



Lojas virtuais que vendem

Manual Anti-Fraude para Comércio Eletrônico

O objetivo deste tutorial é minimizar o risco de perdas financeiras nas lojas virtuais devido ao chargeback.

Explicaremos o seu conceito, as formas que ocorrem e quais soluções podem ser utilizadas na gestão de risco de sua loja virtual.

Sumário

1	<i>Fraudes em vendas com cartão de crédito</i>	1
	Fraudes	1
	Prevenção à fraudes	1
	O temido chargeback	2
	Tipos de fraudes com cartão de crédito	2
	Fraude efetiva:	2
	Auto-fraude:	2
	Fraude amigável:	2
	Desacordo comercial:	2
	Administradora de Cartão de Crédito	3
	Erros que podem ocorrer na liberação automática ou manual	3
	Intermediadores de Transações on-line	3
	Como funciona	3
2	<i>Técnicas comuns de roubo de cartões</i>	4
	Roubos de cartões off-line para uso on-line	4
	Falsa Identidade	4
3	<i>Técnicas de proteção dos dados dos clientes no FastCommerce</i>	4
	Segurança	4
	Segurança no tráfego de informações	4
	Segurança na administração do site.	5
	Segurança no armazenamento de dados	5
	Segurança na análise de crédito a clientes	5
	Segurança física das informações	6
	InfoRisk - Para auxiliar no combate a fraudes e diminuir a inadimplência	6
4	<i>Solução para gestão de risco</i>	7
	Autorização on-line	7
	Como resolver esta questão?	7
	Ferramenta ClearSale	7
	Autenticação do bom cliente	8
	Sobre a ClearSale	9
	Sobre o FastCommerce.	9
	Fontes de pesquisa	9

1 Fraudes em vendas com cartão de crédito

Fraudes

Com o aumento do interesse por parte dos consumidores nas transações virtuais e a crescente diversidade na oferta de produtos na web, o comércio eletrônico convive, na mesma medida, com a intensificação do emprego de táticas sofisticadas de fraudes praticadas pelos ciber-criminosos. O tema desperta cada vez mais a atenção dos varejistas eletrônicos que investem em segurança da informação.

Prevenção à fraudes

Entre as ferramentas de defesa mais adotadas pelos varejistas virtuais estão a validação de código de segurança dos cartões de crédito; o rastreamento do dispositivo de compra (IP); e o registro de dados de clientes com informações das últimas compras.

Todas essas informações auxiliam no controle de pedidos feitos no comércio eletrônico, mas mesmo assim, não existe uma ferramenta única de prevenção de fraudes. A principal questão, além de identificar a compra ilegítima, é ser assertivo para oferecer uma liberação rápida para o bom cliente. A ClearSale oferece soluções de Gestão de Risco para prevenção de perdas. É um sistema de gestão que contém 100% das informações dos clientes, onde as empresas configuram regras dos pedidos, revisando cada solicitação de compra para definir se ela será aceita ou rejeitada.

Essa gestão é de extrema importância para as empresas de e-commerce, no sentido de não afastar o bom cliente e para saber identificar se determinada transação está sendo feita pelo seu cliente ou por um criminoso.

Quando um pedido é enviado para a central e contém informações duvidosas, imediatamente ele é submetido a um procedimento de confirmação de dados para que a transação seja efetivada. Nunca se nega uma transação, mas se ela for suspeita, passa para uma central de análise manual.

O bom funcionamento do Comércio Eletrônico depende da constante busca das empresas por soluções de segurança, além de guardar todas as informações dos clientes, para que na hora da compra o sistema possa autenticar a transação e de fato saber que ela está sendo efetuada pelo verdadeiro usuário.

Não existe 0% de fraude, até porque, se isso acontecer, significa que a empresa não está vendendo. Enquanto houver Comércio Eletrônico, será preciso lidar com a fraude, e que as empresas precisam saber administrar sua rede utilizando as ferramentas que a tecnologia disponibiliza, protegendo assim o bom cliente.

O mais importante é saber com quem estamos lidando, quem são nossos clientes e autenticar essas transações. Não há um sistema perfeito para acabar com a fraude. Os criminosos são talentosos e estão cada vez mais imersos na tecnologia e muitas vezes, sabem mais do que nós.

