TUDO SOBRE FRAUDES ONLINE:
OS PRINCIPAIS TIPOS E COMO SE PROTEGER

ClearSale

INTRODUÇÃO

Negócios que lidam com transações digitais, principalmente no setor de e-commerce, passam constantemente por tentativas de fraudes de cibercriminosos e até mesmo de consumidores que usam de má-fé para levar vantagem em relações de compra e venda.

Esse tipo de problema, quando frequente, mina a capacidade de **previsibilidade de ganhos e projeção de estratégias para o futuro**, além de, claro, significar prejuízos que afetam negativamente qualquer negócio.

Porém, da mesma forma que essas tentativas de fraude se tornam cada vez mais sofisticadas, o mesmo acontece com as estratégias e ferramentas de combate a esse mal. Neste e-book, vamos nos aprofundar no assunto, apresentando a você, leitor, uma visão completa sobre fraudes online.

Nele, você vai entender o conceito, como elas acontecem dentro da rotina de um e-commerce e quais são os benefícios de contar com a melhor solução possível para evitar que isso afete o seu negócio. Boa leitura!

O QUE SÃO **FRAUDES ONLINE?**

Desde que o comércio existe, há também pessoas que tentam tirar proveito de sistemas de consumo para levar vantagem. Pode ser uma apropriação de um produto, pagamento inferior ao preço de mercado, uso de dados ilegítimos ou o próprio furto/roubo de mercadoria.

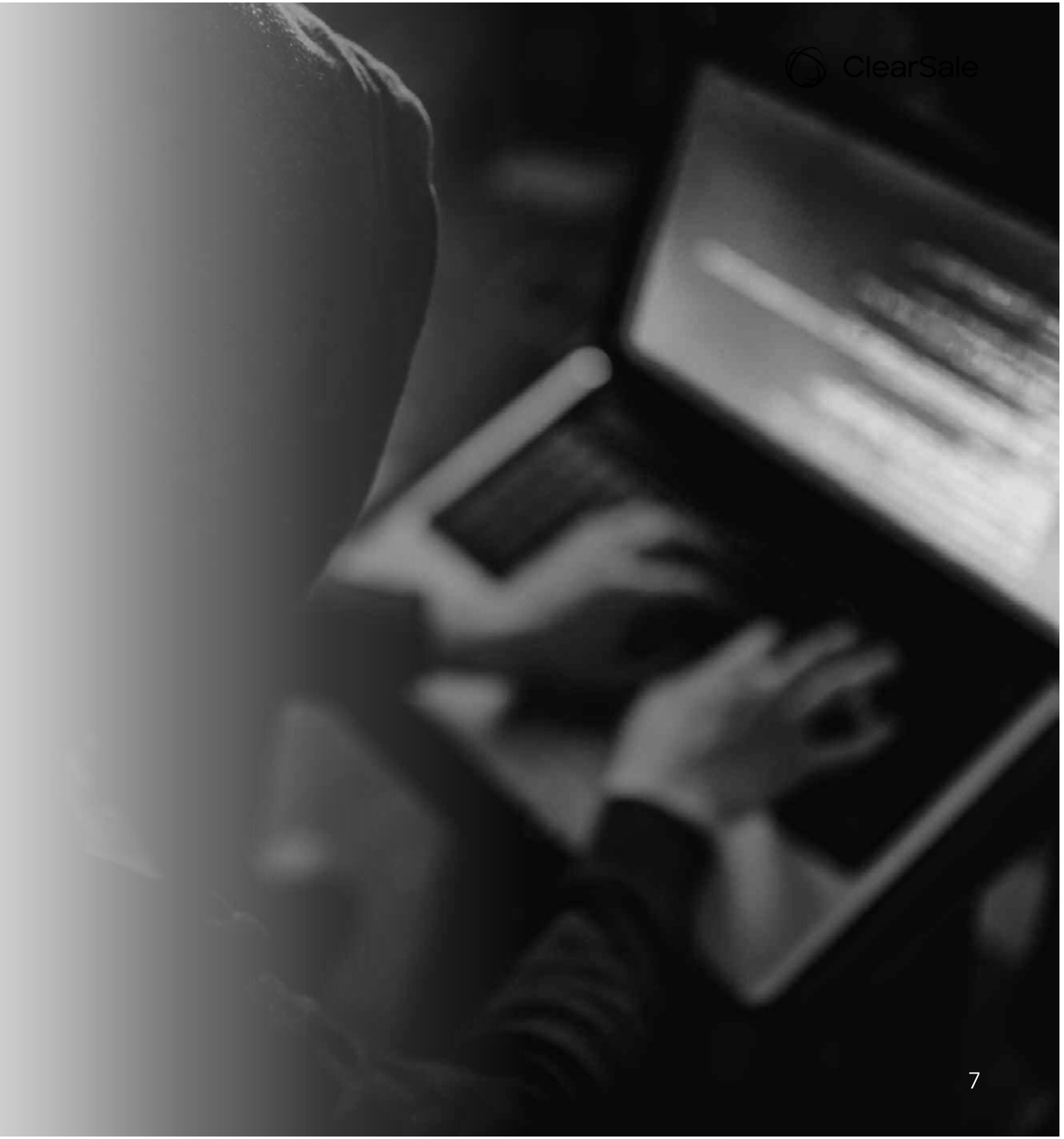
A questão é perene por tanto tempo, que já em 1953 havia uma tentativa importante de determinar de maneira mais sistêmica o evento de fraude. A hipótese de Cressey foi apresentada em uma publicação desse ano, denominada *"Other people's money: a study in the social psychology of embezzlement"*.

Nela, o autor aponta a fraude como uma ação de benefício próprio nociva a terceiros, que se dá por três fatores principais, formando uma espécie de triângulo. São eles:

- **Pressão:** seja emocional ou financeira, que motive o fraudador por ser impelido a cometer o ato por não ter recursos para fazer de maneira legítima;

- **Oportunidade:** quando uma chance de fraude se apresenta de maneira tão fácil, que se torna tentadora ao resolver essas questões financeiras secretamente;

- **Racionalização:** quando o fraudador premedita o ato e o racionaliza como justificável para resolução dos problemas financeiros.



É importante compreender esse tipo de raciocínio por parte do fraudador, justamente para entender quais são os motivos que levam alguém a tomar essa atitude nociva — seja uma pessoa física ou jurídica.

