

stripe

# Panorama da fraude online



# Introdução

Este relatório apresenta uma visão geral abrangente do panorama da fraude online. Durante dois anos, analisamos bilhões de pagamentos em milhões de empresas que utilizam a Stripe e trabalhamos com a Milltown Partners (em parceria com a focaldata) para entrevistar mais de 2,5 mil líderes empresariais em nove mercados ao redor do mundo (Austrália, Canadá, França, Alemanha, Japão, Países Baixos, Singapura, Reino Unido e Estados Unidos).

Unimos nossa própria análise da Stripe aos resultados da pesquisa e conseguimos identificar as principais tendências de fraude do ano passado, como o aumento de disputas relacionadas a produtos em 2020 e a preocupação das empresas de pagamentos recorrentes com o impacto financeiro das fraudes. Também apresentamos no relatório dicas baseadas nos resultados para mostrar como se adaptar a essas tendências de fraude. Finalizamos o relatório com quatro práticas principais recomendadas conforme nossas previsões em relação ao futuro do setor de fraudes.

Categorizamos este relatório em quatro seções:

- Por que houve um aumento de fraudes
- Distinção das fraudes por região e porte da empresa
- O impacto empresarial das fraudes
- Nossas previsões para o combate à fraude

# Resumo executivo

- De acordo com a nossa pesquisa, 64% dos líderes empresariais globais afirmam que, desde o começo da pandemia, ficou mais difícil combater fraudes. Acreditamos que isso aconteça, em parte, devido ao aumento dos tipos e do volume geral de fraudes.
- No começo da pandemia, observamos um aumento temporário de 156% nas disputas relacionadas a produtos, como códigos de disputa de “produto não recebido” e “produto inaceitável”. Nossa hipótese é que os clientes solicitaram reembolso quando os vendedores demoravam semanas, ou até meses, para processar os pedidos devido a interrupções na cadeia de fornecimento.
- Também observamos que 40% mais empresas passaram por tentativas de ataques de teste de cartões. Milhares de novas empresas de e-commerce foram criadas durante a pandemia, e acreditamos que esse crescimento gerou novas oportunidades para os fraudadores.
- Empresas do mundo todo enfrentaram aumento de fraudes, porém companhias na América Latina foram e continuam sendo mais suscetíveis a ataques de fraudadores. Observamos que essas empresas apresentaram uma taxa de fraude 70% maior do que as da América do Norte e 143% maior do que as da região Ásia-Pacífico. Isso acontece devido a diversos fatores específicos da região.
- As empresas de pagamentos recorrentes foram as que mais sofreram com fraudes, especificamente as empresas B2C (business to consumer, empresa que oferece um produto ou serviço para consumidor). Mais de 75% das empresas B2C com um modelo por assinatura na América do Norte, Europa e região Ásia-Pacífico relataram aumento no volume de revisão manual e a necessidade de direcionar mais recursos para combater fraudes no ano passado. Acreditamos que essas empresas voltadas para consumidores apresentam maior reconhecimento de marca, ou seja, seus produtos são fáceis de revender. Por isso, é mais provável que os fraudadores visem esse tipo de empresa.
- O impacto empresarial das fraudes vai além das perdas financeiras. A análise da Stripe descobriu que quanto mais fraudes uma empresa tenta prevenir, maior é a probabilidade de bloquear também cobranças legítimas, reduzindo as taxas de conversão de pagamentos. Para reduzir esses falso-positivos, as empresas podem revisar manualmente alguns pagamentos, mas isso aumenta as despesas operacionais.
- Estimamos que as empresas se adaptarão a essas tendências de quatro maneiras: 1) as intervenções, como o uso da ferramenta de autenticação 3D Secure, terão mais importância; 2) melhores fontes de dados ajudarão as empresas a tomar decisões mais rápidas e precisas; 3) os emissores e as empresas colaborarão mais para simplificar as disputas e reduzir os pagamentos legítimos recusados; e 4) as preferências de pagamento dos clientes continuarão mudando, alterando o panorama da fraude.

## Por que houve um aumento de fraudes

A COVID-19 gerou uma onda histórica de crescimento do e-commerce. As empresas que utilizam a Stripe processaram globalmente mais de US\$ 640 bilhões em pagamentos em 2021, um aumento de 60% em relação ao ano anterior. Esses pagamentos foram feitos por um grupo crescente de empresas: 1,4 mil novas empresas adotaram a Stripe a cada dia no ano passado. Esse crescimento no e-commerce, especialmente de novas empresas, criou mais oportunidades para os fraudadores.

Muitas pessoas estavam fundando empresas pela primeira vez e não tinham as ferramentas nem os recursos para lidar com fraudes ou estavam mais focadas em estabelecer seu negócio e ter lucro, em vez de criar uma estratégia de prevenção a fraudes. Contudo, estas novas empresas não foram as únicas a enfrentar esses desafios, pois até mesmo empresas bem estabelecidas encontraram dificuldades em combater fraudes devido a tipos mais complexos ou volumes mais altos de fraude em relação ao período anterior à pandemia.

Ao mesmo tempo, os fraudadores continuam se tornando mais sofisticados. Eles descobrem novas maneiras de atacar empresas, formando grupos e interagindo com outros fraudadores para compartilhar as “melhores práticas”.



Conforme mais pessoas fazem compras online em nossas lojas, o volume dos pagamentos fraudulentos aumenta. É difícil revisar manualmente todas as transações, então nos concentramos em algumas, pois não há recursos suficientes.

- Profissional de combate à fraude em uma empresa de e-commerce de Singapura



Observamos um aumento nas disputas relacionadas a produtos e nos ataques de teste de cartões:

## **As disputas relacionadas a produtos dobraram em 2020 em relação a 2019**

De março a maio de 2020, o estudo da Stripe descobriu que, em relação a 2019, havia duas vezes mais chances de pagamentos serem contestados usando códigos de disputa como “produto não recebido” e “produto inaceitável”. Nossa teoria é que os clientes solicitaram mais estornos já que os vendedores demoravam semanas, ou até mesmo meses, para processar os pedidos devido à interrupções na cadeia de fornecimento.