O temido chargeback

No comércio eletrônico há a necessidade de saber se o comprador virtual é ele mesmo. A inibição das fraudes é fundamental para assegurar a saúde financeira da loja virtual, uma vez que parte dos prejuízos causados por fraudadores recai sobre o lojista.

Chargeback (que em português significa “estorno”) é o cancelamento feito pela administradora do cartão de uma venda feita com cartão de débito ou crédito, que pode acontecer pelo não reconhecimento da compra por parte do titular do cartão ou pode se dar pelo fato da transação não obedecer às regulamentações previstas no Contrato de Credenciamento e Adesão de Estabelecimentos. O chargeback pode ocorrer devido aos seguintes tipos de fraude: Fraude Efetiva, Auto-fraude, Fraude Amigável e Desacordo Comercial.

Tipos de fraudes com cartão de crédito

Fraude efetiva:

1. Primeiramente o falsário entra no site da loja e efetua uma compra com dados roubados.
2. Depois a administradora de cartões de crédito em contato com o banco emissor, aprova operação baseado no limite do cartão e na validade do mesmo.
3. É dado início ao processo de logística.
4. A entrega é efetuada ao falsário.
5. Ao ver a fatura de seu cartão de crédito o verdadeiro dono do cartão não reconhece a compra, gerando então o chargeback.
6. A administradora do cartão de crédito informa através de carta ao lojista o ocorrido.
7. O lojista fica com todo o prejuízo financeiro da transação.

Auto-fraude:

O verdadeiro dono do cartão usa de má fé, para realizar a compra e depois não reconhecê-la. É um tipo difícil de ser detectado pelo analista, porém com boas possibilidades de recuperação.

Fraude amigável:

É aquela em que não é o dono do cartão que faz a compra e sim uma pessoa próxima a ele como filho, esposa, amante ou familiar. Não existe má fé neste caso, porém o dono do cartão não reconhece a compra, pois não sabe ou não se lembra de tê-la feito.

Desacordo comercial:

Engloba todas as situações não contempladas pelos status anteriores. Exemplo: quando a expectativa do cliente não é atendida pelo produto final, quando há duplicidade de pedidos e também quando a grafia do nome da loja que ele encontra na fatura do cartão de crédito não é reconhecida por ele como a loja na qual ele efetuou a compra.

Administradora de Cartão de Crédito

A responsabilidade da concessão de crédito é das administradoras de cartão. Se a compra em uma loja física é paga com um cartão de crédito, o lojista certamente receberá o valor correspondente, já que uma das obrigações do lojista é colher assinatura do cliente e verificar o documento de identidade do portador.

Nas transações on-line ou Televendas com cartão de crédito, as administradoras partem do princípio de que, não há como o lojista provar que quem está efetuando a compra é realmente o portador do cartão. Por isso, caso o proprietário do cartão não reconheça alguma transação em sua fatura, ele pode solicitar o estorno.

Como a venda não é presencial, a administradora transfere o estorno para o estabelecimento que processou a venda.

Erros que podem ocorrer na liberação automática ou manual

Podem ocorrer alguns erros nas situações em que um pedido é liberado automaticamente ou é analisado manualmente. Na análise manual, existem algumas situações que fogem do ideal para a loja:

- Se ocorrer Aprovação indevida, provavelmente acontecerá o chargeback.
- Se há Demora na decisão, gera-se impacto negativo no cliente na ponta.
- Se há uma Suspensão indevida, teremos um cliente bom que foi impedido de comprar. Se você analista suspender indevidamente, será somente através dos critérios da auditoria que perceberemos falhas em sua autenticação ou pior, pela reclamação do próprio cliente junto ao lojista. Lembre-se: um cliente bom negado dificilmente volta a comprar naquele estabelecimento. Todos perdem!
- Cancelamento pelo cliente: O contato telefônico do analista com o cliente é muitas vezes o único contato do cliente com a loja, desde que fez sua compra pela internet ele pode aproveitá-lo para efetuar um cancelamento que não faria se não tivesse sido contactado. Portanto, quanto menor o número de cancelamentos, melhor terá sido a abordagem e condução da conversa entre você analista e o cliente.
- Na Liberação automática pode gerar somente um possível erro, muito fácil de mensurar: a aprovação indevida, ou seja, o índice de chargebacks é o único freio para a liberação automática.

