Aité PARTNER. ADVISOR. CATALYST.

Como a prevenção de fraude pode expandir seu eCommerce

ABRIL 2021

Preparado para:

cybersource
A Visa Solution

ÍNDICE

LISTA DE FIGURAS

SUMÁRIO EXECUTIVO

O estudo *Como a prevenção de fraude pode expandir seu eCommerce*, encomendado pela Cybersource – uma solução Visa – e desenvolvido pelo Aite Group, explora as mudanças de atitude no que diz respeito à prevenção de fraude. Em vez de se concentrarem só em minimizar as perdas decorrentes de fraude, as empresas mais modernas estão gerenciando essa realidade para expandir o negócio e vender mais.

Algumas das principais conclusões do estudo:

- As fraudes com transações CNP (cartão não presente) ainda representam um risco financeiro e comercial para os estabelecimentos comerciais.
- Senhas fracas e o uso da mesma senha em vários sites facilitam o acesso dos fraudadores às contas on-line.
- Um método emergente para abordar as fraudes nas transações CNP é o uso de hubs de orquestração, que reúnem soluções em nível de conta e transação em um sistema coeso.
- Para prevenir as fraudes, não é mais preciso mais optar entre reduzir as fraudes ou aumentar os índices de aprovação. Os estabelecimentos comerciais estão buscando um equilíbrio entre esses dois pontos.
- Os departamentos de prevenção de fraude estão sendo reinventados e deixando de ser uma função dentro de operações. Cada vez mais, trabalham conjuntamente com os departamentos de vendas, marketing e financeiro para reduzir a abandono do carrinho e impulsionar o crescimento da receita.

INTRODUÇÃO

Empresas de todos os portes estão vendendo seus produtos físicos e digitais on-line, fazendo o eCommerce explodir no mundo todo. A pandemia de Covid-19 acelerou bastante a ascensão do comércio digital. Os fraudadores perceberam isso e, em pouco tempo, já estavam explorando as vulnerabilidades existentes e criando meios criativos de agir. Os estabelecimentos comerciais vivem às voltas com o desafio de equilibrar corretamente a necessidade de oferecer uma excelente experiência ao cliente e de reduzir as perdas com fraude. Normalmente, o risco é avaliado em dois pontos da jornada do cliente: no momento do login e no momento da compra. Os departamentos de prevenção de fraude costumam estar ligados a Operações e se concentram em impedir a ação de fraudadores, o que lhes valeu a alcunha de “prevenção de vendas”. Entretanto, as empresas mais visionárias transformaram a prevenção de fraude em uma área crítica, usando-a para aumentar a receita aprovando mais pedidos legítimos e gerenciar o risco durante toda a jornada do cliente. Este documento explora uma nova maneira de encarar a prevenção de fraude e como estabelecimentos comerciais de todos os portes podem se preparar para o crescimento do eCommerce.

METODOLOGIA

Este documento se baseia em pesquisa primária e secundária conduzida pelo Aite Group e em informações obtidas junto a vários fornecedores de soluções e estabelecimentos comerciais.

A EXPLOSÃO DO ECOMMERCE

O eCommerce já vinha crescendo regularmente há vários anos, mas a pandemia fez esse crescimento disparar quando o mundo se transformou em uma economia digital-first praticamente da noite para o dia. Os índices de crescimento das vendas on-line se mantiveram por volta dos 16% durante a maior parte da década passada, enquanto os de vendas presenciais ficaram bem abaixo dos 10%. Em 2020, as vendas mundiais do eCommerce tiveram um crescimento surpreendente de 27.6% (Figura 1).

Figura 1: Crescimento regional das vendas no varejo via eCommerce em 2020

Nota: Inclui produtos ou serviços comprados pela internet, independentemente do método de pagamento ou de fulfillment; exclui gastos de viagem e ingressos para eventos, pagamentos de conta, impostos ou transferência de valores, venda de comida e bebida no local e venda de produtos que tendem a ser consumidos em excesso.

Fonte: eMarketer e InsiderIntelligence.com

América Latina, América do Norte e Europa Central e Oriental são líderes em crescimento de eCommerce, ficando acima da média global. Nos Estados Unidos, as vendas do eCommerce subiram quase 32%, e um supermercado entrou para a lista dos dez maiores varejistas virtuais ao implementar o serviço de compra on-line com retirada em loja/drive-through. Em três meses, a pandemia impulsionou um crescimento nas vendas on-line nos EUA que, normalmente, ocorreria em dez anos.

