Como a fraude está mudando e como responder

Os riscos e a pandemia de COVID-19

A crise da COVID-19 representa um dos maiores contratempos da história do setor de pagamentos eletrônicos.

Com as quedas nos PIBs, a recessão global em andamento e a provável mudança nos comportamentos do consumidor, muitos aspectos dos empréstimos com cartões de crédito e débito serão impactados. Mas, no curto prazo, são as súbitas mudanças no ambiente de risco que tendem a afetar profundamente a performance geral do setor.

A Visa Consulting & Analytics (VCA) investigou as mudanças no risco dos pagamentos eletrônicos de vários ângulos. Neste documento, falaremos sobre gestão das fraudes.

Quase todos os gerentes de risco experientes já atuaram em meio a uma desaceleração econômica. Alguns podem até ter enfrentado uma crise econômica grave, como a crise financeira global de 2008 e 2009. Embora ainda não seja possível determinar o alcance exato desta crise sem precedentes, sabemos que seu impacto no comportamento do consumidor tem sido extraordinário.

No início de maio, por exemplo, a *Oxford Economics* relatou que o gasto global das famílias tinha caído ainda mais, e mais rápido, do que o PIB[1]. Nesse meio tempo, o *PYMNTS.com*, serviço de notícias voltado à indústria de pagamento, informou que, em apenas oito semanas, observara: "seis vezes mais consumidores trabalhando remotamente, quatro vezes mais consumidores fazendo compras de supermercado *on-line* ao invés de presencialmente, quatro vezes mais consumidores pedindo refeições para viagem de agregadores ou dos seus restaurantes favoritos e três vezes mais consumidores fazendo outros tipos de compras on-line além de supermercado."[2]

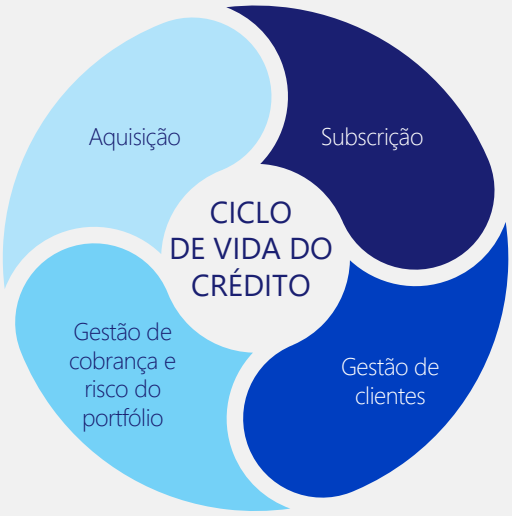
Para os fraudadores, a confusão, a distração e a vulnerabilidade geradas pela crise de COVID-19 são sinônimo de oportunidade. Os criminosos podem usar as mudanças de comportamento para disfarçar suas ações, aproveitar o fato de que bancos e estabelecimentos comerciais estão modificando suas operações e atacar consumidores desprevenidos.

Os gerentes de risco de crédito enfrentam uma tempestade perfeita. Todas as fases do ciclo de vida de crédito estão sob extrema pressão ao mesmo tempo. Para piorar, ninguém sabe como a crise vai evoluir, quanto tempo ela durará e como será a recuperação.

A crise de COVID-19 põe as quatro fases do ciclo de vida de crédito sob extrema pressão

A mudança nos fundamentos econômicos cria a necessidade de repensar o apetite de risco, estabelecer políticas de aquisição mais rígidas e reduzir o custo dessas aquisições.

Com o aumento do risco em todo o portfólio, o volume avança para a área de cobrança, o último recurso para proteger a performance e a reputação.



Com a materialização de novos riscos, passa a ser necessário rever os modelos de subscrição, refletir cuidadosamente sobre a precificação baseada no risco e prestar atenção especial às fraudes.

As práticas de gestão de clientes devem estar alinhadas com as mudanças no comportamento do consumidor – isso inclui a gestão das linhas de crédito, os planos de amortização, a gestão de autorizações e a detecção de fraudes.

