Glassdata

glassdata.io

Relatório · novembro de 2026

Fraude em plataformas de produtos digitais

Por que o antifraude feito para o varejo não protege um intermediador de pagamentos

Wagner Narde e Cesar Fernandes

Glass Data



Por que este material

Antes dos números, um pouco de contexto

A Glass Data é uma plataforma brasileira de orquestração de risco e analisa cerca de R$ 2 bilhões em pagamentos e transferências por mês. Atendemos plataformas de produtos digitais desde 2023, e foi nelas que surgiu a premissa deste material.

As plataformas de produtos digitais importaram do varejo de produtos físicos as estratégias antifraude e, com elas, as premissas do varejo. Na plataforma, essas premissas se invertem: o risco está no repasse ao produtor, não na mercadoria, e as estratégias que mais bloqueiam fraude no varejo são, ao mesmo tempo, as que menos detectam fraude em uma plataforma. Essa inversão custa à plataforma mais receita do que parece a princípio.

Para este relatório, reunimos o que é público sobre fraude em pagamentos no Brasil em 2025 e 2026, lemos as reclamações públicas contra as 11 maiores plataformas do setor e comparamos os resultados com o que medimos nas plataformas de produtos digitais que atendemos na Glass Data.

Este relatório foi escrito para ser compartilhado. Se ele for útil para alguma área da sua empresa, por favor, encaminhe. Se algum dado não corresponder ao que você observa na realidade da sua operação, nos escreva.

Wagner Narde
Cofundador e CEO da Glass Data
wagner.narde@glassdata.io

Resumo executivo

As premissas estão invertidas

As plataformas de produtos digitais adotaram o antifraude feito para o varejo, o comércio eletrônico de produto físico, mas o risco que elas assumem é o de um intermediador de pagamentos, que recebe o pagamento do comprador e repassa ao produtor. Entendemos que as estratégias que mais bloqueiam fraude no varejo são as que menos detectam em uma plataforma de produtos digitais.

No varejo	Na plataforma
O fraudador quer a mercadoria, e a fraude tem ticket alto: R$ 960 a R$ 1.250, contra R$ 516 a R$ 550 da compra legítima (ClearSale, 2024).	**O fraudador quer testar o cartão: centenas ou milhares de cartões em poucas horas, a R$ 5 a R$ 15 cada, um endereço IP por tentativa.**
Valor alto é tratado como sinal de fraude.	**Compras de valor alto têm um quinto da taxa média de fraude. Das compras de um IP usado por três ou mais e-mails em 24 horas, 68% eram fraude.**
A fraude aparece no chargeback, três a quatro semanas depois da venda.	**A fraude aparece no mesmo dia: durante um ataque que observamos, a aprovação caiu a um quarto do normal, ou menos.**

Parte 1 · a premissa errada e o que está em risco

1. O prejuízo está no repasse, não na prateleira.
2. A plataforma é um intermediador de pagamentos, e o antifraude do varejo não foi modelado para esse tipo de risco.
3. O produtor legítimo é penalizado duas vezes.

Parte 2 · quem ataca e como

4. O checkout da plataforma produz cartão validado.
5. O cartão é testado semanas antes de ser usado.
6. Endereço, CPF e entrega não protegem.

Parte 3 · a medida certa é a taxa de aprovação

7. O varejo mede chargeback; a plataforma precisa medir a taxa de aprovação.
8. Ticket alto é o sinal errado.
9. Os sinais que funcionam são outros.
10. O antifraude herdado responde às perguntas do varejista.

Parte 4 · como o risco se materializa

11. As novas regras de 2026 medem a plataforma pelos produtores. O VAMP (Visa Acquirer Monitoring Program), o Excessive Chargeback Program e o programa que monitora lojistas que aplicam golpes, ambos da Mastercard, e o MED 2.0 (Mecanismo Especial de Devolução do Pix) cobram responsabilidade de quem credencia o produtor.

O checklist da seção 12 propõe perguntas para cada área da empresa. Cada item é explicado na seção de mesmo número.

Parte 1

A premissa errada e o que está em risco

Como o estoque digital é praticamente infinito, a fraude parece não custar nada para quem se depara com esse modelo de negócio pela primeira vez. O custo, porém, aparece em outro lugar: no repasse, na reputação da plataforma e na conta do produtor legítimo bloqueada injustamente.

1 **O prejuízo está no repasse, não na prateleira** 5
O valor sai como repasse ao produtor e volta como chargeback, MED ou reembolso, quando o produtor já sacou.