Intermediadores de Transações on-line

No Brasil PagSeguro, PayPal, MoIP e MercadoPago possuem integração com os seguintes meios de pagamentos: cartões de crédito Visa, American Express, Diners, MasterCard, Aura e HiperCard e boleto bancário, entre outros.

Uma das grandes vantagens de utilizar o Intermediador de transação online é garantir, que o lojista fique livre do chargeback, algo potencialmente perigoso para quem vende online.

Se você quer profissionalizar a análise de risco e aprovação de vendas com cartão de crédito, pode criar uma conta em um ou mais destes serviços e automatizar todo o processo, sem precisar de contrato com as administradoras de Cartão. Dessa forma, você fica totalmente protegido de fraudes na Internet, dispensando a necessidade de contratar cada operadora ou banco individualmente.

Como funciona

Ao receber um pedido com status “Aprovado”, o vendedor terá certeza que o Intermediador de transação online analisou e aprovou a transação. É o sinal verde para liberar o serviço ou entregar o produto vendido.

Se estiver tudo de acordo com os termos da compra, o vendedor deve apenas aguardar a liberação de seu pagamento.

Seus clientes pagam com parcelamento no cartão de crédito e você recebe à vista, as taxas de parcelamento são cobradas do comprador.

Esse processo visa aumentar a confiança do comprador, e com isso aumentar o volume de vendas da loja virtual.

2 Técnicas comuns de roubo de cartões

Roubos de cartões off-line para uso on-line

Muitos consumidores ainda se sentem inseguros para realizar uma compra na internet temendo que seus dados possam ser roubados durante a transação, mas esse medo gradativamente vem diminuindo, devido às melhorias dos serviços tecnológicos de segurança de transação na internet. Porém esses mesmos consumidores não enxergam que seus dados de cartão de crédito podem ser roubados em uma compra na loja física ou restaurante.

Os dados de cartão de crédito podem ser copiados em compras em lojas físicas de uma forma muito mais fácil do que pela internet.

A defesa mais eficaz hoje contra este tipo de golpe é a verificação do número de segurança impresso no verso de todos os cartões de crédito.

As soluções de cobrança on-line da Redecard e da Cielo realizam a verificação da validade do código de segurança no momento da compra.

Falsa Identidade

Muitas lojas virtuais costumam realizar consultas às entidades de proteção ao crédito e associações comerciais quando recebem um pedido. Os fraudadores então utilizam informações de pessoas sem restrições nestes órgãos para realizarem compras fraudulentas e passarem por este tipo de teste. Como as administradoras de cartão não fornecem ao lojista uma forma de conferirem o verdadeiro dono do cartão de crédito sendo usado na compra, o golpista pode utilizar-se de dados pessoais de uma de uma pessoa e cartão de crédito de outra para realizar a compra e não ser barrado pelas consultas de crédito ou validação de CPF.

3 Técnicas de proteção dos dados dos clientes no FastCommerce

Segurança

O **FastCommerce** é extremamente seguro tanto para os visitantes e clientes das lojas quanto para os próprios lojistas. Isto porque uma das prioridades da tecnologia **FastCommerce** é com a segurança, em seus diversos aspectos:

Segurança no tráfego de informações

Como protocolo de segurança de tráfego, o **FastCommerce** utiliza o Extended Validation Secure Socket Layer(EV SSL), que é o padrão superior da indústria e está entre os melhores disponíveis para transações comerciais seguras. Ele criptografa todas as informações trafegadas, de modo que não possam ser lidas ou alteradas por terceiros enquanto estão transitando pela Internet. É o mesmo tipo de segurança usado pelos melhores sites de home banking.

Todas as informações cadastrais e financeiras são enviadas em modo seguro, o que pode ser facilmente verificado no navegador, que exibirá um cadeado fechado na área externa.

