White Paper

A estratégia antifraude tem um novo papel: facilitador da inovação

Patrocinado por: CyberSource

Jerry Silva
11/03/2020

Este documento é uma tradução de sua versão original, escrito em inglês. Caso haja divergências entre o original e a tradução em português, a versão original deve prevalecer.

OPINIÃO DA IDC

As soluções contra fraudes tradicionalmente se concentram em contenção de perdas, mas isso não é suficiente na era da transformação digital, em que os comércios online estão expandindo os canais de contato com seus clientes, adotando modelos de comércio automatizados e contínuos e empregando uma infinidade de novas formas de pagamento. Os estabelecimentos comerciais digitais precisam de uma estratégia antifraude que abra as portas para inovação e expansão *seguras*, impedindo perdas por fraudes e otimizando as taxas de aceitação de transações. Uma combinação de regras ágeis e análises avançadas é essencial para esta estratégia. Como os *players* do comércio digital, na era da transformação digital, estão colocando em prática estratégias avançadas de gerenciamento de fraudes?

NESTE WHITE PAPER

As empresas de comércio eletrônico de diversos setores enfrentam um desafio semelhante em relação à prevenção de fraudes: devem conter ataques e perdas sem afetar a experiência do cliente com recusas excessivas de transações.

Como se isso já não fosse um grande desafio, a estratégia antifraude deve ser ágil o suficiente para acompanhar as organizações à medida que expandem sua presença no comércio eletrônico, ampliam seus negócios além das fronteiras geográficas e se transformam digitalmente, possibilitando o envolvimento do cliente através de uma infinidade de dispositivos e novos canais.

Construir este tipo de estratégia abrangente e sensível de gerenciamento de fraudes é uma jornada que pode ser assustadora para muitas organizações. À medida que os comércios investem na criação de produtos, em estratégias de lançamento no mercado e na inovação no varejo, eles não necessariamente desejam comprometer recursos para criar uma grande equipe de operações antifraude ou gerenciar soluções complicadas de integração de dados no local.

Portanto, muitas organizações estão mudando a maneira como abordam o gerenciamento de fraudes. Esta mudança começa com a adoção de uma solução que ajude a tomar decisões altamente precisas em tempo real, usando regras flexíveis e testáveis e análises avançadas. Porém, muitas vezes isto inclui a adoção de uma abordagem híbrida para o gerenciamento e operações da solução, dando

suporte a especialistas internos com uma equipe externa de especialistas em fraudes e soluções que podem oferecer monitoramento 24 horas, decisões automatizadas e suporte. Essa abordagem híbrida permite que os comércios digitais implementem, testem e adaptem regras continuamente, por meio de uma equipe externa e sem comprometer muitos recursos internos nessa tarefa .

Este *white paper* da IDC Financial Insights apresenta as principais conclusões de entrevistas com executivos de prevenção a fraudes, representando três diferente segmentos — um varejista de moda global, um líder em artigos esportivos para atividades ao ar livre e uma grande companhia aérea — que compartilham insights sobre a criação de programas abrangentes e adaptáveis de gerenciamento de fraudes para controlar perdas e melhorar as taxas de aceitação, ao mesmo tempo em que suas organizações se expandem para novos canais, em novos países e com novas linhas de produtos.

Na adaptação de suas soluções antifraude, cada organização entrevistada implantou a CyberSource, uma solução Visa, e usou uma combinação única de regras flexíveis, modelos preditivos de fraude com análises avançadas de dados históricos e atuais e machine learning projetado para prever ou calcular o resultado para cada transação de aceitação, rejeição ou verificação manual, reduzindo as perdas por fraude.

A INOVAÇÃO EM COMÉRCIO DIGITAL REQUER PROTEÇÃO SOFISTICADA CONTRA FRAUDES

O comércio eletrônico representa 15% do total de vendas de varejo em todo o mundo, sendo que a expansão internacional deve impulsionar um crescimento consistente. A expansão geográfica está se tornando possível em grande parte devido à inovação entre os provedores de soluções de pagamentos, que permitem que os estabelecimentos comerciais digitais aceitem mais facilmente métodos de pagamento de diferentes mercados, bem como transações com cartões estrangeiros.

Enquanto isso, os estabelecimentos comerciais estão investindo na transformação digital de forma a melhorar a experiência de compra do consumidor, elevar as taxas de conversão e criar uma experiência de "comprador fidelizado" que se alinha à expectativa de satisfação instantânea. Já tendo ampliado os recursos de compras online e com dispositivos móveis, os comércios hoje buscam criar uma experiência unificada, consistente e em tempo real entre vários canais. Os consumidores devem poder buscar um item em seu dispositivo móvel, concluir a compra online e buscar mercadorias em uma loja física, tudo em uma única transação. Além disso, a previsão é que os consumidores terão engajamento cada vez maior no comércio conectado, através de serviços por assinatura, com pagamentos automatizados conduzidos por uma variedade de dispositivos IoT ou conectados. Espera-se que, em 2020, 32% dos comércios invistam em tecnologias de inovação de varejo, incluindo comércio conectado e que, até 2024, 15% de todos os pagamentos sejam feitos com dispositivos “vestíveis”, enquanto 10 bilhões de dispositivos estarão conectados a serviços financeiros, de acordo com pesquisas de insights sobre varejo da IDC.

Esta complicada intersecção da expansão internacional com a inovação de canais e engajamento do cliente deve gerar não apenas novas e ilimitadas oportunidades para os comércios como trazer consigo novos riscos de fraude, que exigem soluções robustas e foco na gestão de um ambiente no qual o tempo entre o ato da compra e sua concretização fique cada vez menor.

Fraudadores sabidamente visam novos serviços e produtos com a suposição de que os comércios terão vulnerabilidades imprevistas em um ambiente ainda não testado. Infelizmente, a história confirma essas vulnerabilidades. Os varejistas têm relatado consistentemente um aumento rápido nos

ataques de fraude na abertura de canais de dispositivos móveis, assim como na entrada em novos mercados. Além disso, como já se verificou no setor bancário, o tamanho do varejista pouco importa quando se trata de ser um alvo. Quando as maiores instituições começaram a reforçar suas defesas, bancos comunitários e cooperativas de crédito menores tornaram-se alvos de fraudes. Não há motivo para acreditar que os varejistas estarão imunes a ataques apenas porque são relativamente menores.

