e de risco muito elevado também é outro caso suspeito de fraude.

Para análise de uma gama muito extensa de dados, sistemas informatizados inteligentes têm sido desenvolvidos, a adoção de ferramentas e técnicas estatísticas têm se ampliado e o uso da técnica de inteligência competitiva "Mineração de Dados" (*Datamining*) tem se tornado diferencial na detecção de fraudes.

Datamining é a tarefa do estabelecimento de novos padrões de "conhecimento", geralmente imprevistos, partindo-se de uma massa de dados previamente coletada e preparada para este fim (Sulaiman & Souza, 2001, p.265-266). A Mineração de Dados busca associar fatos históricos que resultaram comprovadamente em fraudes, de forma que o sistema possa identificá-los imediatamente à ocorrência dos mesmos fatos, exigindo, em alguns casos, posterior confirmação da fraude.

O uso da técnica de *datamining* na detecção de fraudes em cartões de crédito é imprescindível na atualidade. Ao se realizar uma compra pela *internet*, por exemplo, tudo é muito simples para o comprador: "clica" aqui e ali, aguarda uns minutos e compra efetuada. Entretanto, por trás da simplicidade da transação esconde-se todo um sistema de segurança, inclusive quanto à possibilidade de fraudes. O sistema de detecção de fraudes manda alertas, por exemplo, se houver uma compra de diamantes às 4 horas da manhã ou se um usuário fez uso do cartão de crédito em curto intervalo de tempo em local distante um do outro.

Uma das mais novas tecnologias aplicadas na detecção de fraudes em cartões de crédito é a de Redes Neurais. As Redes Neurais Artificiais (RNA' s) se assemelham às estruturas neurais biológicas, pois tem capacidade computacional adquirida por meio de aprendizado e generalização. Como os tipos de golpes não são sempre os mesmos, ao contrário, modificam-se e aperfeiçoam-se diariamente, os sistemas convencionais tendem a não detectar uma fraude por não possuir capacidade de aprendizado automático. A Rede Neural Artificial é um sistema que utiliza técnicas de inteligência artificial para aprender novos padrões de fraude e conter novas tentativas de fraude sem intervenção humana (Trezub, 2004, p. 22).

Retornando ao caso dos cartões de crédito, em geral as pessoas costumam fazer uso do cartão de crédito dentro de um padrão bem definido. Ou seja, alguns o usam, por exemplo, somente para compras de mercado, combustível e vestuário. O sistema de redes neurais percebe quando há uso do cartão em padrões diferentes, neste caso exemplificado, em gastos excessivos com lazer e cultura.

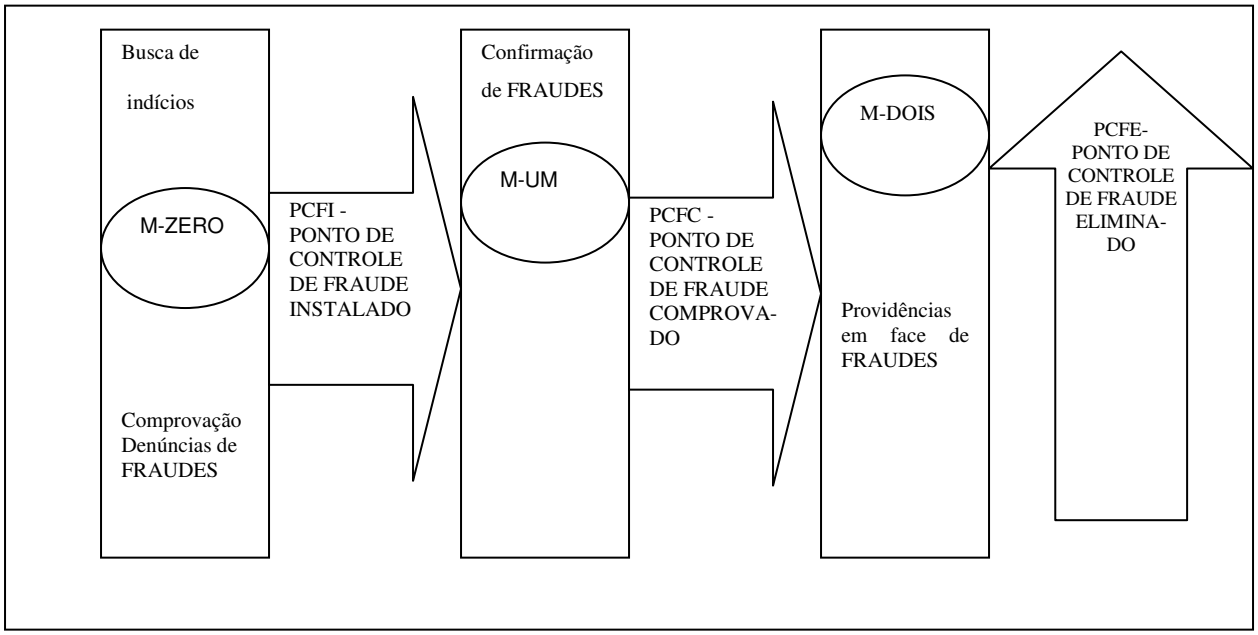
A detecção de fraudes passa por três momentos básicos. O ciclo de vida do ponto de controle de fraude (Gil, 1999, p.21) tem os seguintes momentos:

- Momento Zero: Busca de indícios/comprovação de denúncias;
- Momento Um: Confirmação da fraude;
- Momento Dois: Tomada de providências em face da existência de fraudes.

Para atuação no ciclo de vida da fraude é necessário ter profissionais com perfil técnico-operacional de tecnologia de informática, com profundo conhecimento do negócio e com experiência em fraudes para atuar em equipe de busca, comprovação ou eliminação de fraude.

Na figura 3, ilustramos o fluxo da estrutura dos três momentos do ciclo da fraude:

Figura 3: Ciclo de vida da fraude



Fonte: Gil, 1999, p. 22, adaptado com simplificações pelos autores.

Em geral os sistemas de detecção de fraude apontam o indício ou a suspeita dentro de um grau probabilístico. Esta exige confirmação e posterior eliminação.

8. COMENTÁRIOS FINAIS

Concluindo este estudo, pode-se denotar que o crescimento do comércio eletrônico tende a exigir mais e mais estudos e técnicas de combate à corrupção e fraudes realizadas através dos meios eletrônicos. Embora já se tenha caminhado bastante nas formas de prevenção e de detecção de fraudes eletrônicas e através da *internet*, muito ainda há que ser desenvolvido.

No que concluíamos esse artigo, lançamo-nos o seguinte questionamento: qual será o próximo tipo de fraude em cartões de crédito? Primeiramente imaginamos que tudo que uma pessoa precisa para uso de cartões de crédito através da internet são nome e endereço do titular do cartão, número do cartão e os números de verificação (*PIN*). Dessa forma, aquele que conseguir se apropriar dessas informações, sem que o titular do cartão perceba, terá grande chance de êxito na fraude. Qual não foi nossa surpresa ao tomar conhecimento de casos recentes em que alguém se dizendo representante da VISA ou outra administradora de cartão, com base no nome e endereço obtidos em listas telefônicas, realizava contatos telefônicos com

os titulares de cartões, com a história de que estavam investigando a possibilidade de fraude no cartão de crédito referente compras fictícias. Alguns, sem duvidar da idoneidade da pessoa, acabavam por informar os dados restantes que os fraudadores precisavam: número do cartão e *PIN*.

Nos casos de uso dos cartões para compras presenciais no comércio, nota-se que muitas lojas já possuem um equipamento específico de leitura magnética do cartão e autenticação da senha do titular. Neste caso, imaginamos a possibilidade futura de alguém conseguir através do mesmo equipamento realizar a cópia do cartão e guarda das senhas digitadas. Em caso recente apresentado no Programa Fantástico da Rede Globo (04/12/2005), a Polícia Federal prendeu uma quadrilha internacional de fraudadores que clonava cartões de crédito e de débito automático. Os fraudadores substituíam o equipamento por um outro igual, porém com um *chip* instalado que capturava os dados dos cartões e senhas, sem que o comerciante percebesse. Cada *chip* teria capacidade de armazenar os dados e senhas de 1,4 mil cartões. A estimativa de cartões e senhas que haviam sido capturados através deste mecanismo era de 20 mil.