Segurança na administração do site

Diversas estratégias de segurança foram adotadas para tornar o acesso ao site administrativo o mais seguro possível:

- As páginas do site administrativo possuem segurança SSL com Validação Extendida (EV).
- Logon e senhas podem ser digitados através de teclado virtual.
- Da mesma forma como nos melhores sistemas de internet banking, a página inicial do site administrativo mostra informações sobre acessos ao site administrativo, incluindo:
 1. data/hora do último logon
 2. data/hora e IP da última tentativa de acesso com senha inválida
 3. data da última alteração da senha
 4. verificação de versão do navegador
- Após determinado período de inatividade do usuário, o site administrativo realiza logoff automático. Novamente, conforme ocorre nos melhores sites de internet banking.
- Se o usuário esquecer sua senha, poderá solicitar o envio de frase de lembrete de senha para seu e-mail. A senha propriamente dita nunca é remetida, pois os protocolos usuais de e-mail não apresentam segurança adequada para o envio de informações sigilosas.
- Todas as senhas administrativas têm tamanho mínimo de 6 caracteres (recomendamos senhas compostas por números e letras com pelo menos 8 caracteres).
- O **FastCommerce** faz logoff automático do site administrativo sempre que o IP de acesso se altera. Este recurso visa impedir ataques através de técnicas de cross-site scripting.
- O logoff automático também acontece quando o usuário fecha ou sai da página do site administrativo onde fez o logon.
- A loja pode configurar um firewall personalizado, para impedir acessos indesejados à loja. É possível cadastrar filtros de visitação, utilizando critérios de bloqueio tais como o endereço IP, a origem (Referer) ou o navegador (user-agent) do visitante.

Segurança no armazenamento de dados

Todas as informações financeiras dos clientes e da loja são armazenadas com criptografia forte (RC4-like). Além disso, as senhas dos usuários do site administrativo são armazenadas com função hash one-way (Unix-like). Nem mesmo os administradores da loja ou DBAs do **FastCommerce** têm acesso às mesmas.

As lojas são totalmente independentes de cookies e da data e hora do computador do visitante. A navegação e os pedidos serão realizados normalmente mesmo que o browser do cliente não aceite cookies.

Segurança na análise de crédito a clientes

O site administrativo do **FastCommerce** oferece diversos recursos para avaliação de risco de crédito a clientes:

- Informações sobre pedidos anteriores, tempo de permanência no site, páginas visitadas, etc.
- Verificação de CPF no site da Receita Federal.
- Verificação se o CEP corresponde ao endereço informado, no site dos Correios.
- Armazenamento do endereço IP, sistema operacional e browser utilizados pelo visitante.
- Relação das visitas anteriores do cliente.
- Solicitação de código de segurança para todas as compras feitas com cartão.

Segurança física das informações

A infraestrutura do **FastCommerce** contempla componentes de alta disponibilidade, redundância e disaster recovery, o que garante uma operação praticamente ininterrupta.

O **FastCommerce** opera com servidores próprios, todos com múltiplos processadores de última geração, além de fontes redundantes, espelhamento de disco primário do sistema operacional e disk arrays em RAID, com HDs de alta performance (15.000 rpm).

Todos os equipamentos ficam situados em salas climatizadas individuais com segurança de acesso físico 24h e energia elétrica garantida por estabilizadores e geradores.

O backup dos arquivos e bases de dados é diário, em fitas que seguem um rodízio semanal, mensal e anual. As fitas são mantidas em cofre situado longe dos servidores.

As lojas são acessadas através de diversos links Internet independentes. Um sistema de balanceamento de tráfego automático garante que o link com maior disponibilidade será utilizado pelos visitantes. A análise dos links é feita a cada visita, permitindo desviar o tráfego para outros circuitos caso um ou mais links apresentem problemas.

Estas avançadas medidas de segurança física, de software e de hardware garantem a performance, a privacidade e a alta disponibilidade das lojas que utilizam o **FastCommerce**.

InfoRisk - Para auxiliar no combate a fraudes e diminuir a inadimplência

O InfoRisk é um serviço de auxílio às análises de risco feitas pela loja. Trata-se de um serviço pré-pago para consulta de informações sobre os clientes da loja. O serviço inclui:

