ISSN: 2175-1897

E-commerce - Principais modalidades praticadas e técnicas utilizadas para detecção e prevenção de Fraudes

RODRIGO FIGUEREDO DE ALMEIDA[1]
NAPOLEÃO GALEGALE[2]

Resumo – No e-commerce brasileiro em média 1,5% de todas as transações realizadas é de forma fraudulenta, o que ocasiona prejuízos à empresa, além das perdas relativas aos casos de suspeita de fraude que representam 4,6% dos casos gerando descarte de pedidos, incluindo neste montante, pedidos legítimos que poderiam vir a gerar receita a instituição. Soma-se a isto o fato de 31% das transações passarem por revisão manual o que aumenta o custo operacional e reduz a margem de lucro da empresa. O presente artigo analisa as principais modalidades de fraude no e-commerce brasileiro, bem como as técnicas de prevenção e detecção de fraudes, através de dados bibliográficos e pesquisa em organizações governamentais e não governamentais.

Palavras-chave: Fraude, e-commerce, detecção de fraude, prevenção fraude.

Abstract - On Brazilian e-commerce occurs fraud on average 1.5% of all transactions that causes financial loss to the company, in addition occurs losses related to cases of fraud suspected that represents 4.6% of the cases, generating discard orders that includes legitimate customer purchases that could generate revenue to the company. Add to this the fact that 31% of transactions are done through manual review that increases the operating costs and reduces the profit margin of the company. The article will analyze the most common fraud modalities on Brazilian e-commerce, as well the most popular techniques of detection, using for this a bibliographic data and research on governmental and non-governmental organizations.

Keywords: Fraud, e-commerce, fraud detection, fraud preventing.

[1] Centro Paula Souza – São Paulo – Brasil / e-mail: rodrigof.almeida@gmail.com
[2] Centro Paula Souza – São Paulo – Brasil / e-mail: nvg@galegale.com.br

1. Introdução

Com o advento dos avanços tecnológicos e o fomento na quantidade de serviços bancários prestados aos clientes, bem como com o surgimento de fontes alternativas para a execução de pagamentos e o incremento dos canais eletrônicos, trouxe consigo uma infinidade de benefícios para os clientes e para as próprias instituições bancarias, mas ao mesmo tempo trouxe consigo preocupações no que concerne à segurança destes canais, visto que estes canais são fontes frequentes de ataques de quadrilhas fraudadoras, o que obriga as instituições financeiras a investir cada vez mais para que sejam disponibilizados serviços eletrônicos mais seguros e robustos, devido aos grandes valores transacionados e os riscos inerentes às operações financeiras.

Neste cenário a internet se tornou um espaço fértil para a ação de fraudadores, que utilizam as mais diversas formas para burlar a segurança destas instituições, ocasionado prejuízos e impactando os seus resultados financeiros.

Desta forma se faz cada vez mais necessário à utilização de técnicas que permitam a obtenção de conhecimento através da análise de bases, bem como as transações realizadas de forma online, com o intuito de detectar movimentos suspeitos que indiquem fraudes e desta maneira se possa tomar uma ação preventiva a fim de mitiga-la.

De acordo com a pesquisa realizada pelo Serasa Experian as perdas decorrentes das fraudes em transações financeiras no Brasil no ano de 2013 foram de dois bilhões e trezentos milhões de reais, dos quais, um bilhão e duzentos milhões de reais foram decorrentes de fraudes off-line oriundas do roubo de identidade, 500 milhões de reais foram decorrentes de perdas do comercio eletrônico e 600 milhões de reais foram perdidos via movimentação bancaria através do internet banking.

De acordo com os dados desta pesquisa cerca de 30% dos usuários de cartão de credito já tiveram algum tipo de problema relacionando a fraudes no Brasil, o que coloca o Brasil torna em termos percentuais no quinto lugar do ranking mundial ficando atrás apenas de países como os Estados Unidos e México com 37%, Emirados Árabes com aproximadamente 33% dos usuários e Reino único com 31%, sendo a decorrência destes golpes em grande parte ocasionados durante a compra de produtos eletrônicos (ROSA, 2014).

O objetivo deste estudo é identificar as principais modalidades de fraude existentes no e-commerce e quais as principais técnicas utilizadas para a detecção e prevenção de possíveis fraudes.

