



GUIA ESTRATÉGICO

Sistema Antifraude em Pagamentos

As decisões que definem o resultado.
Um guia para quem responde por fraude, chargeback e conversão

Para CFOs, Diretores Financeiros
e Heads de Operação



R\$ 100,4 mi

protegidos por tecnologia antifraude no setor financeiro brasileiro no primeiro semestre de 2026. Quase o dobro do mesmo período de 2025.

No primeiro semestre de 2026, o setor financeiro brasileiro registrou mais de **1,7 milhão de tentativas de fraude de identidade** na entrada e no cadastro de clientes, segundo a Serasa Experian. É uma tentativa a cada nove segundos.

A iugu é uma Instituição de Pagamento autorizada pelo Banco Central que fornece infraestrutura e tecnologia financeira para operações de médio e grande porte.

O guia nasce dessa prática: quem processa milhões de transações aprende como a fraude entra e em que momento a conversão se perde.

Ele foi feito para times de risco, finanças, produto e tecnologia que precisam definir qual camada antifraude entra na arquitetura da empresa.

Sumário

01 O cenário das fraudes no Brasil

Quem está sendo atacado · Os vetores mais comuns · O custo que não aparece no DRE

02 Como funciona um sistema antifraude?

O score de risco e seus limites · O que um sistema antifraude não resolve · Como prevenir fraudes em pagamentos

03 Como escolher um sistema antifraude para pagamentos?

Decisão 1: regra ou modelo estatístico? · Decisão 2: bloquear ou revisar? · Decisão 3: qual erro custa mais? · Decisão 4: quem assume o chargeback?

O cenário das fraudes no Brasil



A fraude em pagamentos não é um problema pontual de segurança. É uma variável de resultado que afeta diretamente a margem, a taxa de conversão e a experiência do cliente legítimo.

Para quem processa transações em escala, o modelo mental de "proteger ou aprovar" deixa de ser suficiente. A questão passa a ser: qual é o custo de cada decisão, em cada ponta?

Quem está sendo atacado?

A fraude não escolhe verticais. Ela migra para onde o controle é mais fraco e o volume, mais alto. Em 2026, os setores mais afetados no Brasil combinam três características: alta recorrência transacional, processo de onboarding digital e base de clientes distribuída geograficamente.

- **E-commerce e marketplaces:** Alvo preferencial de fraude de cartão não presente, com chargeback como vetor primário de perda.
- **Fintechs e plataformas de pagamento:** Foco em fraude de identidade sintética no onboarding, abrindo contas com dados mesclados de pessoas reais e fictícias.
- **Empresas SaaS com cobrança recorrente:** Vulneráveis à fraude de teste de cartão, em que bots validam dados roubados em cobranças de baixo valor.
- **Operações B2B com split de pagamento:** Expostas à fraude interna e ao desvio de repasse, especialmente em modelos de marketplace com múltiplos recebedores.

Os vetores mais comuns

Quatro tipos de fraude concentram a maior parte das perdas em operações de pagamento no Brasil. Cada um opera com lógica diferente e exige resposta diferente.

Fraude de identidade

Uso de dados reais de terceiros para abertura de conta, contratação de serviço ou realização de compra. É o vetor mais volumoso e o que mais cresce em operações digitais.

Identidade Sintética

Combinação de dados reais e fictícios para criar uma identidade que passa pelas checagens básicas de cadastro. O perfil se comporta como legítimo por meses antes de acionar o golpe.