Infelizmente, é um tipo de ocorrência que continuará acontecendo, independentemente de época ou tecnologia associada. O que empresas podem fazer é **criar e adquirir mecanismos de proteção que mitiguem esses riscos** dentro de uma rotina que se adapta à realidade de seus tempos atuais.

A fraude na era pós-internet

As fraudes online, em sua origem, partem dos mesmos elementos apresentados no triângulo de Cressey. São as mesmas motivações muito antes da tecnologia se tornar tão presente em nossas vidas. Porém, a forma como a fraude acontece se transformou muito nos últimos anos, exatamente por causa da **transformação digital.**

Com a automação de processos de gestão e vendas em e-commerce e a implementação de pagamento online, as fraudes deixaram de ser majoritariamente a tentativa de enganar pessoas para se tornarem a tentativa de enganar sistemas.

Isso tem muito a ver também com o foco que existe hoje na coleta e gestão de dados pelos negócios. Com a informação ganhando um valor enorme para empresas, ela também se valoriza para os criminosos — que podem utilizar essas brechas para se apropriarem de dados de terceiros na execução dessas fraudes.

Portanto, o **combate a fraudes** atualmente exige muito mais preparo e utilização de soluções inteligentes de monitoramento, já que é impossível para seres humanos controlarem de forma manual cada transação realizada em sua loja virtual.

Se estamos falando de um crescimento de negócio baseado em eficiência operacional, as análises antifraude precisam cada vez mais apresentar **agilidade de conferência.** Isso para não quebrar a experiência de usuários legítimos ao mesmo tempo em que identifica com sucesso aqueles que estão tentando aplicar algum tipo de golpe.

Ou seja, a tecnologia antifraude hoje se tornou um dos pilares do sucesso de um e-commerce. Se o seu faturamento está diretamente ligado ao seu número de vendas online, cada fraude se apresenta como um risco à sua estabilidade e ao crescimento sustentável.

QUAIS SÃO OS BENEFÍCIOS DE **INVESTIR EM ANTIFRAUDE NA EMPRESA?**

Antes de falarmos sobre os principais tipos de fraude online e como combatê-las, queremos reforçar a importância de ter esse conhecimento e trabalhar para reduzir esses riscos em um e-commerce. Veja quais são os principais abaixo!

Evitar prejuízos

O primeiro motivo é o mais óbvio e direto possível: fraudes online significam prejuízo para as empresas que são **vítimas de cibercriminosos**.

Na maioria das vezes, quando bem-sucedido, o golpe faz com que sua loja fique sem o produto e sem o dinheiro. E isso significa perder faturamento, que pode ser utilizado no futuro para o crescimento do próprio negócio.

Reduzir custos

O trabalho inteligente de antifraude não é apenas para evitar prejuízos, mas para fazer isso com o sistema mais eficiente possível, a fim de que a empresa não despenda tantos recursos nesse esforço.

Quanto melhor é a solução de combate, menos o e-commerce precisa gastar com controle manual, verificações constantes de pedidos e **custos envolvidos com a reparação de danos** causados pela fraude.

Nesse sentido, investir em tecnologia antifraude se torna muito mais barato do que usar esses recursos sempre que precisar apagar incêndios.

Ter uma base mais sólida na tomada de decisões

Os prejuízos de sofrer tentativas de fraude com frequência não são apenas financeiros, mas atrapalham o próprio trabalho da equipe do e-commerce em seus objetivos de crescimento. As fraudes dificultam bastante a tomada de decisões dentro da rotina de diretores porque **contaminam indicadores**.

Como a identificação de extravio de mercadorias ou o próprio estorno de valores em *chargebacks* podem demorar semanas, é provável que algumas dessas decisões sejam feitas com base em valores de faturamento que não correspondem à realidade. Logo, isso pode causar um desequilíbrio nas contas que atrapalha a sustentabilidade do negócio.

Dar previsibilidade a investimentos

Ainda sobre sustentabilidade, essa incerteza dos valores reais de faturamento perante fraudes pode dificultar muito seu planejamento para investir no próprio negócio no futuro.

As empresas que querem ser competitivas na era digital precisam estar sempre pensando no próximo degrau a subir. Quais novos mixes de produtos, fornecedores, nichos, soluções de gestão e até serviços de relacionamento com o cliente podem ser implementados nos próximos meses ou anos?

Quanto mais frequente os eventos de fraude no negócio, mais difícil se torna esse planejamento, que precisa ser pensado em prazos cada vez mais curtos.

Isso tudo tem a ver com a **estabilidade do faturamento.** A partir de indicadores de venda, como conversão, fidelização e Custo de Aquisição do Cliente (CAC), é possível notar uma tendência de crescimento nas vendas — e usar isso como projeção para o ponto que você deseja colocar o e-commerce em determinado período.

No entanto, é possível que esses números não se sustentem com o tempo, com o excesso de estornos e a perda de mercadoria. É uma situação que traz insegurança para investir, sem a certeza de que haverá o caixa suficiente para pagar da maneira como foi projetado.

Buscamos reforçar esse ponto exatamente por sua importância na competitividade do futuro. Afinal, ganha a corrida quem nunca para de inovar. E não existe inovação sem uma visão clara do que vem pela frente.