2. Referencial Teórico

2.1 Principais modalidades de fraudes praticadas no e-commerce

Ao longo dos anos foram desenvolvidas diversas modalidades de fraudes com o intuito de obter vantagem de forma ilícita prejudicando tanto clientes, como varejistas do setor.

O roubo de dados é uma das modalidades mais conhecidas e tem por objetivo obter dados que permitam a autenticação do cliente em um determinado site, onde o fraudador se passa pela vítima do golpe. O roubo destes dados pode ocorrer através da captura via teclado, telas falsas, e-mails com links para páginas falsas dentre outras técnicas.

O roubo de sessão ocorre em sites aonde a simples captura de dados de autenticação não é o suficiente, visto que o site gera senhas diferentes a cada autenticação. Neste caso o fraudador opta por esperar o cliente realizar a transação e então captura a senha para utilizar naquele momento e cometer a fraude.

Na técnica de modificação de transação o ataque ocorre de forma on-line na máquina da vítima, aonde um aplicativo malicioso instalado localmente fica aguardando o cliente realizar uma transação, desta forma o aplicativo poderia modificar os dados da transação, adulterando os dados originais.

Man-in-the-middle é uma técnica que caracteriza-se pela interceptação de dados durante o trafego entre o site de e-commerce e o cliente. Nesta modalidade de ataque o fraudador consegue modificar as informações trocadas entre o site e o cliente (WONGTSCHOWSKI, 2011).

Segundo a BOA VISTA SCPC (2013) existe três modalidades principais de fraudes cometidas com o cartão de credito.

A primeira refere-se à fraude efetiva que é caracterizada pelo roubo dos dados do cliente por parte do fraudador que efetua a compra no site. Quando o titular do cartão recebe a fatura e comunica a operadora de cartão de credito que não reconhece a compra é efetuado o *chargeback,* que é o estorno do valor debitado do cliente que teve seus dados fraudados. Ocasionando prejuízo ao varejista.

A segunda modalidade é conhecida como auto fraude, no qual o verdadeiro titular do cartão informa não reconhecer à compra para exigir estorno da fatura. Esta pratica é de difícil monitoramento por parte do e-commerce e geralmente só ocorre quando este tipo de cliente tenta repetir a estratégia.

A terceira modalidade é a fraude amiga, no qual a compra é efetuada por alguém próximo ao titular do cartão, como filhos ou esposa, por exemplo, que possuem todos s seus dados. Neste caso o titular por desconhecer a compra

acaba solicitando o estorno do valor. Muitos dos casos, porém, ao ser contato pela loja virtual acaba reconhecendo a compra.

2.2 Técnicas de prevenção de fraude

Em um ambiente altamente competitivo como o e-commerce qualquer tipo de fraude pode vir a se tornar um problema crítico ao negócio. Neste cenário a prevenção e detecção de fraudes se tornaram uma das prioridades e a utilização de aplicações como KDD e Data Mining uma solução.

Devido à imprevisibilidade sobre a legitimidade das transações ocorridas no mercado como operações de e-commerce, pagamentos com cartões de credito, transações via smartphones, entre outras operações, umas das maneiras mais eficazes e de menor custo é buscar evidencias destas fraudes é através dos dados disponíveis, utilizando para isto algoritmos matemáticos que identifiquem estes padrões, sendo o motor destas soluções diversas técnicas como redes neurais, algoritmos genéticos, econometria, reconhecimento de padrões estatísticos entre outros.

O KDD (Knowledge Discovery in Data bases) que é a descoberta de conhecimento em base de dados pode fornecer subsídios para o processo de detecção e prevenção de fraudes, além de fornecer parâmetros comportamentais dos fraudadores a fim de aumentar a acuracidade das previsões em relação à detecção de novas fraudes.

A detecção de fraudes em cartão de crédito utilizando *data mining* apresenta uma série de desafios, pois primeiramente existem milhões de transações no cartão de crédito que são processadas a cada dia. Para trabalhar com estas quantidades de dados é necessário o uso de técnicas eficientes e de baixo custo para poder operar em escala. Em segundo lugar é necessário se atendar ao fato que os dados são altamente enviesados, visto que a maioria das transações são legitimas e apenas uma minoria é de fraude, aonde o uso de técnicas inadequadas pode deixar de detectar adequadamente um caso de fraude e em terceiro lugar cada transação possui um valor diferenciado e com potencial de perda diferenciado aonde um único caso de fraude não detectado pode gerar prejuízos superiores a dezenas de outros casos (CHAN et al, 1999).