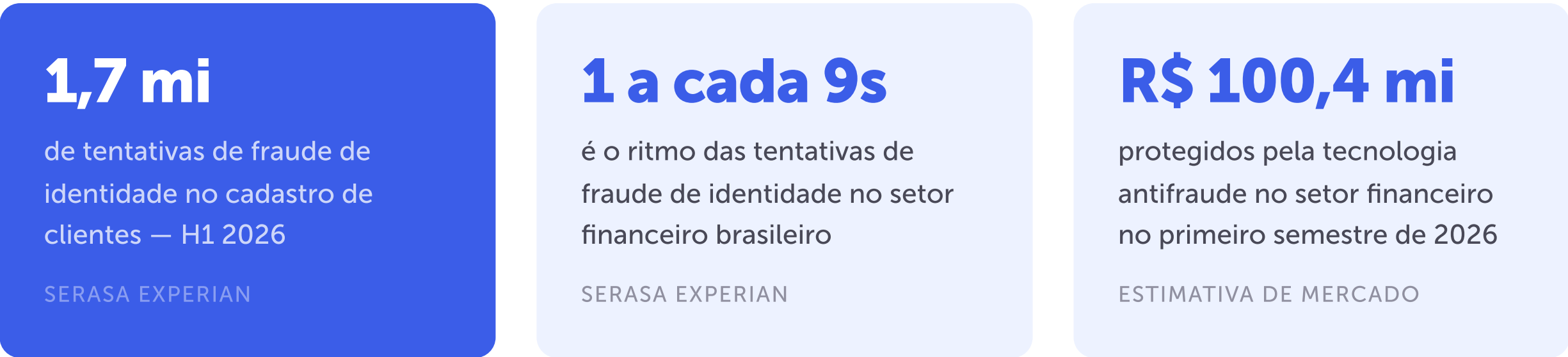
Fraude amigável (friendly fraud)

Cliente legítimo contesta uma compra que realizou, acionando o chargeback como instrumento de reembolso indevido. É invisível para sistemas de score e responde por parcela relevante das contestações em e-commerce.

Teste de cartão (card testing)

Bots realizam transações de baixo valor para validar dados de cartões roubados antes de usá-los em compras maiores. Afeta desproporcionalmente empresas com planos freemium ou cobranças de R\$ 1.

O custo que não aparece no DRE



O custo direto da fraude (chargeback, estorno, produto enviado sem pagamento) é mensurável. O custo indireto raramente aparece no DRE: aumento de tarifa de processamento por índice de contestação elevado, perda de clientes legítimos bloqueados por falso positivo, custo operacional da revisão manual e desgaste da marca.

Para o CFO, o número que importa não é apenas quanto a fraude custou. É quanto de conversão foi sacrificada para conter a fraude que ocorreu.

Como funciona um sistema antifraude?



Um sistema antifraude opera como uma cadeia de decisão automatizada. A cada transação, ele coleta sinais — comportamentais, cadastrais, transacionais e de dispositivo — e os converte em uma avaliação de risco. Essa avaliação determina se a transação é aprovada, bloqueada ou encaminhada para revisão manual.

A camada que sustenta essa decisão pode ser construída sobre três fundamentos distintos, usados de forma isolada ou combinada.

O score de risco e seus limites

O score de risco é o produto final do sistema antifraude. É um número — geralmente em uma escala de 0 a 1.000 — que representa a probabilidade de uma transação ser fraudulenta. Quanto maior o score, maior o risco estimado.

O score é calculado a partir de variáveis como: histórico do portador do cartão, geolocalização no momento da compra, fingerprint do dispositivo, velocidade de transações no CPF ou cartão, correspondência entre dados cadastrais e dados do pedido, e padrões comportamentais na sessão de compra.

O desafio operacional está nos pontos de corte (thresholds). Definir o score acima do qual a transação é bloqueada é, na prática, definir o equilíbrio entre aceitar fraude e recusar cliente legítimo.

APROVAÇÃO AUTOMÁTICA

REVISÃO

BLOQUEIO AUTOMÁTICO

Score 0500 — Threshold de revisão800 — Threshold de bloqueio1.000

Cada operação calibra esses thresholds de acordo com seu perfil de risco, ticket médio, setor e apetite por chargeback.

Não existe configuração universal.

O que um sistema antifraude não resolve?

Definir o escopo real do sistema antifraude é tão importante quanto escolhê-lo. Operar com expectativas erradas gera investimento mal alocado e lacunas na defesa que ninguém fecha porque todos acreditam que já estão cobertos.