- Consulta por CPF: exibe até 3 telefones e respectivos endereços de instalação relacionados ao CPF do cliente.
- Consulta por telefone: exibe o endereço de instalação do telefone do cliente.
- Consulta de cheque: informa restrições sobre outros cheques que o titular tenha emitido (sem fundos, sustados, roubados, cancelados e extraviados). Exibe o nome completo do emitente, data de nascimento ou fundação, situação do CPF/CNPJ junto à Receita Federal e detalhes do telefone, incluindo os últimos 5 telefones informados pelo emitente.
- Consulta completa: informa restrições de crédito do CPF/CNPJ do cliente, incluindo a quantidade de falências, concordatas, ações judiciais, protestos, cheques sem fundos, pendências/restrições financeiras e participação em insucessos empresariais para pessoa física. A opção “Com controle” pesquisa também a quantidade de consultas efetuadas no CPF/CNPJ nos últimos 5 meses.
- Consulta veicular: exibe os dados do cadastro do DENATRAN referentes ao veículo com a placa informada ou de até 4 veículos relacionados ao CPF/CNPJ do cliente. Retorna informações completas de cada veículo, incluindo os dados do proprietário e a quantidade de veículos que estão em nome deste. Informa também sobre alerta de roubo ou furto, data e município da ocorrência.

4 Solução para gestão de risco

Autorização on-line

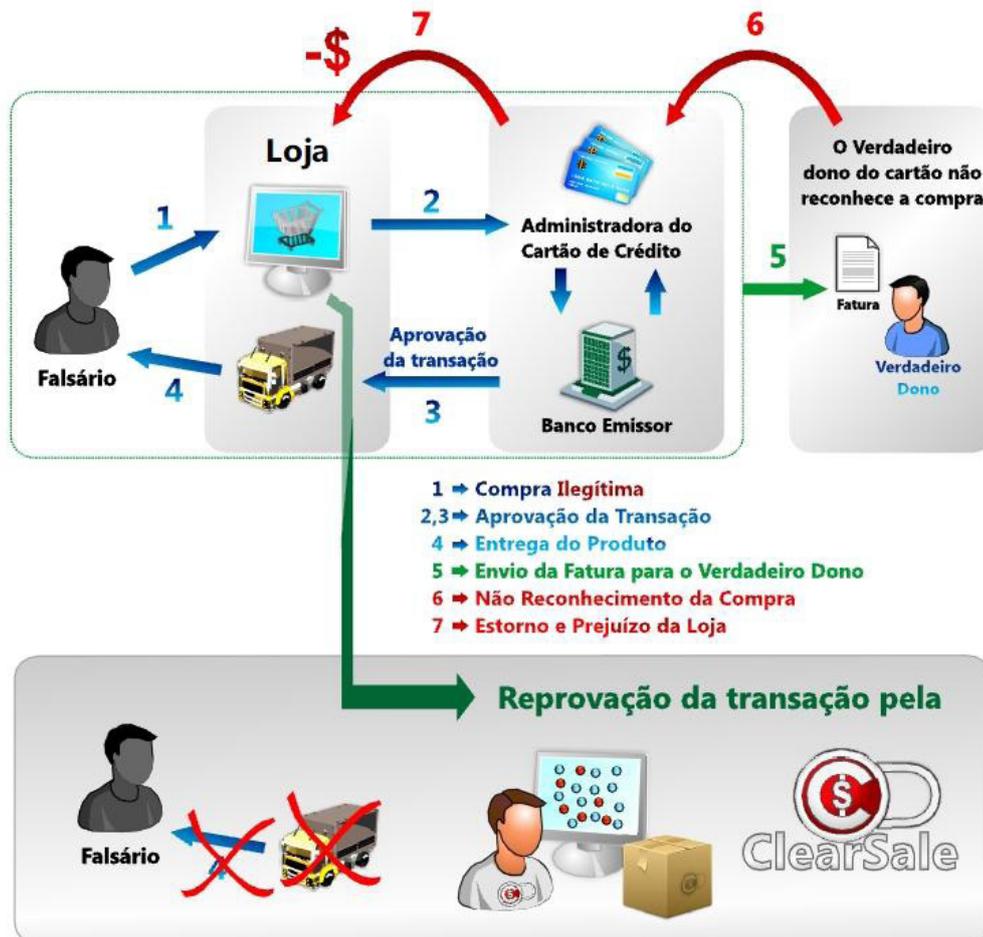
As soluções mais usualmente oferecidas pelas administradoras de cartões ao lojistas direciona o cliente ao site administrativo de cartões de crédito para que digite os dados do cartão de crédito. Desta forma os dados do cartão não são armazenados na loja e isenta o lojista da responsabilidade de armazenar os dados do cartão de crédito e a transação é aprovada em tempo real. Porém no comércio eletrônico há a necessidade de saber se o comprador virtual é ele mesmo.