1 *"Coronavirus Watch As restrictions ease, a slow revival", Oxford Analytics,* 4 de maio de 2020: *http://resources.oxfordeconomics.com/coronavirus-watch-as-restrictions-ease-a-slow-revival?oemost recent content download id=0000029&interests trending topics=coronavirus*
2 *"Why Consumers Aren't In A Rush To Reopen The Economy", PYMNTS.com,* 4 de maio de 2020: *https://www.pymnts.com/coronavirus/2020/no-rush-to-reenter-physical-world/*

Portanto, a indústria de pagamento está vivendo uma mudança profunda e súbita na natureza do risco dos pagamentos eletrônicos. No curto prazo, a mudança deve afetar profundamente a performance geral de qualquer negócio de pagamento eletrônico. Neste documento, falaremos sobre a gestão de clientes, que engloba a detecção e a gestão de fraudes.

A detecção e a gestão de fraude envolvem três pontos importantes:

1 Primeiro e mais importante: a situação atual é propícia para os fraudadores.

Alguns dos tipos de atividade reportados são ataques de força bruta, tentativas de saques em caixas automáticos e golpes de *phishing*, compras falsas de criptomoedas e "*click-and-collect*". Além disso, os incidentes de cibersegurança continuam sendo um grave motivo de preocupação. Emissores, estabelecimentos comerciais e credenciadores precisam estar sempre alertas a tudo o que está acontecendo.

Para completar, os índices de fraude tendem a ser mais altos no canal de *eCommerce*; assim, qualquer mudança no mix de pagamentos CP (cartão presente) para CNP (cartão não presente) tende a aumentar a relação fraude/vendas.

2 Segundo: a crise diminuiu a utilidade de muitos dos sistemas usados pelas equipes de prevenção se fraude.

Por exemplo, muitas ferramentas de detecção de fraude trabalham para identificar padrões de gastos incomuns. Mas como a crise mudou o comportamento de gastos, quase tudo ficou fora do padrão, o que inevitavelmente aumenta a proporção de falsos positivos detectados.

3 Terceiro: emissores, estabelecimentos comerciais e credenciadores devem se preparar para uma alta na "fraude em primeira instância".

Muitos dos consumidores que estão passando por sérias dificuldades financeiras podem se sentir tentados a contestar transações legítimas. Da mesma forma, consumidores confinados em casa acabam exagerando nas compras on-line, se arrependem e iniciam uma série de reclamações e disputas. Por fim, a expectativa é de aumento nas solicitações de cartões feitas por fraudadores.

Ao mesmo tempo, o aumento nas transações CNP torna o aumento nas 'fraudes amigáveis' quase inevitável. Ao conferirem suas faturas, muitos portadores de cartão poderão encontrar transações que parecem fraudulentas – gastos em categorias em que antes não havia transações on-line, nomes de estabelecimentos comerciais que não facilitam a correlação do item comprado com o montante da transação e múltiplos lançamentos para uma única compra (por exemplo, quando a loja lança o valor da compra e do frete separadamente).

Embora ainda seja cedo para avaliar o impacto total da crise, a indústria de pagamento está se preparando para uma grande disrupção. Por exemplo, vários grandes processadores de pagamento estão retendo depósitos para se proteger do aumento esperado nos *chargebacks;* além disso, com a crise, os portadores de cartão americanos hoje contestam duas ou três vezes mais transações do que antes[3].

O desafio para o gerente de risco é manter-se extremamente alerta e se adaptar às novas realidades sem prejudicar a qualidade da experiência do cliente. Em um momento de mudança nos comportamentos de pagamento e de formação de novos hábitos, adotar uma estratégia de gestão de fraude exageradamente rígida pode facilmente levar um consumidor a optar por outro cartão.

3 *"Hit by Coronavirus—and a 30% Holdback by the Payment Processor", Wall Street Journal,* 15 de junho de 2020: *https://www.wsj.com/articles/hit-by-coronavirusand-a-30-holdback-by-the-payment- processor-11592040601*

Verdades universais

Embora ainda precisemos determinar como a crise evoluirá, bem como seus impactos de longo prazo, algumas verdades universais são inquestionáveis.

Quando se trata de pagar, os consumidores sempre buscaram – e continuarão buscando – a combinação ideal de confiança, conveniência, rapidez, simplicidade e aceitação universal.