Dispositivos móveis e serviços de fulfillment são fatores que contribuem fortemente para promover as vendas on-line, especialmente em áreas do mundo onde faltam redes de telefonia fixa. Em dezembro de 2020, 5,24 bilhões de pessoas tinham um smartphone, o que representa 67% da população mundial.[1] Consumidores da América Latina, Oriente Médio, África e pessoas que residem em áreas remotas e não urbanas do mundo, ganharam acesso a mercados e

1. *"How Many Smartphones Are in the World?"* BankMyCell, acessado em 12 de janeiro de 2021, https://www.bankmycell.com/blog/how-many-phones-are-in-the-world.

empresas por meio de dispositivos móveis e serviços de entrega que sempre estiveram fora do seu alcance. Até 2023, a previsão é que 22% das vendas no varejo sejam realizadas on-line.[2]

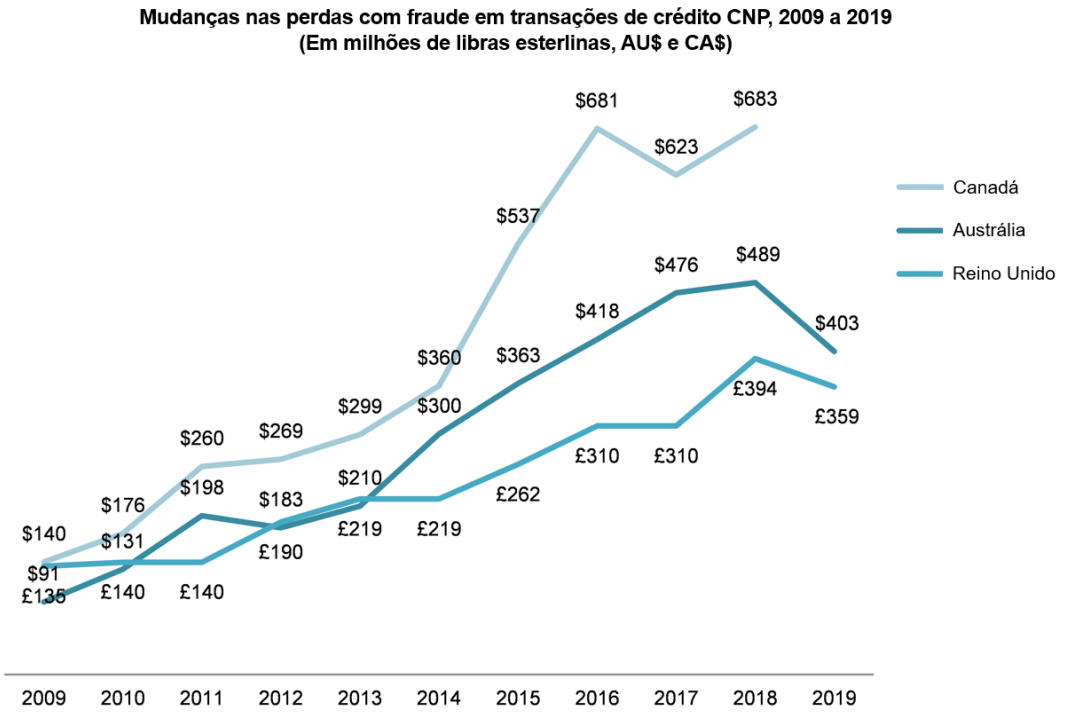
ELES SEGUEM O DINHEIRO

As empresas não são as únicas que sabem que as vendas on-line estão crescendo – os fraudadores também estão cientes disso. Os pagamentos com cartão, método de pagamento predominante nas compras on-line, não são protegidos pela tecnologia EMV, o que os torna um alvo fácil. As empresas de cartão protegem os portadores de cartão contra transações fraudulentas com uma política de zero *liability* e criaram regras para atribuir a responsabilidade financeira à instituição financeira ou ao estabelecimento comercial. De modo geral, a fraude de eCommerce é responsabilidade do estabelecimento comercial e o crescimento dessas fraudes tem feito os comerciantes buscarem ativamente soluções que os protejam. Considerando que a indústria de pagamentos estima que as fraudes de eCommerce geram perdas na faixa de 20 a 30 bilhões de dólares anualmente, isso não chega a surpreender.

Alguns países são mais eficientes do que outros quando se trata de mitigar a fraude de eCommerce. Reino Unido, Austrália e Canadá viram as fraudes nas transações de crédito CNP aumentarem anualmente entre 2009 e os últimos anos da década de 2010. Essas perdas caíram nos últimos anos, graças a iniciativas do setor, diretrizes governamentais ou uma combinação das duas coisas (Figura 2).

2. Daniela Coppola, *"E-Commerce Share of Total Retail Sales Worldwide From 2015 to 2023*," Statista, 26 de novembro de 2020, acessado em 12 de janeiro de 2021, https://www.statista.com/statistics/534123/eCommerce-share-of-retail-sales-worldwide/.

