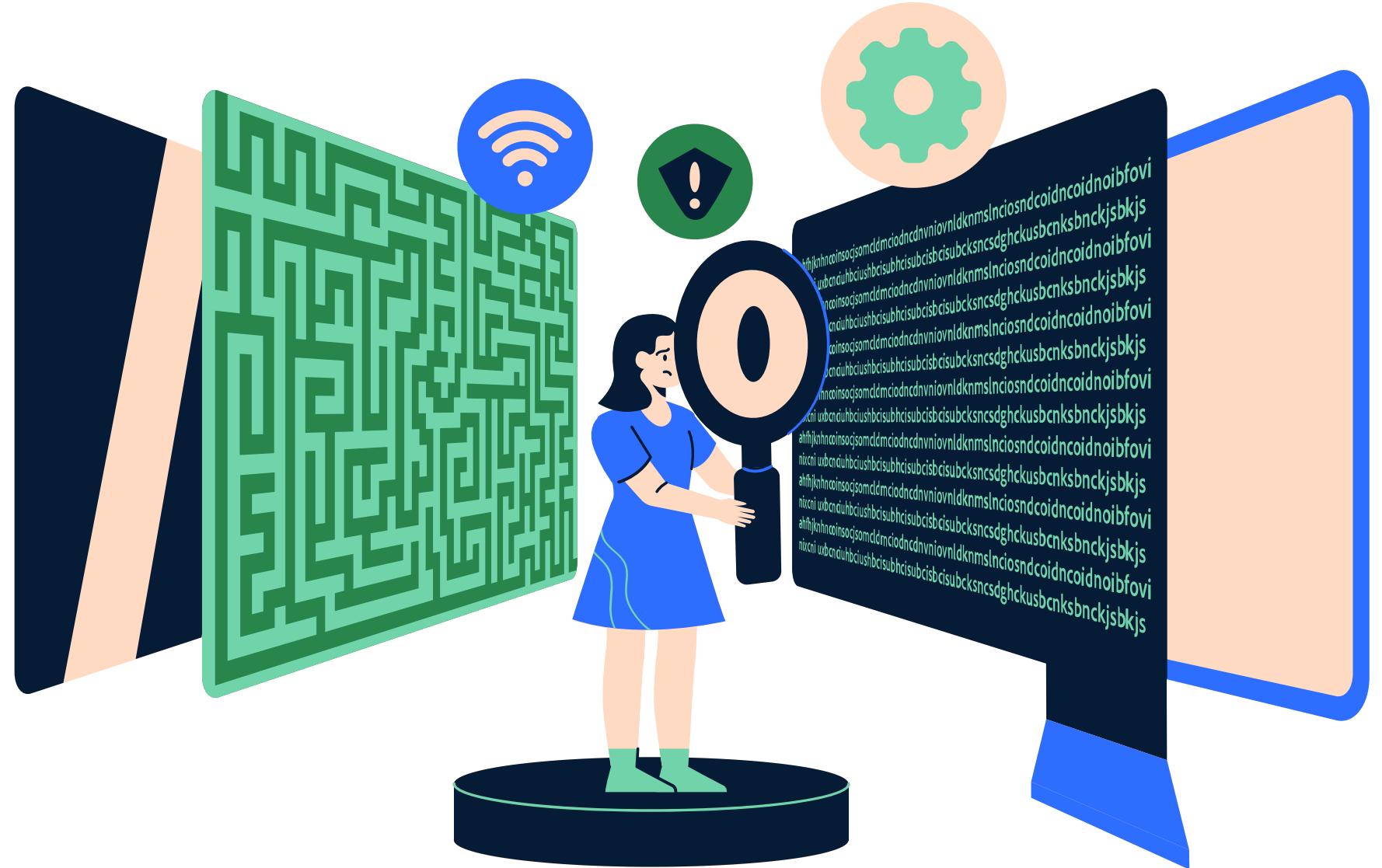


# SQL ile Fraud Riskinin Analizi



Caspian Bank – Data Analitika Layihəsi



# Layihənin Məqsədi

**Problem:** Bank sektorunda fırıldaqçılıq (fraud) əməliyyatları həm maliyyə itkilərinə, həm də müştəri etibarının azalmasına səbəb olan ciddi bir riskdir.

**Məqsəd:** Bu layihənin əsas məqsədi, mövcud tranzaksiya məlumatları bazası üzərində çoxşaxəli bir təhlil apararaq fırıldaqçılıq hallarının xüsusiyyətlərini, davranış modellərini aşkar etməkdir.