Em contrapartida, a área de prevenção de fraude sempre trabalhou – e continuará trabalhando – com três parâmetros interrelacionados.

Estes três parâmetros continuarão determinando a função e as ações da área de prevenção de fraude. O formato do triângulo pode estar mudando, mas os fundamentos se manterão. O trabalho de um gerente de risco é manter o equilíbrio e a ponderação.

Os detalhes da resposta dependerão das circunstâncias do emissor, do tamanho e das características do seu portfólio, do ambiente de fraude em que ele opera e da gravidade da crise em seu mercado local. A VCA reuniu nove imperativos que, em nossa opinião, são relevantes a todos os emissores, onde quer que eles operem.

Nove imperativos para as equipes de prevenção de fraude durante a pandemia de COVID-19

#1

Prepare-se para golpes de teste de conta – como ataques de enumeração ou de força bruta

No momento, este pode ser seu maior risco.

Os fraudadores estão se aproveitando do aumento global nos volumes de compra via *eCommerce* para disfarçar os golpes de teste de conta. Usam ataques de enumeração ou de força bruta para enviar pedidos de autorização sistematicamente para o BIN de um emissor na tentativa de obter credenciais de pagamento legítimas.

Portanto, fique de olho em aumentos incomuns no número de transações. Cuidado com as transações que são declinadas porque o número da conta é inválido e os pedidos de autorização em série (por exemplo, vários pedidos seguidos com alguns segundos de intervalo, vindos da mesma fonte).

Se suspeitar de um ataque, aja rápido e investigue a situação. Além disso, cuidado com os pedidos de autorização usando números de contas sequenciais e redobre a proteção a contas com números similares.

#2

Fique de olho em suas redes de caixas automáticos e esteja pronto para agir imediatamente

Muita atenção ao '6011' – o MCC dos caixas automáticos

Se você sofrer um ataque de saque em caixa automático, as perdas podem ser rápidas e substanciais.

Revise suas regras e limites de saques diários. Acompanhe a quantidade de transações e valores médios dos saques. Procure picos irregulares e tenha um plano para responder imediatamente.

#3

Trabalhe com todo o ecossistema de *eCommerce* e ajude seus pares a ajudá-lo

Uma de nossas melhoras defesas é o trabalho conjunto e a união de esforços de todo o setor. Participe ativamente de fóruns da indústria de pagamento e do setor de segurança pública, e converse com seus pares para avaliar tendências e possíveis soluções. E não se descuide dos seus relatórios de fraude. Quanto antes você enviar seus relatórios, mais cedo os sistemas da Visa podem aprender com eles. Ferramentas como *Visa Advanced Authorization* (VAA) e *Visa Risk Manager* (VRM) nos permitem eliminar os riscos emergentes antes que eles se transformem em tendências.

#4

Saiba que qualquer brecha em sua armadura pode ser descoberta e exposta rapidamente

Os fraudadores vão procurar pontos vulneráveis em suas operações e na segurança dos seus portfólios.

Por exemplo, se a sua equipe de prevenção de fraude não trabalha durante a noite ou nos finais de semana, este é o momento de ampliar sua cobertura. Da mesma forma, se seu pessoal está trabalhando de casa, mas não tem acesso às ferramentas e tecnologias que usariam na empresa, elimine essa disparidade.

E fique atento aos riscos a que seus fornecedores estão expostos. Por exemplo, se você terceiriza parte das suas operações de prevenção de fraude, como esse terceiro está lidando com a crise?

Este é o momento de otimizar sua capacidade de prevenir fraudes, não de comprometê-la.

#5

Informe, oriente e incentive seus portadores de cartão

Use todos os canais para se comunicar proativamente com seus portadores de cartão e aproveite a oportunidade para orientá-los e tranquilizá-los.

Avise que você está trabalhando mais para evitar fraudes e, por isso, eles poderão receber mais comunicados relacionados a fraude e/ou pedidos de verificação que o normal.

Fale sobre as fraudes mais comuns ou que estão despontando em seu mercado. E lembre-os dos tipos de alerta ou serviços de SMS que você oferece.