À medida que os comércios começam a aceitar novos tipos de pagamento em diferentes regiões, eles podem não ter regras ou modelos desenhados para monitorar e avaliar os riscos específicos desses fluxos de transações. Isto é especialmente desafiador. O IDC Financial Insights prevê que, até 2024, 60% dos comércios em todo o mundo aceitarão entre um e cinco tipos de pagamento localizados em mercados estrangeiros para expandir sua presença no comércio digital. Deve-se supor que a adoção de cada um desses tipos de pagamento exigirá uma proteção diferenciada. Por exemplo, será impossível ajustar um modelo de fraude de cartão a uma transação direta do banco ou carteira digital, ambos os quais estão ganhando cada vez mais força na Europa e na Ásia.

Por fim, os comércios também devem se preocupar com ataques em compras multicanais. Os fraudadores sabem muito bem que os comércios estão expandindo o engajamento multicanal do cliente e enxergam isso como uma fraqueza. Recentemente, tem se verificado um aumento nas fraudes em compras multicanal, em que os pedidos de compra são realizados online mas retirados na loja (modelo BOPUS), de forma que os fraudadores induzem a aceitação de um pagamento ilegítimo pela internet e, em seguida, retiram mercadorias físicas na loja, muitas vezes sem precisar apresentar documentos pessoais.

Para aumentar o desafio, embora os comércios tenham trabalhado para proteger os canais móveis e online, eles ainda podem não ter as ferramentas para proteger o call center, onde existe mais um ponto cego no elemento humano. Muitos ataques começam com o uso pelos fraudadores de agentes de engenharia social para obter mais dados de credenciais do cliente, que podem então ser usados para autorizar uma compra online ou para se fazer passar por um cliente durante uma transação telefônica. Em outros casos, os fraudadores manipulam os agentes para fazer alterações nos endereços e emails para iniciar o processo de aquisição total da conta.

RISCOS E VETORES DE FRAUDE EVOLUEM CONSTANTEMENTE

À medida que os comércios criam estratégias em torno da proteção antifraude para sua expansão internacional e para engajamento sem atritos com seus clientes, eles também devem ficar de olho na constante evolução dos vetores de fraude.

Os ataques de cartão não presente (ou CNP, compras feitas por canais remotos) hoje representam cerca de 50% do total de perdas com cartões em todo o mundo e devem atingir US$ 35 bilhões até 2022, segundo *The Nilson Report.* As transações feitas com cartões de pagamento roubados representam cerca de 30% do total de estornos, o que dobra o impacto sobre o comércio que sofre a perda do bem e a exigência de reembolso do dinheiro pelo item perdido. No geral, 55% das empresas relatam um aumento na fraude online, de acordo com a Experian.

Para dificultar ainda mais a situação, os comércios geralmente usam sistemas de gerenciamento de estornos e fraudes fechados em silos de informação, criando pontos cegos no monitoramento de transações e dificultando o alinhamento de seus esforços contra novos e, às vezes, imprevistos ataques de fraude.

A sempre presente ameaça cibernética no comércio digital

Os ataques de fraude no comércio digital variam muito, mas muitos são alimentados pelo fluxo interminável de dados violados ou roubados no mercado clandestino. Uma coleção de dados de cartões de pagamento, números de conta, CVVs, datas de validade e endereços pode ser comprada na dark web por US$ 1 por conta. Esses dados são operacionalizados em larga escala por sofisticadas quadrilhas de fraude, que usam automação e analítica para planejar seus ataques. Um exemplo comum são quadrilhas que usam robôs para testar constantemente os dados de cartão e credenciais com pequenas transações até encontrarem aqueles que funcionam, abrindo a porta para compras muito maiores ou para vender os dados no mercado clandestino.

Aquisição sofisticada de contas: a engenharia social combinada com o ataque cibernético

À medida que os fraudadores vão sofisticando cada vez mais suas organizações e tecnologias, eles compilam meticulosamente os dados roubados e violados com outros dados extraídos das redes sociais, bem como através de engenharia social e ataques cibernéticos, como phishing ou pagejacking, para tomar posse total de contas ou identidades e perpetrar ataques mais prolongados e retornos maiores.

No phishing, os fraudadores imitam um indivíduo ou fonte confiável para obter dados confidenciais. Por exemplo, um indivíduo pode receber uma mensagem de email que se apresenta como proveniente de uma instituição financeira, sugerindo que há um problema na conta e solicitando que o indivíduo verifique as informações pessoais por meio de um formulário vinculado. Outra estratégia de fraude parecida é o pagejacking, em que os fraudadores clonam uma página da web ou um site inteiro e, em seguida, usam estratégias de otimização de pesquisa para elevar esse site fraudulento acima do site legítimo na pesquisa online. Usuários desavisados muitas vezes acessam o site falso e divulgam, sem querer, seus dados confidenciais.

Em todos os casos, os fraudadores podem usar esses dados confidenciais para obter acesso a uma conta, geralmente começando por ações que não envolvem dinheiro, como alteração de endereços e emails, para que possam autenticar e receber pedidos. Esses ataques também podem incluir a aquisição de dispositivos, em que o fraudador migra o número de telefone da vítima para o seu próprio dispositivo, permitindo que a vítima se autentique quando as senhas únicas são enviadas. Isto pode levar a novas aquisições de contas usando dados e acessos existentes no dispositivo.

Depois de tomar posse total da conta, os fraudadores podem começar com pequenas compras por um longo período, com o objetivo de passar despercebido pelo consumidor. Com o tempo, os fraudadores adquirem esses conjuntos completos de credenciais e abrem novas contas em nome de uma vítima, muitas vezes sem ser detectados, pois muitos consumidores não têm alertas de novas contas configurados em agências de crédito ou outros serviços.