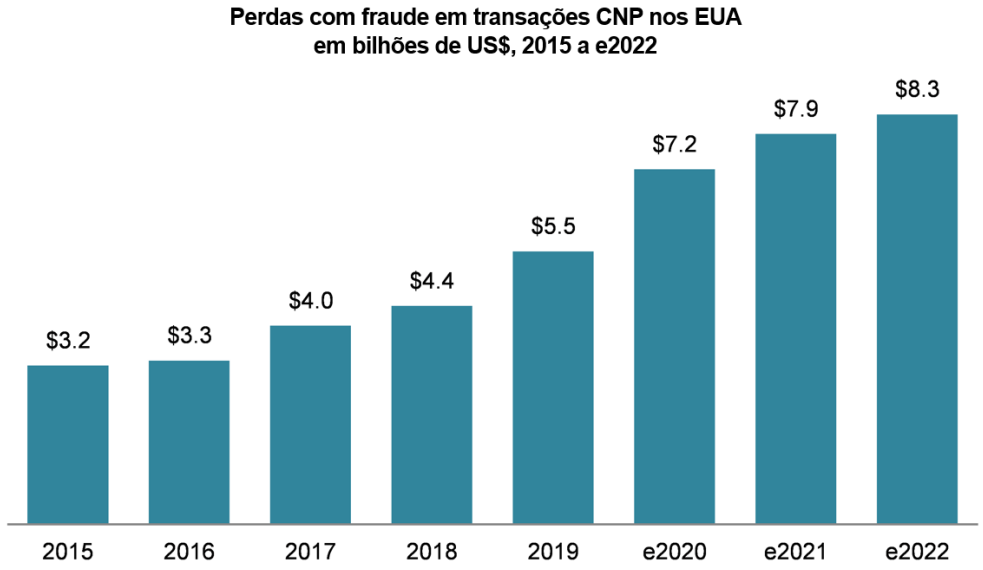
Figura 2: Mudanças nas perdas com fraude em transações de crédito CNP



Fonte: UK Finance, AusPay, Canadian Banking Association

Nos Estados Unidos, as perdas com fraude em transações de crédito CNP aumentaram por vários anos e devem continuar crescendo até 2022. Parte desse aumento se deve à relutância dos estabelecimentos comerciais em afetar a experiência do consumidor negativamente se adicionarem fricção no processo de compra e checkout (Figura 3).

Figura 3: Perdas com fraude em transações CNP nos EUA

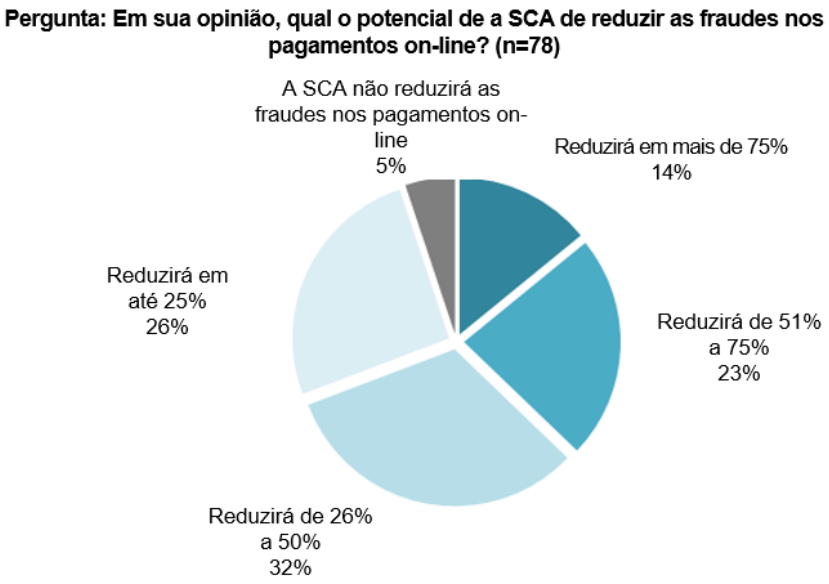


Fonte: Aite Group

A União Europeia (EU) adotou novos requisitos para baixar seus índices de fraude de eCommerce. Na maioria dos países da UE, o componente de autenticação forte do cliente (SCA, na sigla em inglês) da revisada Diretriz de Serviços de Pagamento (PSD2) entrou em vigor em 1º de janeiro de 2021). Algumas das principais exceções e respectivas datas de entrada em vigor são Alemanha (15 de março de 2021), França e Itália (1º de abril de 2021) e Reino Unido (14 de setembro de 2021). As empresas que operam na UE devem implementar a SCA nessas datas. Essa forma superior de autenticar a identidade do consumidor aumenta a segurança das transações de eCommerce, reduzindo as perdas com fraude em transações CNP. Baseados uma pesquisa realizada com 88 executivos da área de pagamento na Europa em novembro de 2019, o Aite Group e a conferência *Merchant Payment Ecosystem* (MPE) coletaram diferentes opiniões sobre os benefícios em potencial da SCA (Figura 4).[3] O resto do mundo observa atentamente o lançamento da SCA e seus impactos nas perdas com fraude.