#6

Confie em sua equipe de análise

Muito provavelmente, a chave para identificar padrões de fraude novos ou desconhecidos está em seus próprios dados transacionais. Assim sendo, desafie continuamente seus analistas a descobrir novos *insights*.

Um ponto importante: se hoje seus ciclos de reporte são trimestrais ou mensais, reduza-os e adote uma frequência semanal ou diária.

Além disso, é provável que, antes da pandemia, os índices de fraude de CNP ficassem distorcidos pelo grande volume de transações relacionadas a viagens. Para fazer uma comparação mais homogênea, exclua as transações relacionadas a viagens, que provavelmente serão poucas depois do início dos *lockdowns*.

#7

Responda ao aumento de alertas de fraude de forma rápida, sistemática e sensata

Inevitavelmente, você receberá muitos alertas de risco. Aceite que (devido à migração em massa para o *eCommerce* e o aumento nos gastos fora do padrão) as pontuações de risco perderão parte de sua efetividade.

Assim, reavalie suas regras de performance para refletir a mudança forçada nos comportamentos diários de pagamento e priorize suas atividades de investigação. Atualize seus modelos de risco rapidamente. Por exemplo, modelos de fraude supervisionados precisarão ser ajustados rapidamente e com mais frequência devido às mudanças de comportamento. Com a COVID-19, quase todos os gastos estão fora do padrão, o que eleva os índices de falsos positivos. Assim sendo, reporte as novas fraudes o quanto antes, incluindo novas descobertas, e faça os ajustes necessários.

E, se você ainda usa técnicas baseadas em regras, chegou a hora de se modernizar e adotar os mais recentes ativos de dados, ferramentas e tecnologias.

#8

Reavalie seus planos de gestão de crises e eventos cibernéticos à luz da COVID-19

É bem provável que seus planos de gestão de crises e avaliações de cibersegurança tenham sido elaborados sob circunstâncias muito diferentes. Reavalie-os levando em conta a circunstâncias criadas pela COVID-19 e defina o que precisa ser alterado e como.

Por exemplo, com que rapidez e eficiência você conseguiria lidar com um grande comprometimento de dados ou evento cibernético? Qual seria o seu nível de exposição? Suas equipes e seus sistemas conseguiriam responder rapidamente?

#9

Lembre-se do elemento humano

Se o pior acontecer e uma conta vier a ser comprometida, comunique-se com o cliente de forma aberta e proativa. O que um cliente normalmente espera:

- Que você o informe, em caso de fraude
- Que você acredite nele
- Que tudo se resolva em poucos dias
- Que você o mantenha informado a cada passo
- Que você o oriente no processo de recuperação
- Que você o ensine a evitar fraudes no futuro

Aproveite para transformar uma situação potencialmente difícil em um motivo para o cliente continuar leal à sua marca.

Embora a pandemia de COVID 19 tenha afetado empresas de todas as partes, situações desafiadoras também oferecem oportunidades. A equipe da Visa Consulting & Analytics pode orientar sua empresa quanto à melhor forma de responder à pandemia de COVID-19.

Sobre a Visa Consulting & Analytics

Somos uma equipe global composta por centenas de consultores de pagamento, cientistas de dados e economistas espalhados por seis continentes.

- Nossos consultores têm décadas de experiência na indústria de pagamento e são experts em estratégia, produtos, gestão de portfólio, risco, recursos digitais e mais.
- Nossos cientistas de dados são experts em estatística, análises avançadas e machine learning e têm acesso exclusivo aos insights da VisaNet, uma das maiores redes de pagamento do mundo.
- Por fim, nossos economistas entendem a conjuntura econômica que afeta os gastos do consumidor e oferecem insights exclusivos e oportunos sobre as tendências de consumo no mundo.

A combinação de nossa profunda expertise em consultoria na área de pagamentos, nossa inteligência em estratégias econômicas e a ampla variedade de dados a que temos acesso nos permite identificar insights e recomendações práticas que contribuem para a tomada de decisões comerciais melhores.

Para obter ajuda para abordar alguma das ideias ou imperativos acima, contate seu executivo de conta Visa para agendar um horário com a equipe Visa Consulting & Analytics ou envie um e-mail para VCA@Visa.com. Se preferir, visite-nos no Visa.com/VCA