Aparentemente, a América Latina apresentou as taxas mais baixas de disputas relacionadas a produtos, mas acreditamos que isso ocorreu devido ao comportamento dos emissores na região. No México, as disputas são sete vezes mais propensas a serem relatadas sem um código de motivo do que todos os países juntos. No Brasil, as disputas são 50% mais propensas a serem relatadas como fraudes.

### **Práticas recomendadas para prevenção a disputas relacionadas a produtos:**

- Sua política de devolução deve ser clara, transparente e razoável. Por exemplo, inicie o período de devolução quando o cliente receber o item em vez de quando o item for enviado.
- Adicione o nome da sua empresa diretamente na fatura do cartão de crédito.
- Estabeleça um processo formal de disputa.
- Avise os clientes antes de processar o pagamento. As empresas de assinatura devem garantir que os clientes recebam pelo menos um lembrete sobre o próximo pagamento.
- As empresas de e-commerce devem exigir a assinatura do cliente na entrega do pedido.

## **Tentativas de ataques de teste de cartões visaram 40% mais empresas**

O teste de cartões ocorre quando alguém tenta determinar se um cartão roubado está ativo para poder utilizá-lo para fazer compras. Um fraudador pode fazer isso ao comprar dados de cartões de crédito roubados e tentar validar ou fazer compras com esses cartões para determinar quais cartões ainda são válidos.

Durante o primeiro ano da pandemia, houve um pico de 40% no número de empresas que passaram por tentativas de ataques de teste de cartões. Essa tendência se aplicou a empresas novas e estabelecidas. Entretanto, segundo dados da nossa plataforma, as empresas novas (as que haviam se registrado na Stripe há até 90 dias) foram mais visadas pelos ataques de teste de cartões.

Os ataques de teste de cartões podem afetar negativamente as empresas de várias formas. O influxo de transações devido a um ataque de teste de cartões pode gerar custos mais altos de processamento de pagamentos e risco de indisponibilidade (se uma empresa não conseguir

gerenciar o aumento no tráfego, o site pode cair). Além disso, os ataques bem-sucedidos de teste de cartões prejudicam o ecossistema financeiro global. As empresas podem estar propensas a processar pagamentos com cartões roubados, resultando em mais disputas. Devido ao risco para o ecossistema financeiro, as empresas podem ser penalizadas pelos emissores e pelas bandeiras de cartão por permitirem esses ataques.

Outra [análise da Stripe](#) de novembro de 2021 descobriu que as instituições de caridade são bastante afetadas por ataques de teste de cartões: 11% de todos os ataques de teste de cartões que observamos tiveram instituições de caridade como alvo. Por quê? Muitas instituições de caridade permitem que os doadores (neste caso, fraudadores) escolham um valor de doação bem pequeno, como US\$1,00 ou US\$5,00. Transações de valores baixos são menos suscetíveis a serem percebidas pelo titular real do cartão em um extrato. Além disso, as instituições de caridade são mais propensas a terem equipes antifraude menores e carecer de recursos para bloquear transações. Não só as instituições de caridade (e qualquer empresa vítima de teste de cartões) perdem dinheiro, como também são penalizadas pelos bancos por permitirem esses ataques.

### Melhores práticas para prevenir ataques de teste de cartão

- Otimize a integração com o seu provedor de pagamento. Muitos provedores de pagamento aplicam diferentes proteções para mitigar um ataque de teste de cartões, mas o sucesso desses controles depende da qualidade da sua integração e dos dados que você envia ao provedor. Em geral, quanto mais dados sua integração fornece, mais bem-sucedida pode ser a prevenção a teste de cartões.
- Mantenha suas chaves da API em segurança. Sua chave secreta da API pode ser usada para fazer qualquer chamada da API em nome da sua conta, como criar cobranças ou realizar reembolsos. Trate sua chave secreta da API como você trataria qualquer outra senha e conceda acesso apenas a quem precisar dela.
- Habilite o CAPTCHA em seu fluxo de checkout para diferenciar entre clientes legítimos e bots de teste de cartões.
- Defina limites para controlar o volume de tráfego de entrada e saída em seu site. Por exemplo, se os testadores de cartão criam novos perfis de cliente para poder validar cartões, você pode limitar o número de novos clientes provenientes de um único endereço IP em um dia.
- Considere exigir que os clientes façam login na conta para fazer um pagamento.

# A diferença entre as fraudes por região, país e porte da empresa

A importância de combater a fraude é universal: 90% dos líderes que entrevistamos na América do Norte, Europa e região Ásia Pacífico dizem que prevenir fraudes no e-commerce é importante para as empresas. No entanto, há diferenças sutis na atividade das fraudes conforme o setor e a localização da empresa, sugerindo um panorama complexo.

## Fraude por região e país

*A maior quantidade de dados de pagamentos da Stripe se refere à empresas da América do Norte, então usaremos essa região como referência para outras partes do mundo na análise desta seção.*

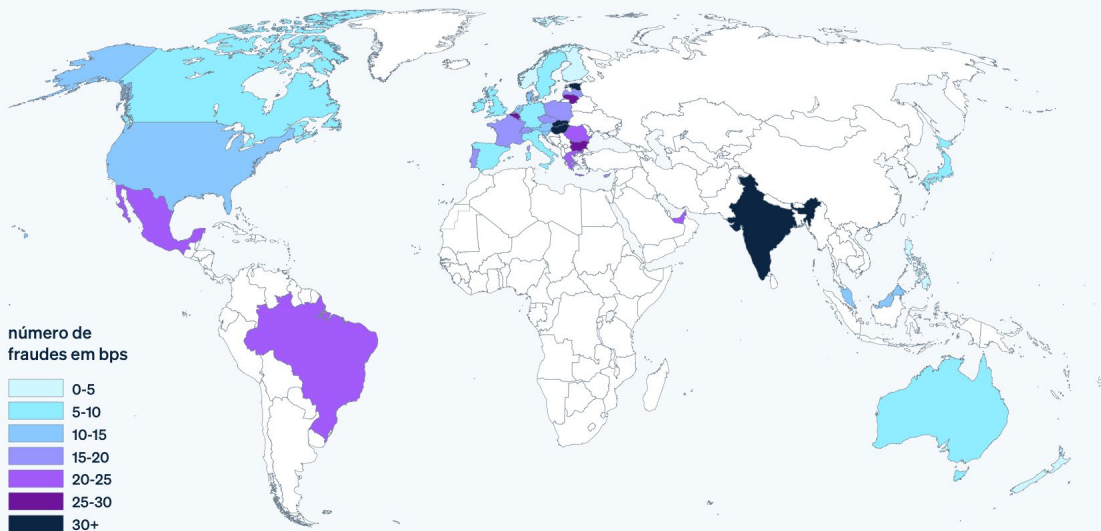
Nossos dados evidenciaram que a América Latina teve as mais altas taxas de fraudes de cartão do mundo durante o período analisado: 97% mais alta do que a América do Norte e 222% mais alta do que a região da Ásia-Pacífico. As regras também tendem a favorecer os titulares de cartão durante o processo de disputas, fazendo com que as empresas fiquem especialmente vulneráveis às fraudes. Além desses fatores locais, o mercado está cada vez mais ampliando sua presença online (houve um aumento de **518%** nas novas empresas que começaram a usar a Stripe na América Latina em 2021), criando ainda mais oportunidades para fraudadores.

