Como identificar e administrar os principais riscos de fraude

Como proteger seus clientes e sua empresa das fraudes.

PayPal

Índice

Fique um passo à frente dos fraudadores

O crime cibernético acontece em todo lugar. O prejuízo dessa prática no mundo é de US$ 1 trilhão por ano[1] — e, infelizmente, ninguém está imune. Os fraudadores atacam todos os setores da economia de todos os países, não importa se a organização é uma empresa pequena local ou uma gigante multinacional.

Mas, conhecendo os tipos de ataque mais comuns em cada situação, as empresas podem se preparar melhor para se antecipar e combater as fraudes.

US$ 1 Tri

é o prejuízo anual que o crime cibernético gera no mundo.[2]

82%

das grandes empresas relataram um aumento nas tentativas de fraude em 2021.[3]

18%

de aumento no prejuízo gerado pelas fraudes no comércio eletrônico, no comparativo anual.[4]

3,3x

Cada dólar perdido por fraude gera um custo de cerca de US$ 3,30 em tempo e outras despesas.[5]

1 em 5

acessos a contas são uma tentativa de roubo.[6]

1 em 5

usuários brasileiros da internet foram alvo de ataques de phishing, segundo relatórios oficiais do ano passado.[7]

1, 2. Center for Strategic & International Studies (2020), The Hidden Costs of Cybercrime **3.** Cybersource (2021), 2021 Global Fraud Report **4.** Payments Dive (2021), E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds
5. LexisNexis (2020), 2020 True Cost of Fraud Study – E-Commerce/Retail Report **6.** Arkose Labs (2022), 2022 State of Fraud & Account Security Report **7.** CISO Mag (2021), Brazil Implements Tougher Reforms to Fight Cybercrime

Por que a segurança cibernética deve ser sua prioridade

A fraude e o crime cibernético não fazem bem aos negócios. É claro, existe o potencial de perda de receitas ou bens adquiridos maliciosamente. Mas também existe o enorme custo envolvido em lidar com as tentativas de fraude — mais de três vezes maior do que a perda de receita gerada por elas.[8]

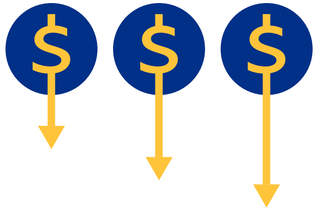
Se sua empresa sofre com fraudes de pagamento, os prejuízos possíveis são três.

- Os bens e serviços que você oferece podem ser roubados. Nesse caso, você tem uma perda direta e precisa pagar para repor o estoque.
- O verdadeiro titular do cartão quer o dinheiro de volta, e o processador de pagamentos ainda cobra uma tarifa de chargeback, ou seja, você perde com o estorno e com os custos operacionais envolvidos.
- Você precisa dedicar tempo e recursos para lidar com fraudes e reclamações de clientes genuínos que tiveram sua conta invadida. Com isso, sua empresa passa a ter maiores custos operacionais.

E como se não bastasse, as empresas sofrem dano à reputação quando o ataque é de larga escala ou ganha apelo midiático. Mesmo que os ataques não ganhem a atenção do público, uma elevada incidência de estornos ou outras tentativas de fraude podem fazer seu provedor de pagamento ver sua empresa como de alto risco e, com isso, fazer mais exigências onerosas e aumentar o custo de processamento para você.[9]

Além disso, as autoridades regulatórias, incluindo órgãos antilavagem de dinheiro, podem aplicar sanções e multas por conta de violações de dados ou do processamento acidental de transações fraudulentas.

Este guia aborda alguns dos tipos mais comuns de fraude em diversos setores e explica como lidar com eles.