3. Veja o relatório do Aite Group *Strong Customer Authentication: Friend or Foe?*, janeiro de 2020.

Figura 4: Opiniões sobre o impacto da SCA nas fraudes em transações CNP



Fonte: Pesquisa do Aite Group com 88 executivos da área de pagamento na Europa realizada em cooperação com a MPE em novembro de 2019

MÉTODOS PARA MITIGAR AS FRAUDES

Os estabelecimentos comerciais podem se concentrar em dois pontos ao implementarem soluções para mitigar fraudes: proteger a conta ou proteger a transação financeira.

SOLUÇÕES DE PREVENÇÃO DE FRAUDE EM CONTAS

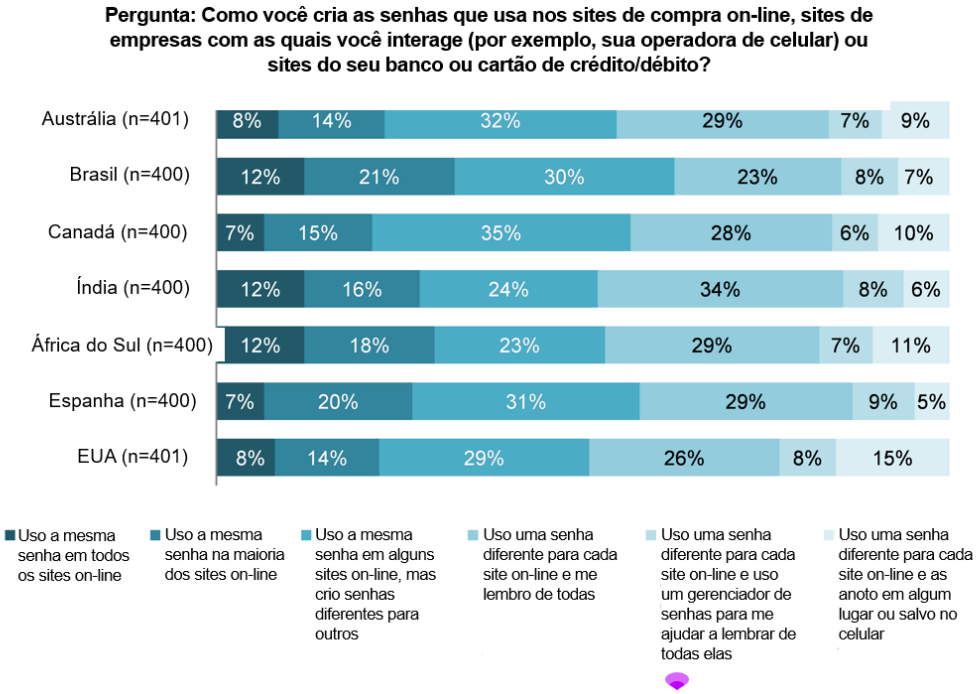
As fraudes relacionadas à conta têm por alvo a conta digital mantida pelo cliente em um estabelecimento comercial. Os fraudadores usam informações pessoais identificáveis obtidas por meio de violações para criar uma conta on-line ou se apoderar da conta de um cliente. Desde 2013, foram violados mais de 30 bilhões de registros contendo nomes de usuário, senhas, endereços residenciais, números de telefone e outros dados – e esse número cresce a cada ano.

Sabemos que os usuários criam senhas fracas e usam a mesma senha em vários sites. Uma pesquisa do Aite Group descobriu que metade dos consumidores usa a mesma senha em vários ou todos os sites (Figura 5).[4] Para os fraudadores, é muito fácil conduzir testes em grande escala para identificar combinações válidas de nome de usuário/senha. Uma vez identificadas, há boas chances de as credenciais funcionarem em outros sites também. Um estudo realizado pela NordPass com mais de 275 milhões de senhas comprometidas, identificou que três senhas comuns representavam quase 13% do total de senhas afetadas (“123456,” “123456789” e

4. Veja o relatório do Aite Group *Second Annual Global Security Engagement Scorecard™*, outubro de 2017.

"senha"). Só 44% das senhas eram únicas.[5] Com os compradores on-line usando senhas tão simples e repetitivas, não é de se surpreender que as contas sejam atacadas pelos fraudadores.