Fraude de identidade falsa: gerando perdas

As credenciais roubadas também podem ser usadas para alimentar fraudes de identidade falsas, nas quais os criminosos associam fragmentos de dados de identidade válidos com informações falsas para formar uma entidade totalmente nova e abrir novas contas. Os fraudadores podem associar um número válido de CPF de uma criança – um número que nunca foi usado – a um endereço real de entrega e um número de telefone real e, em seguida, gerar um nome e data de nascimento falsos. O objetivo é combinar informações suficientes para estabelecer as credenciais de uma nova conta de

pagamento. Os cinco principais bancos emissores registraram perdas de mais de US$ 5 bilhões relacionadas à fraude de identidade falsa, segundo a IDC Financial Insights.

Fraude em programas de lealdade e recompensas: ataques que atraem pouca atenção

Assim como ocorre com as fraudes de contas novas, os fraudadores também estão se concentrando na área tipicamente pouco monitorada de programas de fidelidade e recompensa. Conforme os consumidores acumulam pontos de fidelidade por meio de seus cartões de crédito ou programas de recompensa no comércio digital, os fraudadores usam táticas de aquisição de conta para utilizar estas recompensas e pontos para realizar compras. Embora os consumidores frequentemente se inscrevam em programas de recompensas, é sabido que muitos não resgatam seus pontos ou verificam a situação de suas contas, o que significa que os ataques passam despercebidos, em grande parte, por longos períodos.

Fraude amigável

A estranhamente denominada *fraude amigável* ocorre quando um cliente genuíno comete uma fraude conscientemente em sua própria conta. Os cenários variam amplamente, mas podem incluir clientes que fazem uma compra, recebem as mercadorias e ligam para o emissor do cartão dizendo que não receberam o item. Os estabelecimentos comerciais têm dificuldade em evitar esse tipo de fraude, pois as transações vêm de clientes conhecidos.

SOLUÇÕES DE FRAUDE COMO FACILITADORAS DE INOVAÇÃO

Embora novos processos comerciais, formas de pagamento e integrações de canais possam abrir novas portas para fraudadores dedicados, esses riscos potenciais não devem coibir a inovação. De fato, antes as equipes de prevenção a fraudes dificultavam a visão das equipes de produtos, que desejavam lançar novos serviços, e hoje podem se concentrar na implementação de soluções robustas antifraude que podem ajudar a viabilizar a inovação.

As soluções e estratégias antifraudes no comércio digital devem ter como objetivo três benefícios principais: reduzir perdas e estornos, aprimorar a experiência do cliente e aumentar a conversão de vendas. O caminho para realizar isso é através de soluções de monitoramento de fraudes que avaliam transações e tomam decisões de risco em tempo real com base em uma ampla variedade de dados. Isto fornece uma visão holística, tanto da transação em si como da entidade que gerou o evento.

Nos primórdios da expansão do comércio eletrônico, os estabelecimentos comerciais analisavam quase todos os pedidos para avaliar riscos. Essa prática desacelerava muito as operações e gerava decisões sem nuances de falsos positivos e recusas. Isso só deteriorava o relacionamento com o cliente.

A próxima fase do monitoramento de fraudes usava automação limitada para tomar decisões de risco nas transações. Esses sistemas geralmente eram criados com base em regras básicas semelhantes e tomavam decisões sobre risco com base em elementos como incompatibilidade entre o endereço de entrega e o endereço da conta. Mas essa automação simples deixava de analisar essas transações fraudulentas em um contexto ou padrão mais amplo.

Hoje, as soluções antifraude em comércio digital de última geração oferecem detalhamentos reforçados por regras minuciosamente ajustadas e baseadas em análises avançadas, alimentadas por um grande volume e variedade de dados de um único comércio ou entre organizações. Isso fornece a capacidade de enxergar anormalidades "normais" nas transações, bem como anomalias muito reais que indicam fraude. Essas soluções usam regras baseadas em históricos de perfis e transações das empresas e organizações. Por exemplo, as soluções podem observar comportamentos por determinados períodos de tempo, destacando que uma empresa específica geralmente compra passagens aéreas para vários outros indivíduos, indicando que esse é um comportamento normal que não deve ser destacado para revisão ou causar a recusa da transação. Por fim, o objetivo de tomar melhores decisões leva a uma redução de pedidos recusados e à melhoria da experiência do cliente, sem comprometer a segurança.

Para que regras com nuances possam funcionar, os sistemas antifraude devem considerar um amplo conjunto de dados para obter uma visão holística do risco. No monitoramento de fraudes em tempo real, a solução deve levar em consideração o máximo possível de informações sobre a transação. As informações mais diretas envolvem o valor da transação, a hora do dia e a região. Mas, no contexto, a solução saberia mais sobre o comprador. Quão comum é essa transação em comparação com outras feitas no passado por esta mesma conta? Este comprador normalmente faz compras em horários estranhos da noite? Existe algum motivo para a geolocalização do dispositivo ser diferente do endereço vinculado à conta do comprador? Esses tipos de perfis podem ser criados ao longo do tempo, seja uma conta do consumidor com um comércio ou pela vinculação de dados históricos a um dispositivo ou a uma conta de cartão entre várias organizações.

É cada vez mais possível – e importante – entender o comportamento do usuário por meio de dados que vão além do dispositivo. As soluções antifraude mais modernas avaliam a identificação do dispositivo, o endereço de IP, a resolução da tela, a autenticação e os dados biométricos comportamentais relacionados à entidade para criar um perfil de comportamento normal e, então, um contexto correspondente de anomalia.

Mesmo com os melhores dados e ferramentas de tomada de decisão em tempo real, deve-se presumir que cada comércio lida, em sua base de consumidores, com diferentes desafios de fraude e perfis de compra que mudam a toda hora. Como tal, as ferramentas antifraude devem ser ajustadas de acordo com as necessidades específicas de cada comércio, o que exige um sistema flexível de geração de políticas. Essas regras serão aprimoradas para encontrar padrões vinculados a fraudes específicas à região, à medida que os comércios entram em novos mercados. As regras também serão usadas para entender o comportamento normal e anormal nas transações multicanal e em novos dispositivos.

A agilidade para ajustar as regras também ajuda os comércios a lidar com condições de mercado em rápida evolução ou com ataques verticais específicos ao setor ou à organização. Por exemplo, alguns varejistas podem ajustar suas regras com base em horários específicos de pico de vendas e ciclos de compra de produtos ou por tipo de produto. Eles podem ajustar essas regras ao fim de uma temporada ou quando passar uma “febre” por um produto.