Empresas na Europa, no Oriente Médio e na África apresentaram taxas de fraudes bem menores do que a América do Norte, o que reflete o impacto das regulamentações de **SCA (strong customer authentication, autenticação forte de cliente)**, que obrigam empresas a adicionarem a autenticação de dois fatores ao fluxo de checkout.

Também houve uma variação considerável entre países. Por exemplo, a França tem quase o dobro da taxa de fraude da Alemanha, enquanto Singapura apresentou uma taxa de fraude que corresponde à metade da região Ásia-Pacífico como um todo. Essa variação da fraude entre os países pode dificultar ainda mais para as empresas globais combaterem as fraudes. Por isso, nunca haverá uma abordagem única para o gerenciamento de fraudes.

## Taxa de fraudes por país identificadas pelo Stripe Radar

O Stripe Radar usa *machine learning* para detectar e bloquear fraudes para quaisquer tipos de negócios.



### Recomendações:

Se você tiver a possibilidade e recursos suficientes, recomendamos analisar os comportamentos dos clientes, as tendências do mercado e as regulamentações de cada país onde você opera para entender melhor os golpes e os tipos de fraude mais comuns de se enfrentar. No entanto, conforme as empresas crescem, essa complexidade pode se tornar muito difícil de gerenciar, ressaltando a importância de usar uma ferramenta sofisticada e automatizada contra fraudes.

## Fraude por porte da empresa e modelo de negócio

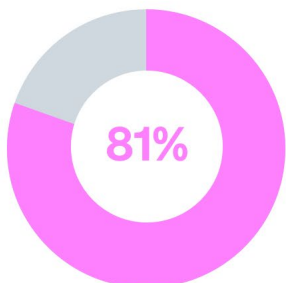
Os líderes empresariais interpretam o risco de fraude de forma diferente dependendo do porte da empresa e do modelo de negócio. Por exemplo, nossa pesquisa com usuários da América do Norte, Europa e Ásia-Pacífico mostrou que a importância da prevenção a fraudes aumenta conforme a dimensão da empresa e, como já esperado, as maiores têm mais recursos para investir na estratégia de prevenção a fraudes em relação às menores. Entretanto, apenas recursos não previnem fraudes. De acordo com nossa pesquisa, os líderes empresariais com equipes antifraude grandes foram mais propensos a enfrentar desafios operacionais ao gerenciar fraudes e são mais suscetíveis a relatar maiores perdas devido a fraudes.

Essas tendências podem indicar oportunidades para empresas menores: as empresas em crescimento podem optar por desenvolver uma estratégia antifraude aprofundada neste momento, quando ainda são pequenas, para ficarem à frente do problema. Contudo, direcionar tempo e recursos

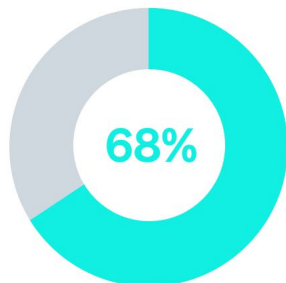


para combater fraudes pode acontecer às custas do crescimento da empresa, e as empresas menores devem considerar as contrapartidas.

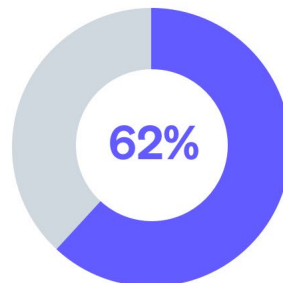
### Os líderes de empresas maiores apresentam maior probabilidade de considerar a fraude no e-commerce muito importante



Empresas maiores

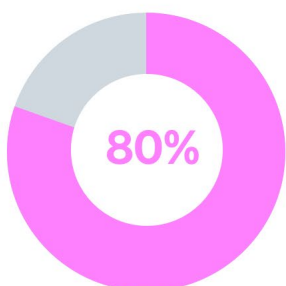


Empresas em crescimento

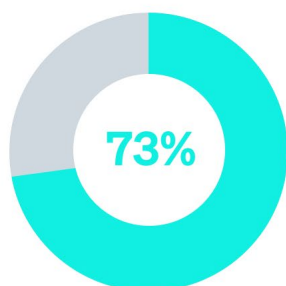


Startups

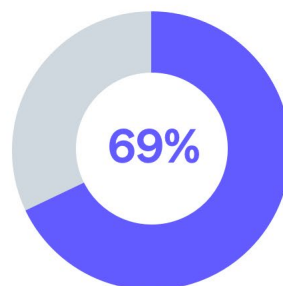
### Os líderes de empresas maiores apresentam maior probabilidade de concordar com o fato de que esperam implementar mais recursos para prevenção a fraudes neste ano do que no ano passado