Figura 5: Como os consumidores globais criam senhas



Fonte: Pesquisa do Aite Group com 2.802 consumidores, setembro de 2016

A fraude em conta é difícil de ser detectada por muitas razões. Quando um fraudador tem acesso ao nome de usuário e senha de um cliente e usa essas informações para acessar sua conta on-line, é difícil saber se quem está lá é o cliente ou um fraudador. Isso ser pode problemático por dois motivos. Primeiro, se o estabelecimento comercial on-line armazena os dados do cartão de crédito ou débito do cliente para compras futuras, não é difícil para o fraudador fazer uma compra e enviá-la para um endereço sob seu controle. Segundo, os fraudadores podem entrar no programa de fidelidade de uma companhia aérea, hotel ou outras empresas e roubar os pontos acumulados pelo cliente. Assim, é cada vez mais imperativo proteger esses dois tipos de conta on-line.

Há vários tipos de soluções de prevenção de fraude em nível de conta, como serviços de verificação (identidade, endereço de e-mail, documentos de identificação oficiais), preenchimento de credenciais por bots, impressão digital do dispositivo, biometria (física e comportamental), autenticação do dispositivo móvel e outros. Algumas dessas soluções são passivas, ou seja, são transparentes para o usuário e oferecem uma boa experiência para o consumidor. Outras são ativas, pois exigem o engajamento do usuário. Foi comprovado

5. "*Top 200 Most Common Passwords of the Year 2020*," NordPass, acessado em 12 de janeiro de 2021, https://nordpass.com/most-common-passwords-list/.

recentemente que o uso da impressão digital do dispositivo (ou *device fingerprint*)combinado a biometria comportamental é um meio eficaz de identificar fraude.

SOLUÇÕES DE PREVENÇÃO DE FRAUDE TRANSACIONAL

As fraudes transacionais têm por alvo as compras on-line, onde credenciais roubadas (normalmente, um cartão de crédito ou de débito) são usadas para adquirir produtos físicos ou digitais que os fraudadores podem converter em dinheiro rapidamente. Quando um comprador clica no botão “Comprar agora” na página de checkout, o sistema de autorização avalia se a compra é fraudulenta e decide se aprova ou não a transação. Os estabelecimentos comerciais têm a opção de usar essas ferramentas antes que a rede seja acionada (antes do envio da autorização à rede de pagamento e à instituição financeira) ou depois que a rede é acionada (depois de receber a resposta da rede de cartão e da instituição financeira). Essas ferramentas de prevenção de fraude usam uma combinação de machine learning (ML) e motor de regras para determinar a ação apropriada. Em alguns casos, a transação suspeita pode ser enviada à equipe de revisão manual, onde uma pessoa analisa e decide aprovar ou declinar.

De modo geral, os esforços dos estabelecimentos comerciais para reduzir fraudes começaram em nível de transação. Com o tempo, as ferramentas de prevenção de fraude nas transações evoluíram e passaram a incluir detecção de fraude em nível de conta. A vantagem de usar uma solução que atua nas duas frentes é que isso permite o uso de dados em nível de conta para informar um modelo de ML em nível de transação antes de a transação ser gerada, aumentando os índices de detecção de fraude e de aprovação. Essas soluções combinadas são chamadas também de hubs de orquestração, onde um sistema central atua como um regente de orquestra e cada solução de fraude é um músico que participa da execução da sinfonia. Para os estabelecimentos comerciais, os hubs oferecem uma API única que dá acesso a uma solução holística para proteger tanto a conta, quanto a transação, simplificando bastante a implementação e a gestão operacional.

COMO EQUILIBRAR A EXPERIÊNCIA DO CONSUMIDOR

Independentemente de o estabelecimento comercial usar uma solução em nível de conta, uma solução em nível de transação ou uma solução combinada, a experiência do consumidor deve ser sempre levada em conta. Há dois termos que os estabelecimentos comerciais detestam: “fricção” e “abandono do carrinho”. Fricção é o número de ações que um cliente precisa realizar em uma compra on-line. Isso inclui criar uma conta on-line, identificar-se no momento da compra, inserir um código de uso único (OTP, na sigla em inglês) no site, etc. O abandono do carrinho acontece quando os consumidores adicionam itens ao seu carrinho de compras, mas não finalizam a compra. A fricção pode resultar em abandono do carrinho e perda de vendas.

Um estudo do Aite Group com 1.400 consumers no Reino Unido, Singapura e Estados Unidos sobre o impacto da fricção no abandono do carrinho revelou dados interessantes. Os usuários consideravam a criação de uma conta on-line e a comprovação de sua identidade no momento do pagamento similarmente inconvenientes. Em média, 30% a 40% dos usuários disseram que esses dois tipos de fricção muito provavelmente os levariam a abandonar a transação de eCommerce. Quando questionados sobre a necessidade de inserir um OTP, 15% a 29% dos usuários disseram que muito provavelmente isso os levaria abandonar a transação. A faixa é baseada em usuários que se autoidentificam como compradores de eCommerce que compram

com pouca, média ou muita frequência. Analisando as faixas etárias, consumidores com 55 anos ou mais se mostraram ligeiramente mais dispostos a aceitar a fricção.[6] As melhores soluções de prevenção de fraude otimizam a experiência do cliente ajustando a fricção ao risco, quando necessário, para proteger o cliente e o estabelecimento comercial.