Machine Learning e agilidade das regras

Oferecer agilidade não se resume apenas à capacidade de criar regras rapidamente; significa também ter os dados corretos para definir a política de risco, além de possuir a habilidade de testar a eficácia dessas regras. As soluções antifraude de última geração devem incluir análises avançadas e monitoramento de desempenho. Com análises avançadas, as ferramentas podem processar grandes

quantidades de dados, incluindo fraudes conhecidas, e aproveitar modelos de machine learning para identificar padrões de comportamento associados a esses ataques. O monitoramento de desempenho é um sistema de retroalimentação que ajuda a orientar os modelos.

Os modelos de machine learning podem ser "ensinados" a buscar comportamentos específicos e a definir grupos de atividades entre transações ativas que indicam um possível ataque. Em ambos os casos, eles são automatizados e têm a capacidade de filtrar dezenas de dados para obter uma visão mais detalhada. Frequentemente, os modelos de machine learning podem ser utilizados de acordo com regras recomendadas de implementação.

Em alguns casos, esses dados serão extraídos de um único comércio, mas alguns fornecedores de soluções antifraudes podem analisar grandes conjuntos de informações de diversas organizações. Trabalhando com várias organizações, as equipes de operações antifraude podem segmentar os comportamentos de fraude por segmento, geografia ou tamanho da organização (entre muitos outros fatores). A segmentação permite que surjam padrões de fraude específicos a cada mercado, permitindo que os fornecedores de soluções avisem proativamente o comércio de um segmento específico sobre a iminência de um ataque, para que este possa criar regras e análises para se preparar.

Depois que as regras são recomendadas, elas devem ser testadas em um ambiente isolado, com dados reais de produção, para avaliar seu desempenho e seus resultados. Por fim, o comércio, em conjunto com seu fornecedor de soluções antifraudes, deve gerar relatórios consistentes sobre o desempenho das regras para avaliar as mudanças no mercado e a possível degradação devido à mudança nos comportamentos de fraude. É aqui que a importância de regras ágeis e análises adaptáveis realmente entra em jogo.

Soluções antifraude: conduzindo a experiência do cliente, aprimorando a conversão

Em última instância, é necessária uma combinação de análises orientadas por dados, geração ágil de regras e machine learning para que os comércios consigam efetivamente atenuar suas perdas por fraude e também fornecer uma experiência sem fricção ao cliente.

A capacidade de gerar regras e políticas de forma ágil equilibra o volume de fraude que a organização está disposta a permitir a fim de reduzir o atrito com o cliente. Se as regras forem muito rígidas, as taxas de aceitação de compras cairão e a insatisfação do cliente poderá aumentar. Os especialistas em fraude devem levar em consideração o custo dos falsos positivos e a consequente frustração do cliente, em equilíbrio com os ataques bem-sucedidos. O custo de falsos positivos pode ser medido de perto por transações perdidas, mas mais difícil de avaliar é o impacto de longo prazo nos relacionamentos com os clientes e na redução de clientes recorrentes. Frequentemente, quando os fornecedores de soluções antifraude oferecem monitoramento de desempenho de regras, um indicador de desempenho (KPI) mensurável é o número de pedidos recusados, bem como o custo de investigação de transações não fraudulentas.

Otimização operacional: redução de revisões e serviços gerenciados

Além de medir o sucesso pelas perdas controladas e a aceitação otimizada de compras, as equipes de operações antifraude também devem medir a redução ou o controle no custo das operações. Gerir uma equipe de operações antifraude pode ser caro; desperdiçar recursos em avaliações e investigações desnecessárias, resultantes de falsos positivos, aumenta esse custo. Dessa forma, os

especialistas em fraude devem criar regras com o propósito de reduzir o número de horas de trabalho, sem comprometer a segurança ou o atendimento ao cliente.

Além disso, os responsáveis pelos esforços antifraude no comércio digital podem procurar otimizar suas operações adotando serviços antifraude gerenciados externamente. O modelo gerenciado pode assumir várias formas. Em alguns casos, os fornecedores de soluções antifraude oferecem decisões em tempo real como serviço, enquanto as equipes locais do comércio criam as políticas e regras de risco. Em outros casos, a equipe externa fornece a criação de regras e as decisões, enquanto uma equipe local faz a avaliação e a investigação de forma manual. Finalmente, é possível terceirizar toda a operação. Em todo caso, o objetivo seria reduzir a complexidade e o custo das operações, estendendo horas e tendo flexibilidade no número de funcionários para que os recursos possam ser aumentados durante as épocas de pico de fraude ou reduzidos em outras épocas.

MODELANDO KPIS: A CHAVE PARA MANTER O EQUILÍBRIO

Criar uma estratégia antifraude é uma empreitada complexa que requer um equilíbrio cuidadoso entre o controle de perdas por fraude e a otimização da aceitação de pedidos e da experiência do cliente.

À medida que buscam adotar modernas soluções antifraude, os especialistas devem criar um conjunto de valores mensuráveis ou indicadores de desempenho que demonstrem a eficácia de suas estratégias antifraude em relação aos seus objetivos comerciais. Além disso, eles devem avaliar se sua estratégia antifraude é um inibidor ou facilitador de inovação.

Os especialistas em fraude devem considerar o desenvolvimento dos seguintes KPIs:

- Perdas por fraude comparadas às taxas de aceitação:
  - Taxas de aceitação e rejeição de transações
  - Taxas de estorno e motivos
  - Taxas de falsos positivos e taxa de detecção de valor
  - Perdas por fraude
- Otimização operacional:
  - Porcentagem de transações enviadas para revisão manual (incluindo fraudes e não fraudes)
  - Horas de trabalho necessárias para revisão e investigação manuais
  - Tempo gasto na gestão de dados
  - Tempo gasto na gestão de regras e seu desempenho
- Experiência do cliente e inovação:
  - Capacidade organizacional de expandir e inovar
  - Tempo para lançar o produto e controle de fraude a cada novo lançamento
  - Atrito com o cliente, incluindo o tempo gasto na autenticação e conclusão da transação
  - Recorrência dos clientes
  - Reclamações de clientes relacionadas a fraudes e/ou recusas

CYBERSOURCE EM AÇÃO

A CyberSource, uma solução da Visa, fornece soluções de gateway de pagamento de comércio digital e gerenciamento de fraudes que conseguem combinar agilidade na criação de regras, análises avançadas e serviços gerenciados de fraude. Em sua atuação, a CyberSource assume uma função colaborativa com seus clientes de comércio digital para fornecer uma abordagem abrangente ao gerenciamento de fraudes. Nas seções a seguir, os três cenários demonstram como as soluções da CyberSource são colocadas em ação para se adiantarem às fraudes em rápida evolução, ajudando a atender aos principais objetivos empresariais e apoiando a inovação.