Bank sektorunda fırıldaqçılıq (fraud) halları həm müştərilər, həm də maliyyə təşkilatları üçün ciddi maliyyə və reputasiya itkisinə səbəb ola bilir. Hazırkı layihə SQL üzərindən aparılır və aşağıdakı hədəfləri özündə birləşdirir:

1. Mövcud vəziyyəti təhlil etmək
2. Fraud risk faktorlarını üzə çıxarmaq
3. Bank üçün strateji tövsiyələr hazırlamaq

# **DATASETLƏR HAQQINDA MƏLUMAT**



## Customers (müzəkerilər)

- customer\_id
- first\_name
- last\_name
- date\_of\_birth
- city
- country
- registration\_date

## Cards (kartlar)

- card\_id
- customer\_id
- card\_number
- card\_type
- credit\_limit
- card\_status
- issue\_date

## Cədvəllər

### Merchants (satıcılar)

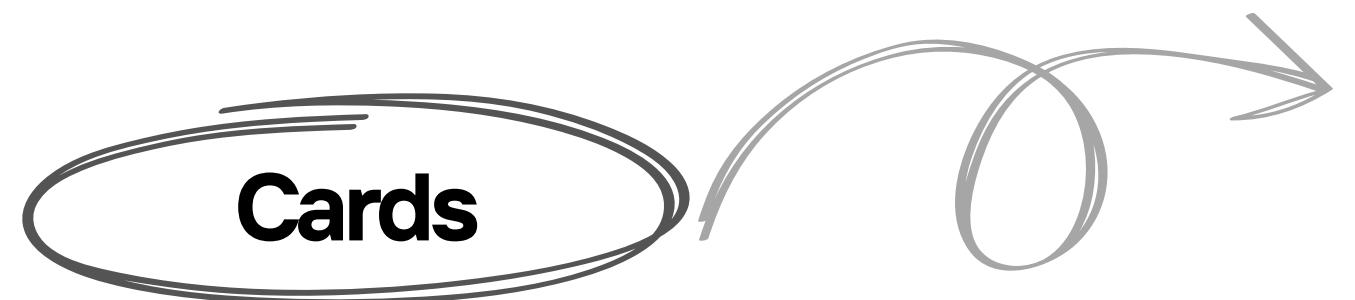
- merchant\_id
- merchant\_name
- merchant\_category
- merchant\_country

### Transactions (əməliyyatlar)

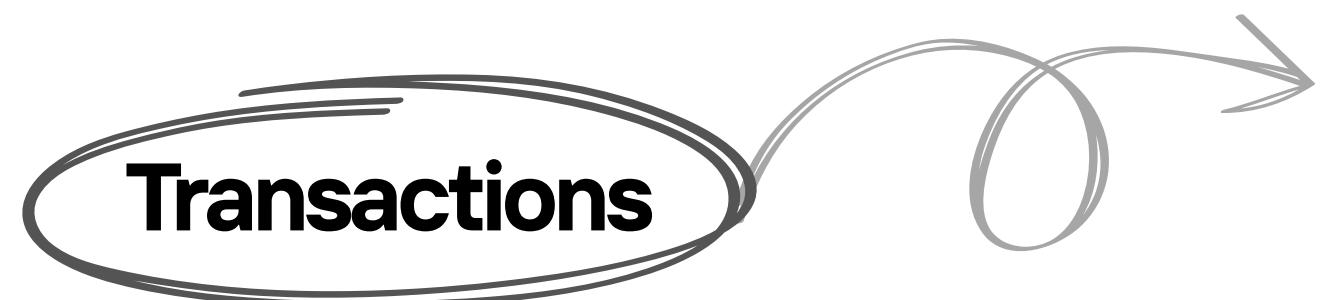
- transaction\_id
- card\_id
- merchant\_id
- transaction\_amount
- transaction\_datetime
- transaction\_location
- transaction\_status
- is\_fraud



Sütun	Data tipi	İzah
customer_id	INT (PK)	Müşterinin unikal identifikatoru
first_name	VARCHAR(50)	Müşterinin adı
last_name	VARCHAR(50)	Müşterinin soyadı
date_of_birth	DATE	Doğum tarixi
city	VARCHAR(50)	Müşterinin yaşadığı şəhər
country	VARCHAR(50)	Müşterinin ölkəsi
registration_date	DATE	Bank sisteminə qeydiyyat tarixi