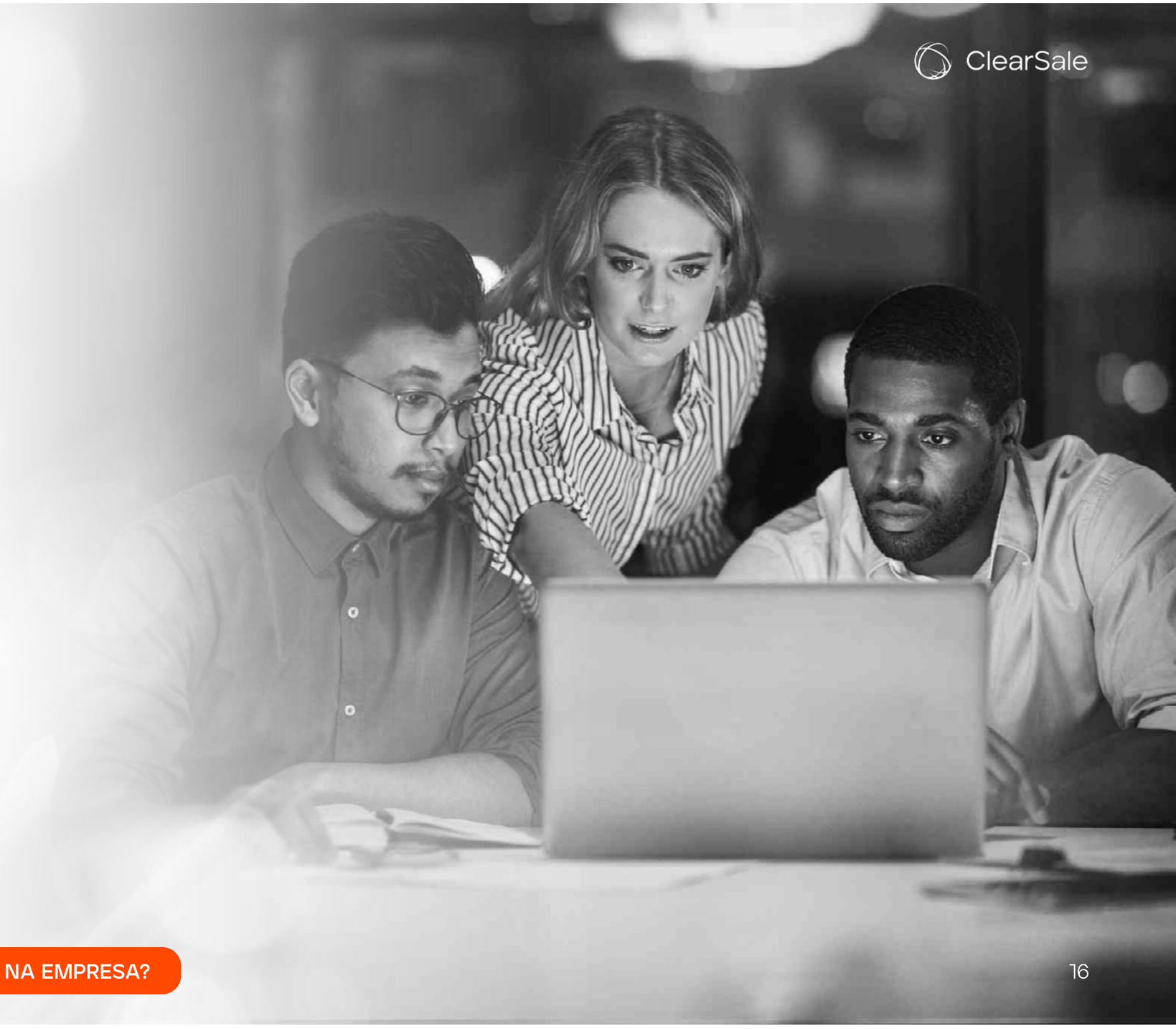
QUAIS SÃO OS BENEFÍCIOS DE INVESTIR EM ANTIFRAUDE NA EMPRESA?

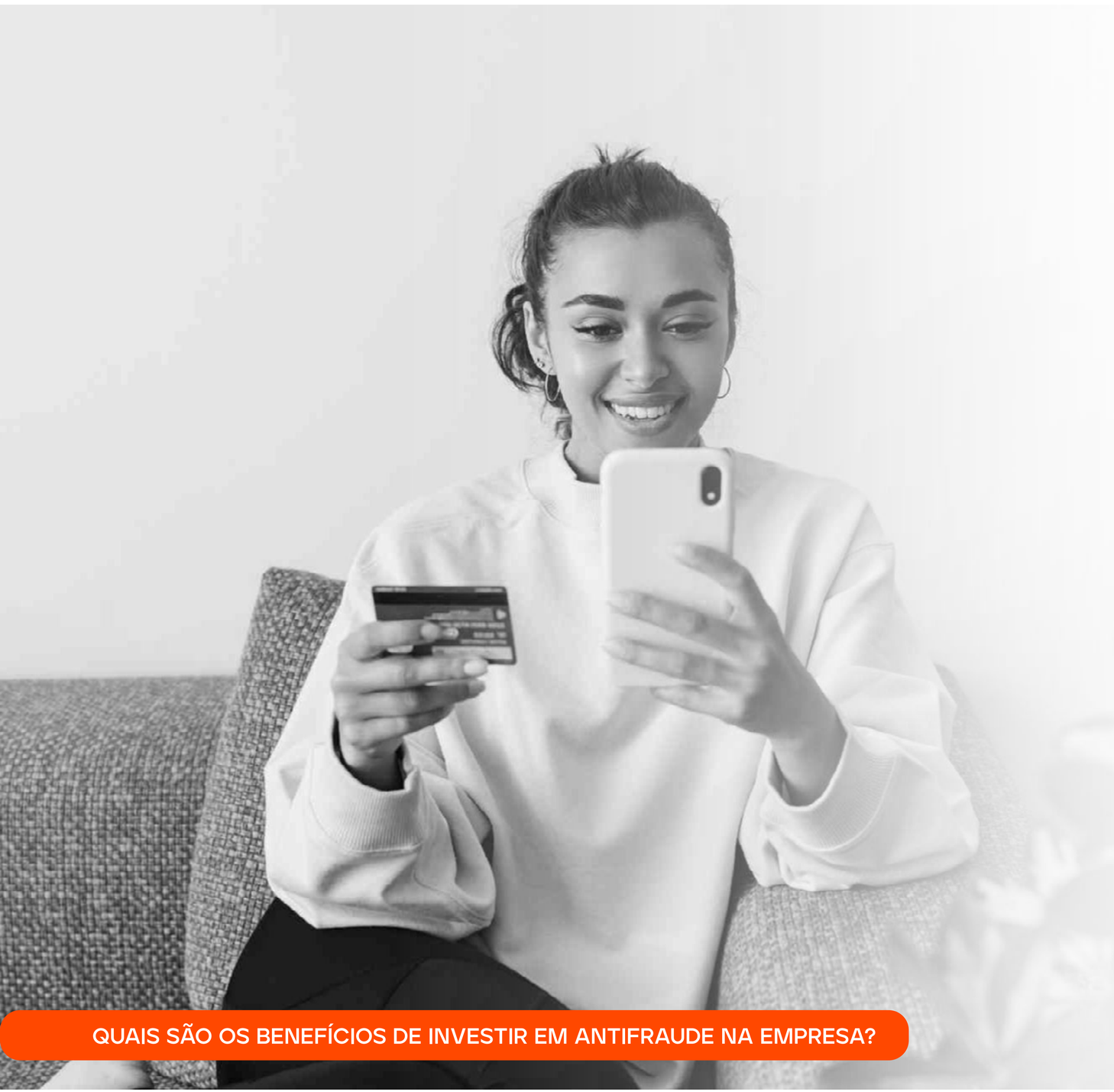
Tornar o papel dos colaboradores mais estratégico

Falamos bastante nos últimos itens sobre monitorar indicadores, fazer projeções e tomar decisões. Mas como fazer isso se você tem que se preocupar constantemente em analisar e lidar com possibilidades de fraude?