O mundo é feito por pessoas, as quais pensam diariamente nas mais diferentes formas de enriquecimento material. Muitos não medem os meios para alcançar uma vida coberta de todos os tipos de bens que desejam, agindo de forma imoral, antiética e até mesmo ilícita e criminosa. O avanço do comércio virtual tende a elevar o número de fraudes eletrônicas e exigir crescimento proporcional na segurança da informação e do processamento de compras através da *internet* e meios eletrônicos.

Dificilmente se chegará um dia a expurgar todos os tipos de fraudes eletrônicas realizadas, mas espera-se estar preparado para combatê-las veemente de forma a não deixar que estas impeçam o crescimento econômico e o bem estar social, em que a disponibilidade de informação é peça chave.

9. REFERÊNCIAS

BRASIL, Constituição da República Federativa do. Disponível em: http://www.senado.gov.br/sf/legislacao/const/ . Acesso em: 16 nov 2005.

CAMARGO, Francisco. *Fraudes eletrônicas assustam setor financeiro*, Disponível em: http://webinsider.uol.com.br/imprimir.php?id=2045 . Acesso em: 16 nov 2005.

CARTILHA FEBRABAN – Você e seu Banco. 3 Ed. São Paulo: 2005. Disponível em: http://www.febraban.org.br/Arquivo/Cartilha/cartilhas.asp . Acesso em 25 nov 2005.

CHARLTON, Kate; TAYLOR, Natalie. *On line Credit Card Fraud Against Small Business.* Canberra, Australian Institute of Criminology: 2004. Disponível em: www.aic.gov.av/publications/rpp/60/section4.html . Acesso em: 25 nov 2005.

CONTABILIDADE, Resolução nº 820 de 17/12/1997 do Conselho Federal de. Disponível em: http://cfcspw.cfc.org.br/resolucoes_cfc/Res_820.DOC . Acesso em: 25 nov 2005.

ESTATÍSTICAS dos Incidentes Reportados ao CERT.br. Disponível em: http://www.cert.br/stats/incidentes/ . Acesso em 16 nov 2005.

FEBRABAN – Dados do Setor quanto Investimentos em Tecnologia da Informação (TI). Disponível em: http://www.febraban.org.br/Arquivo/Servicos/Dadosdosetor/tecnologia_2005_dadossetor.asp . Acesso em: 16 nov 2005.

FRAUDE. In: PRIBERAM DICIONÁRIO DA LÍNGUA PORTUGUESA ON LINE, 2005. Disponível em: http://www.priberam.pt/dlpo/dlpo.aspx . Acesso em: 16 nov 2005.

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. *Crimes na Internet: Elementos para uma Reflexão sobre a Ética Informacional*. **R. CEJ**, Brasília, n.20, p. 67-73, jan./mar. 2003. Disponível em: http://www.cjf.gov.br/revista/numero20/sumario.htm . Acesso em: 24 ago 2005.

GIL, Antonio de Loureiro. *Fraudes Informatizadas*. 2ª edição. São Paulo: Atlas, 1991.

NOVO golpe com cartão de crédito. Programa Fantástico da Rede Globo. 04 dez 2005. Disponível em: http://fantastico.globo.com/Jornalismo/Fantastico/0,,AA1084445-4005-0-0-04122005,00.html . Acesso em: 07 dez 2005.

PINHEIRO, Reginaldo César. *Os Crimes Virtuais na Esfera Jurídica Brasileira.* São Paulo: IBCCrim, v. 101, p. 18-19, abril 2001.

SULAIMAN, Alberto; SOUZA, Jano Moreira de. ***Data Mining*** *Mineração de Dados*. In: TARAPANOFF, Kira (org.). *Inteligência Organizacional e Competitiva.* Brasília: UnB, 2001. p. 265-278.

TREZUB, Maurício. *Guia de Prevenção à Fraudes – Ecommerce para Lojistas.* 2004. Disponível em: http://www.camara-e.net/seminario2005/images/novas/guia_fraudes.pdf . Acesso em: 25 nov 2005.

TURBAN, Efraim; McLEAN, Ephraim. WETHERBE, James. *Tecnologia da Informação para Gestão: Transformando os Negócios na Economia Digital*. 3ª. Ed. São Paulo: Bookman, 2004. Cap. 15, p. 532-563.