2 **A plataforma é um intermediador de pagamentos** 6
As bandeiras e o Banco Central responsabilizam a plataforma pelos produtores que ela credencia, e a verificação do produtor (KYC, Know Your Customer) precisa ser contínua.

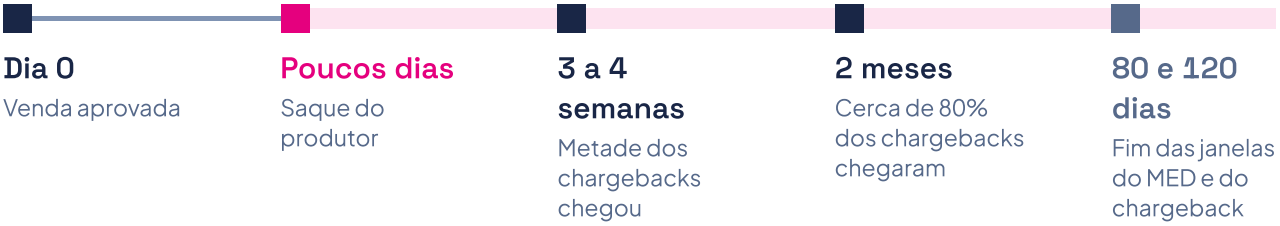
3 **O produtor legítimo é penalizado duas vezes** 7
Primeiro, como laboratório do fraudador; depois, com a conta bloqueada sem explicação do motivo.

1. O prejuízo está no repasse, não na prateleira

O varejista perde a mercadoria. A plataforma de produtos digitais perde o repasse que o produtor já sacou quando a contestação chega.

Do repasse à contestação

Em magenta, o saque. Na faixa rosa, o período em que o valor já saiu e ainda pode voltar.



Indicador	No varejo	Na plataforma
O que se perde	A mercadoria enviada	**O repasse que o produtor já sacou**
Como o valor volta	Chargeback	**Chargeback, MED ou reembolso**
Quem arca no fim	O varejista	**A plataforma, quando o produtor já sacou**
Quando a perda aparece	No chargeback, semanas depois	**No dia do saque, antes de qualquer contestação**

Em um caso que atendemos, a plataforma aprovou centenas de milhares de reais em vendas de um produtor recém-cadastrado, que sacou o valor em poucos dias. O primeiro chargeback chegou semanas depois, e cerca de 60% dessas vendas foram confirmadas como fraude.

O esquema é conhecido. Em junho de 2026, a Polícia Civil de São Paulo deflagrou a Operação Chargeback contra um grupo suspeito de gerar links de pagamento em uma plataforma, pagar com cartões de comparsas, transferir o dinheiro entre os membros e depois contestar as compras com os emissores. O prejuízo estimado da plataforma foi de R$ 263 mil.

> **O que isso muda**
>
> A pergunta da plataforma não é "esta compra vai virar chargeback?", e sim "quanto do que repassei nos últimos 30 dias ainda pode voltar, e de quem eu recupero?".

Fonte: Glass Data, caso de um cliente, em faixas; prazos de chargeback medidos em vendas com pelo menos seis meses de observação. InfoMoney, Operação Chargeback, junho de 2026. Janelas de contestação: regras das bandeiras e IN BCB 766.

2. A plataforma é um intermediador de pagamentos, e o antifraude do varejo não foi modelado para esse risco

Um varejista tem um risco, o comprador. A plataforma tem dois: o comprador e o produtor que ela credencia para receber pagamentos.

3,9 anos	idade mediana das empresas ativas no Brasil: CNPJ novo, isoladamente, não é sinal de risco
4 de 11	das plataformas analisadas têm reclamações de verificação de identidade ou biometria recusada e de saque bloqueado
R$ 500 milhões	em pagamentos em 12 meses: acima desse volume, a liquidação do subcredenciador passa a ser centralizada (Circular BCB 3.886/2018)

- A Circular 3.886 atribui a quem credencia o produtor a responsabilidade de identificá-lo e monitorá-lo. Conhecer o produtor (KYC) é a ferramenta que o varejo não tem, porque o varejista é o próprio vendedor.
- A verificação no cadastro pode falhar nos dois sentidos: barra o produtor pequeno e legítimo e deixa passar o produtor de fachada. O produtor do caso da seção 1 foi aprovado no cadastro.
- O cadastro define o limite inicial do produtor; o risco aparece no que ele faz depois de aprovado. Por isso o KYC precisa ser contínuo.

