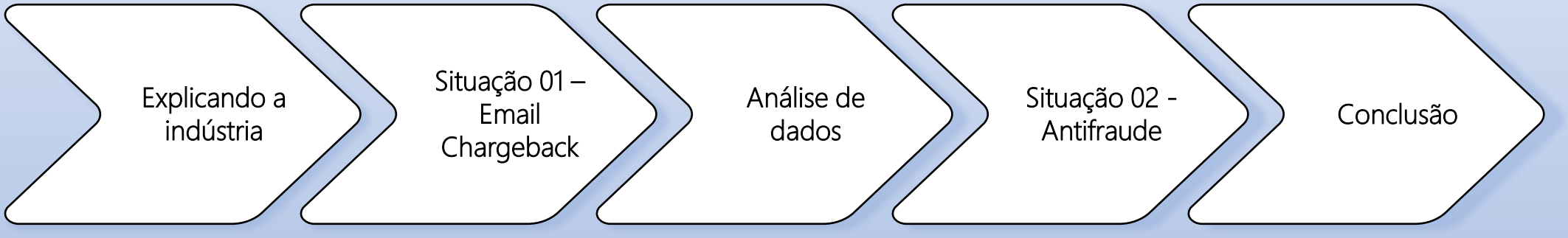
Payment Analyst - Case

André Gimeniz Galvão

andreggalvao/CloudWalk-test (github.com)

cloudwalk

Cronograma


Explicando a indústria
Situação 01 – Email Chargeback
Análise de dados
Situação 02 - Antifraude
Conclusão

Explicando a indústria
Entidades

Adquirentes
Seu papel é analisar, processar e liquidar as transações financeiras por meio de cartão de crédito e débito. Ou seja, eles fazem a comunicação com a bandeira ou com os bancos emissores.

Subadquirentes
Fazem a conexão entre os clientes, os lojistas e as adquirentes. É responsável por transmitir os dados da transação ao adquirente e liquidar os recebíveis junto aos varejistas.

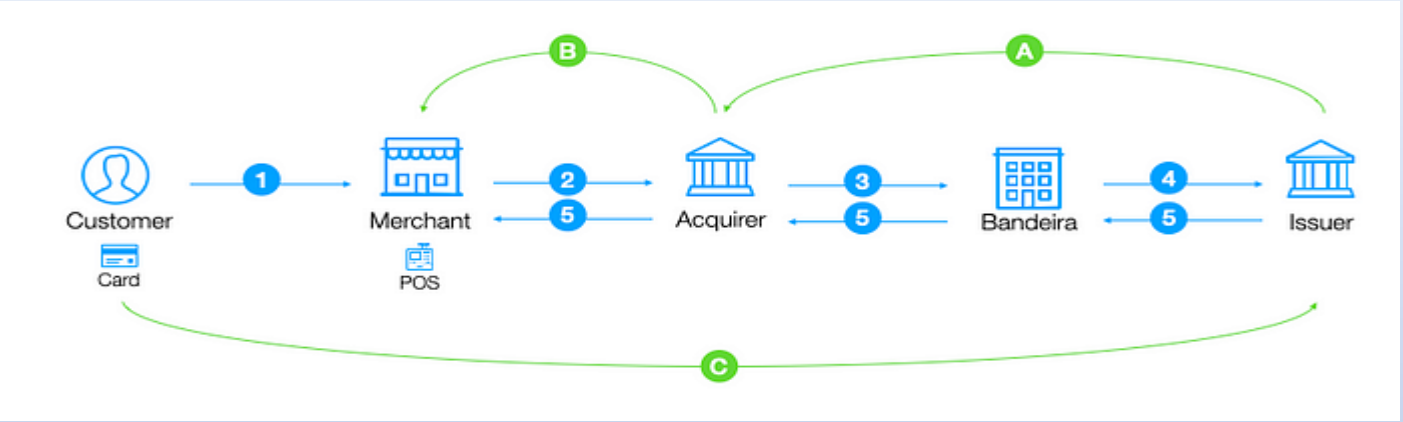
Gateway de pagamento
É uma interface que transporta informações entre adquirentes, lojistas e bancos emissores. Seu papel é processar os dados no momento em que a compra é finalizada.

Antifraude
O antifraude é a tecnologia responsável por analisar o nível de risco da compra via internet

Bandeiras de cartão
Elas exercem um papel regulatório no setor, estabelecendo regras para as transações em si, como número de parcelamentos, e também no quesito de segurança.

