mandiri sekuritas

Fraud Risk Detection

ANALISIS DATA PERBANKAN

PRESENTED BY:

APRILIA SANIATUL RAHMAWATI

Pendahuluan

Latar Belakang

Pertumbuhan transaksi digital semakin tinggi seiring berkembangnya teknologi. Resiko fraud ikut meningkat, terutama pada kasus:

- Pengguanaan kartu yang sudah bocor di **dark web,**
- Kartu **tanpa chip** yang lebih mudah dipalsukan, dan
- **Error transaksi** yang bisa menandakan upaya penipuan atau sistem bermasalah.

Tujuan

Analisis data transaksi perbankan ini diperlukan agar bank dapat lebih cepat mendeteksi pola mencurigakan yang mungkin mengindikasikan terjadinya penipuan.

mandiri sekuritas

Dataset

Data	Variabel
Cards	id, client_id, card_brand, card_type, card_number, expires, cvv, has_chip, num_cards_issued, credit_limit, acct_open_date, year_pin_last_changed, card_on_dark_web
Transactions	id, date, client_id, card_id, amount, use_chip, merchant_id, merchant_city, merchant_state, zip, mcc, errors
Users	id, current_age, retirement_age, birth_year, birth_month, gender, address, latitude, longitude, per_capita_income, yearly_income, total_debt, credit_score, num_credit_cards

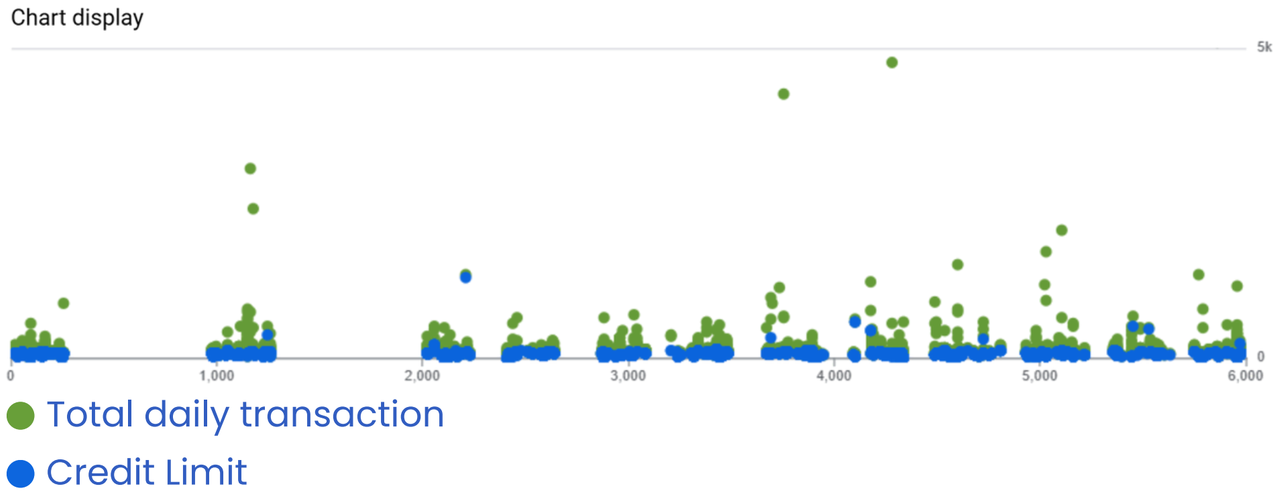
Daily Transaction Exceeding the Credit Limit

Analisis ini tujuannya untuk mendeteksi perilaku pengguna atau pola transaksi harian yang melebihi batas kredit yang sudah ditetapkan.

Query

```sql
# Detect daily transactions exceeding the credit limit
SELECT
  t.card_id,
  DATE(t.date) AS trx_date,
  SUM(t.amount) AS total_daily_trx,
  c.credit_limit,
  CASE
    WHEN SUM(t.amount) > c.credit_limit THEN 'DAILY LIMIT EXCEEDED'
    ELSE 'OK'
  END AS status
FROM `dataset.transactions_cleaned` AS t
JOIN `dataset.cards` AS c
  ON t.card_id = c.id
GROUP BY t.card_id, trx_date, c.credit_limit
HAVING SUM(t.amount) > c.credit_limit
ORDER BY total_daily_trx DESC;
```

Hasil



Hasil menunjukkan masih terdapat **cukup banyak transaksi** harian yang nilainya **melebihi credit limit**. Temuan ini perlu diawasi llebih lanjut untuk memahami pola transaksi nasabah, apakah wajar atau berpotensi mengarah ke risiko fraud.