Na maioria dos cenários de detecção de fraudes existentes nas empresas, a escolha do modelo de *data mining e* das técnicas de detecção de fraude ocorre por questões praticas de requisitos operacionais, limitações de recursos e do modelo de gestão de fraudes ao invés do melhor modelo matemático (Phua et al, 2010).

3. Método

A realização deste estudo será efetuada a partir do levantamento da literatura já existente. Serão realizadas pesquisas bibliográficas e documentais para a obtenção dos dados. Aos dados bibliográficos serão agregadas informações obtidas em sites na internet, pertencentes a organizações governamentais e não governamentais que divulgam dados e textos relativos ao tema abordado na pesquisa, bem como base de dados econômicos.

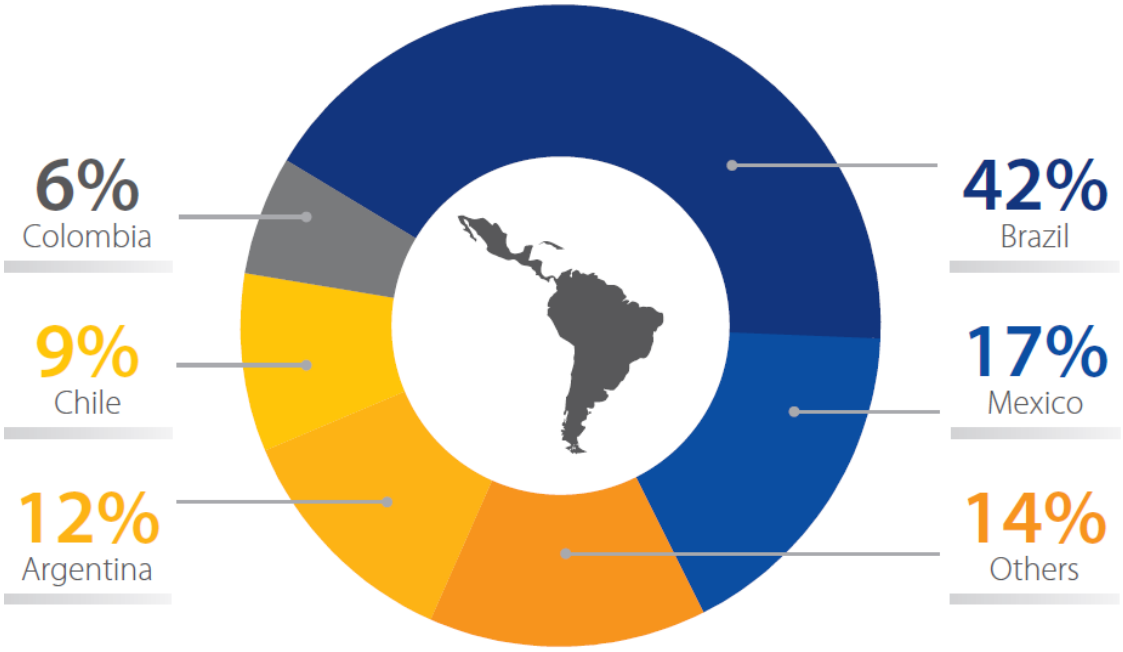
4. Resultados e Discussão

4.1 Fraudes e-commerce na América Latina

Segundo a empresa Cybersource que atua no mercado de pagamento on-line para empresas de e-commerce, além de desenvolver ferramentas de prevenção à fraude e que conta com aproximadamente 60 bilhões de transações por ano (CIELO, 2012), estima que o e-commerce na América Latina deverá até o final do ano de 2016 alcançar cerca de 66,7 bilhões de dólares em volume de vendas (EINSTITUTO, 2016) ante os 59,1 bilhões de dólares do ano anterior (EINSTITUTO, 2015).

Deste valor o Brasil deverá transacionar aproximadamente 42% conforme ilustra a figura 1.

Figura 1 - Distribuição do e-commerce na América Latina.



Fonte: EINSTITUTO (2016)

A empresa Cybersource realizou um estudo com 203 empresas entre clientes e não clientes que tinham por característica uma forte política de gerenciamento de fraudes no e-commerce. Estas empresas juntas transacionaram no ano de 2014 cerca de 25 bilhões de dólares. Este estudo teve por objetivo analisar as tendências e práticas do gerenciamento e proteção contra fraudes ocorridas em pequenas, médias e grandes empresas.