Instituição emissora do cartão
Responsável pela emissão do cartão e conceder o crédito ao portador. Em uma transação, ao receber os dados de uma compra, é a instituição emissora que faz a autorização

Explicando a indústria
Fluxos



Fluxo de informação:

1- O cliente paga usando uma POS

2- O POS captura e envia as informações para a adquirente

3- A Adquirente envia para a Bandeira e solicita autorização

4- A bandeira envia as transações para o banco emissor do cartão para obter a autorização.

5- O banco emissor envia a autorização de volta a bandeira e a adquirente, autorizando a compra no POS.

Fluxo da liquidação:

- Dentro do prazo estabelecido pela forma da venda
- o banco emissor transfere o valor para a bandeira do cartão, já descontando a sua taxa de participação no processo.
- O emissor por sua vez, retira sua parcela e repassa ao adquirente
- Por fim o adquirente cobra a sua taxa e paga o comerciante

Explicando a indústria
Chargebacks e cancelamentos

1 Um chargeback é quando um cliente solicita o cancelamento de uma transação de cartão de crédito sem entrar em contato com o comerciante. A administradora do cartão então devolve o dinheiro ao cliente e cobra o comerciante pelo valor da transação.

2 Um cancelamento é um processo iniciado pelo comerciante para devolver um valor ao titular do cartão. Isso pode acontecer se o titular do cartão devolver um produto, se o comerciante emitir um reembolso ou se o comerciante cometer um erro.

3 A maioria dos chargebacks são resultados de fraudes, como quando um fraudador usa o cartão de crédito de outra pessoa para fazer uma compra.

4 Chargeback é prejuízo em dobro, pois geralmente o comerciante fica sem a mercadoria e o dinheiro.

Situação 01 – Email Chargeback

Informações iniciais:

Cliente (lojista) está insatisfeito, pois a documentação enviado ao emissor foi considerada insuficiente para a defesa do caso. O dono do cartão informa que não recebeu o produto e a documentação não prova o oposto. A razão do chargeback está como "Produto/Serviço não provido".

Fato ocorrido:

Em seguida o cliente, informa que o produto foi entregue ao cliente.

Ações a serem tomadas:

1. Entrar em contato com o emissor novamente, destacando que o cliente afirma ter entregado o produto conforme os registros e informações disponíveis.
2. Reavaliar a documentação que foi enviada anteriormente para identificar se há alguma lacuna ou informação adicional que possa ser fornecida para reforçar a defesa.
3. Entrar em contato diretamente com o titular do cartão e tentar resolver a situação de forma amigável para o titular do cartão a reconsiderar a disputa de estorno.
4. Entrar em contato com o cliente, demonstrar o compromisso em resolver o problema com mediação ou arbitragem, para buscar uma solução justa.

As ações tomadas deve estar de acordo com os procedimentos e padrões da CloudWalk.

Análise de dados
Entidades

Dataset fornecido:

- Dataset com 3199 transações e 8 features;
- Transações entre 01/11/2019 a 01/12/2019;
- Sem valores duplicados;
- Device_id com 830 valores faltando;
- 12,2% das transações possuem chargeback.

Hipóteses a serem seguidas:

- Compras suspeitas estão relacionadas a valores;
- Compras suspeitas em relação ao período;
- As compras suspeitas estão relacionadas à frequência do Usuário/Cartão/Estabelecimento.

Sobre as colunas do nosso conjunto de dados:

transaction_id: Número de identificação da transação;

comerciante_id: Número de identificação do comerciante

user_id: Número de identificação do usuário;

card_number: Número do cartão de crédito que efetuou a compra (parcial);