Check the Most Frequent Error Users

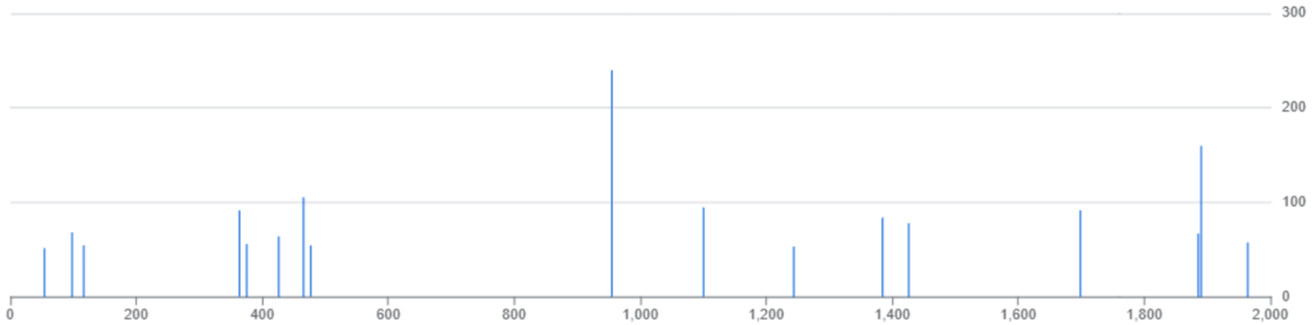
Analisis ini tujuannya untuk mencari client_id (pengguna) yang sering transaksi error, disini akan ditampilkan pengguna yang transaksi error lebih dari 50 kali.

Query

```
# Check for multiple errors during transactions more than 50x
SELECT
  client_id,
  COUNT(*) AS error_trx
FROM `dataset.transactions`
WHERE errors IS NOT NULL
GROUP BY client_id
HAVING COUNT(*) > 50
ORDER BY error_trx DESC;
```

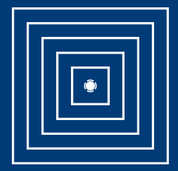
Hasil

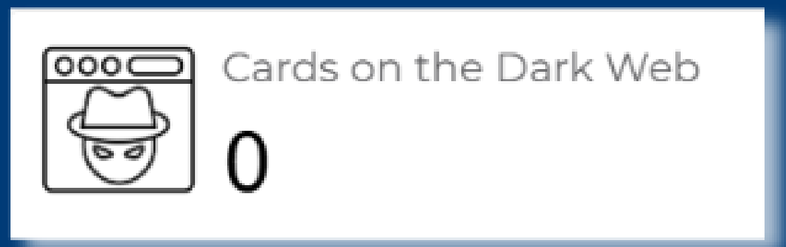
Chart display



Hasil menunjukkan terdapat 17 client yang mengalami error transaksi lebih dari 50 kali. Temuan ini penting untuk ditindaklanjuti, karena error berulang bisa menandakan pola penggunaan yang tidak normal, potensi fraud, atau masalah teknis yang perlu diperbaiki. Bahkan client dengan id 954 mengalami 240 kali transaksi error.