Contar com um **sistema antifraude inteligente e automatizado** é um ganho incrível nesse sentido. Como a solução é capaz de analisar e aprovar/recusar vendas de maneira autônoma, boa parte do peso de fazer esse controle sai dos colaboradores do e-commerce.

Aí sim o seu papel se torna realmente estratégico. Você tem o tempo, os recursos e a estabilidade para se debruçar sobre indicadores e encontrar caminhos de sucesso. É **utilizar a inteligência antifraude como aliada na inteligência de negócio.**





Melhorar a experiência do cliente legítimo

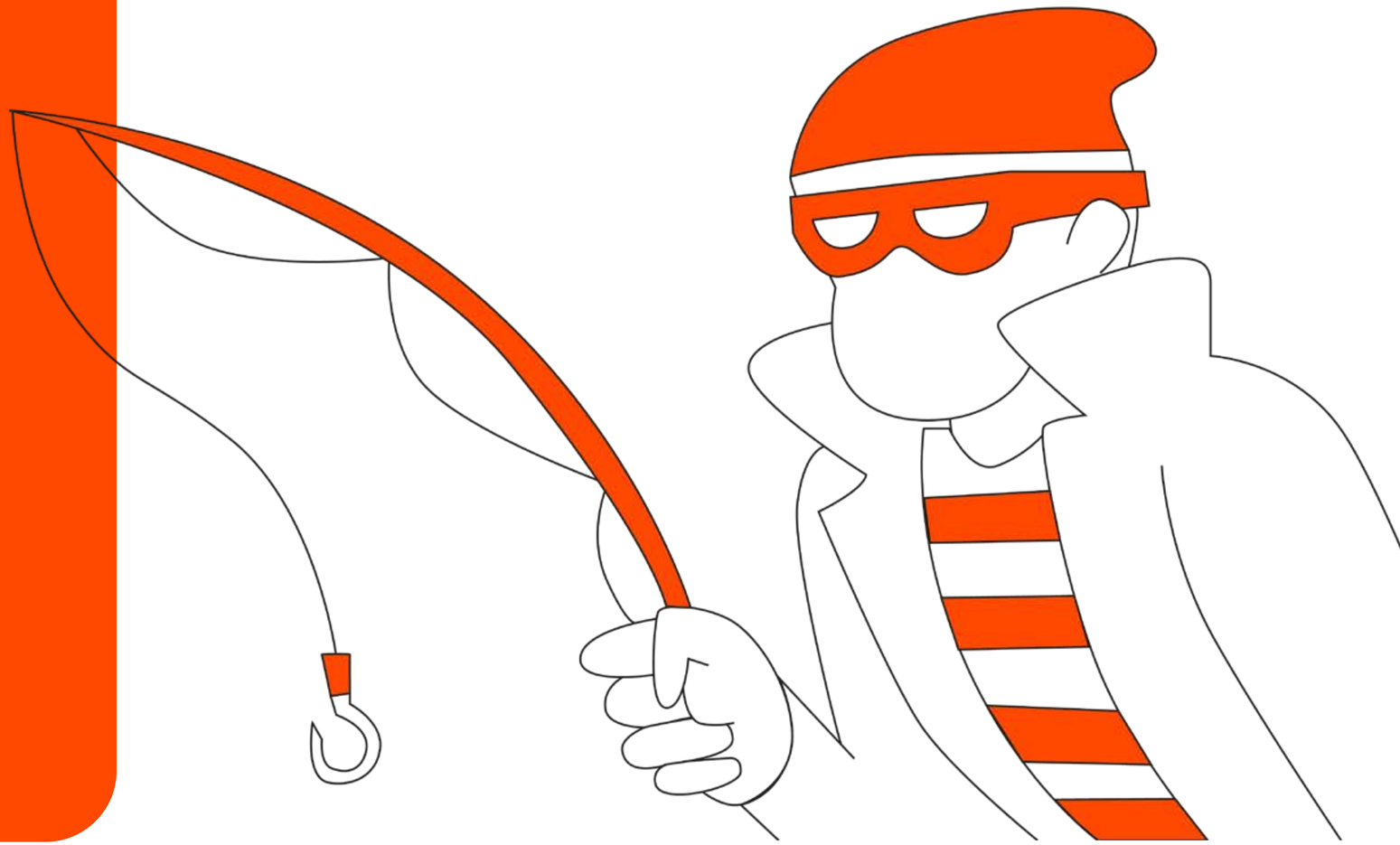
Ter um bom controle das fraudes online permite também que o e-commerce agilize e simplifique essas verificações a cada nova venda. Isso não é apenas segurança para a empresa, mas comodidade para o cliente.

Quanto mais eficiente é a gestão antifraude, menos tempo é gasto entre a solicitação e a confirmação do pedido. Pelo lado do usuário, significa que ele terá um processo de compra mais rápido e que passa uma sensação perceptível de segurança.

Se tem uma verdade incontestável na era digital é a de que **uma boa experiência do usuário gera satisfação**, e satisfação gera fidelização e divulgação espontânea da loja. É uma maneira orgânica e sustentável de crescer.

QUAIS SÃO OS

PRINCIPAIS TIPOS DE FRAUDE?



Como a internet abriu uma possibilidade muito maior de uso de ferramentas com má-fé para fraudes, existem várias maneiras de prejudicar um e-commerce. Porém, as empresas também contam com soluções cada vez mais eficientes e sofisticadas para lidar com esses riscos com tranquilidade.

Mesmo que você tenha acesso a ferramentas automatizadas, entretanto, é muito importante que profissionais responsáveis por essa parte dentro do negócio tenham conhecimento sobre os principais tipos de fraude. Assim, eles podem **tomar atitudes que previnam essas ocorrências** antes que uma solução tecnológica precise entrar em ação.

Que tal, então, saber quais são esses principais tipos que ocorrem com mais frequência e são mais danosos na rotina de um e-commerce?