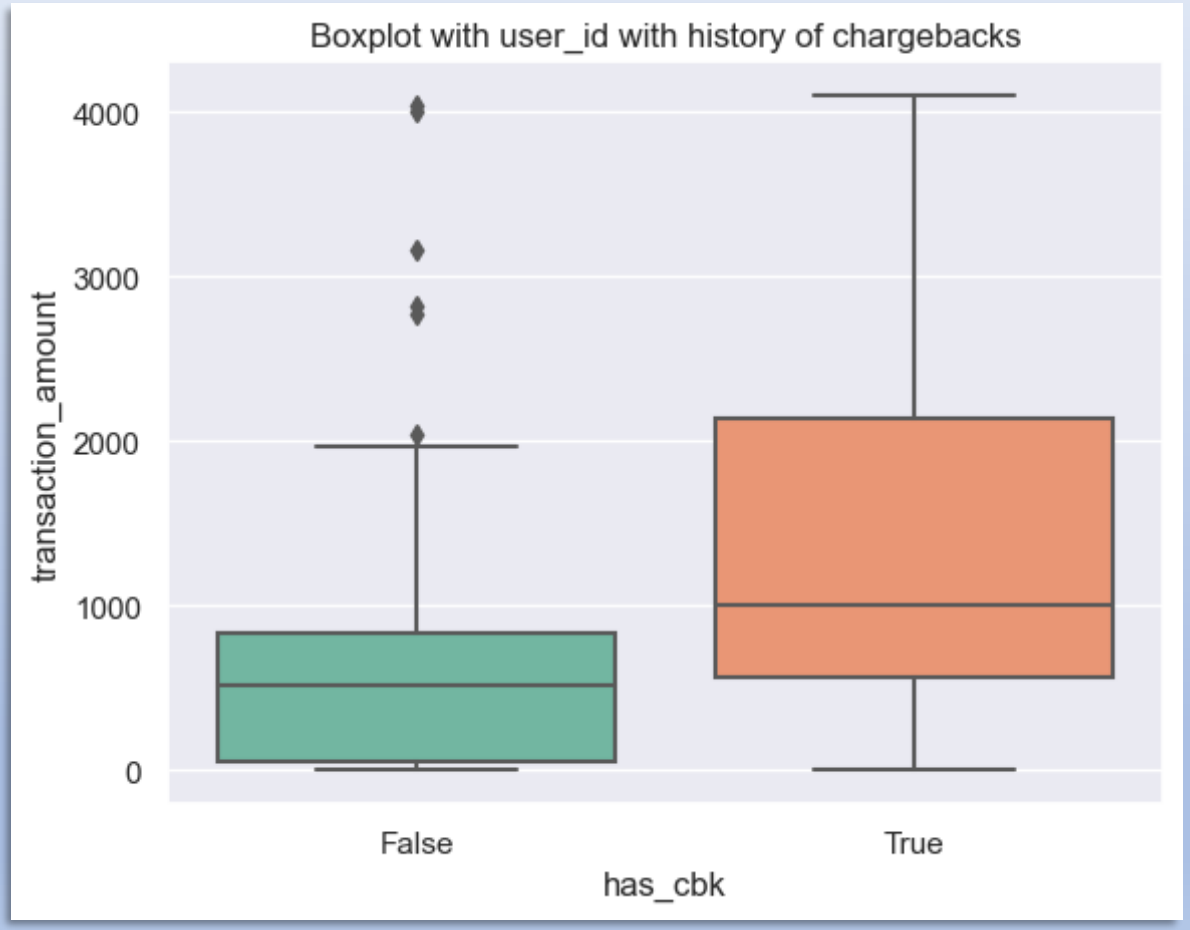
transaction_date: Data da transação;

transaction_amount: Valor da transação;

device_id: Número de identificação do dispositivo no qual a transação foi realizada;

has_cbk: Sinalizador se o chargeback ocorreu ou não.

Análise de dados
Chargeback & Valores



Quando isolado os **user_id** que possuem um histórico de **has_cbk** True, o padrão do boxplot é o mesmo levando em consideração todas as transações.

A análise dos valores e das distribuições das transações **não revelou nenhuma anormalidade**.

No entanto, mais da metade das transações com chargeback **estão acima do terceiro quartil dos valores das transações normais (25%)**.

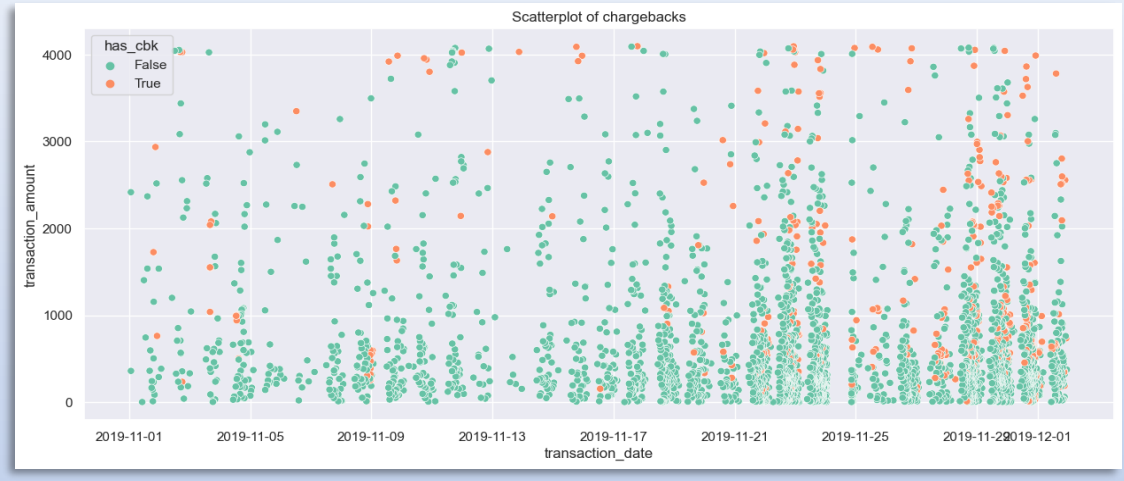
Isso sugere que **as transações com chargeback são mais propensas a serem grandes do que as transações normais.**