Cards on the Dark web





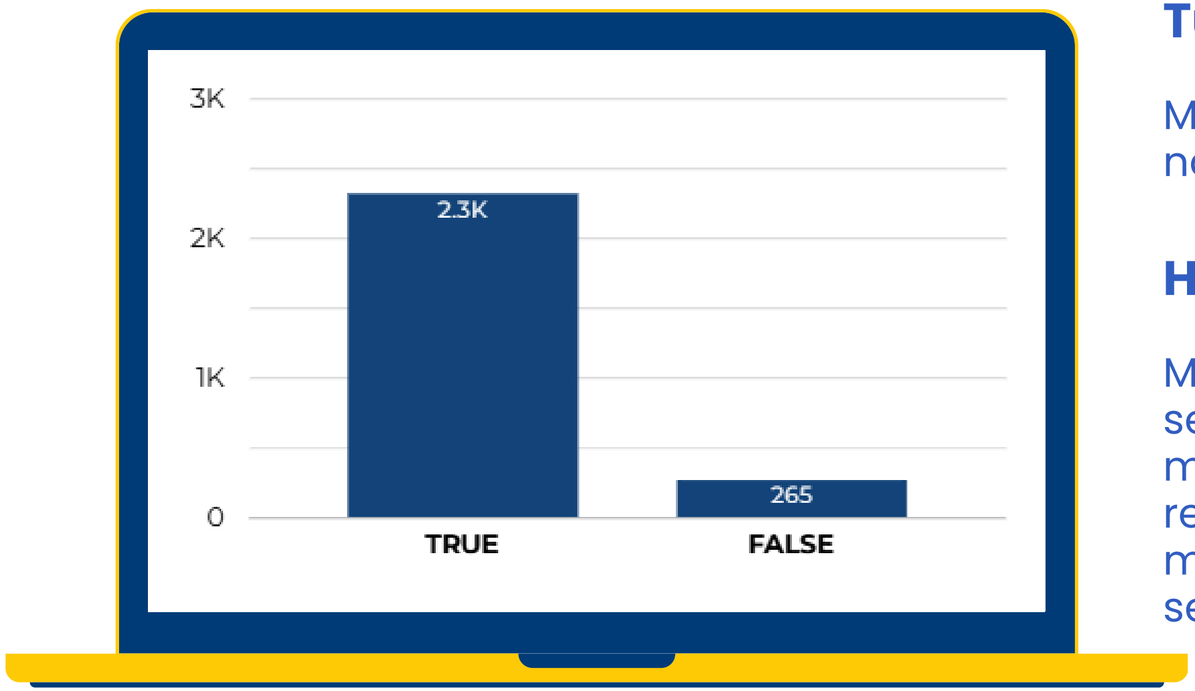
Tujuan:

Untuk menunjukkan status keamanan data nasabah dari potensi kebocoran atau pencurian data

Hasil:

Hasil monitoring tidak ditemukan data kartu yang muncul di Dark Web. Hal ini menunjukkan belum ada indikasi kebocoran data kartu nasabah pada periode analisis.

Cards by Chip Presence



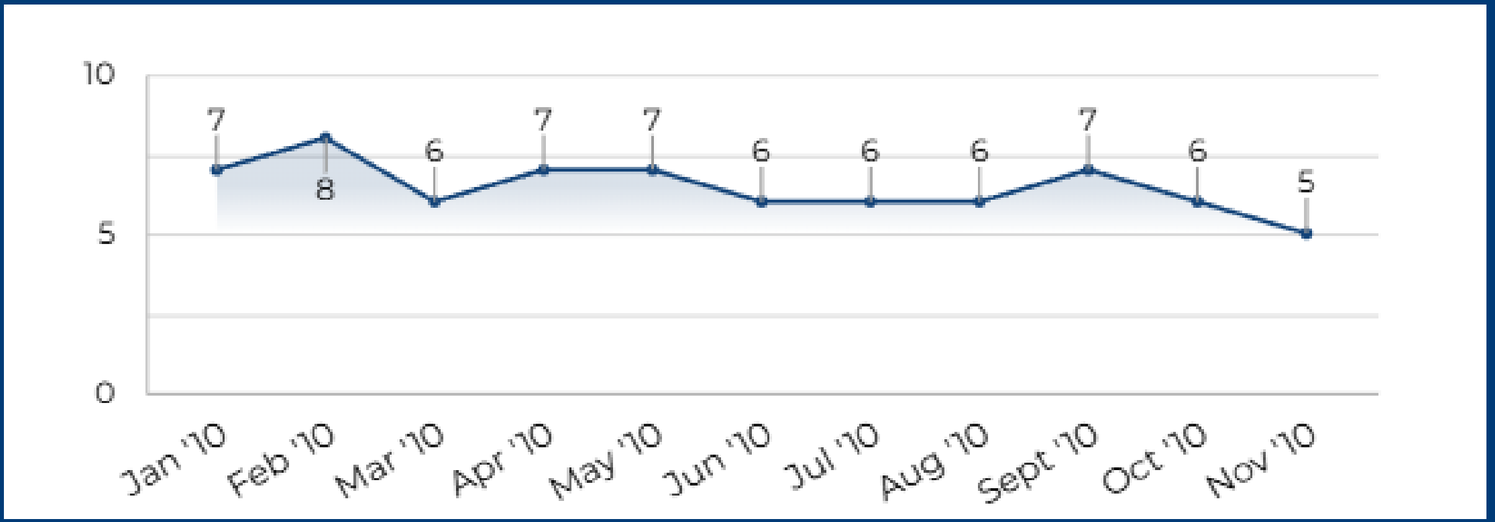
Tujuan:

Menggambarkan tingkat adopsi teknologi chip pada kartu nasabah sebagai indikator keamanan transaksi

Hasil:

Mayoritas kartu nasabah sudah menggunakan chip, yaitu sebanyak 2,3 ribu kartu. Sementara 265 kartu belum menggunakan chip. Kartu non-chip lebih rentan terhadap resiko keamanan, maka diharapkan pihak bank dapat mendorong peningkatan penggunaan chip pada kartu secara menyeluruh untuk perlindungan transaksi.