Ainda existe o alto custo de lidar com as tentativas de fraude:

mais de 3x

o valor da perda de receita.[8]

8. LexisNexis (2020), 2020 True Cost of Fraud Study – E-Commerce/Retail Report **9.** Forbes (2021), High-Risk Merchant Account: What It Is And How It Works

Fraudes de pagamento comuns

Fraude de roubo de conta (ATO)

O roubo de conta é uma forma de roubo de identidade em que os criminosos conseguem acesso a uma conta de um cliente real e fazem compras não autorizadas e/ou roubam dados pessoais e de pagamento armazenados nela. Algumas formas comuns de fazer isso são:

- **Credential stuffing —** Bots fazem um bombardeio de tentativas de acesso a contas usando milhares de combinações de nome de usuário e senha, muitas vezes compradas em lote na dark web.
- **Phishing e outras técnicas de engenharia social —** Os clientes são induzidos a revelar seus dados de acesso, muitas vezes por e-mails ou ligações fraudulentas.

Teste de cartão

Neste caso, os criminosos testam uma imensidão de dados de cartões roubados para ver se ainda são válidos. Normalmente, são usados bots ou scripts de computador para fazer várias transações de valor baixo. A partir daí, os cartões ainda válidos são usados para compras maiores ou vendidos para outros fraudadores.

Fraude de cartão não presente (CNP)

A fraude de CNP ocorre quando uma compra é feita com um cartão não presente fisicamente. Inicialmente, eram compras por telefone ou correio, mas hoje fazem parte do comércio eletrônico também. A fraude de cartão não presente acontece de duas formas: a fraude tradicional, usando dados de cartões roubados, e a fraude amigável, que você pode ver abaixo. Os dois tipos acabam em um pedido de chargeback, ou estorno, do titular verdadeiro do cartão.

Fraude amigável

A fraude "amigável" ocorre quando o verdadeiro titular do cartão contesta uma transação legítima. Às vezes, isso ocorre porque o titular não se lembra de ter feito a compra ou não sabe que um parente usou o cartão para fazer uma compra. Mas, em outras ocasiões, o comprador pode se arrepender de uma compra por impulso ou esquecer de cancelar uma assinatura e, por isso, decide pedir o chargeback em vez de admitir o erro. A fraude amigável também acontece quando um cliente alega falsamente não ter recebido o pedido.

Fraude de chargeback

Quando o titular do cartão contesta uma cobrança, o banco ou a operadora do cartão devolve o valor e cobra uma tarifa de chargeback do vendedor. Os chargebacks podem ocorrer por problemas com a transação (como pedido não entregue ou erro na cobrança enviada ao cartão). Podem acontecer também quando o titular legítimo do cartão identifica uma fraude e pede o chargeback. É verdade que muitos chargebacks são honestos, mas os pedidos de chargeback fraudulentos são uma tendência agora.

Fraude de identidade sintética

Esse é um dos tipos de fraude financeira que mais cresce. Os criminosos criam uma identidade falsa baseada em dados pessoais fictícios ou roubados e passam um bom tempo construindo um histórico de crédito para ter uma identidade falsa. Com um documento de identidade que parece original, os criminosos solicitam cartões de crédito e empréstimos, gastam até o limite e desaparecem. Esse tipo de fraude é difícil de detectar antes que seja tarde demais.

Perfil de fraude no comércio eletrônico

O rápido crescimento do comércio eletrônico no mundo nos últimos anos vem acompanhado de um grande aumento na incidência de todos os tipos de fraude de pagamento.

A fraude amigável e o teste de cartão são os ataques mais comuns no mundo.[10] Os varejistas virtuais relatam um aumento em todos os tipos de ataque, incluindo de chargeback e fraude amigável.[11]

Mais da metade dos vendedores pesquisados relatam uma maior ocorrência de fraudes de identidade e de conta, como fraude de identidade sintética, roubo de conta, roubo de identidade e fraude de conta nova.[12] Dos vendedores pesquisados, 59% também alegam que houve um aumento nas fraudes de cartão não presente.[13]

Segundo os especialistas em fraude da Arkose Labs, uma em cada quatro transações no varejo são um ataque.[14]

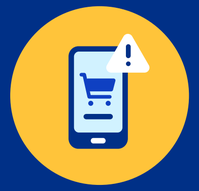
Não é surpresa que as empresas de comércio eletrônico, de todos os tamanhos, cada vez mais consideram as fraudes um grande desafio:

3 em 5

vendedores acreditam que a perda de receita por fraudes de pagamento causa grande impacto na sua empresa.[15]

3 em 5

vendedores acreditam que a perda de produtividade gerada pelas fraudes de pagamento causa grande impacto na sua empresa.[16]



9 em 10

vendedores já consideram a gestão das fraudes no comércio eletrônico “muito ou extremamente importante” para a estratégia da empresa.[17]

1 em 5

vendedores afirma que a segurança dos dados de clientes é um desafio crítico.[18]

10, 17. Cybersource (2021), 2021 Global Fraud Report **11, 12, 13, 15, 16, 18.** FIS Worldpay (2021), Global Payment Risk Mitigation **14.** Arkose Labs (2022), 2022 State of Fraud & Account Security Report

Perfil de fraude nos jogos on-line

Com um alto volume de transações, o desejo dos clientes por uma experiência de pagamento rápida e descomplicada e produtos dentro dos jogos com valor de mercado de US$ 50 bilhões,[19] o mundo dos jogos on-line e esportes eletrônicos sempre foi um alvo interessante para os fraudadores.

Estima-se que apenas a venda de contas roubadas do Fortnite coloca US$ 1 bilhão por ano no bolso dos criminosos.[20]

O problema para as empresas de jogos é que os ataques de fraude são extremamente lucrativos para os cibercriminosos. Como destaca a Arkose Labs, é possível lançar ataques de bot por apenas US$ 15 por dia e revender as contas tomadas por até US$ 3.000.[21]

Segundo a Arkose, os jogos on-line foram o setor da economia mais atacado em 2020[22] e, embora tenha havido uma estabilidade em 2021, os tipos de ataque se diversificaram.[23]

Os principais tipos de ataque de fraude no setor de jogos on-line foram:

- **Roubo de conta —** 2 em cada 3 ataques de 2021 tiveram como alvo o acesso de usuários.[24] Um dos métodos de ataque é o credential stuffing, em que bots são utilizados para testar diversas combinações de nome de usuário e senha. Depois de violar as contas, é possível roubar e vender itens no jogo e dados de pagamento e pessoais.
- **Phishing e outras técnicas de engenharia social**, que geralmente levam ao roubo de conta ou de dados de pagamento e pessoais.
- **Fraude amigável**, que ocorre quando o cliente contesta uma transação legítima, também é comum no setor. O cliente pode contestar também porque não lembra da transação, não se comunicou com o parente que fez a compra ou se arrependeu de uma compra por impulso.
- **Teste de cartão** também é uma fraude comum no ramo de jogos por conta do alto volume de compras normalmente de baixo valor, o que é ideal para ocultar a atividade maliciosa de teste de cartão.

A região da Ásia-Pacífico é a maior fonte de receita do setor de jogos on-line, registrando 250 milhões de jogadores de celular em 2021.[25] China, Japão, Coreia do Sul, Indonésia e Austrália são cinco dos 10 maiores geradores de receita do setor de jogos de celular.[26] Ao mesmo tempo, as empresas de jogos e tecnologia da região são o principal alvo de ataques de fraude.[27]

O mercado de jogos brasileiro gerou US$ 2,3 bilhões de receita em 2021 e deve crescer mais de 5% em 2022, segundo estimativas.[28] É o maior mercado do setor na América Latina.

19. Intellicheck (2021), How companies can prevent fraud in online gaming **20.** Business Insider (2020), Stolen Fortnite accounts are being sold on the black market... **21, 22.** Arkose Labs (2021), How to Level Up in the Fight Against Online Gaming Fraud **23.** Arkose Labs (2021), Fraud in Online Gaming: A Midyear Snapshot of 2021 Attack Trends **24, 27.** Arkose Labs (2022), 2022 State of Fraud & Account Security Report **25.** Transperfect (2021), What Does Global Gaming Industry Growth Look Like in 2021? **26.** Newzoo (2021), Global Mobile Market Report 2021 **28.** PagBrasil (2022), Brazilian Gaming Market May Grow Nearly 6% by 2022

Perfil de fraude nas empresas de SaaS e serviços

Segundo a Arkose Labs, o risco de empresas de tecnologia sofrerem um ataque de fraude em 2021 foi cinco vezes maior do que no ano anterior.[29]

As empresas de SaaS e outras de assinatura são especialmente vulneráveis a ataques de fraude porque toda conta armazena dados de pagamento.