Análise de dados
Chargeback & Período

Ao analisar o dataframe no **período de 24/11/2019 a 01/12/2019**, constatamos que a quantidade de transações durante esses 8 dias representa aproximadamente **42,2% do total**. Além disso, nesse mesmo período, **ocorreu cerca de 58,8% de todas as transações com chargeback.**

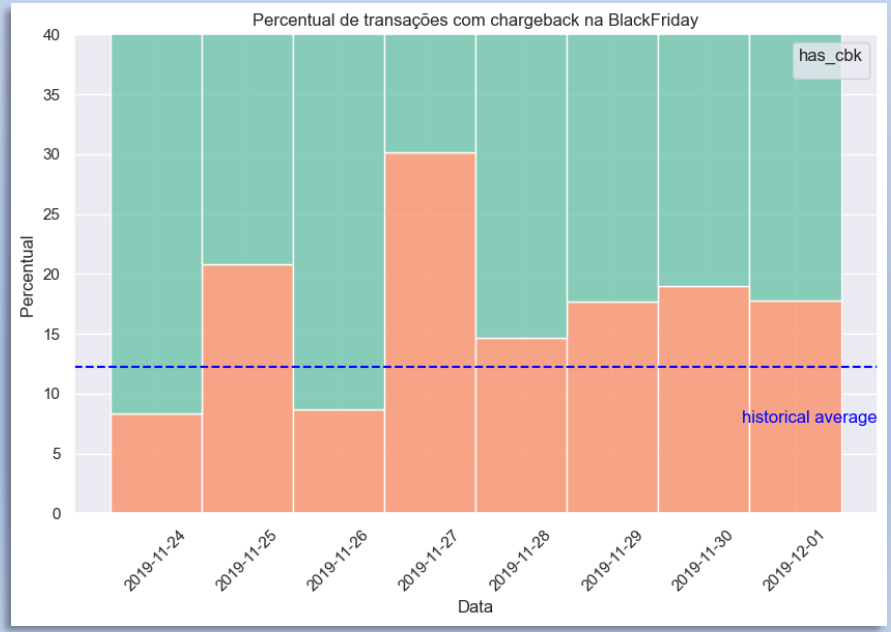
A incidência acima da média de estornos durante a Black Friday indica uma **maior vulnerabilidade do sistema de pagamento** nesse período. Isso requer uma atenção especial para garantir a segurança das transações e evitar prejuízos.

Essa análise ressalta a importância de **avaliar o desempenho do sistema de pagamento durante períodos de alta demanda**, como a Black Friday e implementar estratégias para reduzir os chargebacks para garantir uma experiência de compra segura e satisfatória para os consumidores.

