ESTUDO DE CASO PARA PAYMENT ANALYST

CANDIDATO: Diorge Polli de Lima

Fluxo de Pagamento e Papel dos Principais Participantes:

O fluxo de pagamento é o processo pelo qual uma transação financeira é realizada entre o portador (consumidor) e o lojista (estabelecimento comercial). Esse fluxo envolve vários participantes que desempenham papéis distintos para garantir a efetivação e a segurança da transação. Vamos entender o papel de cada um desses principais participantes:

1. Portador: O portador é o cliente que realiza a compra usando um cartão de crédito ou débito. Ele é quem paga o valor total da venda, incluindo as taxas de intermediação que são descontadas ao longo do processo, caso o lojista decida não absorver esse custo.

2. Lojista: O lojista é o estabelecimento comercial que realiza a venda utilizando algum esquema de pagamentos eletrônicos. Ele pode ser uma loja física ou um prestador de serviços. Sinônimos para esse termo seriam empreendedor, empresário ou dono do negócio.

3. Credenciadora (Adquirente): A credenciadora é responsável por credenciar a loja para aceitar pagamentos eletrônicos. Ela faz a captura, processamento e liquidação da venda, conectando todas as partes envolvidas no pagamento. Empresas como Cielo, Rede, Stone, PagSeguro, entre outras, atuam como credenciadoras.

4. Facilitadores: Os facilitadores, também conhecidos como intermediadores ou sub-adquirentes, são empresas que oferecem uma solução completa para a realização de pagamentos. Eles gerenciam o relacionamento entre o comprador e o vendedor e protegem dados pessoais, como informações de cartões de crédito. Além disso, unificam as taxas desses serviços. Exemplos de facilitadores incluem PayPal e Adyen

5. Bandeira: As bandeiras, como Mastercard, Visa, Elo, entre outras, são responsáveis por organizar todo o arranjo de pagamentos. Elas regulamentam e verificam se as regras estão sendo cumpridas. Além disso, verificam as informações do cartão inserido para pagamento, identificando o portador e encaminhando a venda para ser autorizada pelo emissor correto.

6. Banco Emissor: O banco emissor é responsável por emitir o cartão utilizado na venda. Ele concede crédito ao portador (no caso de uma venda a crédito) e verifica a existência de saldo suficiente para autorizar a transação (no caso de venda a débito). Além disso, o banco emissor é responsável por garantir a segurança do portador durante a transação, verificando possíveis comportamentos incomuns.

Diferença entre Adquirente, Sub-adquirente e Gateway:

1. Adquirente (Credenciadora): O adquirente ou credenciadora é uma empresa licenciada que analisa e aceita estabelecimentos em seu programa de cartões e processos de transações financeiras. Elas são responsáveis pela comunicação da transação entre a loja e a bandeira (Visa, Mastercard, Amex) e credenciam estabelecimentos para o aceite dos cartões. O adquirente atua na conexão direta entre a loja e a bandeira durante a transação.

2. Sub-adquirente (Facilitador ou Intermediador): Os sub-adquirentes são facilitadores que oferecem uma solução completa para a realização de pagamentos. Eles atuam como intermediadores entre a loja

do vendedor e a instituição financeira responsável pelo pagamento, transmitindo os dados e oferecendo opções de pagamento. Os sub-adquirentes gerenciam o relacionamento entre compradores e vendedores, protegem dados pessoais e oferecem uma experiência de pagamento unificada.

3. Gateway de Pagamento: Os gateways de pagamento facilitam a transação entre a loja do vendedor e a instituição financeira responsável pelo pagamento, transmitindo os dados e oferecendo uma opção interessante de meio de pagamento. Eles podem oferecer recursos como carrinho de compras, transmissão segura de informações (como certificação de segurança, gestão de risco, PCI) e diversidade de opções de pagamento. Os gateways não fazem a intermediação direta com as bandeiras, mas oferecem serviços de processamento e segurança nas transações.

Chargebacks, Diferença em Relação a Cancelamentos e sua Conexão com Fraude:

O chargeback, também conhecido como contestação de compra, é um processo estabelecido e regulado pelas bandeiras de cartão, como Visa, Mastercard, etc. Ele foi criado para garantir mais segurança para vendedores e compradores que utilizam o cartão como meio de pagamento.

O chargeback ocorre quando o portador do cartão contesta uma transação, alegando diversos motivos, como fraude, erro na cobrança, não reconhecimento da compra ou problemas com o produto/serviço adquirido. Nesse caso, o valor da transação é devolvido ao portador, e o lojista pode ser responsabilizado pelo prejuízo.

É importante destacar que o chargeback difere de um cancelamento. Enquanto o chargeback é solicitado pelo cliente junto ao emissor do cartão, o cancelamento parte do próprio lojista que realizou a venda. O cancelamento pode ocorrer por vários motivos, como o produto entregue com defeito, o comprador decidir devolver o item ou até mesmo erros de parcelamento e valor ao passar o cartão.