Backcountry.com: uma abrangente estratégia antifraude para avaliar riscos de entidades e transações

Em 1997, a Backcountry.com foi fundada como uma pequena empresa online destinada à venda de equipamentos exclusivos para esportes ao ar livre – sua primeira linha foi uma coleção de equipamentos de segurança para avalanches. A empresa expandiu-se rapidamente, com uma ampla variedade de equipamentos esportivos, presença internacional e posição de liderança de mercado em seu segmento entre grandes marcas.

Nos primeiros dias da Backcountry, enquanto seus pedidos cresciam rapidamente, ainda era relativamente fácil gerenciá-los com processos geralmente manuais. Como tal, a estratégia antifraude da empresa foi construída com base no uso de regras simples e na revisão manual de quase todos os pedidos. Mas essa abordagem se tornou insuficiente para lidar com a diversificação das linhas de produtos, a expansão dos mercados geográficos e a introdução de um canal móvel que, combinados, quase instantaneamente causaram novos riscos e ataques.

No início, a Backcountry implementou suas próprias regras de risco, projetadas para capturar o que pareciam ser anomalias simples nas transações dos clientes (por exemplo, endereços de cobrança e entrega incompatíveis eram direcionados para revisão manual). Mas com maior volume e diversidade na base de clientes, isso se tornou impossível. Além do mais, fraudadores sofisticados conseguiam descobrir as regras. Por fim, o processo antifraude estava atrapalhando o crescimento dos negócios.

Quando a Backcountry decidiu criar uma estratégia antifraude, tinha uma forte equipe de especialistas no assunto que sabia como resolver casos complicados pela ampla experiência com revisões manuais. A Backcountry queria otimizar essa equipe, garantindo que estivesse analisando e investigando apenas fraudes verdadeiras e não falsos positivos. A organização também não queria aumentar o número de funcionários da equipe antifraude de forma que a tornasse um centro de custos.

Iniciativa antifraude da Backcountry: precisão na criação de regras

A Backcountry finalmente construiu sua iniciativa antifraude usando o Decision Manager da CyberSource como centro de avaliação de risco de transações em tempo real. A CyberSource fornece monitoramento de fraude como serviço, recebendo dados de transações e entidades por meio de uma API da Backcountry e tomando decisões para aprovar ou rejeitar a transação ou recomendar revisão manual. A equipe de especialistas em fraudes da Backcountry cria as regras desenhadas para acionar alertas de risco com base em seu extenso histórico de verificação e investigação.

A Backcountry e a CyberSource trabalharam para criar regras de risco o mais específicas possível, a fim de tomar decisões mais direcionadas. As equipes analisaram dados históricos de transações,

inclusive fraudes conhecidas, para buscar padrões subjacentes de risco e, em seguida, usaram essas informações para criar regras específicas por região, canal, dispositivo e linha de produtos, entre outros fatores.

A granularidade de regras permite que a empresa monitore mais de perto as fraudes em produtos de maior risco. Em um caso, a equipe escreveu regras específicas para uma pessoa que a equipe chama, em tom de brincadeira, de "mulher das barracas" – uma fraudadora que liga periodicamente para o call center para comprar barracas usando cartões de crédito falsos. Também existem tendências sazonais que não correspondem às de outros varejistas. No outono, Backcountry recebe um padrão de fraudadores que buscam comprar casacos caros para revender no mercado clandestino no inverno.
Com o Decision Manager, a equipe cria regras de decisão mais rigorosas para as transações de casacos de inverno, que podem ser menos estritas após a temporada.

Ao mesmo tempo, essas regras permitem que a Backcountry compreenda melhor o tráfego legítimo que apresenta um comportamento aparentemente anômalo. Por exemplo, uma avaliação atenta das tendências revelou à equipe que os compradores legítimos geralmente não fornecem as informações de cobrança mais precisas, enquanto os fraudadores fornecem conjuntos de informações totalmente completos. Escrever regras baseadas nesse conhecimento assegura que os clientes legítimos sejam encaminhados para completar seus dados, mas não são recusados ou enviados para revisão manual.

Entendendo o risco de entidade

À medida que a estratégia antifraude da Backcountry evoluiu, ficou claro que o caminho para a melhor decisão de risco possível exigiria avaliar fatores além de dados e históricos transacionais – incluiria também a avaliação do risco da entidade vinculada à transação.

Por exemplo, a equipe da Backcountry foi atingida por uma série de ataques de grupos de fraude, provenientes de dispositivos com a mesma resolução de tela. A equipe aprendeu que precisava incluir a resolução da tela do dispositivo como um elemento ou dado na avaliação do risco. O Decision Manager da CyberSource permite a integração com uma variedade de soluções de risco, que gera dados que podem enriquecer a visão do risco da entidade.

Com a capacidade de integração, a equipe da Backcountry decidiu que usaria a identificação do dispositivo, o histórico de email e a conexão IP como fatores na tomada de decisões, juntamente com os dados da transação. Isso significa que, para cada decisão, o histórico transacional – como valores incomuns ou velocidade incomum de transações – pode ser combinado com dados sobre o dispositivo da entidade ou biometria comportamental. Essas correlações destacam o comportamento normal e anormal no dispositivo, por exemplo, como elemento central da avaliação do risco da entidade que conduz a transação. Em alguns casos, a equipe escreveu regras que determinariam quais transações seriam enviadas às soluções de plug-in de API para uma investigação mais aprofundada da entidade. Em outros casos, dados de enriquecimento são usados como parte do fluxo de monitoramento de transações em tempo real.