O risco de empresas de tecnologia sofrerem ataques de fraude foi

5x

maior em 2021 do que em 2020.[29]

- **A fraude de roubo de conta** é uma ameaça comum às empresas de SaaS. Os criminosos usam as contas invadidas para comprar serviços e bens ou vender a outros criminosos.
- Usar dados de um cartão roubado para abrir contas falsas e fazer compras **(fraude de CNP)** e usar essas contas para abusar de ofertas de teste gratuito também são comuns no ramo de SaaS.
- Os **chargebacks** também são um grande desafio do setor. Na realidade, o mercado de software tem o maior índice médio de chargeback por transação, com 0,66%.[30] Alguns chargebacks são inocentes; as pessoas acabam se esquecendo dos serviços que assinaram, mas muitos são realmente fraudulentos.

29. Arkose Labs (2022), 2022 State of Fraud & Account Security Report **30.** Expert Market (2021), Chargeback Fraud Statistics 2022

Como prevenir fraudes de pagamento

Frustrando ataques de roubo de conta

Alguns provedores de pagamento, como o PayPal, oferecem autenticação multifator (MFA) ou de dois fatores (2FA). Essa pode ser uma forma muito eficaz de bloquear o credential stuffing e o uso de dados de acesso roubados em ataques de phishing. Na realidade, a autenticação de dois fatores foi citada como "muito importante" por quase metade dos vendedores.[31]

A MFA ou a 2FA exige que o cliente realize mais uma forma de autenticação (como inserir um código numérico de uso único) que é enviada para o celular ou o e-mail pré-registrado por ele. Com isso, os fraudadores não conseguem simplesmente usar dados de acesso roubados; neste caso, eles precisariam ter acesso também ao dispositivo móvel ou ao e-mail do dono da conta.

Como o primeiro passo do roubo de conta (usar bots para realizar ataques de credential stuffing) costuma ser automatizado, uma medida simples como implementar uma tecnologia de CAPTCHA — que exige intervenção humana — também pode ajudar bastante.

Detectando e lidando com testes de cartão

Esses ataques envolvem um grande volume de pequenas transações em curto espaço de tempo. Em ambientes de alto volume, como o comércio eletrônico e os jogos on-line, as transações de teste de cartão podem passar despercebidas e, sem proteção, os vendedores podem receber uma enxurrada de pedidos de chargeback de repente por causa de um ataque. Esses ataques também podem afetar a disponibilidade da infraestrutura do vendedor por conta do excesso de tentativas de autorização malsucedidas.

O PayPal usa algoritmos de aprendizado de máquina e tomada de decisão em tempo real para ajudar a diferenciar transações legítimas de fraudulentas e identificar padrões de fraude, como em testes de cartão. O PayPal compara as tendências históricas às informações da transação, como endereço IP, tipo e ID do dispositivo, endereço de e-mail e outras.

A eficácia de uma tecnologia de aprendizado de máquina vem da qualidade dos dados que ela recebe. Nesse quesito, o PayPal tem uma enorme vantagem por conta da nossa rede bilateral.

Com mais de 400 milhões de consumidores e 30 milhões de contas de vendedor dos mais diversos setores, o PayPal tem uma vastidão de dados sobre consumidores e perfis de risco. Essas informações sobre o vendedor e o comprador envolvidos em uma transação nos ajuda a determinar se a transação é fraudulenta ou não, mesmo quando o comportamento de fraude é extremamente sofisticado.[32]

Mais de **400 milhões de consumidores** e **30 milhões de vendedores** usam o PayPal.[32]

31. FIS Worldpay (2021), Global Payment Risk Mitigation **32.** PayPal (2020), How Data Science, Machine Learning and Artificial Intelligence Lead to Higher Authorization Rates

Reduzindo a fraude de cartão não presente

Para combater a fraude de cartão não presente, a melhor estratégia é solicitar o máximo de informação possível do pagador, entre elas, o código de segurança (CVV), além de implementar recursos de prevenção de fraudes, como o 3D Secure (3DS) e a autenticação multifator.