QUAIS SÃO OS PRINCIPAIS TIPOS DE FRAUDE?

Phishing e roubo de identidade

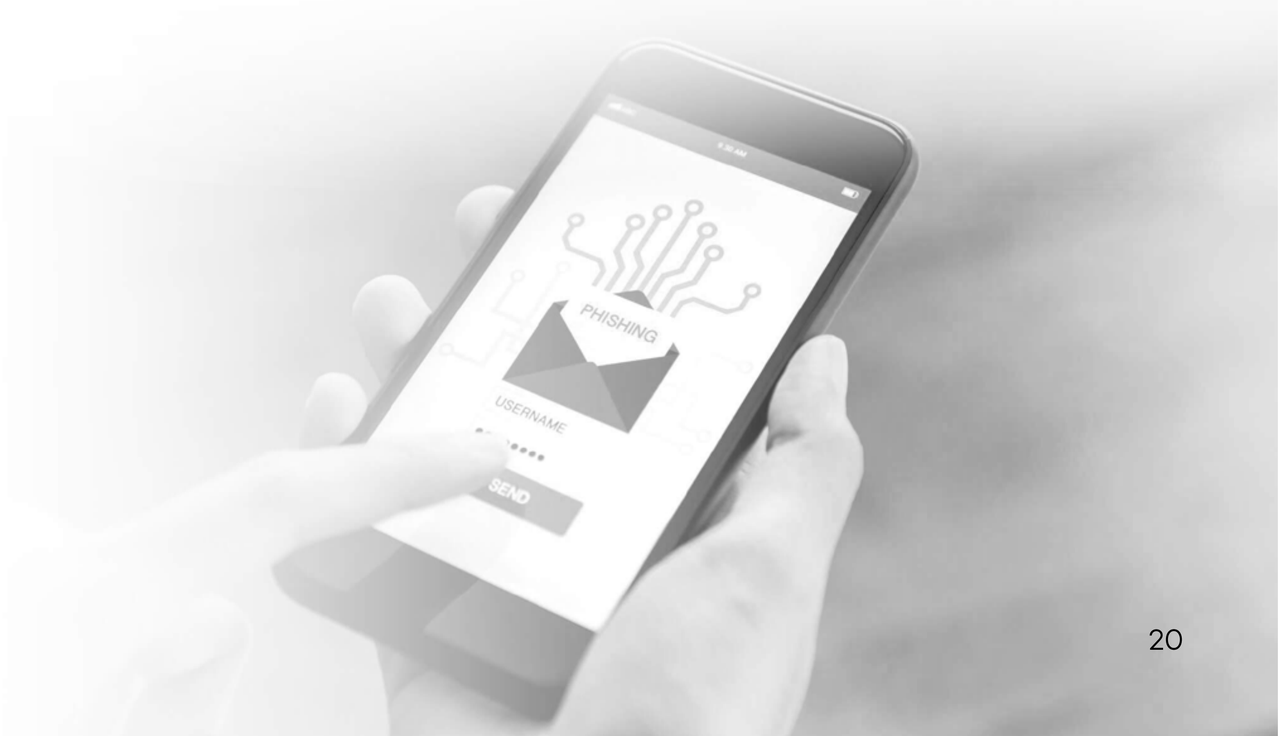
Phishing é um termo em inglês que remete ao ato de pescar. No caso, em vez de peixes, a pescaria tem como alvo os dados de usuários de uma determinada loja virtual.

Isso é feito ao utilizar um conceito chamado de engenharia social: quando, em vez de tentar invadir um sistema, o cibercriminoso engana a vítima de maneira que ela própria forneça dados legítimos de acesso a ele.

A maneira mais comum dessa fraude acontecer no e-commerce se dá assim: a pessoa má intencionada cria uma cópia praticamente perfeita da sua loja, trocando só uma letra ou usando um typo comum na hora de escrever o endereço na barra do navegador.

Ao pensar que está na página legítima, o usuário utiliza seu login e senha para entrar e recebe uma mensagem de erro. Nesse momento, os dados de acesso já estão em posse do criminoso, que pode utilizá-los para entrar na conta legítima do e-commerce e, a partir das informações salvas, realizar compras com o cartão de outra pessoa.

Aqui, o consumidor vitimado, claro, vai denunciar uma compra que não reconhece à sua instituição financeira. Com isso, o valor é estornado e quem fica no prejuízo é a loja.



Como se proteger do phishing

Existem duas táticas principais para que um e-commerce reduza consideravelmente a ocorrência de phishing:

- Testar constantemente os endereços similares ao da sua loja ou buscar no Google possíveis clones do site que estão captando dados de seus clientes e denunciá-los pela prática;

- Acrescentar **verificação de dois fatores** para o acesso à conta de clientes na sua loja. Além de login e senha, o usuário precisa confirmar quem é ele por outro dispositivo de verificação, como seu celular ou sua conta de e-mail — tornando muito mais difícil o uso indevido dessas credenciais.

Chargeback

O **chargeback**, ou pedido de estorno, também é uma fraude muito comum de se lidar quando se trabalha no setor de e-commerce.

Nesse tipo de fraude, o cliente faz a compra sem levantar maiores desconfianças a princípio: dados pessoais legítimos, dados de cartão verificados e endereço válido. Com uma aparente legitimidade das informações, o sistema autoriza a conclusão da compra e a loja envia o pedido.

É aí que o problema acontece. Assim que recebe a encomenda, na má-fé esse cliente **aciona sua instituição bancária e diz não reconhecer aquela cobrança**, solicitando o estorno do valor. Como, muitas vezes, a prioridade é do consumidor, esse valor é devolvido ao criminoso e a empresa fica sem o pagamento pelo produto que já foi enviado.

Como se proteger do chargeback

Um primeiro ponto a ser levantando sobre o chargeback é que os e-commerces precisam investir em soluções eficientes de controle, registro de dados e monitoramento para terem as informações necessárias na defesa de ocorrências de fraude — e até conseguirem denunciar os fraudadores quando for possível identificá-los.

Porém, é preciso citar que esses processos podem ser demorados, custosos e, em casos que envolvem phishing e outros tipos de apropriação de identidade, talvez nunca sejam solucionados. Portanto, **a melhor maneira de se proteger contra chargeback é a prevenção.**

Ferramentas de inteligência especializadas em antifraude podem encontrar padrões de comportamento e conflitos de dados muito sutis que apontam para uma possível tentativa de fraude. Ao ter essa anomalia detectada, elas impedem a conclusão da compra e garantem mais segurança ao negócio.