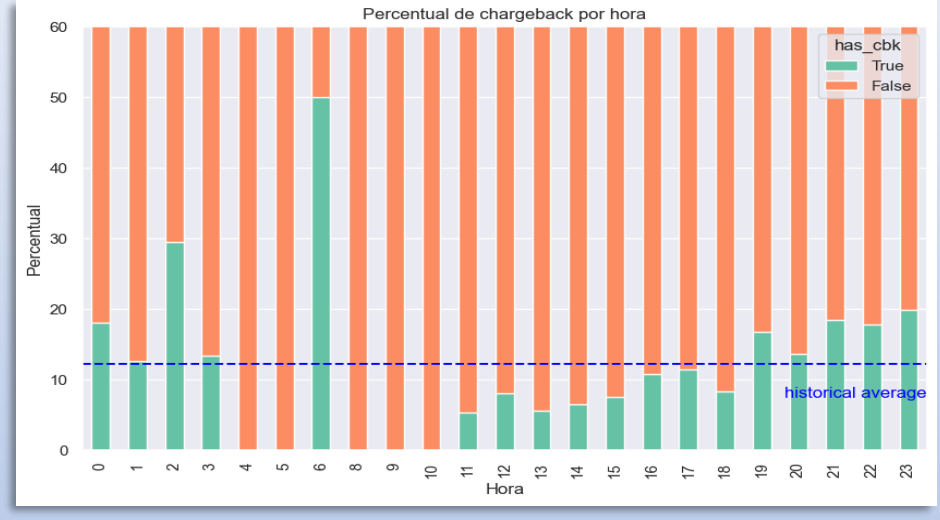


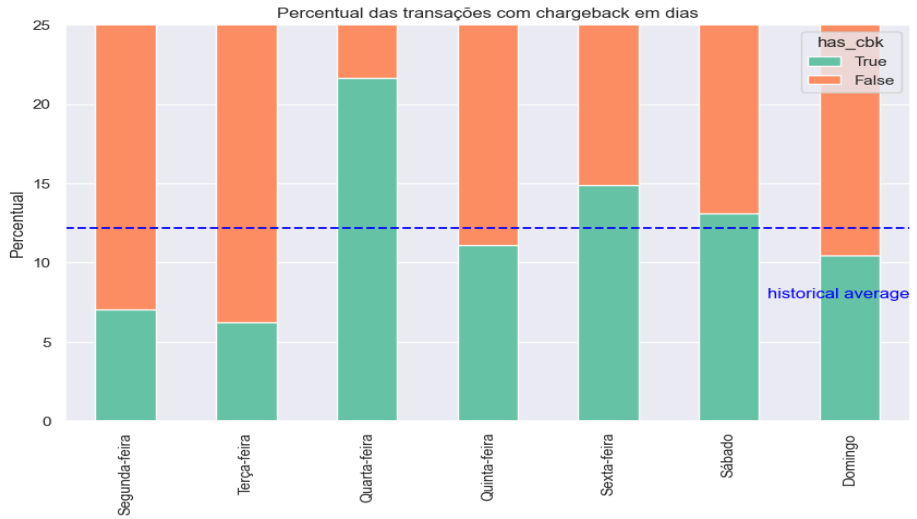
Legenda

Legenda



Análise de dados
Chargeback & Período





A análise por hora revela que a maioria dos chargebacks ocorre entre as 19h e as 3h, com um pico adicional às 6h, e por dia ocorre entre quarta-feira e sábado.

Essa informação é crucial para uma melhor alocação de recursos e planejamento do time, pois indica turnos em que há uma maior incidência de chargebacks.

Com base nessa análise, a empresa pode direcionar esforços adicionais e recursos para esses dias específicos, a fim de monitorar e mitigar os riscos de chargebacks de forma mais eficaz.