De acordo com a Cybersource a automação é essencial para que as empresas possam gerenciar a fraude de forma mais eficiente, pois processos que envolvam revisão manual, mesmo que para um pequeno número de pedidos gera um custo significativo, além de dispender muito tempo.

De acordo com a pesquisa as empresas latino-americanas estão utilizando largamente a revisão manual, chegando em média a 31% dos casos, sendo que esta proporção se manteve praticamente inalterada em relação ao estudo do ano anterior e cerca de 86% das empresas ainda utilizam revisão manual (EINSTITUTO, 2015). No ano de 2015, este numero teve uma leve redução e caiu para 83% dos casos (EINSTITUTO, 2016).

O estudo identificou que os comerciantes da América Latina têm dificuldade de mensurar de forma adequada o desempenho de suas estratégias de gerenciamento antifraude e cerca de 40% não são capazes de efetuar a medição, o que acaba gerando altas taxas de chargeback, que é o estorno do valor debitado do cliente que teve seus dados fraudados.

Sem poder mensurar de forma adequada os comércios da América Latina têm dificuldade de aperfeiçoar os seus processos de detecção e prevenção de possíveis fraudes.

As taxas observadas entre os participantes foram em média 1,4% o que representa mais que o dobro do percentual se for comparada com países como os Estados Unidos e o Canada que apresentam média de 0,6% de taxa de chargeback. No Brasil está média foi de 1,6% no ano de 2014(EINSTITUTO, 2015) e teve uma leve redução para 1,5% dos casos no ano de 2015 (EINSTITUTO, 2016).

Outro fator importante a ser analisado é a taxa de rejeição de pedidos que fornece um bom indicar dos pedidos que as empresas consideram suspeitos durante o processo de triagem. Este número indica a quantidade de fraudes que podem ter sido evitadas, mas também engloba pedidos genuínos que foram cancelados.

Na América Latina este índice também é elevado se comparado o Canada e aos Estados unidos, chegando a 8% dos pedidos, enquanto os Estados Unidos e o Canada têm como média 2,8%. No Brasil esta média é de 4,6% (EINSTITUTO, 2016).

As empresas ao desenvolverem processos mais eficientes de gerenciamento de fraude poderão aceitar um maior número de pedidos genuínos e ao mesmo tempo minimizar os custos decorrentes de fraudes e de revisão manual, reduzindo desta forma custos e aumentando a lucratividade.

4.2 O Cenário da fraude no e-commerce no Brasil

De acordo com a empresa ClearSale especializada em soluções antifraude e que tem aproximadamente 80% do e-commerce varejista brasileiro utilizando os seus sistemas, apontou em seu mapa de fraudes no ano de 2014 um crescimento nos índices relativos a tentativas de fraudes, destacando o Norte e o Nordeste de forma negativa. Segundo os estudos o Brasil teve uma média de 3,98% de tentativas de fraudes nas transações oriundas do e-commerce, ou seja, a cada R$ 100,00 movimentados no comercio eletrônico, cerca de R$ 3,98 são referentes a tentativas de fraude ou oriundos de compras ilegais.

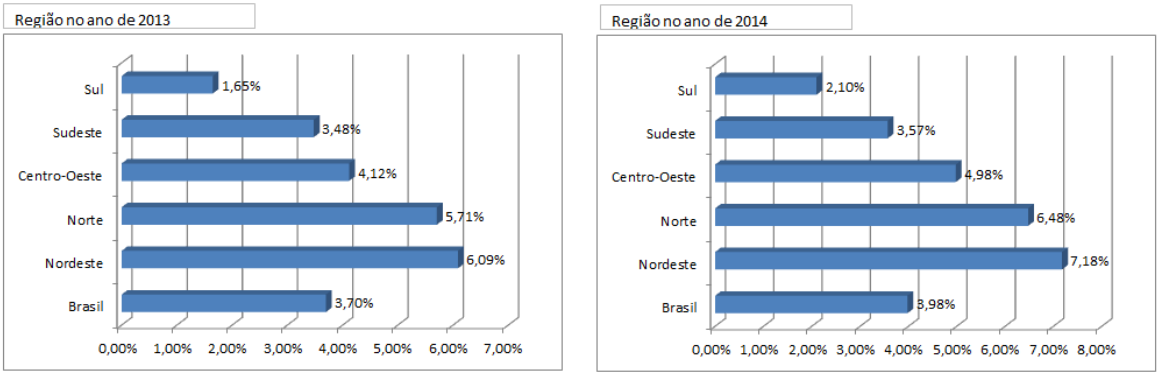
Ao segmentar por região pode-se verificar que a região sul foi a que se mostrou mais segura, com um índice de 2,1% de tentativas de fraude enquanto a região sudeste apresentou um índice de 3,57% e o centro-oeste apresentou um índice de 4,98%. Como destaque negativo teve-se a região nordeste com 7,18% das tentativas e a região norte com 6,48% das tentativas (VIEIRA, 2015).