Empresas maiores



Empresas em crescimento



Startups

**Empresas em crescimento:** empresa cuja receita anual é de US\$ 2 milhões a US\$ 60 milhões.

**Empresa maiores:** empresa cuja receita anual >US\$ 60 milhões.

**Startup:** empresa cuja receita anual <US\$ 2 milhões.

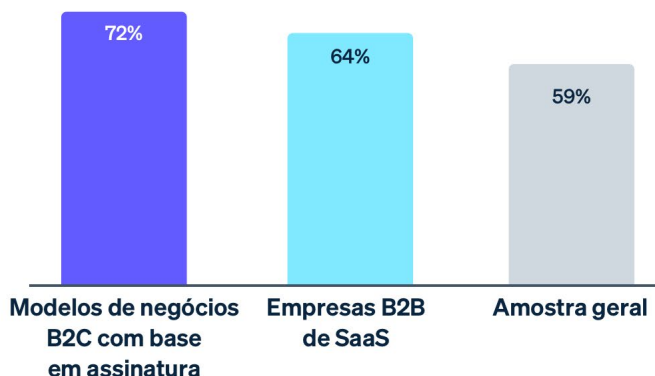
Também analisamos os resultados da nossa pesquisa com base no modelo de negócio, categorizando as empresas conforme segue:

- Software como serviço (SaaS)
- Assinaturas B2C
- Marketplaces e plataformas
- E-commerce

Descobrimos que as empresas com modelo de pagamentos recorrentes foram as que mais se preocuparam com o impacto financeiro das fraudes. Em relação a outros modelos de negócio

que pesquisamos, os líderes de combate a fraudes em empresas com pagamentos recorrentes apresentaram maior preocupação em perder dinheiro devido a fraudes e foram mais propensos a pensar que perderam uma proporção maior da receita devido a fraudes em 2021, em comparação ao período pré-pandemia. Essas preocupações podem ser resultado do modelo de negócio: como geram receita de acordo com um cronograma definido (como mensal ou trimestralmente) e como as taxas de fraude aumentaram no ano passado, eles são mais propensos a pensar que essa tendência continuará à medida que sua empresa cresce.

**As empresas de receita recorrente apresentam maior probabilidade de afirmar que estão preocupadas em perder mais dinheiro devido a fraudes em 2022 do que em 2021**



Especificamente, as empresas B2C na América do Norte, Europa e Ásia-Pacífico com modelo por assinatura sofreram mais com o ônus operacional das fraudes. Eles foram mais suscetíveis a relatar que os casos de revisão manual aumentaram em 2021, que direcionaram mais recursos para combater fraudes e que precisaram adiar planos de investimento ou expansão para gerenciar fraudes.

Nossa teoria é que as empresas B2C enfrentaram mais fraudes por haver uma maior propensão a serem marcas conhecidas, facilitando a revenda de produtos ou serviços roubados pelos fraudadores (como a compra de uma assinatura digital com um cartão de crédito roubado, vendendo-a posteriormente por um preço menor).

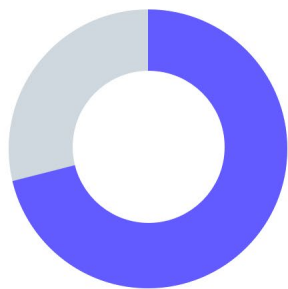
## O impacto empresarial das fraudes

As fraudes custam caro. Na verdade, 59% dos entrevistados esperam que as empresas percam mais receita devido a fraudes neste ano do que no ano passado.

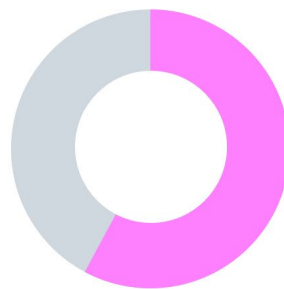
As empresas perdem dinheiro por causa de disputas por fraudes e ao tentar preveni-las. Por exemplo, se sua empresa perder uma disputa, você é responsável por pagar mais do que o valor da transação original. Geralmente, as fraudes geram tarifas de reembolso (custo associado à anulação pelo banco do pagamento com cartão) e mais tarifas das bandeiras devido à disputa.

No entanto, nossa pesquisa descobriu que o impacto empresarial das fraudes vai além dos prejuízos financeiros. Muitas empresas precisam ampliar suas equipes antifraude ou direcionar recursos de produtos ou engenharia para gerenciar as despesas gerais operacionais, removendo recursos valiosos do produto principal.

## O impacto empresarial da fraude vai além das perdas financeiras



**72%**  
dos líderes empresariais globais precisaram **direcionar recursos de produtos ou engenharia para combater fraudes**



**58%**  
dos líderes empresariais globais precisaram **adiar os planos de expansão ou investimento devido a fraudes**

## Menores taxas de conversão de pagamento

Na análise da Stripe, descobrimos que, quanto mais fraudes uma empresa tenta prevenir, maior é a probabilidade de bloquear também cobranças legítimas.

Pagamentos legítimos recusados, ou falso-positivos, referem-se às situações em que um cliente regular tenta fazer uma compra, mas não consegue. Pagamentos erroneamente recusados podem fazer com que a reputação e o lucro bruto das empresas sejam prejudicados. Na realidade, **33% dos consumidores** disseram que não comprariam novamente em uma empresa após um pagamento recusado sem razão.

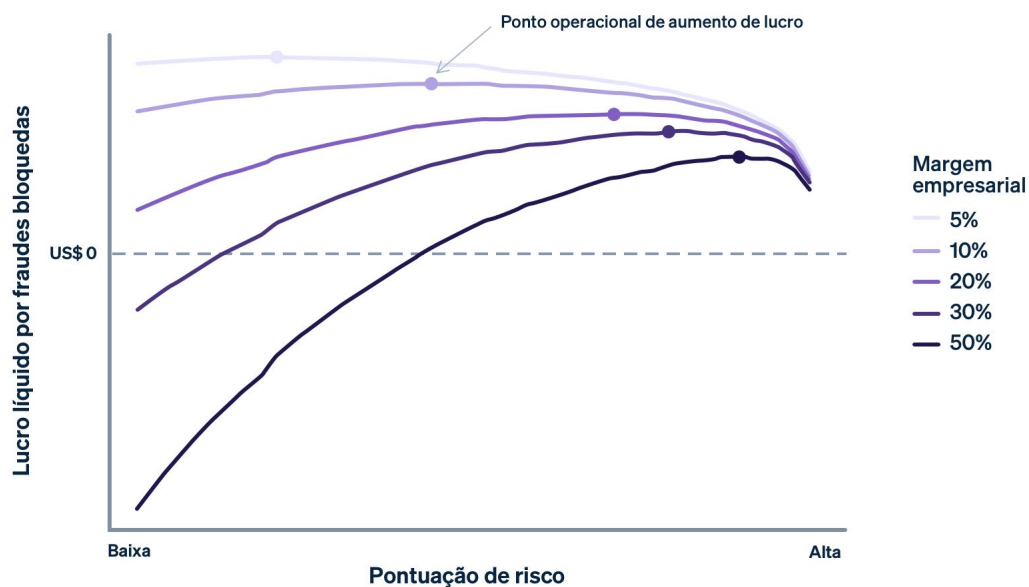


Até mesmo um único problema de fraude pode causar muitas complicações e nos fazer perder um comprador legítimo devido a revisões adicionais de segurança.