> **O que isso muda**
>
> O antifraude do comprador é metade do problema. A outra metade é o KYC do produtor, na entrada e de forma contínua depois do cadastro, e é a metade que a regulação e as bandeiras passaram a cobrar.

Fonte: Migalhas, Circular BCB 3.886/2018. Glass Data, CNPJ novo não é sinal de risco, novembro de 2026. Reclame Aqui, 11 plataformas de produtos digitais, novembro de 2026.

3. O produtor legítimo é penalizado duas vezes

Primeiro, o fraudador usa o checkout do produtor para testar cartões. Depois, a plataforma bloqueia a conta do produtor.

11 de 11	plataformas de produtos digitais analisadas com reclamações de bloqueio de conta ou saldo retido
180 dias	de bloqueio relatados por produtores, sem indicação da transação que o motivou
1,8% a 7,9%	das reclamações de cada plataforma mencionam "golpe"
mais de 10	clientes de uma mesma produtora receberam do banco um alerta de golpe ao pagar por Pix, em menos de um mês

- A queixa que se repete é a falta de explicação: qual venda, qual política, até quando.
- A Justiça já condenou plataformas por isso: o Tribunal de Justiça da Bahia determinou que uma delas liberasse o saldo de um produtor e pagasse danos morais por não ter comprovado o aviso prévio nem a fraude.
- No varejo, o falso positivo é um cliente que não comprou. Na plataforma, é um produtor sem renda por meses.

> **O que isso muda**
>
> A plataforma precisa separar, no índice de cada produtor, os ataques que ele sofre da conduta dele e mostrar a ele quais vendas e qual política motivaram cada bloqueio.

Fonte: Reclame Aqui, 11 plataformas de produtos digitais, busca por termo e leitura de cerca de 300 reclamações, novembro de 2026. AdmDireito, TJBA, processo 0110061-36.2025.8.05.0001.

Parte 2

Quem ataca e como

Três inversões explicam por que o ataque a uma plataforma não se parece com a fraude que o varejo aprendeu a bloquear.

No varejo	Na plataforma
O fraudador quer a mercadoria e precisa de um endereço de entrega.	O fraudador quer saber se o cartão está ativo. Um pagamento de R$ 5 a R$ 15 basta. Seção 4 · p. 9
A fraude aparece junto com o pedido: o fraudador compra para receber a mercadoria.	O cartão é testado semanas antes de ser usado, em ondas que mudam de forma em dias. Seção 5 · p. 10
Endereço, CPF e frete confirmam que quem recebe é o titular do cartão.	Não há entrega, e o CPF é vazado junto com o cartão capturado. Seção 6 · p. 11

4. O checkout da plataforma produz cartão validado

O fraudador não quer o curso. Ele tem uma lista de cartões vazados e precisa saber quais ainda funcionam antes de usá-los ou vendê-los. O checkout de uma plataforma de produtos digitais serve para isso: aceita pagamentos de poucos reais, não pede endereço de entrega e devolve a resposta do emissor em segundos.

Raio-x de um ataque de teste de cartão

O que observar	Como aparece
Volume	Centenas ou milhares de cartões diferentes em poucas horas
Origem dos cartões	Poucos BINs (Bank Identification Number, os primeiros dígitos do cartão, que identificam o banco emissor)
Endereço IP	Um IP diferente por tentativa, espalhado por muitas redes de origem
Alvo	Vários produtores ao mesmo tempo
Valor	Tickets baixos, de R$ 5 a R$ 15

- O ataque muda de forma em poucos dias: primeiro, muitos cartões vindos de muitos IPs; depois, o mesmo cartão passando por vários produtores; depois, muitas tentativas concentradas em um único produtor.
- O cartão aprovado não é usado na plataforma. Ele é vendido ou usado em outro estabelecimento, às vezes meses depois: a Visa encontrou testes em 85% a 93% das contas vendidas em duas lojas clandestinas de cartões, feitos pelo menos 12 meses antes da venda.
- O teste de cartão não tem uma versão semelhante para Pix ou boleto. Nesses meios, o risco é o produtor que recebe e não entrega (seções 7 e 11) e a lavagem de dinheiro, com vendas simuladas e saque em seguida.

> **O que isso muda**
>
> A taxa de recusa, isolada, não é o alarme. O alarme é a relação entre as tentativas: o mesmo cartão em vários produtores, o mesmo IP com muitos e-mails, muitos cartões de um BIN em pouco tempo.