- Fraude amigável (friendly fraud), em que o cliente realizou a compra e aciona contestação indevidamente — o comportamento é idêntico ao de uma compra legítima
- Erros operacionais internos, como duplicidade de cobrança ou falha de conciliação
- Chargebacks por insatisfação com produto ou entrega, que são disputas comerciais, não fraudes
- Fraude envolvendo o próprio colaborador da empresa com acesso a sistemas internos

Como as empresas podem prevenir fraudes em pagamentos?

Prevenção eficaz opera em camadas. Nenhuma solução isolada cobre o espectro completo da fraude em pagamentos — e a empresa que trata o problema como se fosse resolvido por um único produto cria pontos cegos que o fraudador explora.

Camada de identidade

Validação do CPF, biometria facial, prova de vida e cruzamento com bases externas no momento do cadastro. Reduz a entrada de identidades sintéticas e fraudulentas antes do primeiro pagamento.

Camada transacional

Score de risco em tempo real a cada transação, com regras dinâmicas que respondem a padrões de ataque. É aqui que a maioria dos sistemas antifraude opera.

Camada comportamental

Análise do comportamento na sessão: velocidade de digitação, movimentação do mouse, padrão de navegação. Detecta bots e comportamentos atípicos que o score de transação sozinho não captura.

Camada de contestação

Gestão estruturada de chargebacks com documentação da transação, comunicação proativa e representação em disputas. Reduz a perda em casos de fraude amigável e erros operacionais.

Como escolher um sistema antifraude para pagamentos?

A escolha de um sistema antifraude não é uma decisão de TI. É uma decisão de arquitetura financeira que define quanta fraude a empresa está disposta a absorver, quanta conversão está disposta a sacrificar e quem responde pelos erros de cada lado.

Decisão 01 - Regra, modelo estatístico ou os dois?

Os sistemas antifraude operam com dois paradigmas distintos de decisão, que podem ser combinados.

Regras manuais

Condições explícitas definidas pela equipe: "bloquear cartões emitidos fora do Brasil em compras acima de R\$ 3.000".

Vantagem: explicável, auditável, responde rápido a ataques conhecidos.

Limite: não captura padrões novos antes que sejam catalogados.

Modelo estatístico (ML)

Algoritmo treinado em histórico de transações que aprende padrões de fraude sem que eles sejam explicitados manualmente.

Vantagem: detecta fraudes novas e variações de ataque.

Limite: exige volume de dados e tempo de treino. Menos explicável para auditorias.

"Empresas que só usam regras manuais ficam para trás quando o fraudador muda de vetor. Empresas que só usam ML perdem explicabilidade quando o regulador pergunta por que um cliente foi bloqueado."

Guia de Decisão iugu

Decisão 02 - Bloquear na hora ou revisar depois?

O tempo de resposta do sistema antifraude determina a experiência do cliente legítimo tanto quanto a eficácia contra o fraudador.

Bloqueio em tempo real (< 2 segundos)

- ✓ Zero atrito para o cliente aprovado. Sem custo de fila de revisão.
- ✗ Exige alta precisão. Erros de bloqueio chegam imediatamente ao cliente e geram abandono de carrinho.

Revisão manual assíncrona (minutos a horas)

- ✓ Permite análise humana em casos limítrofes. Reduz falsos positivos em transações de alto valor.
- ✗ Cria fricção, especialmente em compras por impulso. Exige equipe e processo estruturado de análise.

A resposta depende do perfil da operação. Tickets altos com margem elevada suportam revisão manual. Compras de baixo valor por impulso exigem aprovação instantânea — qualquer espera leva ao abandono. O modelo híbrido — bloqueio automático nos extremos e revisão nos limítrofes — tende a ser o mais eficiente para operações de volume diversificado.

Decisão 03 - Qual erro custa mais na sua operação?