GESTÃO DE FRAUDE: PREVENÇÃO DE PERDA VS. ATIVO DE NEGÓCIO

Tradicionalmente, o objetivo de uma solução antifraude é controlar e reduzir as perdas com fraude. O departamento de prevenção de fraude costuma estar ligado ao grupo de operações e sua performance é medida pelo montante de perdas irrecuperáveis. Muitas vezes, isso foi motivo de preocupação para os stakeholders internos, como os departamentos de vendas de eCommerce, financeiro e marketing, cujo foco é maximizar as vendas. É comum as pessoas acharem que a redução de fraudes implica necessariamente em prejuízos ao cliente na forma de compras legítimas negadas por suspeita de fraude. É como se fosse preciso escolher uma das opções. Uma empresa pode limitar suas perdas com fraude ou maximizar seus índices de aprovação, mas não fazer as duas coisas. Nesse ambiente conflitante, acontece de o departamento de prevenção ser visto como departamento de "prevenção de vendas".

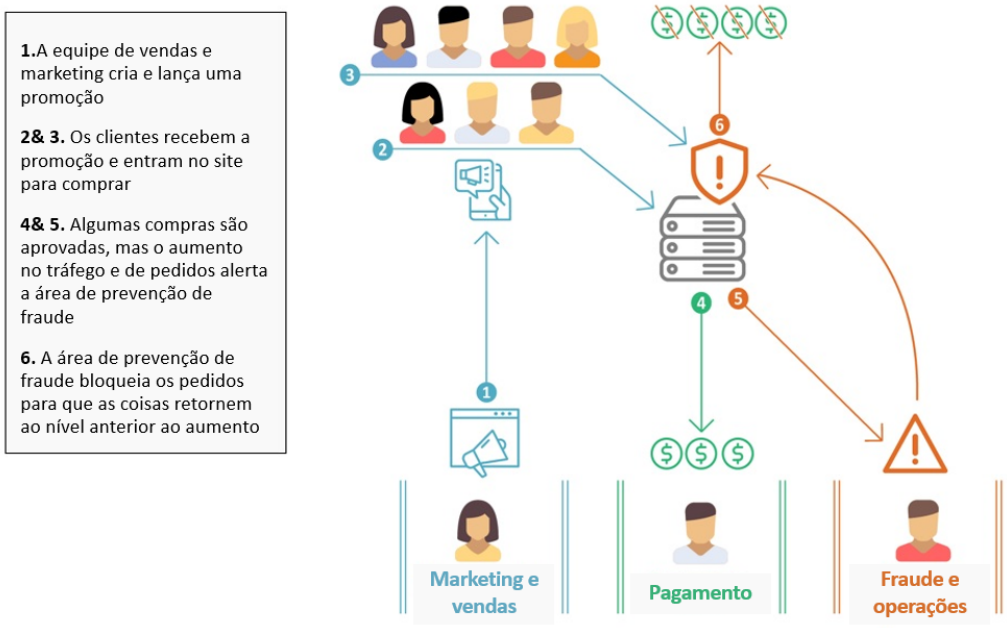
Mas será que tem que ser assim?

Em vez de escolherem se reduzem as fraudes *ou* aumentam os índices de aprovação, alguns estabelecimentos comerciais estão trabalhando para reduzir as fraudes *e* aumentar os índices de aprovação, equilibrando essas métricas para aumentar o número de pedidos legítimos aceitos. O departamento de prevenção de fraude está ganhando espaço e trabalhando com outros stakeholders internos para impulsionar o crescimento. A prevenção de fraude é vista como um ativo de negócio e parte do processo de planejamento, junto com vendas e marketing.

Em um caso de uso, os departamentos de vendas e marketing de um estabelecimento comercial planejaram uma promoção oferecendo desconto em vários produtos para gerar tráfego no site e aumentar as vendas. O departamento de prevenção de fraude não foi informado. Quando a promoção começou, o departamento de prevenção de fraude notou um aumento substancial no tráfego do site, bem como no número de compras e no valor do tíquete médio. Isso fez com o sistema antifraude disparasse alertas para o comportamento anormal. Foram implementados controles de risco para limitar a atividade e voltar aos níveis normais. A empresa perdeu vendas, desperdiçou o dinheiro investido em marketing e os clientes ficaram irritados. (Figura 6).

6. Veja o relatório do Aite Group *Global Consumers' Authentication Preferences: Have Your Cake and Eat It Too*, setembro de 2018.