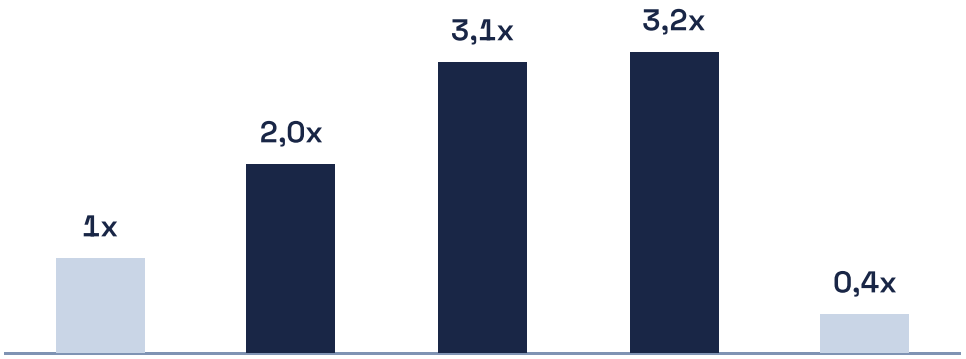
Fonte: Glass Data, ataques observados nas plataformas que atendemos. Visa, Fall 2025 Threats Report.

5. O cartão é testado semanas antes de ser usado

Um ataque que observamos nas plataformas que atendemos durou três semanas. O cartão validado é usado depois, em outro estabelecimento, quando o teste já terminou.

Tentativas de pagamento por semana, antes, durante e depois do ataque

Volume em múltiplos da semana normal mais movimentada. Abaixo, a parcela bloqueada pela estratégia de risco e a aprovação em índice (semana normal = 100).



	Normal semana mais alta	Semana 1 do ataque	Semana 2 do ataque	Semana 3 do ataque	Depois
Bloqueadas pela estratégia	até 44%	78%	85%	85%	8%
Aprovação (índice)	100	até 25	até 25	até 25	100

4 em 5	tentativas do ataque bloqueadas pela estratégia de risco antes de chegar à adquirente
quase todos	os bloqueios concentrados em poucos BINs
cerca de 40%	dos bloqueios nos produtores mais atingidos; o restante espalhado por muitos outros

> **O que isso muda**
>
> O sinal de alarme é a alta no volume de tentativas acompanhada de queda na aprovação. A resposta está nos sinais de rastreamento de vínculos, e não em uma política mais dura de valor alto (seção 8).

Fonte: Glass Data, tentativas de pagamento por semana nas plataformas que atendemos. Volume em múltiplos da semana normal mais movimentada, para não identificar clientes.

6. Endereço, CPF e entrega não protegem

O antifraude do varejo pergunta se quem recebe a mercadoria é o titular do cartão. Em produto digital, não há entrega. Já o dado do CPF quase sempre acompanha o número do cartão vazado. Ou seja, a proteção através desses dados é fraca.

24/10/2026	a Sansec, empresa de segurança, identifica um código que copia dados de cartão nos checkouts da Convertr, plataforma brasileira de comércio eletrônico de moda
26/10	o código é ajustado aos campos da API de pagamento
27/10	o código é removido
5	dados copiados: número, validade, código de segurança, nome e CPF

- Na integração de análise de fraude de uma grande adquirente brasileira, a requisição prevê endereço de cobrança e de entrega, e só cartão de crédito é analisado.
- A Convertr declarou que não houve acesso a dados sensíveis; a análise da Sansec diz o contrário. Não há relatório forense público que concilie as versões.
- No boleto, consumidores relatam ter recebido no DDA (Débito Direto Autorizado) boletos em nome da plataforma sem ter comprado nada: é o CPF de um terceiro usado no checkout.

> **O que isso muda**
>
> Conferir CPF e nome prova só que os dados foram digitados corretamente, não que quem paga é o titular do cartão. As âncoras que persistem são o cartão, o endereço IP e o produtor.

Fonte: Cielo, pagamentos com análise de fraude. Sansec, via BleepingComputer e Hard2bit, outubro de 2026.

A medida certa é a taxa de aprovação

Metade dos chargebacks chega três a quatro semanas depois da venda. Já a taxa de aprovação cai no dia do ataque. Aqui mostramos por que a plataforma precisa medir a taxa de aprovação, por produtor e por dia.