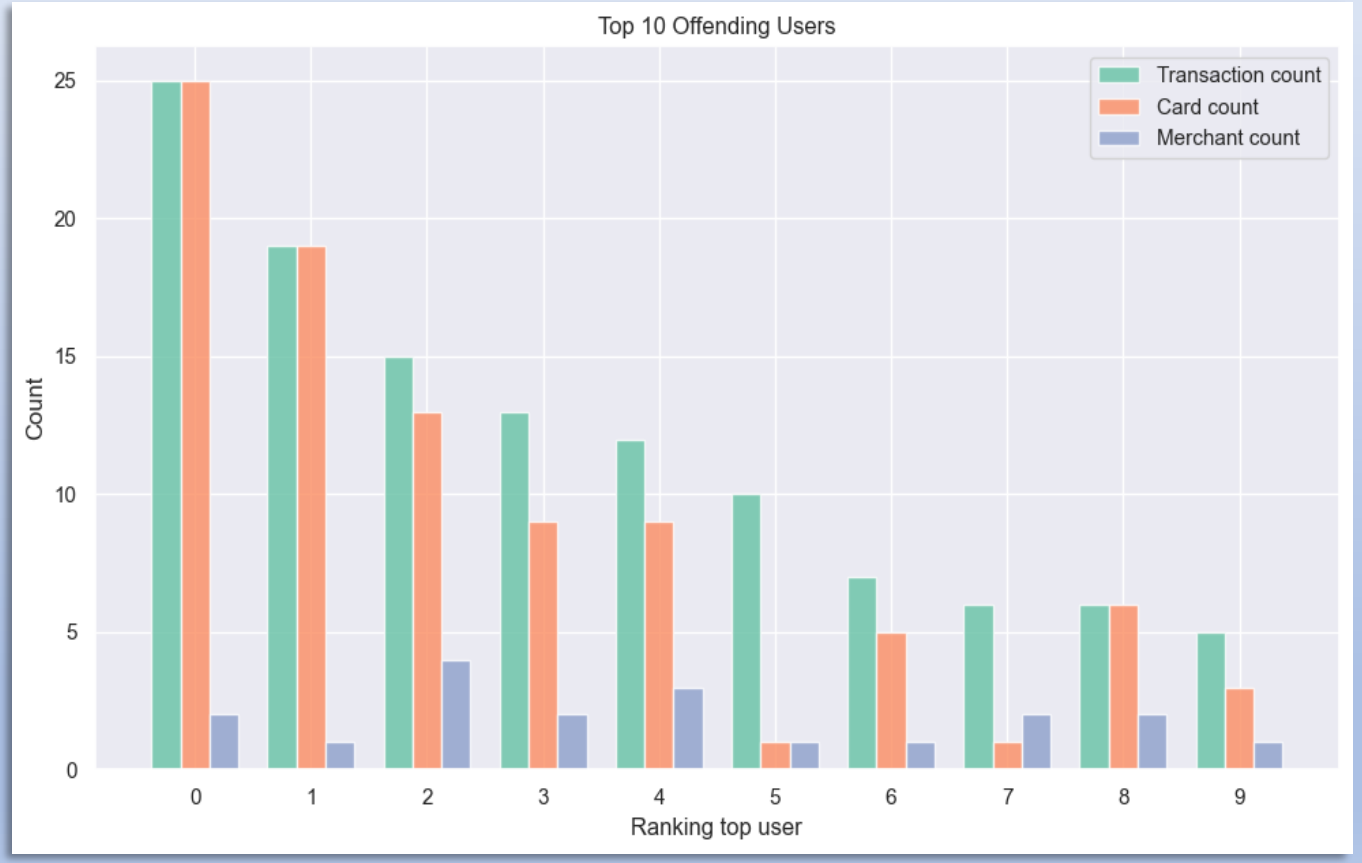
Isso pode envolver o aumento da equipe de suporte ao cliente, reforço nas medidas de segurança e detecção de fraudes, além de melhorias nos processos de atendimento e resolução de disputas problemáticas.

Análise de dados

Chargeback & merchant, user and card_number

Esse padrão de múltiplos user_id associados aos mesmos merchant_id pode indicar a possibilidade de atividades suspeitas, como o uso de dispositivos compartilhados ou a utilização de identidades diferentes para realizar transações.

Essa análise permite identificar usuários mais ofensores e estabelecer padrões de comportamento a partir dos dados observados.



Análise de dados
Conclusões

- É necessário monitorar e analisar as transações que apresentam valores acima das médias históricas. Elas podem indicar um maior risco de estornos ou comportamentos fraudulentos;
- Observou-se que o intervalo das 19h às 3h é o período com maior probabilidade de ocorrência de estornos. Durante esse período, é importante adotar medidas adicionais de segurança e monitoramento para mitigar os riscos;
- A análise indica que transações realizadas entre quarta-feira e sábado, nos intervalos de intervalo das 19h às 3h e às 6hrs, têm maior probabilidade de resultar em estornos;
- Condutas suspeitas envolvendo múltiplas transações e diferentes cartões: usuários que realizam várias transações com diferentes cartões em determinados estabelecimentos comerciais;
- Durante o evento da Black Friday houve um aumento significativo na quantidade de estornos. Isso ressalta a importância de as empresas estarem preparadas para lidar com esse momento de alta demanda, reforçando os sistemas antifraude, aumentando a equipe de suporte e adotando estratégias proativas para minimizar os riscos de estornos;
- Com base nessas observações, é fundamental que as empresas adotem medidas proativas para identificar e mitigar os riscos de estornos, garantindo uma experiência positiva aos clientes e protegendo a integridade financeira do negócio. Isso inclui investir em sistemas de segurança robustos, análise de dados para detecção de padrões suspeitos, monitoramento em tempo real das transações e oferecimento de suporte eficiente aos clientes durante momentos de alta demanda.