Como resolver esta questão?

O cliente que compra pela internet procura principalmente, agilidade, comodidade e segurança. Portanto, solicitar que o cliente envie documentos para aprovar vendas online é contraproducente e espanta muitos compradores.

Ferramenta ClearSale

A solução é identificar, antes de liberar o pedido, se o cliente é realmente o portador do cartão de crédito.



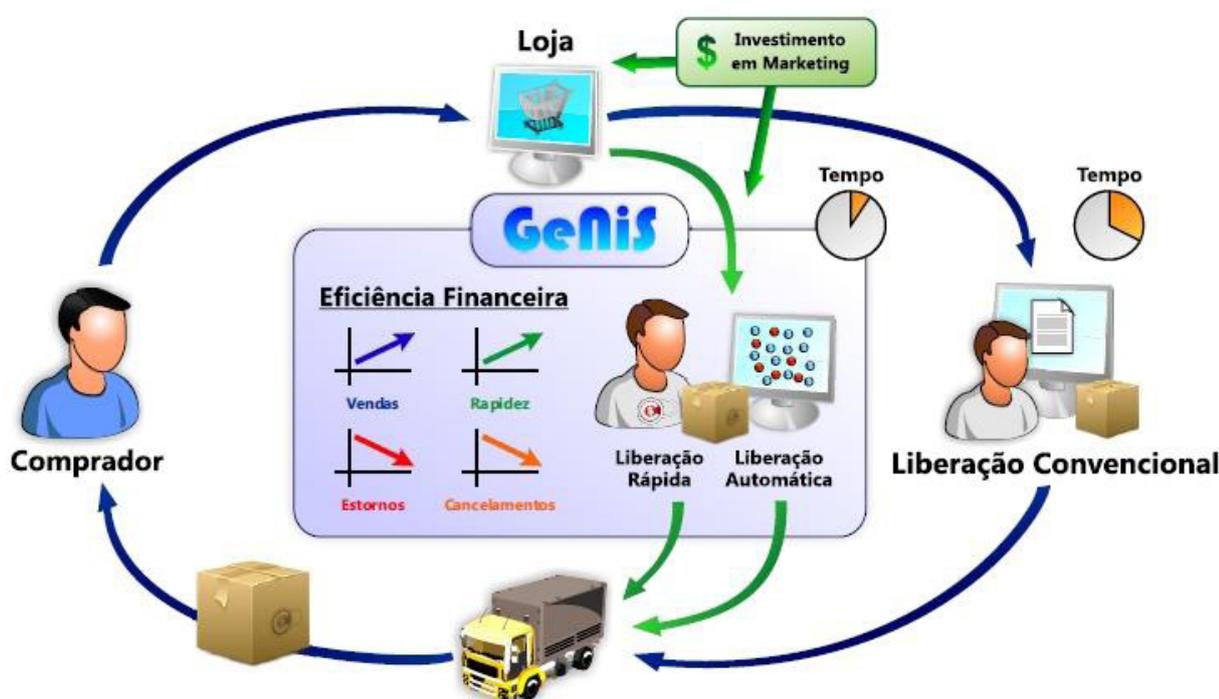
Antes da administradora do cartão de crédito, o pedido deve passar pela ferramenta da ClearSale, recebe o score e, quando não é liberado automaticamente, seguirá para análise manual onde, após análise assertiva, os pedidos receberão um dos status finalizadores (Aprovado, Cancelado, Reprovado, Suspeito e Fraude Confirmada). Pedidos que forem finalizados como “Aprovados” seguirão posteriormente o fluxo normal para entrega.

Os passos 5, 6 e 7 demonstram como pode ocorrer o chargeback, quando há ou não reconhecimento da compra.