Adquirindo uma visão de risco entre mercados com machine learning

Embora a equipe antifraude da Backcountry tenha desenvolvido uma profunda experiência no estudo dos dados da organização para determinar suas regras de risco, a CyberSource conseguiu aplicar ainda mais nuances às regras, adicionando sua perspectiva sobre padrões de fraude e risco de muitos comércios.

A CyberSource, que atende centenas dos maiores comércios online do mundo, criou uma solução de gerenciamento de fraudes a partir de modelos de machine learning que analisam grandes conjuntos de dados de pagamento de todas essas empresas de varejo. Isso é especialmente importante na identificação de quadrilhas de fraude que atingem, primeiro os comércios mais vulneráveis, até que estes ajustem seus controles e depois passam para a próxima organização.

A Backcountry vem acertando cada vez mais na identificação de fraudes agora que os modelos de machine learning da CyberSource sugerem regras, possibilitando que a empresa mantenha listas de observação de entidades altamente precisas com base em uma variedade mais ampla de variáveis de risco.

Medindo o desempenho: além do controle das perdas por fraude

Como todo comércio, a Backcountry mede o desempenho pela redução de perdas por fraude junto com a capacidade de aumentar a taxa de aceitação de pedidos. A Backcountry procura reduzir as taxas de cancelamento ou de transações que são enviadas para verificação e então finalmente canceladas.

Por fim, a Backcountry deseja otimizar as operações de sua equipe antifraude. Um fator central de sucesso para tal, é a redução da necessidade de revisão manual e a garantia de que os casos que exigem investigação, tenham maior probabilidade de serem fraudes reais do que falsos positivos.

Mas o sucesso na prevenção de fraudes não é um objetivo pontual. Como os comportamentos dos fraudadores mudam constantemente e as táticas de colocação de produtos no mercado continuam evoluindo, a Backcountry mede o sucesso pela agilidade. Nesse caso, definimos a agilidade como a capacidade de escrever facilmente regras que podem ser rapidamente testadas, implementadas e revogadas quando possível.

É essa agilidade que garantirá que o programa antifraude seja um facilitador contínuo da automação e inovação, ao invés de uma barreira.

Philippine Airlines: evitando fraudes sofisticadas ao abrir os portões digitais

Há sete anos, a Philippine Airlines (PAL) enfrentou os mais desafiadores dilemas de fraude no varejo. No momento em que a empresa precisava expandir o engajamento de clientes no âmbito digital e de centro de contato, os ataques de fraude se tornaram mais sofisticados, causando grandes perdas e taxas de estorno, que ultrapassaram os limites dos programas de monitoramento das redes de cartões e geraram advertências de bancos.

Na tentativa de controlar a situação, a empresa usou uma ferramenta interna para criar regras rigorosas utilizando listas positivas e negativas, mas isso apenas reduziu as taxas de aceitação de pedidos e dificultou fortemente o engajamento dos clientes com os canais. Conforme os fraudadores continuavam a ficar mais sofisticados, a ferramenta interna deixou de ser suficiente para detectar pedidos suspeitos, o que levou a PAL a sofrer vários ataques de fraude.

Para controlar este nível de fraude, a PAL reestruturou sua estratégia antifraude, implementando o mecanismo de decisão em tempo real da CyberSource com regras e modelos direcionados que ajudariam a identificar fraudes sem prejudicar a experiência do cliente.

Os objetivos da implementação eram reduzir as taxas de fraude, aumentar a aceitação de pedidos e melhorar a experiência do cliente, ao mesmo tempo em que a organização expandia os tipos de transações que poderiam ocorrer entre canais, incluindo o digital e o centro de contato. Para fazer isto, a PAL queria especificamente basear suas regras e modelos nas recomendações encontradas em um robusto conjunto de dados extraídos de várias companhias aéreas e agências de viagens da região.

No programa de fraude reestruturado da PAL -– há sete anos em produção -– a CyberSource opera o Decision Manager remotamente. Ao receber dados por meio de uma API da companhia aérea, a solução consegue avaliar -– em tempo real -– as decisões baseadas em risco para aceitar, recusar ou revisar transações com base nas regras de limite de risco do cliente. A PAL cria suas próprias regras de detecção de riscos, além das regras criadas por um especialista em fraudes da CyberSource.

Esta abordagem combinada significa que a maioria das regras é construída sobre um amplo conjunto de dados, incluindo histórico de transações e boas práticas da CyberSource, e é adaptada para analisar os riscos associados às variáveis e parâmetros identificados pela PAL. O monitoramento de avaliação contínuo mostra o desempenho dessas regras e alerta para a sua desatualização devido a possíveis alterações nos comportamentos de fraude ou sazonalidade, permitindo um ajuste muito rápido da política e dos limites. A PAL usa o ambiente de testes da CyberSource para experimentar regras novas ou adaptadas nos dados de produção para avaliar proativamente seu desempenho e executar modelos de análise de fraudes passadas para encontrar melhores resultados para as regras.

Medindo o desempenho: operações otimizadas, redução de fraude e melhor experiência do cliente

Como primeiro passo de sua abrangente iniciativa antifraude, a PAL reduziu drasticamente suas perdas por fraude e a organização não chegou nem perto de atingir o limite de estorno das redes de cartões.
Hoje, a PAL mede seu sucesso de maneiras mais sofisticadas.

Um KPI medido constantemente são as taxas de aceitação de pedidos pela organização, que afetam diretamente a experiência do cliente. Além disso, o sucesso continua a ser medido pela agilidade das regras. As regras da PAL são um trabalho em andamento constante e orientado. As políticas são ajustadas regularmente para otimizar o faturamento considerando as taxas de rejeição e perdas aceitáveis, além de abordar fatores variáveis do mercado.

A longo prazo, a PAL continuará a usar essa agilidade para expandir produtos, alcance de mercado e acessibilidade de canal. Desde o seu lançamento, a iniciativa da PAL adicionou o canal móvel ao seu programa antifraude e poderá abrir novos canais à medida que surgirem em um ambiente protegido, com regras que podem ser personalizadas para cada caso de uso.

Um varejista de moda internacional: cobertura de fraudes para permitir rápida expansão geográfica

O crescimento de uma empresa de varejo de alta moda, que vendia uma única marca em suas lojas físicas para um grande revendedor internacional multimarcas com presença no comércio eletrônico multicanal, exige uma estratégia antifraude totalmente nova.