QUAIS SÃO OS PRINCIPAIS TIPOS DE FRAUDE?

Fraude em marketplaces

Muitas lojas virtuais utilizam os marketplaces como **maneira de aumentar a visibilidade de seus produtos** e conseguir um alcance maior, mesmo quando ainda são menores. Em geral, são plataformas robustas e que oferecem soluções próprias de segurança, mas que nem por isso estão livres de tentativas de crime.

As fraudes mais comuns em marketplaces costumam ser bastante parecidas com o chargeback. No caso, em vez de acionar a instituição financeira para o estorno, criminosos utilizam o suporte da plataforma para apontarem que não receberam o produto como prometido pela loja, mesmo que isso tenha sido feito.

Como se proteger de fraudes em marketplaces

Mesmo que signifique uma margem de lucro melhor para o e-commerce, o ideal dentro de marketplaces é utilizar o sistema deles próprios de gerenciamento de pedidos e até de entrega.

Dessa maneira, fica muito **mais fácil provar a má-fé** do consumidor nos casos de chargeback. Com os dados registrados dentro da própria plataforma, você demonstra o processo da preparação do pedido até o caminho de entrega, contando inclusive com a confirmação de recebimento pelo cliente.

Fraude de interceptação

A fraude de interceptação é mais incomum, mas não pode ser desprezada. Quando o criminoso consegue dados de clientes que têm pedidos em andamento, agem para tentar **interceptar a entrega alterando o endereço da compra.**

O que fazem é entrar em contato com o suporte da loja por meio de seu sistema de e-commerce ou, algumas vezes, diretamente com atendentes solicitando a mudança desse destino do pedido.

A desculpa costuma ser um descuido de ter colocado um endereço de um parente em vez do próprio, ou até dizer que surgiu uma viagem de emergência e precisa enviar para a casa de um amigo que receba pelo criminoso.

Quando bem-sucedido o processo, a loja altera esse endereço e envia o pedido para outro local sem qualquer conhecimento do cliente legítimo — que, claro, abre uma reclamação quando a encomenda muda o status para "entregue" sem ter recebido nada.

Como se proteger da fraude de interceptação

Muitas lojas, para evitarem esse tipo de fraude, **não aceitam mudanças no endereço de entrega** após a confirmação do pedido, exigindo que o cliente cancele a compra para, então, refazê-la com o novo endereço.

Essa talvez seja a melhor forma de abordagem para mitigar esse risco, mas não é a única. Outra proposta interessante é exigir a verificação de dois fatores. Mesmo que o criminoso possua os dados do cliente e seja convincente, ele **não conseguirá confirmar a mudança** sem acesso ao e-mail ou telefone celular da vítima, por exemplo.

Abuso de erros evidentes de sistema

Esse é o evento mais comum nos casos que chamamos de fraude de oportunidade, que motiva até mesmo pessoas que nunca cometeram qualquer crime a se arriscarem para ganhar alguma vantagem. O abuso do erro evidente ocorre quando, por erro humano ou tecnológico no registro, **um produto entra em venda por um preço muito abaixo do mercado.**

Muitas vezes, esse erro é compartilhado em redes sociais e várias pessoas tentam comprar algo que esteja com um preço bem menor do que o valor médio de mercado. Por exemplo, um celular de R$ 2 mil que entra na vitrine da loja virtual por apenas R$200,00.

Como se proteger de abusos de erros

Esse tipo de fraude é cada vez mais incomum à medida que as plataformas de e-commerce vão se tornando mais sofisticadas e capazes de identificar e alertar quando há uma anomalia no preço registrado pelo produto.

Nesse caso, o **treinamento** das pessoas que utilizam o software, a **atenção** e os procedimentos **multi-etapas de verificação** são suficientes para evitar esse risco.

E é sempre bom lembrar que, embora o código do consumidor obrigue as empresas a cumprir os valores que ela mesma apresenta para seus produtos, existe essa exceção em preços claramente fora da realidade média.

Ou seja, quando um produto conhecido está muito abaixo do que realmente custa, presume-se a má-fé do consumidor. Portanto, o mais importante nesse caso é **agir rapidamente** e cancelar as compras feitas antes que isso se torne um problema maior.

COMO REDUZIR

O RISCO DE FRAUDES?

Ao longo do último capítulo, falamos sobre ações que você pode tomar para lidar especificamente com tipos de fraude mais comuns. Mas existem ainda práticas e estratégias que ajudam a reduzir as fraudes como um todo, independentemente de sua natureza. Que tal irmos mais a fundo nesses pontos? Veja como eles ajudam a manter o e-commerce mais seguro.

Estude melhor as fraudes online

Você pode pensar neste e-book como o primeiro passo para um estudo mais profundo sobre as fraudes a que seu negócio está sujeito no dia a dia de seu relacionamento com clientes. O guia que fornecemos aqui é apenas o início.

Então, aprofunde-se ainda mais em causas e consequências, comportamentos fraudulentos e como esses criminosos tentam enganar pessoas e sistemas. **Quanto mais você sabe sobre fraude, mais você entende de antifraude** — a capacidade da empresa em prevenir e combater esse tipo de ato criminoso.

Com **informação e inteligência**, você pode ser a maior proteção para que sua loja cresça de maneira segura e sustentável.

Capacite os profissionais

Além de sistemas melhores, é importante reforçar que plataformas digitais são tão seguras quanto a pessoa menos preparada que a utiliza.

Atualmente, muitas dessas práticas de monitoramento antifraude são automatizadas, mas é sempre bom contar com um corpo de profissionais que domina as ferramentas e sabe identificar riscos para potencializar a ação da tecnologia.

COMO REDUZIR O RISCO DE FRAUDES?

Melhore seu compliance

O compliance é a culminação de preparo de pessoas e de ferramentas dentro da rotina de um negócio. É estar em conformidade com normas internas, diretrizes de processos e determinações legais.

Um bom **monitoramento de compliance** vai **evitar brechas de procedimento que se tornam oportunidade de fraude** para cibercriminosos. Por exemplo, é capaz de reduzir bastante a possibilidade de engenharia social para acesso não autorizado ao sistema de gestão da empresa.