- Profissional de combate a fraudes em uma empresa SaaS no Canadá

Há uma paridade entre prevenir mais disputas e reduzir o número de clientes legítimos bloqueados. Ao prevenir mais fraudes, o número de clientes idôneos bloqueados aumenta. Por outro lado, reduzir o número de clientes idôneos bloqueados equivocadamente costuma elevar a probabilidade de acontecerem mais fraudes reais. Essa contrapartida também depende da sua solução antifraude: você sempre terá que gerenciar essa contrapartida se sua solução contra fraudes for estática e se você não investir em recursos contínuos para melhorá-la. Por outro lado, se sua solução antifraude contar com modelos de prevenção que se adaptam constantemente, essa contrapartida pode ser um desafio menor.

Devido à ligação entre prevenir disputas e bloquear pagamentos legítimos, as empresas podem selecionar um limiar de bloqueio de pagamento para maximizar os lucros. Esse ponto de ampliação dos lucros é onde há a maior diferença entre os custos de fraudes evitados e o bloqueio de lucros idôneos.



**Pontuação de risco** é o limiar em que as transações são bloqueadas por meio do Stripe Radar (as configurações padrão bloqueiam as transações quando excedem uma pontuação de risco de 75).

**Lucro líquido por fraudes bloqueadas** é o resultado dos custos totais de fraudes evitadas menos o valor de transações legítimas bloqueadas que gerariam lucro.

**Ponto operacional de aumento de lucro** é o ponto exato em que uma empresa maximiza o lucro líquido por fraudes bloqueadas, acontecendo a otimização entre o bloqueio de transações fraudulentas e a aprovação de transações idôneas.

**Como interpretar o gráfico:** conforme o limiar de risco aumenta ao longo do eixo x, há uma probabilidade maior de a transação ser fraudulenta. Quanto maior o apetite ao risco, menos transações são bloqueadas. Conforme você bloqueia mais transações, o lucro líquido por fraudes bloqueadas aumenta, mas também há uma maior probabilidade de bloquear transações legítimas.

A estratégia entre prevenir fraudes e bloquear transações legítimas depende da margem por transação. Por exemplo, empresas com margem alta (50%) ao longo da linha azul-escuro no gráfico podem ser mais suscetíveis a aprovar mais transações e ter um apetite de risco mais alto, porque cada transação legítima aprovada é muito mais valiosa (em relação a uma empresa com uma margem menor, por exemplo).

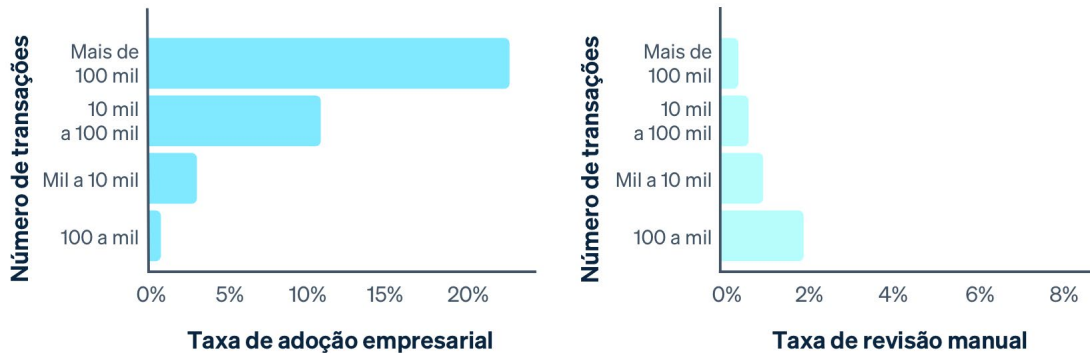
## Despesas gerais operacionais

Em uma tentativa de reduzir falso-positivos, as empresas podem revisar manualmente alguns pagamentos sinalizados para confirmar se são realmente fraudulentos. Isso é bastante trabalhoso; as empresas precisam de uma equipe de analistas de combate a fraudes para avaliar o risco com base em diversos fatores, como detalhes da transação e histórico do cliente.



É muito frustrante, porque significa que precisarei direcionar recursos para solucionar isso ou a situação pode sair do controle.

- Profissional de combate a fraudes em uma empresa SaaS na Austrália



Proporção de empresas ativas e elegíveis que usam a Stripe e adotam revisões manuais (taxa de adoção empresarial) e a proporção média de transações revisadas manualmente (taxa de revisão manual) por número de transações no ano passado (os números mencionados são os limites superiores dos grupos)

Descobrimos que empresas maiores são mais propensas a adotar revisões manuais, mas quanto maiores, menor a fração de transações que revisam. Por exemplo, mais de 20% das empresas que tiveram mais de 100 mil transações no ano passado usaram revisões manuais, mas revisaram menos de 1% do total de transações. Empresas grandes têm recursos para revisar manualmente as transações, mas guardam essas revisões manuais para transações de maior risco.

### Recomendações para reduzir as despesas gerais operacionais:

- Para empresas de e-commerce de médio a grande porte, uma solução baseada em *machine learning* pode ajudar a combater fraudes em escala, sem precisar de outros recursos de engenharia.
- Grandes empresas costumam usar diversas soluções pontuais (como ferramentas específicas de CAPTCHA ou leitor de cartão) junto com software antifraude ou como inteligência para seus próprios modelos de reconhecimento de fraudes.