Taxa de aprovação semanal nas plataformas que atendemos

Em índice: a aprovação de uma semana normal é 100. Valores relativos, para não identificar clientes



7 O varejo mede chargeback; a plataforma precisa medir a taxa de aprovação 13

8 Ticket alto é o sinal errado 14

9 Os sinais que funcionam são outros 15

10 O antifraude herdado responde às perguntas do varejista 16

7. O varejo mede chargeback; a plataforma precisa medir a taxa de aprovação

O chargeback chega tarde e indica pouco nesse caso. A taxa de aprovação cai no dia do ataque.

Chargeback, a medida do varejo

3 a 4 semanas

Até a metade dos chargebacks chegar; cerca de 80% em até dois meses. O varejo mede a fraude quando ela já virou perda.

mais da metade

Da fraude confirmada nas plataformas que atendemos nunca virou chargeback: a própria plataforma estornou a venda antes.

Taxa de aprovação

No mesmo dia

A taxa de aprovação cai no dia do ataque, antes de qualquer contestação.

1/4 ou menos

Da aprovação de uma semana normal, nas três semanas do ataque.

- A taxa de aprovação cai tanto por ataque quanto por estratégia de risco mal calibrada. Por isso o monitoramento deve ser por produtor, por dia, separando bloqueio, recusa do emissor e aprovação.
- Aprovação baixa tem custo. As bandeiras cobram por retentativa excedente: a Visa a partir da 21ª tentativa em 30 dias, a Mastercard R$ 2,00 a partir da 8ª e a Elo R$ 0,80 a partir da 16ª. Estabelecimentos com taxa alta de chargeback também tendem a ter mais vendas recusadas pelos emissores.
- No Pix, a medida equivalente é o MED por produtor; no boleto, a reclamação e o pedido de reembolso.

> **O que isso muda**
>
> Acompanhe, para cada produtor e cada dia, tentativas, bloqueios, recusas e aprovações. O chargeback serve para confirmar, mais tarde, o que esse acompanhamento já mostrou.

Fonte: Glass Data, plataformas que atendemos. Cielo, programa de retentativa das bandeiras. Stripe, guia de taxa de autorização.

8. Ticket alto é o sinal errado

No varejo, a fraude tem ticket acima do legítimo. Na plataforma, abaixo.

No varejo

R$ 960 a R$ 1.250

Ticket da tentativa de fraude no varejo em 2024 (ClearSale). O fraudador quer a mercadoria.

R$ 516 a R$ 550

Ticket das compras legítimas no varejo, no mesmo período.

Na plataforma

R$ 5 a R$ 15

Ticket do teste de cartão na plataforma. O fraudador quer validar o cartão.

0,2x

A taxa média de fraude nas compras acima de duas vezes a mediana do produtor. Em 2026, o ticket da fraude aprovada foi cerca de metade do ticket legítimo.

Categorias mais atacadas no varejo em 2024

Tentativas de fraude sobre pedidos, por categoria (ClearSale, 212 milhões de pedidos)



- Em quantidade, a política de valor alto bloqueia o melhor cliente do produtor e concentra pouca fraude. Em valor, o quadro é outro: cerca de 70% do dinheiro fraudado estava em vendas de R$ 1 mil ou mais, espalhadas por quase cem produtores. Para o ticket alto, a resposta está nos sinais de relação e na autenticação adicional (3DS).

> **O que isso muda**
>
> Em plataforma de produtos digitais, valor alto é, no máximo, sinal para identificar fraudes no produtor. Como sinal de comprador, custa aprovação e não devolve precisão.

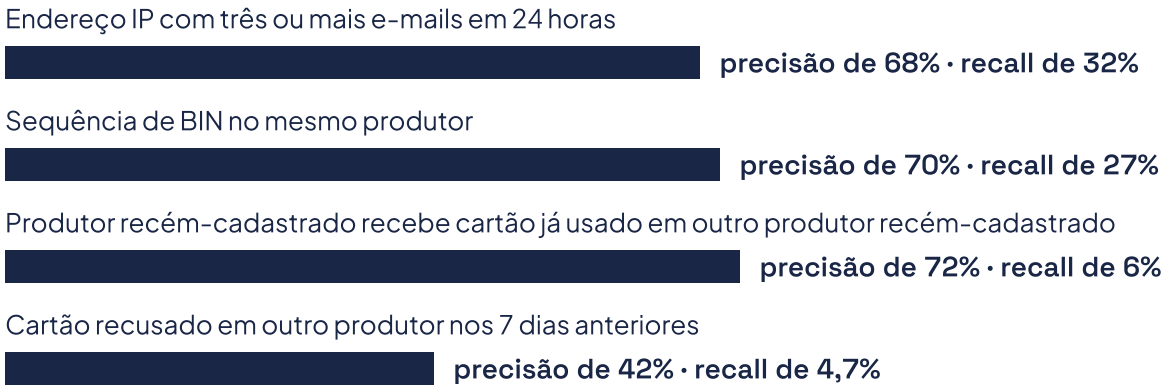
Fonte: ClearSale, Mapa da Fraude 2025. Serasa Experian, 1º trimestre de 2026. Glass Data, 250 mil transações aprovadas nas plataformas que atendemos.