Compliance é um trabalho em conjunto, de gerenciamento, ações e comunicação. Seja com três colaboradores ou 300, é importante que todos entendam seu papel nessa rede de eficiência e tenham determinações claras para a prática de seu trabalho.

Fique de olho nos principais indicadores

Para o setor de e-commerce, existem três indicadores fundamentais para determinar o sucesso da sua estratégia antifraude. São eles:

- **Tempo de resposta** para a aprovação ou rejeição de um pedido, que se relaciona diretamente com o tempo de análise de dados em busca de uma possível fraude;

- **Taxa de aprovação de pedidos**, apontando principalmente qual é a porcentagem das compras iniciadas que são rejeitadas por possível fraude;

- **Índice de chargeback**, que determina a porcentagem de vendas que resultam em pedidos de estorno.

Uma empresa está bem estruturada para lidar com fraudes quando há um equilíbrio entre essas métricas. O ideal é um tempo de resposta rápido, com taxa alta de aprovação e um índice baixo de chargeback. Porém, sabemos que isso nem sempre é possível.

Uma verificação mais apurada vai diminuir o tempo de resposta, enquanto uma taxa de aprovação maior pode aumentar também o chargeback. Portanto, o **ideal é trabalhar no balanço entre eles** para um ponto ideal de experiência fluída aos consumidores, mas com um rigor maior que evite fraudes.

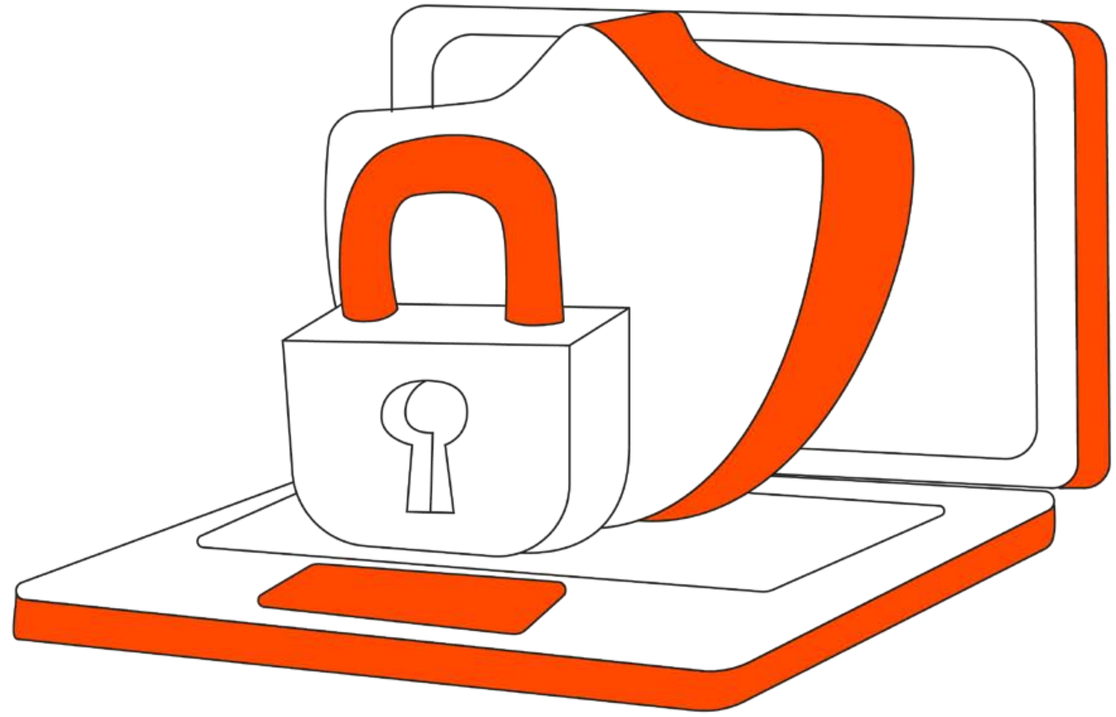
Invista em tecnologia

A melhor maneira de ter aprovações rápidas, mas sem riscos, é investindo em soluções de tecnologia que façam isso. Logo, é fundamental contar com um bom sistema de gestão automatizada, como um **ERP ou SAP.**

Essas são plataformas agregadoras de dados que facilitam o monitoramento de indicadores e a identificação de problemas persistentes no faturamento da empresa. Mas também é muito importante contar com **ferramentas especializadas no combate antifraude.**

COMO FUNCIONA

O ANTIFRAUDE DA CLEARSALE?



O grande diferencial da ClearSale, que nos fez virar referência em antifraude nos nossos mais de 20 anos de experiência, é **saber utilizar a informação em favor da segurança.**

Nossas soluções antifraude são construídas com base no monitoramento profundo e constante da evolução de métodos de fraude ao longo de todos esses anos, que servem de fundação para o aprimoramento contínuo de ferramentas de análise e controle.

É assim que funciona a tecnologia antifraude para e-commerce da ClearSale. Um software capaz de analisar processos e padrões e utilizar uma imensa base de dados de mercado para **autenticar rapidamente** a legitimidade de pedidos feitos na sua loja virtual. Mas como isso funciona na prática?

A base dessa tecnologia inovadora de inteligência de dados está no **Data Lake** da ClearSale. Lago de dados é o nome dado a um repositório de informações armazenadas em seu estado bruto, que cria um imenso volume de registros coletados de determinadas fontes.

No nosso caso, esse lago é formado por dados armazenados e minerados por mais de 20 anos de trabalho antifraude. Quer ter uma ideia do tamanho dessa base de inteligência que a ClearSale coloca à sua disposição? Veja alguns números impressionantes:

150 mil novos telefones reconhecidos todos os dias;

9 em cada 10 e-mails usados no e-commerce reconhecidos;

111 mil novos e-mails reconhecidos todos os dias;

95,8% de cobertura nacional de CPFs;

+108 mi de pares de CEP e CPF;

1,7 bi de dados na base de relacionados;

240 mi de dispositivos (IPs e DeviceIDs);

+139 mi de hotphones da população economicamente ativa no Brasil;

+4,75 mi de transações fraudulentas capturadas.

Essa abrangência e variedade de informações nos permite ter uma **base de dados acima da média do mercado.** Com o cruzamento dessas informações em nossa solução, é possível encontrar discrepâncias mínimas nos dados fornecidos ou até padrões que seriam imperceptíveis em modelos mais simples de atuação antifraude.