Mais uma vez, provedores de pagamento que usam aprendizado de máquina alimentada com dados em tempo real, como o PayPal, podem ajudar a reduzir a ocorrência de fraudes de CNP. O PayPal é pioneiro no uso de tokenização de rede,[33] o que dificulta o uso fraudulento de dados de cartão roubado.

Combatendo a fraude amigável

A fraude amigável é comum tanto no comércio eletrônico quanto no mercado de jogos. Esse é um método difícil de detectar e provar. Porém, ter bons registros e implementar boas políticas que provem que o pedido é legítimo e que foi enviado e recebido pode ajudar a refutar alegações falsas. Um exemplo seria exigir a assinatura no recebimento do pedido.

Muitas reclamações de fraude amigável começam com transações válidas, por isso, ter uma política de devolução clara e generosa, um ótimo atendimento ao cliente e boa comunicação também pode ajudar a impedir alguns clientes de pedir um chargeback maliciosamente.

Sempre solicitar o código de segurança (CVV) do cartão e implementar o 3D Secure também são formas de criar barreiras para a fraude amigável.

A Proteção ao Vendedor do PayPal também é outro recurso que beneficia as empresas.[34]

Reduzindo a fraude de chargeback

Como quase todas as fraudes de pagamento geram chargebacks, reforçar suas defesas contra fraude de modo geral ajuda nesse sentido.

Uma das melhores formas de reduzir a fraude de chargeback é trabalhar com um processador de pagamentos, como o PayPal, que tenha uma tecnologia avançada de prevenção de fraudes. As técnicas de fraude evoluem o tempo todo, por isso, para ficar à altura das ameaças, você precisa de uma solução de prevenção de fraudes que acompanhe esse movimento e colete dados em tempo real.

Prevenindo a fraude de identidade sintética

Identidades sintéticas conseguem se passar por verdadeiras porque muitas instituições financeiras usam sistemas de pontuação obsoletos e/ou automáticos para oferecer crédito. Muitas vezes, usar um maior volume de dados, incluindo dados de terceiros, pode revelar as inconsistências comuns às IDs falsas.

Os dados da enorme rede bilateral de vendedores e consumidores do PayPal são uma fonte de dados abundante para nossos modelos de detecção de fraudes baseados em aprendizado de máquina.

33. PayPal (2020), How Network Tokenization Leads to Higher Authorization Rates and a Better Customer Experience **34.** Sujeito a termos e condições

Como o PayPal ajuda a gerenciar o risco de fraude

O objetivo da tecnologia de pagamento do PayPal, desenvolvida ao longo de 20 anos, é reduzir o risco de fraude e dar confiança ao consumidor na hora de comprar.

O PayPal é uma marca reconhecida que transmite confiança no mundo todo. Os consumidores valorizam o fato de não ter seus dados pessoais compartilhados em hipótese alguma. Ter uma experiência de pagamento pensada para ser simples, segura e conveniente também é bastante apelativo aos compradores de hoje.

Com o PayPal, os vendedores podem oferecer uma série de formas de pagamento com um único processo de integração. Com o PayPal, os vendedores podem oferecer uma série de formas de pagamento com um único processo de integração, o que facilita a gestão e a organização dos pagamentos em um lugar central.

As empresas ainda têm a Proteção ao Vendedor do PayPal para transações qualificadas[35] e normas de prevenção de fraudes, como o 3D Secure.

O PayPal oferece recursos avançados de prevenção de fraudes. Nossa rede bilateral de mais de 400 milhões de usuários ativos no mundo é uma fonte abundante de dados, que alimentam nossos modelos de aprendizado de máquina para aumentar nossa precisão, adaptabilidade e capacidade de detecção de fraudes em tempo real. Com isso, as rejeições de transação desnecessárias são reduzidas e a chance de tratar bons clientes como fraudadores por engano também diminui.