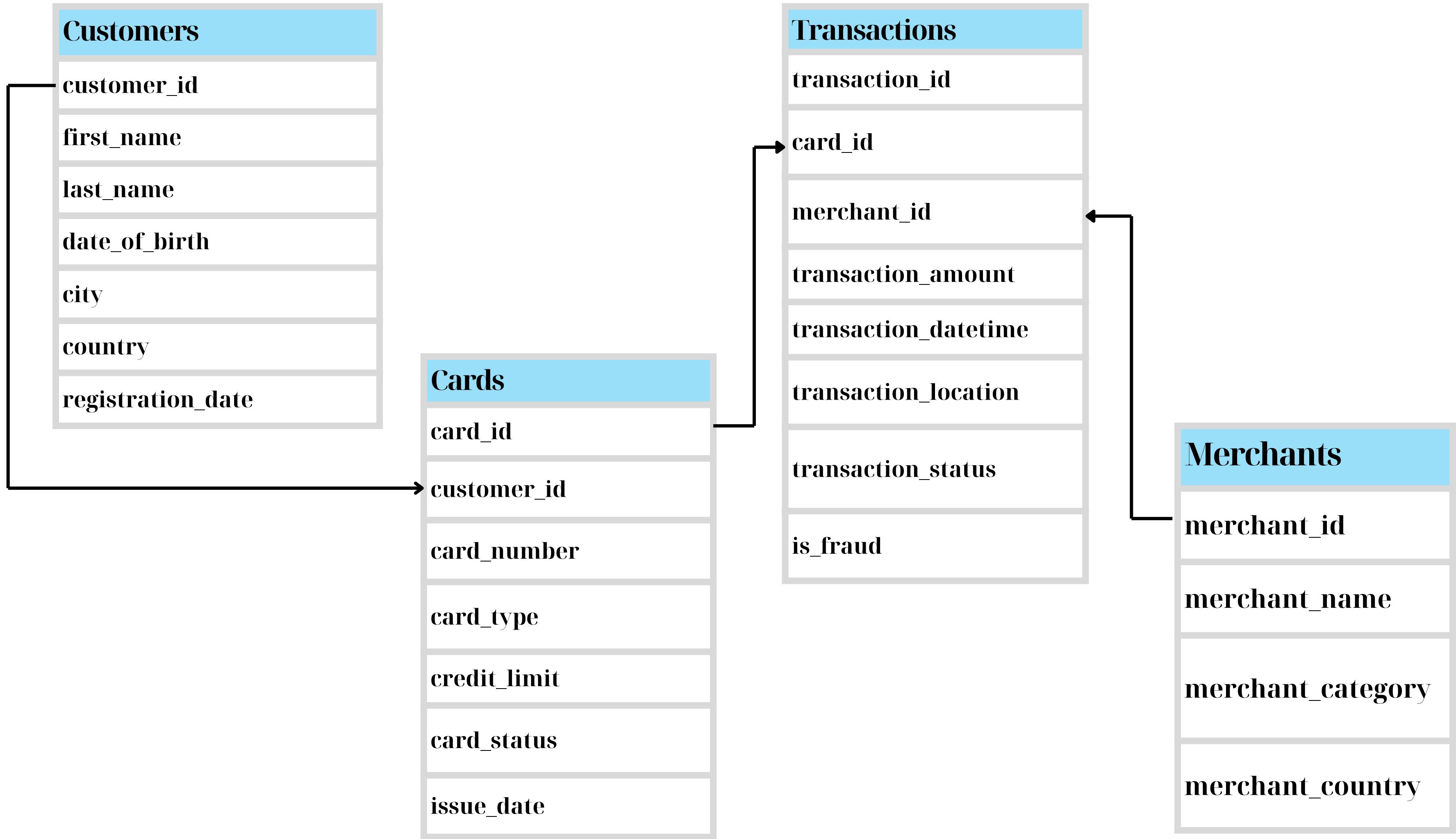
Sütun	Data tipi	İzah
card_id	INT (PK)	Kartın unikal identifikatoru
customer_id	INT (FK)	Kart sahibinin ID-si
card_number	VARCHAR(20)	Kart nömrəsi (simulyasiya olunmuş)
card_type	VARCHAR(20)	Kart növü (Visa, MasterCard və s.)
credit_limit	NUMBER(10,2)	Kartın kredit limiti
card_status	VARCHAR(20)	Kart statusu (Active, Blocked, Stolen və s.)
issue_date	DATE	Kartın buraxılma tarixi