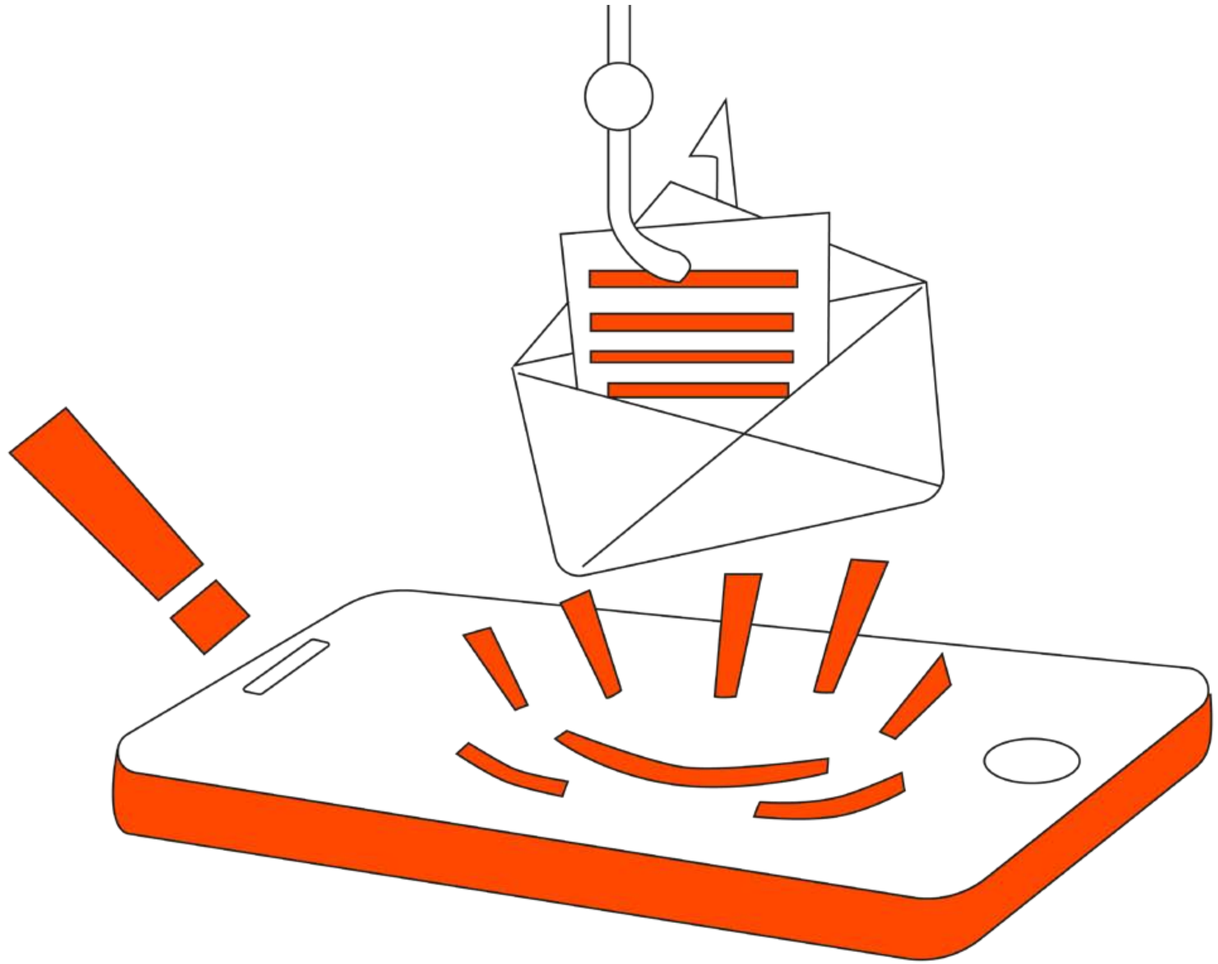
Dentro do e-commerce, nossa experiência se estende a todo o segmento, de delivery a artigos de luxo. O antifraude ClearSale é capaz de se adaptar a qualquer necessidade e, com isso, atuar na verificação de integridade de compras em qualquer perfil de público. É com esse foco em inteligência que já temos parceria com mais de 5.000 clientes.

Evoluímos constantemente a nossa solução para que ela seja capaz de **dar às empresas o melhor dos três indicadores que apontamos**: melhor taxa de aprovação, menor índice de chargeback e tempo de resposta mínimo para concluir vendas.

Tudo isso de maneira automatizada e inteligente, tirando dos profissionais do e-commerce o peso de terem que lidar com esses riscos. Ao ter a certeza de que as fraudes são um risco mínimo, você pode focar seu esforço e da sua equipe em uma atuação mais estratégica para atrair e converter ainda mais clientes.

COMO FUNCIONA O ANTIFRAUDE DA CLEARSALE?

CONCLUSÃO



Este e-book foi pensado para que você pudesse se aprofundar na realidade da fraude online e o que ela significa para os e-commerces atuais. Para isso, falamos sobre as origens e as características desse tipo de risco, os principais tipos a que lojas virtuais estão sujeitas diariamente e o que você pode fazer para reduzir essa incidência no seu negócio.

Por fim, apresentamos a **solução antifraude da ClearSale**, uma grande ajuda para lidar com esse problema com tranquilidade, eficiência e segurança. Incentivamos você a conhecer mais sobre fraudes e sobre a solução da ClearSale, capaz de mitigar esses riscos.

Como dissemos algumas vezes durante este conteúdo, **a informação é a maior arma que um negócio digital tem para crescer.** Muito sucesso!

ClearSale

A ClearSale (CLSA3), com mais de duas décadas de experiência no combate às fraudes digitais, é referência em inteligência de dados e oferece um portfólio completo com soluções flexíveis e adaptáveis às necessidades individuais de cada negócio, composto por múltiplas camadas de proteção e antecipação de riscos em diversos setores, como e-commerce, mercado financeiro, vendas diretas, telecomunicações, dentre outros.

Por meio da sua base de clientes, a ClearSale possui um robusto banco de dados que impulsiona um efeito de rede de proteção singular, sendo a empresa que melhor conhece o comportamento digital do consumidor brasileiro. Os especialistas em fraude da companhia lideram a gestão de riscos, dedicados a detectar padrões de ataques e implementar soluções tecnológicas com o mínimo de fricção para combater qualquer tipo de fraude.

Saiba mais sobre as soluções de antifraude para e-commerce da ClearSale

Clique aqui