Ao comparar os mesmos dados com o ano anterior pode-se perceber que as regiões continuaram nas mesmas posições, mas houve um incremento nos índices do ano de 2013 para o ano de 2014, sendo que a região nordeste foi à

região que apresentou o maior incremento, indo de 6,09% para 7,18% e a região sudeste foi a que teve o menor incremento indo de 3,48% para 3,57%.

Na figura 2 é possível ver o comparativo dos dois anos.

Figura 2 – Comparativo dos dois anos.



Fonte: Adaptado de VIEIRA, L (2015)

De acordo com a ClearSale as altas tentativas de fraudes em algumas regiões podem ser decorrentes da recente alta na oferta de crédito para a população local, principalmente via cartão de credito o que é corroborado pelo crescimento do acesso à internet na região. Este comportamento ocorre, sobretudo em itens que possuem alto fluxo de revenda, como smartphones, por exemplo, (VIEIRA, 2015).

Segundo o SERASA (2015), os fraudadores que atuam em sites de e-commerce com dados de cartões de credito de terceiros optam por agir com mais frequência durante a madrugada. A conclusão deste estudo do Serasa Experian remete ao período de novembro de 2014 a janeiro de 2015, sendo que a maioria destas fraudes ocorre no período da 1 hora da madrugada até às 5 horas, sendo que são registradas mais tentativas de golpes durante as quintas-feiras.

O Serasa Experian estima que a maioria das lojas virtuais que atuam no território brasileiro e fecham suas operações tem como principais motivos os prejuízos decorrentes de fraudes, visto que para este tipo de golpe não é necessário apresentar fisicamente o cartão de credito, bastando o número do cartão, data de validade e código de segurança. A loja por não possuir informações relativas a irregularidades como roubo, perda ou notificação do cliente reportando o desconhecimento daquela compra em eu cartão de credito acaba providencia a entrega da mercadoria para o suposto cliente. Este tipo de problema se agrava pelo fato da maioria dos detentores de cartão de credito não acompanhar diariamente a sua fatura de cartão de crédito, conferindo estes valores apenas perto do período de fechamento da fatura, que ocasiona a ligação para a operadora de cartão de credito informando o desconhecimento da compra somente após a entrega da mercadoria para o fraudador. Ao ser acionada pelo cliente a administradora do cartão de credito providenciará o

cancelamento do crédito a loja, este procedimento é conhecido como chargeback (SERASA, 2015).

5. Considerações finais

As perdas financeiras decorrentes das fraudes oneram enormemente o e-commerce no Brasil, com uma média de 1,5% de chargeback que são relativos a fraudes realmente efetuadas e cerca de 4,6% de transações que são rejeitadas por suspeita de fraudes ocasionando perda de vendas que poderiam ser genuínas, somando-se a isto os altos custos decorrentes de revisão manual que chegam em média a 31% dos casos o que faz com que a margem de lucro destas empresas seja comprometida e muito provavelmente que o preço final seja repassado aos consumidores finais.

As empresas brasileiras necessitam fomentar os seus processos de detecção de fraudes a fim de reduzir os seus índices para níveis semelhantes a empresas americanas e canadenses que apresentam taxas de chargeback próximos a 0,6%.

Para isto é necessário que as empresas revisem os seus processos e invistam em tecnologias que propiciem a detecção de padrões de comportamento, utilizando para isto, por exemplo, algoritmos matemáticos que auxiliem na identificação destes padrões e que façam uso de soluções como técnicas de redes neurais, algoritmos genéticos, econometria, *data mining*, reconhecimento de padrões estatísticos entre outros.

Outro ponto importante é não permitir que as técnicas de prevenção de fraudes afetem o conforto do usuário ou dificulte a compra o que poderia ser danoso ao site de e-commerce e prejudicar as vendas.