O chargeback tem uma forte conexão com fraudes no mundo da adquirência, sendo que em 91% dos casos de contestações em e-commerce, a causa é a fraude. As fraudes geralmente acontecem a partir de compras aparentemente legítimas, mas realizadas com cartões de crédito clonados ou roubados. Existem também as chamadas "fraudes amigáveis", em que o cliente legítimo solicita o chargeback após receber o produto ou serviço.

Para evitar a ocorrência de chargebacks e proteger os lojistas, é fundamental adotar práticas de segurança e medidas antifraude. A análise de risco, a verificação de informações e a adoção de tecnologias de prevenção de fraudes são essenciais para mitigar os riscos e garantir a segurança das transações. Além disso, manter uma comunicação aberta com o cliente, oferecer assistência e buscar soluções justas e satisfatórias para ambas as partes são ações importantes para prevenir e resolver disputas de chargeback.

Problema com o Cliente

Em relação ao nosso cliente o primeiro ponto a se destacar é ter empatia e mostrar que estamos ao seu lado, porque esse mecanismo de chargeback só funciona bem para proteger os consumidores, o prejuízo da prática fica totalmente a cargo do estabelecimento que vendeu o produto ou serviço. Por isso, as consequências da fraude são tão prejudiciais e agressivas para os varejistas. Nós como empresa

devemos deixar um canal de rápida resposta a ele para sanar as dúvidas e mostrar que estamos à disposição. Segundo orientar ao cliente de maneira mais efetiva entrando em contato com o emissor e solicitando quais seriam os documentos necessários para comprovar sua veracidade. Como por exemplo em uma compra online, todos os documentos da transportadora comprovando a entrega e a assinatura de recebimento. Logo após essas considerações e continuando com a tratativa negativa do lado do emissor, considere a arbitragem: Em alguns casos, se o emissor do cartão não aceitar sua defesa, você pode optar por arbitragem. A arbitragem é um processo em que um terceiro neutro revisa a disputa e toma uma decisão final. Verifique as políticas e procedimentos de arbitragem do emissor do cartão antes de prosseguir com essa opção. Pois o perdedor do processo pode receber uma multa alta, mas caso o prejuízo do cliente vá ser grande e ele tenha certeza de que está certo é uma saída. Geralmente quem arbitra nesses casos é a bandeira.

Por fim não tendo uma resolução positiva pode-se tentar ajuda-lo e conscientizar sobre a importância dos mecanismos para evitar fraudes, analise o caso de chargeback e identifique maneiras de evitar disputas semelhantes no futuro. Melhore seus processos internos, fornecendo um serviço de atendimento ao cliente sólido e garantindo que todas as transações sejam documentadas adequadamente.

Lembre-se de que cada caso de chargeback é único, e nem sempre é possível reverter a decisão do emissor do cartão. No entanto, ao tomar as medidas adequadas e fornecer evidências sólidas, você aumenta suas chances de resolver com sucesso disputas de chargeback em que o estabelecimento tem a razão.

Exemplo de resposta:

Agradecemos por entrar em contato conosco em relação ao chargeback. Entendemos completamente a sua preocupação e queremos que saiba que estamos ao seu lado durante todo o processo.

É verdade que o mecanismo de chargeback foi projetado para proteger os consumidores, mas também entendemos as consequências negativas que isso pode trazer para os varejistas. Nossa equipe está empenhada em ajudá-lo a resolver essa questão de forma justa e satisfatória.

Já verificamos nossos registros e identificamos que enviamos todos os documentos de defesa ao emissor do cartão. Lamentamos que nossa defesa não tenha sido suficiente para convencê-los até o momento.

Para ajudar nesse processo, sugerimos que você entre em contato diretamente com o emissor do cartão e solicite quais documentos adicionais seriam necessários para comprovar a veracidade da entrega. Por exemplo, se a compra foi feita online, podemos fornecer todos os documentos da transportadora que comprovem a entrega, incluindo a assinatura de recebimento.

Caso o emissor do cartão não reconsidere sua posição, podemos avaliar a possibilidade de arbitragem como uma alternativa. A arbitragem é um processo justo e neutro, no qual um terceiro imparcial revisa a disputa e toma uma decisão final. Certifique-se de verificar as políticas e procedimentos de arbitragem do emissor do cartão antes de prosseguir com essa opção.

Queremos garantir que você se sinta apoiado e compreendido durante todo esse processo. Nossa equipe está aqui para ajudar e conscientizar sobre a importância de tomar medidas para evitar fraudes no futuro. Analisaremos cuidadosamente esse caso de chargeback e implementaremos melhorias internas para garantir que transações futuras sejam documentadas adequadamente e com o máximo de segurança.

Entendemos que cada caso de chargeback é único, e nem sempre é possível reverter a decisão do emissor do cartão. No entanto, saiba que faremos o possível para resolver essa disputa de forma justa e satisfatória. Continuaremos a manter a comunicação aberta com você e a fornecer assistência em cada etapa do processo.