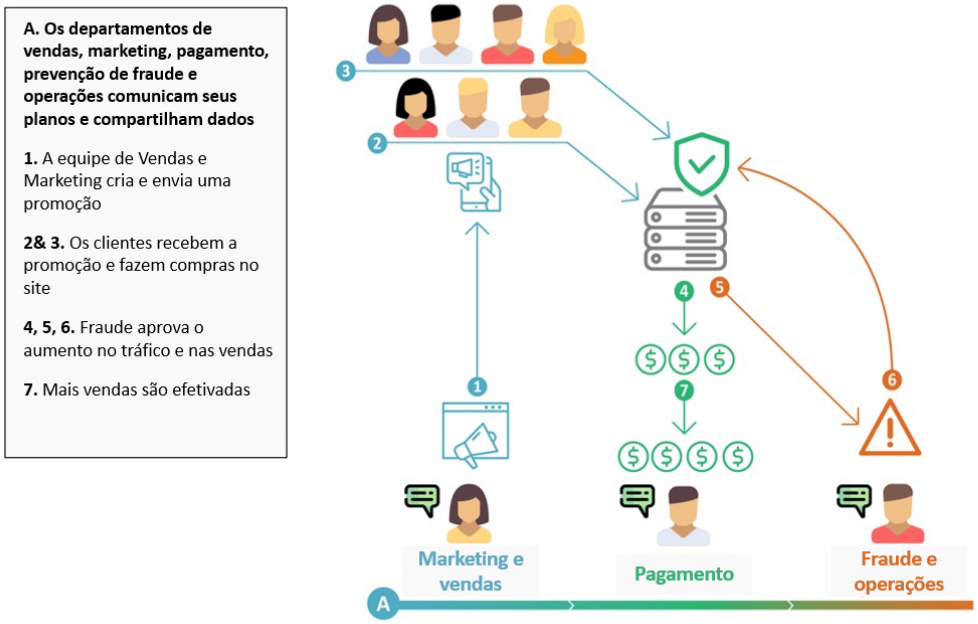
Figura 6: Ambiente empresarial isolado



Fonte: Aite Group

Estabelecimentos comerciais proativos estão derrubando os muros organizacionais e colocando as áreas de vendas, marketing, pagamento, fraude e operações para trabalhar colaborativamente, comunicando seus planos e compartilhando dados para otimizar as estratégias de prevenção de fraude e risco. Por exemplo, as ferramentas de prevenção de fraude podem ser modificadas para levar em conta o aumento no número de pedidos e os níveis de risco decorrentes de promoções. A equipe de pagamento pode compartilhar informações sobre os índices de aprovação e trabalhar com a equipe de prevenção de fraude em planos para melhorá-los. Operações pode permitir que o departamento de prevenção de fraude tenha acesso ao sistema de gestão de pedidos para saber quem são os clientes leais e evitar que o sistema antifraude decline suas transações. O departamento de prevenção de fraude pode usar os chargebacks recebidos para mostrar aos departamentos de vendas/marketing os motivos das disputas dos clientes a fim de que eles melhorem a clareza dos sites e/ou deem mais destaque aos termos e condições no processo de checkout. Trabalhando com as outras áreas, equipe de prevenção de fraude pode se tornar um ativo estratégico para o crescimento do negócio (Figura 7).

Figura 7: Ambiente de negócio colaborativo



Fonte: Aite Group

RUMO À PERFEIÇÃO

Em um mundo perfeito, uma ferramenta de prevenção de fraude identifica e aprova todas as transações legítimas e declina todas as fraudulentas. Um sistema antifraude possui duas métricas operacionais sobre as quais o estabelecimento comercial tem controle: os falsos positivos e os falsos negativos. É possível elevar as vendas e a satisfação dos clientes gerenciando essas métricas com eficácia.

Os falsos positivos acontecem quando uma transação legítima não é autorizada, o que deixa o cliente descontente e gera ineficiências internas. Já os falsos negativos acontecem quando uma transação fraudulenta é aprovada, o que gera chargebacks e prejuízos ao estabelecimento comercial. A redução dos falsos positivos maximiza o faturamento do estabelecimento comercial e a otimização dos falsos negativos minimiza os custos – ou seja, a empresa ganha duas vezes.

Falsos positivos e negativos são medidas da eficácia das estratégias antifraude que o estabelecimento comercial implementou na ferramenta/sistema de prevenção de fraude. Os falsos negativos são mais fáceis de gerenciar. Visa e Mastercard dão feedbacks regularmente aos estabelecimentos comerciais sobre os falsos negativos na forma de chargebacks sinalizados com um código de razão de fraude. A Visa fornece esse dado no arquivo TC40, enquanto a Mastercard usa o arquivo SAFE. Os estabelecimentos comerciais podem reduzir os falsos negativos se analisarem os chargebacks atentamente e fizerem os devidos ajustes no sistema antifraude. Uma boa prática é criar um ciclo de feedback no modelo de ML do sistema antifraude e usar os dados das transações sabidamente fraudulentas para treinar o modelo de ML.