Transaction Errors per Month



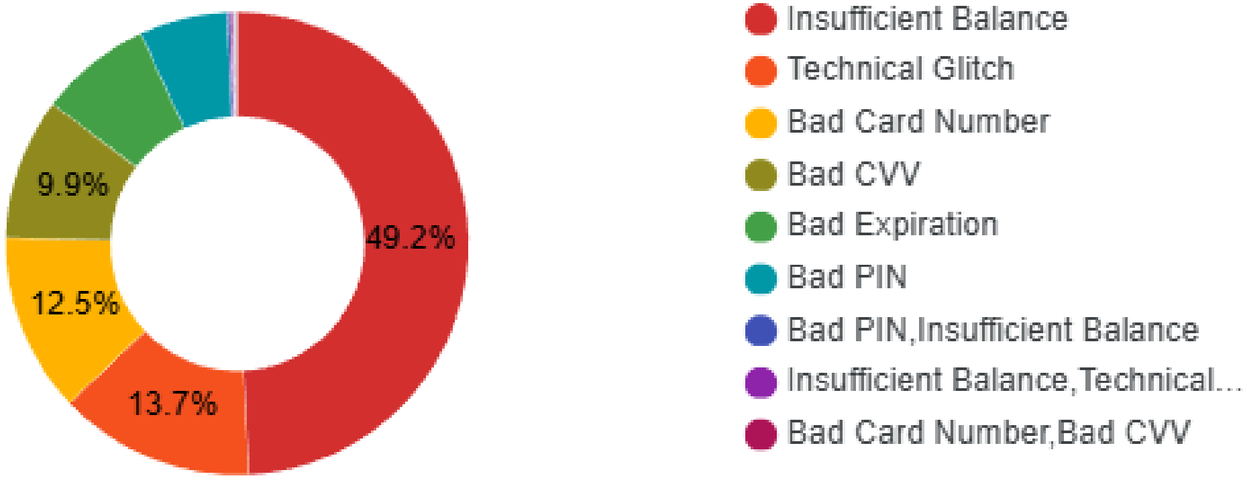
Tujuan:

Memantau error transaksi bulanan dan mengidentifikasi potensi pola masalah sistem.

Hasil:

Jumlah error transaksi per bulan relatif stabil sepanjang bulan Januari - November 2010, dengan rata-rata sekitar 6-7 kasus. Meskipun tren tidak menunjukkan peningkatan signifikan, monitoring tetap diperlukan agar error tidak berdampak pada pengalaman pengguna.

Transactions Error by Type



Tujuan:

Mengidentifikasi penyebab utama error transaksi untuk mendukung prioritas perbaikan sistem dan strategi edukasi nasabah.

Hasil:

Error transaksi sepanjang bulan Januari - November 2010 paling dominan disebabkan oleh *Insufficient Balance* (49,2%), diikuti *Technical Glitch* (13,7%), dan *Bad Card Number* (12,5%). Error lainnya memiliki porsi kecil. Informasi ini membantu prioritas perbaikan sistem dan edukasi pengguna.

Kesimpulan

Secara umum, keamanan kartu masih cukup baik, tidak ada di Dark Web dan mayoritas sudah menggunakan chip. Namun terdapat beberapa temuan penting, yaitu:

- Kasus ekstrem, yaitu transaksi melebihi limit
- Nasahah dengan eror >50 kali masih cukup banyak
- Masih terdapat kartu non-chip
- Error transaksi konsisten tiap bulan
- Dominasi error karena saldo tidak cukup

Sehingga perlu kombinasi langkah penguatan keamanan, perbaikan sistem edukasi nasabah, dan monitoring intensif untuk mencegah resiko ke depannya.

mandiri sekuritas

Thank You

Dashboard: https://s.id/Fraud_Risk_Detection
Git Hub : https://github.com/apriliasania2/Fraud-Risk-Detection.git