## Nossas previsões para o combate à fraude

As fraudes estão sempre evoluindo, e em 2021 não foi diferente. Na verdade, os fraudadores se tornaram ainda mais sofisticados no ano passado, visando as empresas online de novas formas. Descrevemos vários desafios neste relatório, mas o que isso significa para sua empresa? Acreditamos que as empresas devem se adaptar ao panorama atual das fraudes de quatro maneiras:

### 1. As intervenções, como o 3D Secure, terão mais importância

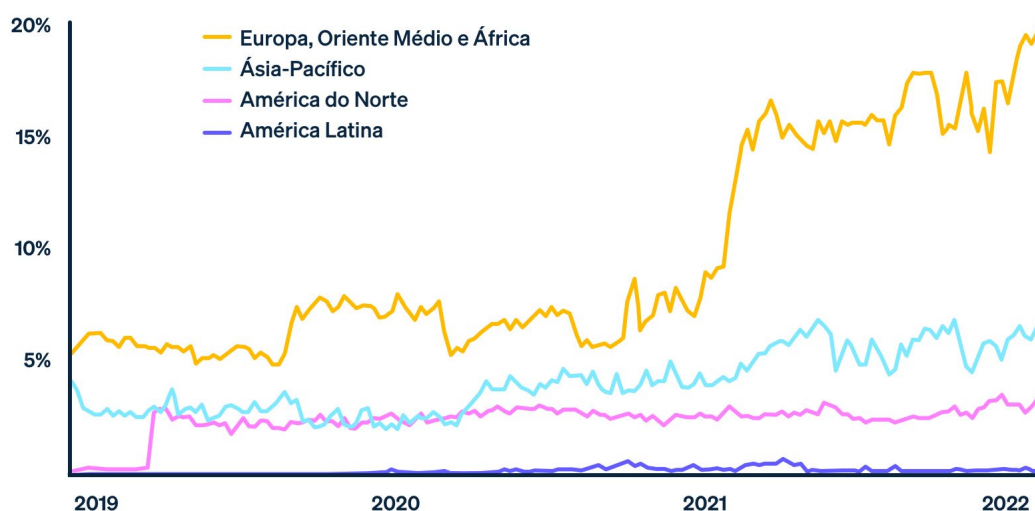
As intervenções possibilitam que você bloqueie ou aprove transações com mais confiança quando achar que são suspeitas, enviando um pedido de autenticação aos clientes (como inserir um código avulso enviado por mensagem de texto).

As intervenções podem ser realizadas de várias formas:

- 3DS**, que exige que os clientes façam uma autenticação de dois fatores antes do pagamento. Esse é o principal método de autenticação de cartão usado para atender aos requisitos de **SCA** na Europa e um mecanismo-chave para as empresas solicitarem **isenções** à SCA.
- Leituras de cartões para confirmar que o cliente tem o cartão físico em sua posse no momento da transação.
- Ferramentas CAPTCHA** que exigem que os visitantes de um site resolvam um enigma simples, como transcrever uma série de números ou letras de uma imagem distorcida.

As intervenções já estão ganhando popularidade. Em 2021, analisamos a atividade de uma intervenção específica, o 3DS, entre as empresas que usam a Stripe e descobrimos que a adoção desse método aumentou no geral, com os melhores resultados ocorrendo fora da América do Norte. Conforme esperado, as empresas europeias apresentaram o maior aumento na adoção do 3DS, porque os requisitos SCA foram totalmente aplicados em quase todos os países europeus elegíveis no ano passado. A popularidade das regulamentações do tipo SCA também está crescendo fora da Europa, com um aumento mais rápido na Índia.

#### Cobertura do 3DS nas cobranças por região ao longo do tempo



Em um experimento, a Stripe descobriu que reduzir o limiar em que o 3DS é acionado resultou em uma diminuição de 74% na taxa de disputas por fraude. Além disso, em relação ao bloqueio direto de pagamentos, o 3DS ainda permite que a maioria deles seja aprovado (67% em todos os níveis de risco, 5% para o nível de risco elevado). Entretanto, o desempenho do 3DS pode variar entre os bancos emissores.

Futuramente, esperamos que o uso de intervenções se intensifique. As empresas aplicarão as intervenções a uma parte maior do volume de transações e usarão tipos mais diversificados, principalmente os que reduzem o atrito no processo de checkout.

### Dicas de utilização de intervenções:

- Envie as transações que você bloquearia atualmente para passar por intervenções, a fim de aumentar a conversão e evitar o bloqueio de pagamentos legítimos.
- As intervenções podem gerar atritos na experiência do cliente, o que pode afetar negativamente a conversão. Otimize com cuidado e teste como acionar estas intervenções para garantir que você não afete adversamente os clientes legítimos.
- Cada intervenção tem uma taxa de aprovação diferente e um impacto distinto na redução de fraudes. Por exemplo, embora as chaves de segurança sejam extremamente eficazes para impedir fraudadores, elas podem prejudicar drasticamente a conversão. Escolha a intervenção certa de acordo com o grau de risco da ação que o cliente está realizando e sua tolerância ao risco/conversão.
- Implemente as intervenções onde elas forem lógicas na jornada do usuário, como ao solicitar uma leitura do cartão físico quando o cliente estiver inserindo os detalhes do cartão.

## 2. Fontes ricas de dados ajudarão as empresas a tomar decisões mais rápidas e precisas

O gerenciamento de fraudes costumava ser bastante manual, exigindo uma equipe de analistas para revisar toda e cada transação. Atualmente, a maioria das empresas utiliza algum nível de *machine learning* e automação para combater fraudes em escala, além de revisões manuais quando necessário (essa abordagem híbrida varia dependendo dos setores e dos modelos de negócio). Os modelos baseados em *machine learning* aprendem a discernir entre transações legítimas e transações potencialmente fraudulentas, e alguns conseguem treinar a si mesmos, o que os torna ainda mais escaláveis e eficientes.

Os modelos de *machine learning* são considerados uma tecnologia de ponta para combater fraudes, e hoje são fundamentais. Na verdade, os recursos de *machine learning* por si só não são mais suficientes para mitigar os riscos de fraudes em constante evolução. Os entrevistados da pesquisa na América do Norte, Europa e Ásia-Pacífico concordam: mais de 50% dos entrevistados, cujo processo de revisão é basicamente automatizado, disseram que o tipo e a quantidade de fraude que enfrentam está evoluindo rapidamente e suas empresas não conseguem acompanhar.