Referências

BOA VISTA SCPC: **Fraudes com cartões de crédito. Quem é o responsável?.** Reportagem [05/11/2013]. BOA VISTA SCPC. Disponível em: http://www.boavistaservicos.com.br/pme/seguranca-e-fraude/fraudes-com-cartoes-de-credito-quem-e-o-responsavel. Acesso em 14/11/2015.

BOENTE, A. N. P.; OLIVEIRA, F. S. G.; ROSA, J. L. A. **Utilização de Ferramenta de KDD para Integração de Aprendizagem e Tecnologia em Busca da Gestão Estratégica do Conhecimento na Empresa.** Anais do Simpósio de Excelência em Gestão e Tecnologia, v. 1, p. 123-132, 2007.

CHAN, Philip K. et al. **Distributed data mining in credit card fraud detection.** IEEE Intelligent Systems and Their Applications, v. 14, n. 6, p. 67-74, 1999.

CIELO: **Cielo e Cybersource anunciam aliança estratégica e trazem solução global de prevenção à fraude em comércio eletrônico para os lojistas brasileiros**. Reportagem [20/03/2012]. Cielo. Disponível em: https://www.cielo.com.br/portal/cielo/cielo-e-cybersource-anunciam-alianca-estrategica.html. Acesso em 08/11/2015.

EINSTITUTO: **Relatório de fraude On-Line 2015 – América Latina**. Instituto Latino-americano de Comercio Eletrônico. Disponível em: http://www.cybersource.com/content/dam/cybersource/pt_LAC/documents/2015-OnlineFraudReport.pdf?utm_campaign=2015%2520LAC%2520Fraud%2520Report%2520Auto%2520Responder%2520-%2520Portuguese&utm_medium=email&utm_source=Eloqua. Acesso em 14/09/2015.

EINSTITUTO: **Online Fraud Report - 2016 Latin America**. Instituto Latino-americano de Comercio Eletrônico. Disponível em: http://www.cybersource.com/content/dam/cybersource/en-LAC/documents/Online_Fraud_Report_2016.pdf?utm_campaign=LAC%202016%20Fraud%20Report%20Auto%20Responder%20-%20English&utm_medium=email&utm_source=Eloqua . Acesso em 25/08/2016.

GOLDSCHMIDT, R.R.; PASSOS, E. **Data Mining: Um Guia Prático**. Rio de Janeiro: Campus, 2005.

NASCIMENTO, Auster M.; REGINATO, Luciane**. Um estudo de caso envolvendo business intelligence como instrumento de apoio à controladoria.** Revista Contabilidade & Finanças, v. 18, p. 69-83, 2007.

PHUA, Clifton et al. **A comprehensive survey of data mining-based fraud detection research.** arXiv preprint arXiv:1009.6119, 2010.

ROSA**,** J.L: **Brasil perde R$ 2,3 bi com fraudes em transações financeiras em 2013**. Reportagem [01/04/2014]. Valor Econômico. Disponível em: http://www.valor.com.br/financas/3502148/brasil-perde-r-23-bi-com-fraudes-em-transacoes-financeiras-em-2013. Acesso em 08/11/2015.

SERASA: **Maioria das fraudes no e-commerce acontece nas madrugadas de quinta**. Reportagem [12/03/2015]. SERASA EXPERIAN. Disponível em: http://noticias.serasaexperian.com.br/maioria-das-fraudes-no-e-commerce-acontece-na-madrugada-de-quinta-feira-revela-estudo-da-serasa-experian. Acesso em 08/11/2015.

THOMÉ, A. C. G. **Redes neurais: uma ferramenta para KDD e data mining**. Disponível em http://equipe.nce.ufrj.br/thome/grad/nn/mat_didatico/apostila_kdd_mbi.pdf. Acesso em 07/11/2015.

VIEIRA**,** L: **ClearSale divulga mapa de tentativas de fraude pela internet**. Reportagem [30/04/2015]. ClearSale. Disponível em: http://portal.clearsale.com.br/novidades/ClearSale-divulga-mapa-de-tentativas-de-fraude. Acesso em 08/11/2015.

WONGTSCHOWSKI, Arthur. **Segurança em Aplicações Transacionais na Internet: O Elo Mais Fraco**. Disponível em: <http://www.teses.usp.br/teses/disponiveis/3/3141/tde-05092006-175654/en.php>. Acesso em 10/11/2015.