9. Os sinais que funcionam são outros

Medimos 250 mil transações aprovadas nas plataformas que atendemos, ao longo de quase um ano. Mais da metade da fraude confirmada corresponde a estornos decididos pelas próprias plataformas.

Concentração de fraude por sinal

Precisão e recall de cada sinal. A marcação de fraude soma o chargeback de fraude e o estorno decidido pela plataforma.



Valor alto (duas vezes a mediana do produtor): um quinto da taxa média de fraude. Precisão e recall não calculados.

65%	precisão de três sinais combinados (sequência de BIN, IP com vários e-mails e cartão entre produtores novos)
45%	da fraude confirmada alcançada por eles (recall)

- Quatro sinais, nenhum atributo de uma transação isolada: são as relações entre transações, em janelas de horas ou dias. Prever o estorno também tem valor: a decisão que a equipe de risco toma manualmente pode ser tomada em tempo real. Bloqueada na compra, a transação não chega ao estorno nem ao chargeback.
- Não concentraram fraude: valor alto, rede de origem, cartão estrangeiro, produtor com fraude anterior e ATO (tomada de conta).

> **O que isso muda**
>
> Os sinais usam dados que a plataforma já tem: cartão, IP, e-mail, produtor e data de cadastro. O que costuma faltar é o cruzamento entre produtores.

Fonte: Glass Data, 250 mil transações aprovadas nas plataformas que atendemos, até maio de 2026. Fraude confirmada por chargeback de fraude ou estorno decidido pela plataforma.

10. O antifraude herdado responde às perguntas do varejista

O antifraude do varejo foi desenhado para outro problema: as escolhas que o tornam bom para o varejo o tornam cego para a plataforma de produtos digitais.

Escolha de desenho	No varejo	Na plataforma
Marcação de fraude usada no treino	Chargeback, que é a perda	O teste de cartão não gera chargeback onde acontece e fica fora da marcação de fraude
Variáveis	Endereço, destinatário, CEP, frete	Vazias ou preenchidas pelo fraudador
Unidade de análise	Um lojista por vez	Os sinais eficazes cruzam produtores
Meio de pagamento	Cartão de crédito	Pix e boleto, onde o risco é o produtor
Lado observado	O comprador	O comprador e o produtor, com KYC contínuo

- Continua útil: velocidade por cartão e dispositivo, listas de cartões comprometidos e autenticação 3DS para ticket alto em produtores novos.

> **O que isso muda**
>
> Pergunte ao fornecedor ou à equipe interna: com que marcação de fraude o modelo foi treinado, que variáveis usa, que unidade analisa e quais meios de pagamento cobre.

Parte 4

Como o risco se materializa

Em 2026, bandeiras e Banco Central passaram a medir a plataforma pelo que os produtores fazem.

Seção 11 · p. 18

As novas regras de 2026 medem a plataforma pelos produtores

Programa	Quem opera	O que mede	Desde
VAMP	Visa	Fraude reportada mais disputas, sobre transações liquidadas, e enumeração (teste de cartão em massa). Lojista: 1,5% e 1.500 ocorrências no mês	out/2026 no Brasil
Excessive Chargeback Program	Mastercard	ECM (Excessive Chargeback Merchant): 100 chargebacks e 1,5% no mês. HECM (High Excessive Chargeback Merchant): 300 e 3%	em vigor
Scam Merchant Monitoring	Mastercard	Queda de 50% ou mais na aprovação em 72 horas, ou aprovação abaixo de 30%, exceto em ataque de BIN; para lojista novo, reembolsos e chargebacks acima de 5% ou 2 emissores reportando golpe	jul/2026
MED 2.0	Banco Central	Bloqueio da conta recebedora na notificação; análise em até 7 dias; rastreio em até 5 camadas; janela de 80 dias	IN BCB 766
Circular 3.886	Banco Central	Identificação e monitoramento dos recebedores; liquidação centralizada acima de R$ 500 milhões em 12 meses	2018

Todos esses programas cobram responsabilidade de quem credencia o produtor, e não só do produtor.