Análise de dados
Mais informação para padrões de fraude

- Localização: pode considerar a localização geográfica da transação com base no endereço IP do dispositivo utilizado para a transação ou a localização física da transação presencial, como o endereço da loja ou estabelecimento comercial onde foi realizada a compra;
- Dados de autenticação: Verifique se a transação foi autenticada usando autenticação adicional, como senha, código de autenticação enviado por SMS ou autenticação de dois fatores;
- Análise de dispositivo: analise os padrões de uso do dispositivo, como o número de dispositivos usados por um usuário, alterações frequentes do dispositivo ou uso incomum do dispositivo pelo usuário;
- Verificação do cartão de crédito: além do número parcial do cartão de crédito, você pode verificar o tipo do cartão, a data de validade e se o cartão foi registrado como roubado ou perdido;
- Comportamento da transação: procure padrões no comportamento da transação, como padrões de compra incomuns, transações de alto valor, várias transações em um curto período de tempo ou transações fora dos hábitos normais de consumo do usuário.
- Dados históricos: analise dados históricos de transações para identificar quaisquer padrões ou tendências recorrentes associados a transações fraudulentas, como dias específicos da semana, períodos de tempo ou valores de transações.
- Tempo de casa: Se o cliente é antigo e possui histórico ou é novo.

Análise de dados
Prevenindo fraudes e chargebacks

- Monitore as transações de alto risco: concentre-se no monitoramento e na revisão das transações que se enquadram no período crítico identificado como tendo o maior número de estornos. Aloque recursos para monitorar e analisar de perto as transações durante esse período para identificar e resolver rapidamente qualquer atividade fraudulenta em potencial;
- Eduque os clientes: Forneça aos clientes informações claras sobre processos de transação, medidas de segurança e etapas que eles podem tomar para proteger suas contas. Eduque-os sobre a importância de manter suas credenciais de login seguras, monitorando regularmente seu histórico de transações e relatando qualquer atividade suspeita imediatamente;
- Métodos de autenticação aprimorados: implemente métodos de autenticação fortes, como autenticação multifator (MFA), para verificar as identidades dos usuários durante as transações. Isso pode incluir o uso de códigos de verificação por SMS, autenticação biométrica ou autenticação baseada em token;
- Preparando-se para feriados movimentados: como observado, a Black Friday traz um risco maior de estornos. Tome medidas proativas para se preparar para esse período, como aumentar os esforços de prevenção de fraudes, melhorar o suporte ao cliente e monitorar de perto as transações durante esse período de alta demanda.

Análise de dados
Monitorando padrões

Para monitorar padrões identificados:

Implementar uma combinação de métodos de monitoramento manuais e automatizados;

Monitoramento de transações em tempo real: utiliza sistemas de monitoramento em tempo real que analisam os dados da transação à medida que ocorrem.

Monitoramento de limites: defina limites ou regras específicas com base em padrões identificados ou comportamento suspeito

Detecção de anomalias: Empregar técnicas de detecção de anomalias para identificar transações que se desviam significativamente dos padrões ou padrões esperados

Análise do comportamento do cliente: analise o comportamento do cliente ao longo do tempo para estabelecer padrões básicos e identificar desvios do comportamento normal.

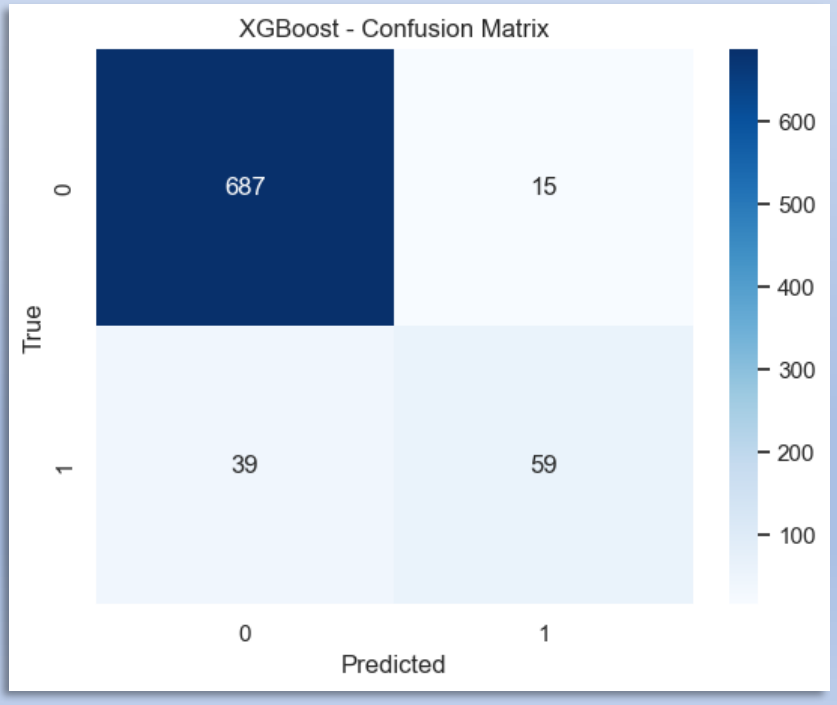
Revisão e investigação manuais: Aloque recursos para realizar revisão e investigação manuais com base em transações sinalizadas ou suspeitas.