Os falsos positivos são mais difícieis de gerenciar porque não existe uma fonte definitiva de informação. Em um mundo ideal, o estabelecimento comercial conseguiria ligar para os portadores de cartão sempre que uma autorização fosse negada para perguntar se eles fizeram a transação. Isso não é realista porque não há recursos suficientes e não se sabe se o telefone informado pertence ao portador do cartão ou ao fraudador. Uma fonte desse tipo de informação é o call center. Muitos clientes legítimos ligam para saber por que sua transação foi indevidamente declinada. O departamento de prevenção de fraude deve trabalhar junto com operações para criar um meio de capturar essa informação valiosa. Outra opção é adotar uma prática comum entre os emissores. As instituições financeiras costumam contatar os portadores de cartão por mensagem de texto, e-mail ou resposta interativa por voz (IVR, na sigla em inglês) quando suspeitam de uma transação e determinar se eles a reconhecem. Estudos mostraram que os portadores de cartão apreciam e valorizam essa prática, pois sentem que a instituição financeira se preocupa com eles. Os estabelecimentos comerciais podem fazer o mesmo, agradando os clientes e coletando dados valiosos sobre falsos positivos para refinar a performance do sistema antifraude. Seria necessário usar uma ferramenta de verificação de identidade para comprovar que o número de telefone ou endereço de e-mail pertence ao portador do cartão e não ao fraudador. Um relatório global sobre fraude de eCommerce elaborado pela Cybersource concluiu que os estabelecimentos comerciais de eCommerce declinam 2.5% de todos os pedidos por suspeita de fraude. Qualquer redução nesse número se traduz em aumento imediato nas vendas, sem custos adicionais – uma proposta bastante atraente para qualquer estabelecimento comercial de eCommerce.[7]

7. "*2019 Global eCommerce Fraud Management Report*", Cybersource, 2019, acessado em 3 de março de 2021, https://www.cybersource.com/content/dam/cybs2019/documents/en/global-fraud-report-2019.pdf.

CONCLUSÃO

Os fraudadores continuam modernizando seus vetores de fraude e usando técnicas cada vez mais sofisticadas. Para ter as defesas apropriadas, o estabelecimento comercial precisa ser muito diligente. Mas prevenir fraude é mais do que barrar transações ilegítimas. A prevenção de fraude pode ser uma vantagem estratégica para o crescimento do seu negócio on-line. Empresas eficazes colocam prevenção de fraude no mesmo patamar que marketing, produtos e vendas. Quando as engrenagens estão bem lubrificadas e trabalham colaborativamente, a performance em geral melhora. O mesmo se dá com o departamento de prevenção de fraude em uma empresa.

Conclusões específicas para os estabelecimentos comerciais:

- O comércio on-line chegou para ficar. As empresas que entenderem isso e otimizarem a experiência dos seus clientes serão vitoriosas.
- Os fraudadores sabem que as preferências dos consumidores mudaram e que eles estão cada vez mais adotando as compras on-line. Isso cria um risco financeiro e de negócio que os estabelecimentos comerciais precisam gerenciar cuidadosamente.
- Há muitas soluções para mitigar as fraudes em nível de conta e de transação. As soluções mais recentes oferecem funcionalidades de hub de orquestração, combinando os dois tipos de solução.
- Independentemente das soluções que escolherem para mitigar as fraudes, os estabelecimentos comerciais precisam monitorar cuidadosamente a experiência do consumidor para evitar o excesso de fricção e o abandono do carrinho.
- Prevenção de fraude não é mais uma função operacional focada exclusivamente na redução de perdas. Conforme as vendas on-line vão ficando mais competitivas, os estabelecimentos comerciais proativos estão apostando mais na gestão e prevenção de fraude para impulsionar o crescimento.

SOBRE O AITE GROUP

O Aite Group é uma empresa global de pesquisa e consultoria que oferece assessoria completa e prática sobre questões empresariais, tecnológicas e regulatórias e sobre seus impactos na indústria de serviços financeiros. Temos expertise na área de bancária, pagamento, seguro, gestão de fortunas e mercado de capital e orientamos instituições financeiras, fornecedores de tecnologia e empresas de consultoria do mundo todo. Trabalhamos em parceria com clientes para revelar seus pontos cegos e fornecer insights para que seu negócio fique mais inteligente e mais forte. Visite-nos na web e contate-nos via Twitter e LinkedIn.

SOBRE O AUTOR

David Mattei
+1.617.398.0908
dmattei@aitegroup.com

CONTATO

Para mais informações sobre os serviços de pesquisa e consultoria, contate:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

Para dúvidas de imprensa e conferências, contate:

Aite Group
+1.617.398.5048
pr@aitegroup.com

Para outras dúvidas, contate:

info@aitegroup.com