Fontes: Visa (ficha do VAMP); Sparsu (início no Brasil); ChargebackStop e Chargebacks911 (Excessive Chargeback Program); Checkout.com (Scam Merchant Monitoring); Banco Central.

11. As novas regras de 2026 medem a plataforma pelos produtores

Cada programa usa um indicador diferente, mas todos somam o comportamento dos produtores na conta da plataforma.

1,5%	e 1.500 ocorrências no mês: patamar de lojista excessivo no VAMP, na América Latina
50%	de queda na aprovação em 72 horas abre investigação no programa de golpes da Mastercard
80 dias	de janela para contestar um Pix pelo MED
9,3%	dos valores contestados pelo MED são recuperados, em média

- No VAMP, a fraude reportada conta mesmo sem chargeback, e as recusas do emissor durante um ataque contam no índice de enumeração.
- O programa de golpes da Mastercard exclui a queda causada por ataque de BIN: a plataforma precisa ser capaz de demonstrar que houve um ataque.

> **O que isso muda**
>
> Cada produtor precisa de um índice próprio de fraude reportada, disputa, aprovação e MED, acompanhado por dia. É dessa forma que as bandeiras e o Banco Central passaram a medir a plataforma.

Fonte: Visa, ficha do VAMP; Sparsu, VAMP no Brasil; Checkout.com, programa de golpes da Mastercard; Banco Central, MED 2.0.

Seção 12

O que rever em cada área

Elaboramos algumas perguntas a serem feitas para as áreas abaixo, com o objetivo de identificar quais premissas estão sendo usadas na elaboração da estratégia de risco. Se a resposta for "não sei" para qualquer pergunta, recomendamos a leitura da seção indicada.

Risco e prevenção a fraude

5 perguntas

- [ ] Você consegue ver, por produtor e por dia, tentativas, bloqueios da estratégia de risco, recusas do emissor e aprovações? **Seção 7**
- [ ] Você tem um sinal que cruza cartão, IP e dispositivo entre produtores, e não só dentro de cada produtor? **Seção 9**
- [ ] Qual é o peso do valor da transação nas suas políticas, e quanto de fraude confirmada esse sinal concentra na sua base? **Seção 8**
- [ ] A conferência de CPF contra nome é tratada como prova de titularidade ou como filtro de digitação? **Seção 6**
- [ ] Qual política conteria um ataque com um IP por tentativa e milhares de cartões de poucos BINs em poucas horas? **Seção 4**

Operações e produtores

5 perguntas

- [ ] Quando um produtor é bloqueado, você consegue mostrar a ele quais vendas e qual política motivaram o bloqueio? **Seção 3**
- [ ] Depois que o produtor é aprovado no cadastro, o que é monitorado nele continuamente? **Seção 2 e 11**
- [ ] Quantos produtores ficam retidos na verificação de identidade por semana, e quantos dos aprovados se tornam um problema nos primeiros 30 dias? **Seção 2**
- [ ] O que acontece quando um produtor troca a conta bancária ou a chave Pix e solicita saque no mesmo dia? **Seção 3**
- [ ] Você separa, no índice de cada produtor, os ataques que ele sofre da conduta dele? **Seção 3**

Financeiro

3 perguntas

- [ ] Quanto do chargeback, do MED e do reembolso do último trimestre não foi possível debitar do produtor? **Seção 1**
- [ ] Quanto do que foi repassado nos últimos 30 dias ainda está dentro da janela de contestação de cartão (até 120 dias) e de Pix (80 dias)? **Seção 1 e 11**
- [ ] O prazo de saque e a reserva variam com o risco do produtor ou são iguais para todos? **Seção 2**

Produto e dados

3 perguntas

- [ ] O checkout carrega scripts de terceiros (análise de tráfego, chat, pixels), e quem revisa o que eles fazem? **Seção 6**
- [ ] Os eventos de pagamento guardam cartão (BIN e final), IP, e-mail, produtor e data de cadastro do produtor, de forma consultável por dia? **Seção 9**
- [ ] As taxas de MED e de Pix gerado e não pago são acompanhadas por produtor? **Seção 7 e 11**

Durante um ataque

3 perguntas

- [ ] Em um pico de tentativas, qual é a resposta de mitigação? **Seção 8**
- [ ] Os sinais de vínculo entre produtores são monitorados e alguém acompanha, no mesmo dia, a aprovação de cada produtor? **Seção 5 e 7**
- [ ] Existe um plano para responder em 72 horas a uma queda brusca de aprovação em um produtor, antes que a bandeira pergunte? **Seção 11**