Quando esse varejista internacional, que solicitou anonimato, começou a construir sua presença no comércio eletrônico internacional, além das lojas físicas, a organização não tinha soluções antifraude.

Havia pouca necessidade de monitoramento de transações de compras na loja, protegidas pela cobertura da rede de cartão de crédito.

Mas a expansão a vendas online e a aceitação de transações com cartão não presente, significou que o varejista subitamente se tornou responsável por perdas. Para aumentar a pressão, o varejista cresceu tão rapidamente em vários mercados que chamou a atenção de fraudadores, aumentando em pouco tempo as perdas e estornos.
A primeira resposta foi começar a recusar pedidos, mas o grupo descobriu imediatamente que esta não era a abordagem correta. Não se pode adotar a prevenção de fraudes ao custo da redução das vendas.

À medida que se propunha a encontrar uma solução antifraude, a empresa aprendeu rapidamente que, mais do que a simples redução de fraudes, era necessária uma estratégia abrangente. O varejista precisava de uma solução que reduzisse o atrito com o cliente, aumentasse a aceitação de pedidos e limitasse as revisões manuais demoradas, além de reduzir as perdas. Especificamente, a organização estava buscando uma solução que permitisse à empresa escrever regras de política flexíveis e, por sua vez, equilibrar de perto a quantidade de perdas por fraude que ela poderia sofrer em relação à otimização da aceitação de pedidos.

O varejista estava especialmente preocupado com a alta satisfação do cliente à medida que entrava em cada nova região geográfica. Durante a expansão, o grupo aprendeu rapidamente que cada mercado tinha desafios únicos de fraude e perfis diferentes de consumidores. Embora a equipe possa confiar nas experiências passadas de clientes similares da CyberSource nesses mercados para ajudar a estruturar uma estratégia inicial antifraude adequada, as soluções antifraude ainda precisam estar bem cientes das nuances de cada região para os produtos específicos.

Ao buscar uma estratégia antifraude, a organização não queria criar uma equipe de combate ao crime ou gastar infinitos recursos de TI gerenciando sistemas complicados. A empresa tornou-se conhecida internacionalmente por táticas inovadoras de varejo, que dependiam de tecnologia interessante. Não queria sair do curso ou perder o foco, desviando recursos intensivos de tecnologia para operações antifraude.

Esse varejista decidiu finalmente implantar o Decision Manager da CyberSource, criando uma relação do que a organização chama de colaboração verdadeira com o fornecedor de gerenciamento antifraudes, agora com oito anos de relacionamento. O Decision Manager fornece monitoramento e decisões em tempo real de todas as transações, usando uma combinação de modelos analíticos avançados e regras de política adaptáveis para identificar vendas potencialmente fraudulentas e aumentar a aceitação dos pedidos. A solução recebe uma grande variedade de dados dos sistemas do varejista, desde os detalhes da transação até o endereço de entrega e cobrança, números de conta, ID do dispositivo, conexão IP e muito mais. O objetivo é estabelecer uma base do comportamento normal do cliente para identificar anomalias que indicam fraude. O melhor tipo de solução faz isso com o tipo de nuance que permite que haja anormalidades "normais".

Além de implementar o monitoramento via Decision Manager, o varejista também contratou uma equipe de especialistas em fraudes para lidar com a revisão manual e outras operações. A equipe da CyberSource trabalha pelo varejista em uma operação de gerenciamento de fraude 24 horas por dia. Enquanto isso, o varejista mantém uma pequena equipe antifraude dedicada no local, que faz a garantia de qualidade dos resultados da equipe da CyberSource, tomando decisões finais sobre

transações suspensas. A equipe do varejista trabalha com a equipe da CyberSource para criar políticas e regras para equilibrar "perdas aceitáveis" com uma experiência do cliente otimizada.

Expansão de mercado e marca propiciada por análises avançadas e regras ágeis

A combinação da criação ágil de regras e análises avançadas é essencial para permitir que esse comércio continue com sua estratégia de expansão geográfica do comércio eletrônico. Como cada novo mercado apresenta ameaças únicas de fraude e introduz novos perfis de consumidores, é essencial entrar em cada região com um conjunto de modelos e regras aprimorados. O problema é que o ajuste fino pode ser difícil logo após a entrada em um novo mercado. É aqui que a experiência regional histórica dos clientes da CyberSource e as análises avançadas se tornam mais importantes.

À medida que a empresa começa a se deslocar para novas geografias, a equipe da CyberSource executa uma análise completa do mercado, realizando análises avançadas de machine learning para processar grandes quantidades de dados de comércios. A análise desses dados possibilita a identificação de tendências de fraude passadas e o estabelecimento de perfis de consumidores para melhor compreender os comportamentos normais e anormais das compras.

O resultado desses modelos permite à CyberSource sugerir regras de decisão sobre fraudes, que podem ser usadas imediatamente em uma nova implementação. A equipe da CyberSource fornece informações para comunicar, por exemplo, a redução das taxas de risco em transações de maior valor em um mercado mais rico ou a limitar transações de alto valor em uma área repleta de fraudes, por exemplo. Sem acesso ao amplo conjunto de dados da Visa e o uso de modelos avançados, poderia levar meses para treinar uma solução antifraude com as nuances necessárias para novos mercados ou lançamentos de novos produtos.

Além disso, as regras podem ser ajustadas para tipos de pagamento específicos para cada um desses mercados.
Enquanto a maioria dos mercados depende de transações com cartões, muitos também têm pagamentos alternativos exclusivos aos sistemas locais. Por exemplo, muitos mercados ainda permitem pedidos com pagamento na entrega, que exigem regras específicas de monitoramento de fraudes. Essas regras podem ser baseadas em históricos de transações ou de valor vinculadas a uma entidade ou endereço, por exemplo.

Criar regras de monitoramento de fraudes com precisão desde o começo de uma implantação, com base em dados avançados, significa que esse varejista pode cumprir seu objetivo de nunca entrar em um mercado com restrições desnecessariamente altas. Do ponto de vista de políticas de prevenção, a empresa tende a entrar em um novo mercado para estabelecer novos relacionamentos, com o menor atrito possível.