O enorme conjunto de dados sobre vendedores, as técnicas avançadas de aprendizado de máquina e a experiência em ciência de dados que o PayPal oferece ainda agilizam a detecção e o bloqueio de novas atividades fraudulentas para todos os vendedores da rede.

Além disso, com o relacionamento que temos com bancos, adquirentes e órgãos reguladores no mundo todo, nossa capacidade de detectar possíveis fraudes antes que aconteçam é muito maior.

A Proteção contra Fraudes do PayPal foi desenvolvida para grandes empresas. Esta é uma solução completa e pronta para usar, integrada à PayPal Commerce Platform, que tem como objetivo dar aos vendedores maior visibilidade e controle sobre o processo de tomada de decisão sobre a legitimidade de cada transação.

Saiba mais sobre como o PayPal ajuda grandes empresas a gerenciar riscos e cumprir as normas vigentes

Saiba Mais

Em resumo, a gestão de risco avançada do PayPal pode trazer:

- Menos chargebacks
- Menos falsos positivos
- Menos complicação para o cliente
- Menos prejuízo por fraude
- Maior eficiência operacional
- Simplificação da experiência do cliente

35. Sujeito a termos e condições

Fontes

1. Center for Strategic & International Studies (2020), The Hidden Costs of Cybercrime
2. Center for Strategic & International Studies (2020), The Hidden Costs of Cybercrime
3. Cybersource (2021), 2021 Global Fraud Report
4. Payments Dive (2021), E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds
5. LexisNexis (2020), 2020 True Cost of Fraud Study – E-Commerce/ Retail Report
6. Arkose Labs (2022), 2022 State of Fraud & Account Security Report
7. CISO Mag (2021), Brazil Implements Tougher Reforms to Fight Cybercrime
8. LexisNexis (2020), 2020 True Cost of Fraud Study – E-Commerce/ Retail Report
9. Forbes (2021), High-Risk Merchant Account: What It Is And How It Works
10. Cybersource (2021), 2021 Global Fraud Report
11. FIS Worldpay (2021), Global Payment Risk Mitigation
12. FIS Worldpay (2021), Global Payment Risk Mitigation
13. FIS Worldpay (2021), Global Payment Risk Mitigation
14. Arkose Labs (2022), 2022 State of Fraud & Account Security Report
15. FIS Worldpay (2021), Global Payment Risk Mitigation
16. FIS Worldpay (2021), Global Payment Risk Mitigation
17. Cybersource (2021), 2021 Global Fraud Report
18. FIS Worldpay (2021), Global Payment Risk Mitigation
19. Intellicheck (2021), How companies can prevent fraud in online gaming
20. Business Insider (2020), Stolen Fortnite accounts are being sold on the black market...
21. Arkose Labs (2021), How to Level Up in the Fight Against Online Gaming Fraud
22. Arkose Labs (2021), How to Level Up in the Fight Against Online Gaming Fraud
23. Arkose Labs (2021), Fraud in Online Gaming: A Midyear Snapshot of 2021 Attack Trends
24. Arkose Labs (2022), 2022 State of Fraud & Account Security Report
25. Transperfect (2021), What Does Global Gaming Industry Growth Look Like in 2021?
26. Newzoo (2021), Global Mobile Market Report 2021
27. Arkose Labs (2022), 2022 State of Fraud & Account Security Report
28. PagBrasil (2022), Brazilian Gaming Market May Grow Nearly 6% by 2022
29. Arkose Labs (2022), 2022 State of Fraud & Account Security Report
30. Expert Market (2021), Chargeback Fraud Statistics 2022
31. FIS Worldpay (2021), Global Payment Risk Mitigation
32. PayPal (2020), How Data Science, Machine Learning and Artificial Intelligence Lead to Higher Authorization Rates
33. PayPal (2020), How Network Tokenization Leads to Higher Authorization Rates and a Better Customer Experience
34. Sujeito a termos e condições
35. Sujeito a termos e condições