Método e autores

Sobre este material

Método

Dados que medimos. Eventos de pagamento das plataformas de produtos digitais que a Glass Data atende, com produtor, BIN e final do cartão, endereço IP, valor, decisão da estratégia de risco e resposta do emissor de cada tentativa. A base histórica da seção 9 tem 250 mil transações aprovadas, ao longo de quase um ano até maio de 2026, com fraude confirmada por chargeback de fraude ou estorno decidido pela plataforma. O ataque da seção 5 foi medido em tempo real; das vendas aprovadas nos BINs do ataque, mais da metade já foi estornada por fraude, e os chargebacks ainda estão chegando.

Fontes públicas. Relatórios de bandeiras, do Banco Central e de empresas de análise, imprensa especializada e operações policiais, com link na versão digital. Onde a fonte é um fornecedor com interesse comercial, indicamos.

Reclamações públicas. Busca no Reclame Aqui de 11 plataformas de produtos digitais em novembro de 2026, por termo, com leitura de cerca de 300 reclamações recentes. A contagem compara ordens de grandeza, não taxa de fraude.

Limites

Precisão e recall dos sinais são agregados e aparecem exatos. Não divulgamos a taxa média de fraude da base nem números que permitam calculá-la. Contando só o chargeback de fraude, a precisão dos quatro sinais fica entre 9% e 33%. Volumes, datas e o caso da seção 1 permitiriam identificar clientes, e aparecem em faixa, em índice ou arredondados. Não nomeamos clientes, produtores nem as plataformas cujas reclamações lemos. Nenhum relatório público que encontramos separa produtos digitais do restante do comércio eletrônico. Na base de chargeback, cerca de um quarto dos registros de novembro de 2026 não corresponde a nenhum evento de pagamento, e os chargebacks sem motivo informado foram contados como fraude. Data de corte: 31 de outubro de 2026 para fontes públicas; maio de 2026 para a base histórica; novembro de 2026 para o ataque e as marcações de fraude.

Autores

Quem somos

Autores



Wagner Narde

Cofundador e CEO

20 anos de experiência em tecnologia para cobranças e pagamentos. Foi CTO e sócio da fintech Vindi, adquirida pela Locaweb em 2021.



Cesar Fernandes

Cofundador e COO

Quase uma década em pagamentos e prevenção a fraudes. Passou pela Feedzai, pela ACI Worldwide e pela Valid, onde liderou a unidade Valid Pay, de Pix e carteiras digitais.

Glass Data

A Glass Data é uma plataforma de orquestração de risco: recebe os eventos de negócio da sua operação, calcula sinais como os da seção 9 e aplica políticas e modelos de análise em tempo real, com rastreabilidade em cada decisão. Se quiser saber mais, escreva para wagner.narde@glassdata.io.

glassdata.io

Fontes citadas

Fontes citadas

- Visa, Fall 2025 Biannual Threats Report; ficha do VAMP (2025).
- Banco Central do Brasil, MED 2.0 e Instrução Normativa BCB 766; Circular 3.886/2018, via Migalhas.
- ClearSale, Mapa da Fraude 2025. Serasa Experian, Mapa da Fraude, 1º trimestre de 2026.
- Cielo, pagamentos com análise de fraude e programa de retentativa das bandeiras.
- InfoMoney, Operação Chargeback, junho de 2026.
- BleepingComputer e Hard2bit, skimmer nos checkouts da Convertr, outubro de 2026 (análise da Sansec).
- Sparsu, VAMP no Brasil, agosto de 2026; ChargebackStop, janeiro de 2026; Chargebacks911 (fornecedores).
- Checkout.com, mudanças no programa de golpes da Mastercard, 2026 (adquirente).
- Stripe, guia de taxa de autorização (fornecedor).
- AdmDireito, TJBA, processo 0110061-36.2025.8.05.0001; Migalhas, condenação por retirada de curso sem aviso prévio.
- Glass Data, blog: CNPJ novo não é sinal de risco (novembro de 2026).
- Reclame Aqui, páginas de 11 plataformas de produtos digitais, consultadas em novembro de 2026.
- Glass Data, dados de plataformas de produtos digitais atendidas, até novembro de 2026.

Glassdata

Fraude em plataformas de produtos digitais. Por que o antifraude feito para o varejo não protege um intermediador de pagamentos.

glassdata.io

Novembro de 2026