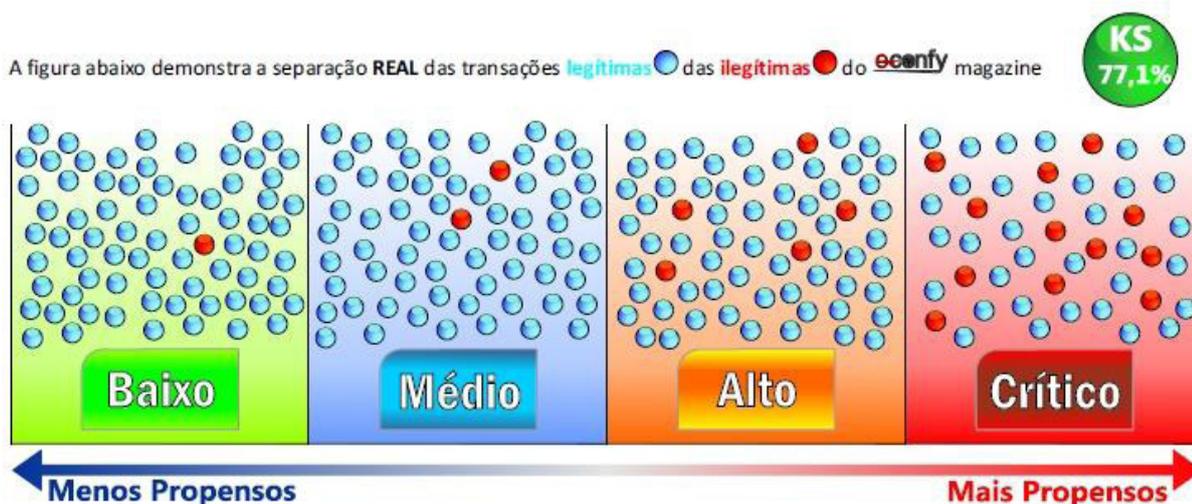
O chargeback pode ocorrer para pedidos que tenham sido aprovados, tanto por analistas como automaticamente.

Autenticação do bom cliente

A ClearSale realiza o processo de autenticação do bom cliente com segurança e rapidez.



Ao analisar um novo pedido o score reúne 233 coeficientes de risco que simula a capacidade analítica humana, o que torna tão assertivo. Esta assertividade tem sido vital para o sucesso dos lojistas.



Sobre a ClearSale

A ClearSale iniciou suas atividades, em 2001, desenvolvendo a solução de gestão de risco para prevenção de perdas no Submarino. Em 2004, a empresa ingressou no mercado varejista através da terceirização na Americanas.com, criando a segmentação do score para separação dos bons pedidos e liberação rápida das vendas do Comércio Eletrônico.

A ClearSale lidera o mercado com mais de 1.700.000 transações processadas mensalmente em seus sistemas.

A principal questão, além de identificar a compra ilegítima, é ser assertivo para oferecer uma liberação rápida para o bom cliente.

- Detectar, evitar e coibir a fraude (falsidade ideológica);
- Autenticar o bom cliente (não cancelando pedidos legítimos com perfil de alto risco);
- Reduzir o tempo médio de entrega.

A assertividade da ClearSale contribui para segurança em todo processo da venda, para todos os envolvidos.

Sobre o FastCommerce

O **FastCommerce** é o sistema de loja virtual mais utilizado do Brasil, com mais de 17 mil lojas virtuais cadastradas desde 1996.

O sistema foi criado pela Rumo Informática, empresa pioneira em comércio eletrônico, e é utilizado por lojas virtuais de todos os segmentos e tamanhos, em diversos países.

O melhor custo x benefício:

O **FastCommerce** é um motor de loja virtual, altamente personalizável, com foco nos resultados financeiros das empresas. O próprio lojista pode criar e gerenciar sua loja virtual de uma forma simples e rápida.

Para uma melhor avaliação do **FastCommerce**, crie AGORA sua loja, que ficará no ar gratuitamente durante quinze dias, em demonstração:

<http://novaloja.fastcommerce.com.br>

Os recursos impressionam, em especial a personalização de layout e as dezenas de relatórios administrativos.

Equipe **FastCommerce**

e-mail: contato@fastcommerce.com.br

<http://www.fastcommerce.com.br>

São Paulo (capital): (11) 5052-9339

Demais regiões (exceto celular): 0800 774 0166

Fontes de pesquisa

Redecard: <https://services.redecard.com.br/novoportal/site/3552/Biblioteca.aspx>

ClearSale: <http://portal.clearsale.com.br/>

<http://www.blogdoecommerce.com.br/o-que-e-chargeback/>

<http://blogpagseguro.com.br/tag/chargeback/>