Análise periódica de dados: realiza análises regulares de dados para identificar tendências e padrões de longo prazo nas atividades de atividade.

Situação 02 – Fraudes com cartão
Machine Learning e Requerimentos antifraudes

Métricas de interesse:

Taxa de detecção de fraudes: 94,62%
Taxa de falsos positivos: 20.27%
Taxa de falsos negativos: 5.31%



Os parâmetros escolhidos para o sistema foram arbitrários e foram implementados apenas para fim de desenvolvimento do projeto:

- Caso o usuário realize 3 transações em menos de 30minutos, a última transação será rejeitada;
- Caso a transação seja superior a R$ 10.000,00 será rejeitada;
- Caso o usuário possua histórico de chargeback, á transação será rejeitada;
- Caso o modelo de Machine Learning declare a transação suspeita ela será rejeitada.

Situação 02 – Fraudes com cartão
End point

Infraestrutura:

- Foi utilizado Uvicorn como servidor web local;
- FastAPI para a comunicação e processamento das transações;
- Através do método POST é feito o envio da transação ao servidor.

```
A "transaction_id":4321
A frequência de transação está dentro do previsto
Valor de transação dentro do estabelecido
Usuário não possui histórico de chargeback
A transação está rejeitada pelo nosso modelo de crédito
A transação deve ser rejeitada
INFO:     127.0.0.1:56103 - "POST /modelo HTTP/1.1" 200 OK
```

```
A "transaction_id":12344
Este cliente tem 3 ou mais transações não suspeitas
Valor de transação dentro do estabelecido
Usuário possui histórico de chargeback
A transação está rejeitada pelo nosso modelo de crédito
A transação deve ser rejeitada
INFO:     127.0.0.1:56088 - "POST /modelo HTTP/1.1" 200 OK
```

```
A "transaction_id":21320399
Comportamento suspeito: 3 ou mais transações seguidas em um período menor de 30 minutos
Valor de transação dentro do estabelecido
Usuário não possui histórico de chargeback
A transação está aprovada pelo nosso modelo de crédito
A transação deve ser rejeitada
INFO:     127.0.0.1:56074 - "POST /modelo HTTP/1.1" 200 OK
```

Exemplo de POST:

```
Invoke-WebRequest -Method POST -Headers @{"Content-Type"
= "application/json"} -Body '{
    "transaction_id": 2342357,
    "merchant_id": 29744,
    "user_id": 3333,
    "card_number": "434505******9116",
    "transaction_date": "2019-11-30T23:20:32.812632",
    "transaction_amount": 373,
    "device_id": 285475
}' -Uri http://127.0.0.1:8000/modelo
```

```
A "transaction_id":1235
A frequência de transação está dentro do previsto
Valor de transação dentro do estabelecido
Usuário não possui histórico de chargeback
A transação está aprovada pelo nosso modelo de crédito
A transação está aprovada
INFO:     127.0.0.1:56041 - "POST /modelo HTTP/1.1" 200 OK
```

```
A "transaction_id":1234
A frequência de transação está dentro do previsto
Valor de transação dentro do estabelecido
Usuário possui histórico de chargeback
A transação está aprovada pelo nosso modelo de crédito
A transação deve ser rejeitada
INFO:     127.0.0.1:56030 - "POST /modelo HTTP/1.1" 200 OK
```

Conclusão

A detecção de fraudes desempenha um papel fundamental na indústria de pagamentos, onde milhões de transações são processadas diariamente.

Com a crescente digitalização dos pagamentos e o aumento das transações online, as empresas de pagamento enfrentam um desafio constante de proteger seus sistemas e clientes contra atividades fraudulentas.

A implementação de sistemas eficientes de detecção de fraudes permite identificar padrões suspeitos, comportamentos anormais e transações fraudulentas em tempo real. Isso ajuda a mitigar os riscos financeiros, minimizar as perdas e preservar a confiança dos consumidores.

Além disso, a detecção de fraudes permite que a indústria de pagamentos atue proativamente na identificação e no bloqueio de atividades fraudulentas, garantindo a segurança das transações e a proteção dos dados sensíveis dos usuários.