Todo sistema antifraude erra nos dois sentidos. A questão é qual erro é mais caro para o modelo de negócio.

Falso negativo

Aprovar a fraude

Chargeback, perda do valor da venda, eventual penalidade por índice elevado junto à adquirente. Mais visível financeiramente.

Falso positivo

Bloquear o cliente legítimo

Perda da venda, desgaste da relação, risco de churn. Mais difícil de medir — não aparece no relatório de fraude.



O setor, o ticket médio e o perfil do cliente definem qual erro tem maior impacto. Uma operação B2B de contratos anuais teme mais o falso positivo — bloquear um cliente de alto valor é perda difícil de recuperar. Uma operação de commodities digitais com ticket baixo e alta inadimplência pode priorizar o controle do falso negativo.

Calibrar o threshold do sistema antifraude é calibrar o equilíbrio entre proteger a operação e não punir o cliente certo.

Esse equilíbrio é uma decisão de negócio, não uma configuração técnica.

Decisão 04 - Quem assume o chargeback?

A alocação do chargeback é uma decisão contratual com impacto direto na margem. Existem três modelos no mercado brasileiro.

Liability shift (repasse ao emissor)

Quando a transação usa autenticação 3DS, a responsabilidade pelo chargeback pode migrar do merchant para o emissor do cartão. A empresa mantém a venda, o risco é absorvido por outro elo da cadeia.

Garantia antifraude pelo processador

Alguns processadores e fintechs de pagamento oferecem cobertura de chargeback por fraude como parte do serviço — mediante análise de risco prévia e conformidade com regras de uso. O custo está embutido na taxa de processamento.

Absorção direta pelo merchant

O modelo mais comum. A empresa responde integralmente por cada chargeback aprovado em sua plataforma. Exige política interna de gestão de contestação e limite máximo de índice de chargeback aceitável pelas adquirentes.

A sua operação está protegida?

Seis perguntas para avaliar o nível real de maturidade antifraude da operação — antes de discutir qual sistema contratar.

- ☒ 1. O time conhece a taxa atual de falsos positivos — clientes legítimos bloqueados — na operação?
- ☒ 2. As regras do sistema antifraude são revisadas com frequência definida, ou só após um ataque?
- ☒ 3. A operação usa 3DS ou algum mecanismo de liability shift para transferir o risco do chargeback?
- ☒ 4. Existe separação clara entre chargebacks por fraude e chargebacks por insatisfação comercial no relatório de contestações?
- ☒ 5. O threshold de score de risco foi calibrado com base no perfil real da operação, ou foi importado de uma configuração padrão?
- ☒ 6. A empresa consegue responder, transação por transação, por que uma compra foi aprovada ou bloqueada?

Como a iugu opera essa camada

A infraestrutura de pagamentos da iugu integra cobrança, antifraude, conciliação e gestão de chargeback no mesmo ecossistema. Cada transação processada carrega rastreabilidade ponta a ponta — da emissão da fatura ao crédito em conta — com dados estruturados que alimentam decisões de risco em tempo real.

Quanto da sua taxa de conversão está sendo sacrificada para compensar decisões de risco que nunca foram calibradas?

Próximo passo

Se a sua operação processa volume relevante de transações e ainda não tem clareza sobre o custo real do falso positivo, o índice de chargeback por tipo ou qual camada antifraude gera o maior retorno, a iugu pode mapear esse cenário em uma sessão de diagnóstico executivo.

Em uma conversa com especialistas, identificamos: o perfil de risco atual da operação; as lacunas entre o sistema em uso e o nível de proteção necessário; o potencial de redução de chargeback sem sacrifício de conversão; e a arquitetura de integração mais adequada ao ecossistema existente.

Fale com um especialista iugu. Mapeie as fraudes que sua operação ainda não vê.

Transforme valores futuros em caixa disponível.



Instituição de Pagamento autorizada pelo Banco Central desde 2020
+14 anos de mercado · R\$ 81 bi processados ao ano