As fraudes financeiras se tornaram mais complexas e variadas ao longo do tempo. Precisamos nos adaptar constantemente a novos padrões e tipos de fraudes.

- Profissional de combate a fraude em uma empresa de serviços profissionais na Alemanha

Acreditamos que a próxima fase da evolução do gerenciamento de fraudes se concentrará em dados de melhor qualidade para aperfeiçoar os modelos de gerenciamento de fraudes. As ferramentas e a tecnologia para isso já estão disponíveis, mas costumam estar separadas em diferentes produtos; as empresas podem ter ferramentas separadas para verificação de identidade e para biometria,



por exemplo. No futuro, prevemos que as empresas conseguirão aproveitar melhor as tecnologias e integrações para consolidar essas informações em um só lugar, oferecendo uma abordagem holística para tornar os modelos de prevenção à fraudes mais eficientes.

Ao analisar os dados relevantes da jornada do cliente, incluindo comportamento, biometria e dados avançados de terceiros, relacionados a números de telefone, endereços de e-mail, os dados vindos dos bancos emissores e até mesmo plataformas de networking social, as empresas podem alcançar novos níveis de precisão na detecção de fraudes.

Embora esse nível de dados seja bastante útil para aprimorar os modelos de fraudes, as empresas precisam ter cuidado ao coletar e armazenar essas informações para garantir a conformidade com as leis globais de segurança e privacidade de dados.

### **3. Os emissores e as empresas colaborarão mais para simplificar as disputas e reduzir os pagamentos recusados sem razão**

Quando um cliente realiza uma compra no seu site, o provedor de pagamento coleta os dados da cobrança e os envia ao banco emissor (o banco do cliente) como uma solicitação de pagamento por meio das bandeiras de cartão, como Visa, Mastercard ou Elo. Os bancos emissores são os tomadores finais de decisão ao aprovar ou recusar uma transação durante a **fase de autorização**. Eles calculam o risco de fraude com base nos sinais limitados que recebem durante este processo.

Por outro lado, as empresas têm dados valiosos de seus clientes e da transação, como o endereço de faturamento e e-mail do cliente. A combinação desses dados com as informações que o emissor já tem pode gerar uma porcentagem maior de transações aceitas.

Melhores taxas de autorização e de fraude são mutuamente benéficas: o banco emissor reduz os prejuízos com fraudes, economiza com custos operacionais e aumenta o volume de transações aprovadas, diminuindo o número de reclamações de clientes sobre pagamentos recusados sem razão. Ao mesmo tempo, as empresas observam maiores taxas de conversão de pagamento e melhor retenção de clientes. No entanto, a maioria das empresas ainda não compartilha esses dados com os emissores, gerando uma assimetria de informações que contribuiu para os **US\$ 443 bilhões** em pagamentos recusados erroneamente em 2021.

Atualmente, uma mudança está acontecendo. Os emissores estão investindo na criação de APIs para melhorar as taxas de autorização, como a **API Enhanced Decisioning Data** da Capital One e a **API Enhanced Authorization da Amex**. Grandes empresas, para as quais cada aumento de ponto percentual na autorização se manifesta em milhões de dólares, também entendem a importância das parcerias de compartilhamento de dados e estão começando a investir na integração com emissores. Ainda assim, há uma lacuna para milhões de outras empresas que não têm capacidade técnica nem volume significativo de pagamentos para justificar o ROI de integrações personalizadas com emissores. Para essas empresas, parceiros financeiros, como a Stripe e outros provedores de pagamento, ajudam a facilitar esta integração por meio de parcerias diretas com bancos emissores.



## 4. As preferências de pagamento dos clientes continuarão mudando, alterando o panorama das fraudes

Formas de pagamento como **compre agora e pague depois** (BNPL), carteiras digitais e PIX estão em ascensão. Especificamente, a adoção dos serviços compre agora e pague depois aumentou: **mais de 50% dos clientes dos EUA** usaram um serviço compre agora e pague depois, que foi a forma de pagamento que cresceu mais rápido em 2020 na **Índia** e no **Reino Unido**.

Todas as formas de pagamento usadas para transações online apresentam algum nível de risco de fraude, e as formas de pagamento sem cartão não são diferentes. Por exemplo, formas de pagamento como compre agora e pague depois apresentam um risco menor de fraude na transação, mas podem ser mais suscetíveis a fraudes de novas contas (modalidade em que os fraudadores criam novas identidades durante o fluxo de onboarding, que pode ser pouco protegido) e controle de conta (quando um terceiro obtém acesso às credenciais da conta do cliente e usa os dados de pagamento para fazer compras fraudulentas).

Porém, as empresas podem mitigar esses riscos ao focar em estratégias de prevenção a fraudes no início do ciclo de interação com o cliente. Em vez de focar na transação em si, as empresas podem examinar atividades fraudulentas no começo da jornada para fazer uma avaliação antes que o cliente (ou fraudador) conclua uma compra. Por exemplo, as empresas devem confirmar a identidade do cliente durante o onboarding, verificar se há contas duplicadas e aplicar medidas de verificação de identidade no login, como a autenticação de dois fatores.

## Como a Stripe pode ajudar

A Stripe oferece um conjunto integrado de produtos de pagamentos que habilita esta proteção para varejistas online e em lojas físicas, bem como para empresas de assinatura, plataformas de software, marketplaces e muito mais. A fim de combater fraudes, milhões de empresas usam a Stripe para:

### Otimizar a experiência de pagamentos

- **Colete mais informações relevantes durante o checkout:** pedir que os clientes **forneçam mais informações relevantes** no checkout ajudará a verificar melhor a legitimidade deles. Por exemplo, solicite o nome e o endereço de e-mail do cliente. Essas informações adicionais podem ser transmitidas para o Stripe Radar, ferramenta antifraude da Stripe, resultando em uma melhor detecção por meio de *machine learning* e fornecendo mais evidências para fundamentar uma possível disputa.
- **Descubra outros métodos de pagamento:** o conjunto certo de meios **de pagamento** pode oferecer flexibilidade aos clientes e reduzir o risco de fraudes. Carteiras digitais, como Apple Pay e Google Pay, exigem verificação adicional do cliente (como biometria, SMS ou senha) para concluir um pagamento, gerando taxas menores de disputas. Da mesma forma, a maioria

dos débitos bancários, em que os fundos são retirados diretamente da conta bancária do comprador, exige que os clientes concordem com um pedido ou verifiquem a propriedade da conta, adicionando mais uma camada de segurança e reduzindo a possibilidade de disputas.