Além da expansão do mercado, o varejista também conseguiu criar regras específicas para as tendências de fraude relacionadas a cada uma de suas marcas. As várias marcas são associadas a diferentes comportamentos de fraude, que podem ser específicos aos tipos de itens que essas marcas vendem ou à base de consumidores que essas marcas atendem.

Relatórios e business intelligence

Essa colaboração entre o varejista e a CyberSource é apoiada por uma série de relatórios que apresentam o desempenho da solução. Visões variadas podem representar o desempenho específico de uma regra, perdas gerais, taxas de estorno e alterações nas taxas de conversão. Além disso, a

equipe de controle de qualidade interna do comércio pode gerar relatórios específicos do sistema CyberSource mostrando o desempenho por região, agente e tempo. O monitoramento constante permite às organizações acompanhar de perto os modelos e regras, à medida que expandem e as tendências de fraude evoluem.

Em última instância, a avaliação do sucesso de uma implantação do Decision Manager para esse comércio depende de vários fatores ricos e interconectados. Como a maioria dos comércios, o verdadeiro sinal de sucesso é a satisfação do cliente e as taxas de conversão, minimizando as perdas e estornos. Além disso, a organização está constantemente medindo a sua eficiência operacional, especificamente através do tempo gasto entre seus verificadores internos com base na precisão dos resultados da CyberSource. Finalmente, um verdadeiro termômetro de sucesso é a capacidade de continuar a expandir e inovar livremente, sem a barreira das fraudes.

ORIENTAÇÃO ESSENCIAL

À medida que o comércio eletrônico evolui para ser um dos principais impulsionadores da economia global, quase todas as empresas adotam uma função de comércio digital – e todas elas precisarão de uma estratégia de fraude mais inteligente do que os fraudadores que as atacam. Os *players* do comércio digital têm muito a levar em conta na criação de estratégias de fraude para o futuro, equilibrando a necessidade de proteger os negócios contra ataques de fraude existentes e emergentes, enquanto encantam os clientes, apoiam as principais estratégias de crescimento dos negócios e possibilitam a inovação. Para ajudar a alcançar esses objetivos, as seguintes orientações devem ser consideradas:

- **Escolha uma solução antifraude robusta e ágil.** Adote uma solução antifraude projetada para enfrentar de forma eficaz os sofisticados desafios atuais de fraude, incluindo fraudes de aquisição de contas, de novas contas, de programas de lealdade e recompensas e fraude amigável. Garanta que sua solução antifraude inclua regras adaptáveis, análises avançadas, machine learning que aproveite a revalidação contínua e monitoramento de desempenho para garantir que os objetivos empresariais sejam cumpridos de forma consistente. Escolha uma solução robusta o suficiente para apoiar a inovação e crescer com seus negócios.
- **Crie estratégias antifraude tendo a inovação como objetivo central.** Uma estratégia antifraude deve permitir a inovação rápida. Boas soluções contra fraudes devem estar no centro da transformação digital – e certamente não dever ser uma barreira. Trabalhe com uma solução antifraude que permita modelos analíticos, que possam ser adaptados para cobrir a expansão contínua de dispositivos, canais, tipos de pagamento e regiões geográficas. Ao adotar essa abordagem, é fundamental envolver as equipes de inovação no planejamento geral da estratégia antifraude.
- **Escolha um estilo de implementação e estratégia.** Adote uma estratégia antifraude que corresponda às necessidades da sua empresa. Isso pode significar um modelo local, gerenciado externamente ou híbrido. Essa escolha pode depender do tamanho da organização e da vontade (incluindo orçamento) de formar uma equipe completa de operações antifraude com cobertura 24 horas. Nos casos de implementação híbrida, é importante escolher um provedor de soluções que atue como um verdadeiro parceiro com a equipe antifraude comercial, atuando como extensões um do outro.
- **Estabeleça metas operacionais.** A escolha de uma estratégia antifraude permite a otimização dos recursos operacionais, reduzindo o tempo perdido na investigação de falsos positivos

e/ou reduzindo o número de horas necessárias para manter os objetivos da iniciativa. Este deve ser um objetivo principal da estratégia antifraude.

- **Identifique KPIs de negócios e prevenção de fraude no mesmo contexto.** A adaptação de uma solução deve servir, tanto para aprimorar a inovação e a experiência do cliente, quanto para reduzir perdas. Como os objetivos de negócios e segurança são interconectados, os KPIs devem ser definidos tendo em mente esta relação.
- **Pense rápido.** O mercado de comércio eletrônico está evoluindo rapidamente e a fraude também. As estratégias antifraude devem permitir que os usuários participem da criação das regras, adaptação de modelos e testes no nível de produção com agilidade suficiente para lidar com essas mudanças rápidas.

Fontes e metodologias

Este white paper da IDC Financial Insights é baseado em várias fontes e metodologias utilizadas rotineiramente pelos analistas da IDC, incluindo:

- Entrevistas individuais com executivos do setor
- Colaboração com analistas da IDC cobrindo outras áreas de setor e tecnologia
- Conhecimento abrangente de produtos e serviços de fornecedores
- Melhores práticas e dados comportamentais acumulados através de pesquisas da IDC
- Experiência individual e cargos de analistas da IDC com anos no setor

A IDC usa abordagens padronizadas para o desenvolvimento de conteúdo para garantir a aderência à política de pesquisa da IDC e consistência com os conselhos dados a seus clientes.

Sobre a IDC

A International Data Corporation (IDC) é a principal fornecedora global de inteligência de mercado, serviços de consultoria e eventos para os mercados de tecnologia da informação, telecomunicações e tecnologia de consumidores. A IDC ajuda profissionais de TI, executivos de negócios e a comunidade de investimentos a tomar decisões baseadas em fatos sobre compras de tecnologia e estratégias de negócios. Mais de 1.100 analistas da IDC fornecem conhecimentos globais, regionais e locais sobre oportunidades e tendências na tecnologia e em vários setores da economia, em mais de 110 países em todo o mundo. Há 50 anos, a IDC fornece informações estratégicas para ajudar nossos clientes a atingir seus principais objetivos de negócios. A IDC é uma subsidiária da IDG, empresa líder mundial em mídia, pesquisa e eventos de tecnologia.

Sede Global

5 Speen Street
Framingham, MA 01701
EUA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com