Se houver mais informações que você gostaria de compartilhar conosco ou qualquer outra dúvida, por favor, não hesite em nos contatar. Estamos comprometidos em trabalhar ao seu lado e encontrar a melhor solução para esse problema.

Agradecemos a sua confiança em nossa empresa e estamos ansiosos para resolver essa questão juntos.

DATA ANALYSIS

Os dados apresentam as seguintes colunas transaction_id, merchant_id, user_id, card_number, transaction_date, transaction_amount, device_id e has_cbk. São 3199 transações, foram encontrados valores nulos apenas de device_id mas o resultado já era esperado.

Em uma análise superficial podemos ver o device_id em branco em 830 operações, o que pode indicar uma transação online, ponto de atenção.

O campo has_cbk tem alguns valores TRUE que indicam um pedido chargeback anterior a essa transação, que pode indicar uma fraude que tenha acontecido previamente, ponto de atenção.

Informações Adicionais que Poderiam Ajudar na Análise

Dados do Usuário:

- Histórico de Compras: Observar o histórico de compras do usuário pode revelar padrões de comportamento e hábitos de consumo. Transações incomuns em relação ao histórico podem sinalizar potencial fraude.
- Localização (IP): Verificar o local de origem da transação através do endereço IP pode ajudar a identificar transações suspeitas feitas a partir de locais inesperados ou de regiões associadas a atividades fraudulentas.
- Meio de Compra: Diferenciar entre compras feitas em dispositivos conhecidos do usuário (como celular ou notebook) e transações em dispositivos desconhecidos pode indicar possíveis tentativas de fraude.
- Horário das Transações: Observar o horário das transações pode ser útil para identificar compras fora dos padrões habituais do usuário, como compras realizadas em horários incomuns ou de madrugada.
- Padrão de Valor Gasto: Analisar o padrão de gastos do usuário, como um valor médio de compras, pode ajudar a detectar transações atípicas que podem indicar atividades fraudulentas.

Dados do Vendedor:

- Ataque Hacker em Compras Online: Verificar o histórico do estabelecimento em relação a ataques hackers ou violações de segurança pode ajudar a identificar possíveis fraudes em compras online.
- Histórico de Chargebacks: Avaliar o histórico do estabelecimento em relação a chargebacks pode indicar um alto volume de contestações, o que pode ser um sinal de problemas com os serviços prestados ou de atividades fraudulentas.

- Valor médio de vendas: Esse dado representa o valor médio gasto pelos clientes no estabelecimento. Analisar compras que excedem significativamente o valor médio pode ser um indicativo de fraude.
- Horário de Funcionamento: Observar se a transação ocorreu fora do horário de funcionamento normal do estabelecimento pode ser um alerta de possível fraude.

O que Fazer para Prevenir Fraudes

Análise em tempo de real de padrão de compra: valor, localização, produto, dispositivo.

- Horário de compra: estabelecer um limite de valor para transações durante certos períodos de tempo como 22 as 06. Uma autenticação de 2 fatores para liberar tais transações como sms, e-mail, dispositivos de segurança.
- Chargeback alert: Utilizar um bloqueio para transações que tenham flag de chargeback e outro fator de risco como valor, horário.
- Tentativas seguidas de transações: impedir transações seguidas em curto espaço de tempo (levar em consideração valor e horário).
- Documentação: Incentivar estabelecimentos a documentar e notificar as transações quando possíveis, no Brasil não se tem o hábito de impressão de notas fiscais mas essa é uma forma de proteger o vendedor de possíveis fraudes e documentando as transações com documentos do comprador.

Como Identificar Padrões de Fraude com SQL

Para monitorar padrões identificados em tempo real usando SQL, pode-se criar consultas SQL e implementar gatilhos que analisam continuamente os dados de transações recebidos e acionam ações com base em padrões específicos. No entanto, é importante observar que, embora o SQL possa ser usado para algumas tarefas de monitoramento em tempo real, pode não ser a solução mais eficiente ou escalável para análises complexas em tempo real.

Monitorar Valores de Transação e Horário de Compra:

Use consultas SQL para rastrear transações durante períodos específicos (por exemplo, das 22:00 às 06:00) e garantir que elas não excedam determinados limites pré-definidos.

Se o valor da transação ou horário violar os limites estabelecidos, você pode acionar alertas ou etapas adicionais de autenticação, como autenticação de 2 fatores.

Alerta de Chargeback: Configure um gatilho SQL que monitore a coluna 'has_cbk' na tabela de transações para detectar qualquer contestação de chargeback.

Se um flag de chargeback for encontrado, você pode tomar ações apropriadas, como bloquear a conta do usuário ou comerciante associado e notificar as partes interessadas relevantes.

Prevenir Transações Consecutivas: Implemente consultas SQL que analisem para identificar transações consecutivas em um curto espaço de tempo, 30min.