## Prevenir fraudes durante o checkout

- **Aproveite a detecção de fraudes por meio de *machine learning*:** a detecção de fraudes com base em regras, que opera conforme a lógica “se x acontecer, então faça y”, não foi criada para empresas digitais modernas e pode gerar perda de receita. O [Stripe Radar](#) se baseia em *machine learning* flexível, com algoritmos que avaliam todas as transações, atribuem uma pontuação de risco e bloqueiam ou permitem transações com base no risco de fraude. Os algoritmos do Radar se adaptam rapidamente aos padrões dinâmicos de fraudes e à sua empresa.
- **Previna fraudes e aumente a taxa de autorização por meio de parcerias com emissores:** por meio de parcerias, os bancos emissores e a Stripe compartilham dados selecionados de risco, quando possível, para ajudar os emissores a bloquear transações fraudulentas e aprovar as legítimas. A integração com os emissores gera valor para o titular do cartão e a empresa: os clientes podem comprar mais e com maior confiança, enquanto as empresas obtêm mais transações aprovadas sem o aumento de disputas por fraudes.
- **Aplice a autenticação de dois fatores de forma dinâmica:** o [Stripe Checkout](#) cumpre os [requisitos SCA europeus](#) e aplica dinamicamente a autenticação, como o 3DS, quando solicitado pelo banco do titular do cartão ou quando houver suspeita de fraude. O Stripe Checkout também inclui o método mais simples de validação de PCI com um SAQ A pré-preenchido, acionando o CAPTCHA somente quando suspeitarmos de ataques de teste de cartões para prevenir fraudes.

## Gerenciar fraudes com sua equipe

- **Crie regras antifraude personalizadas:** com o [Radar for Fraud Teams](#), você pode criar [regras](#) personalizadas para gerenciar como sua empresa lida com os pagamentos, bloqueando aqueles que você considera suspeitos ou os enviando para [revisão](#). Por exemplo, reduza a pontuação de risco exigida para acionar revisões manuais ou revise pedidos grandes de clientes que estão comprando pela primeira vez. O Radar for Fraud Teams também oferece [insights de riscos](#) sobre pagamentos específicos, permitindo que você entenda os fatores mais importantes que contribuem para uma pontuação de risco alta. Use essas informações para criar outras regras mais direcionadas.
- **Revise manualmente os pagamentos de alto risco:** o [Radar for Fraud Teams](#) inclui um processo de [revisão](#) adicional que permite sinalizar determinados pagamentos para fins de verificação, embora eles ainda estejam sendo processados e o cartão de crédito tenha sido cobrado. Apesar de o Radar for Fraud Teams ser comumente usado por organizações maiores, a capacidade de revisar pagamentos manualmente é útil, independentemente do tamanho da

empresa, embora as revisões manuais sejam particularmente eficazes para empresas menores. A revisão manual de pagamentos suspeitos pode ajudar você a agir com mais precisão, antes que ocorra uma disputa. Por exemplo, se você não tiver certeza sobre um pagamento quando estiver revisando, fale com o cliente por telefone ou e-mail. Caso suspeite que um pagamento seja fraudulento, você pode reembolsá-lo.

## Outras dicas de prevenção a fraudes

- **Tenha acesso a insights mais detalhados sobre tendências de fraudes:** o [Stripe Sigma](#) permite analisar rapidamente seus dados na plataforma da Stripe por meio de consultas SQL predefinidas ou personalizadas no Stripe Dashboard. Responda às perguntas complexas sobre sua empresa, entenda por que os clientes contestam pagamentos e qual é sua porcentagem de disputas. Também é possível usar o [Stripe Data Pipeline](#) para enviar dados atualizados da Stripe ao seu banco de dados Snowflake ou Amazon Redshift. Isso permite que você combine facilmente suas pontuações de risco da Stripe com outros dados de fraudes para elaborar relatórios mais acurados.
- **Otimize a conversão e recupere mais receita:** a solução da Stripe para verificação de imagem do cartão ajuda a reduzir o número de transações bloqueadas equivocadamente. Em vez de bloquear transações que possam ser de alto risco, esse recurso permite que os usuários tenham a chance de confirmar que estão com o cartão em mãos ao pedir que escaneiem uma imagem dele (lançamento em 2022).

Para saber mais sobre como o Stripe Radar pode ajudar sua empresa a combater fraudes, leia [nossa documentação](#) ou [registre-se para abrir uma conta](#).

## Outros recursos

Confira outros recursos que vão ajudar você a gerenciar fraudes e proteger sua empresa:

- [Introdução a pagamentos online](#)
- [Práticas recomendadas para prevenção a fraudes](#)
- [Um manual sobre machine learning para detecção de fraudes](#)
- [Radar for Fraud Teams: regras básicas](#)
- [Sobre o Stripe Radar](#)
- [Sobre o Radar for Fraud Teams](#)

# Metodologia

A Stripe analisou bilhões de tentativas de pagamentos de milhões de empresas de 2019 a 2021. Entre pagamentos e empresas, analisamos disputas e os respectivos motivos, previsões dos nossos modelos de *machine learning*, uso de 3DS e atividade de revisão manual das empresas. Em relação às taxas de fraudes dos países, excluimos da nossa análise os que apresentaram menos de 10 mil pagamentos em 2021, pois eram poucas transações para calcular as taxas de fraudes de forma confiável.

No começo de 2022, a Stripe também trabalhou com a Milltown Partners (em parceria com o provedor de dados focaldata) para pesquisar mais de 2,5 mil líderes empresariais em nove mercados ao redor do mundo (Austrália, Canadá, França, Alemanha, Japão, Países Baixos, Singapura, Reino Unido e Estados Unidos), que estimam que suas empresas obtêm pelo menos 10% das respectivas receitas de vendas online.