Sütun	Data tipi	İzah
transaction_id	INT (PK)	Əməliyyatın unikal ID-si
card_id	INT (FK)	Əməliyyatın aid olduğu kart
merchant_id	INT (FK)	Əməliyyatın baş verdiyi satıcı
transaction_amount	NUMBER(10,2)	Əməliyyat məbləği
transaction_datetime	TIMESTAMP	Əməliyyat tarixi və vaxtı
transaction_location	VARCHAR(100)	Əməliyyatın həyata keçirildiyi yer
transaction_status	VARCHAR(20)	Əməliyyatın vəziyyəti (Approved/Declined)
is_fraud	NUMBER(1)	Fraud olub-olmaması (1 = bəli, 0 = xeyr)



Sütun	Data tipi	İzah
merchant_id	INT (PK)	Satıcının unikal ID-si
merchant_name	VARCHAR(100)	Satıcının adı
merchant_category	VARCHAR(50)	Satıcının fəaliyyət növü (market, geyim və s.)
merchant_country	VARCHAR(50)	Satıcının yerləşdiyi ölkə





# Müştəri Seqmentasiyası

İlk addımda, fırıldaqçılıq riskinin hansı müştəri və kart qruplarında daha yüksək olduğunu anlamaq üçün ümumi bir analiz edəcəyik. Müştərilər əməkdaşlıq müddətinə (Yeni, Orta müddətli, Loyal), kartlar isə kredit limitinə (Standard, Gold, Platinum) görə seqmentləşdirilir. Hər kəsişmə üçün ümumi tranzaksiya sayı, fırıldaqçılıq sayı və fırıldaqçılıq nisbəti hesablanır. Bu mərhələ, bankın diqqətini ən riskli seqmentlərə (məsələn, "Yeni müştərilərin Gold kartları") yönəltməsinə imkan verir və sonrakı daha dərin analizlər üçün istiqamət müəyyən edir.

## SQL sorğusu:

```
select
    case
        when months_between(sysdate, cu.registration_date) < 12 then 'yeni'
        when months_between(sysdate, cu.registration_date) between 12 and 36 then 'orta müddetli'
        else 'loyal'
    end as customer_segment,

    case
        when ca.credit_limit < 2000 then 'standard'
        when ca.credit_limit between 2000 and 7500 then 'gold'
        else 'platinum'
    end as card_segment,
from customers cu
join cards ca on cu.customer_id = ca.customer_id
join transactions t on ca.card_id = t.card_id
```

# Notice:

	CUSTOMER_SEGMENT	CARD_SEGMENT	TOTAL_TRANSACTIONS	FRAUD_TRANSACTIONS	FRAUD_RATE_PERCENT
1	loyal	gold	7526	116	1.54
2	loyal	platinum	4474	52	1.16
3	loyal	standard	18932	203	1.07
4	orta müddetli	gold	1310	14	1.07
5	orta müddetli	platinum	831	3	0.36
6	orta müddetli	standard	3510	40	1.14
7	yeni	gold	697	8	1.15
8	yeni	platinum	474	0	0
9	yeni	standard	2246	44	1.96

## Yekun Dəyərləndirmə

- Ən riskli seqment: Yeni müştərilər + Standard kartlar (1.96% fraud).
- Ən etibarlı seqment: Orta müddətli müştərilər + Platinum kartlar (0.36%).
- Ümumi tendensiya: Müştərinin bankdakı təcrübəsi artdıqca (loyal olduqca), fraud faizi azalır.

## Strateji tövsiyə:

- Bank yeni müştərilərin əməliyyatlarını daha çox monitoring etməli, xüsusən standard kartlar üzrə əlavə təhlükəsizlik tədbirləri tətbiq etməlidir.
- Yüksək limitli və uzunmüddətli müştərilərdə risk aşağı olduğundan, onlara daha çevik xidmət (az bloklama, daha çox rahatlıq) verilə bilər.



Növbəti olaraq, Fırıldaqcıların oğurlanmış kart məlumatlarını istifadə etməzdən əvvəl nə qədər gözlədiyini ("yatma dövrü") anlayacayıq. Hər fırıldaqcılıq əməliyyatı üçün ondan əvvəlki son legitim tranzaksiya tapılır və aradakı zaman fərqi (gündərlə) hesablanır. Uzun müddət istifadə edilməyən bir kartda qəfil aktivliyin yüksək risk siqnalı olduğunu təsdiqləyir. Bu, risk qiymətləndirmə alqoritmlərini təkmilləşdirmək üçün kritik bir məlumatdır.

## "Yatan Kart" Riski

## SQL sorğusu:

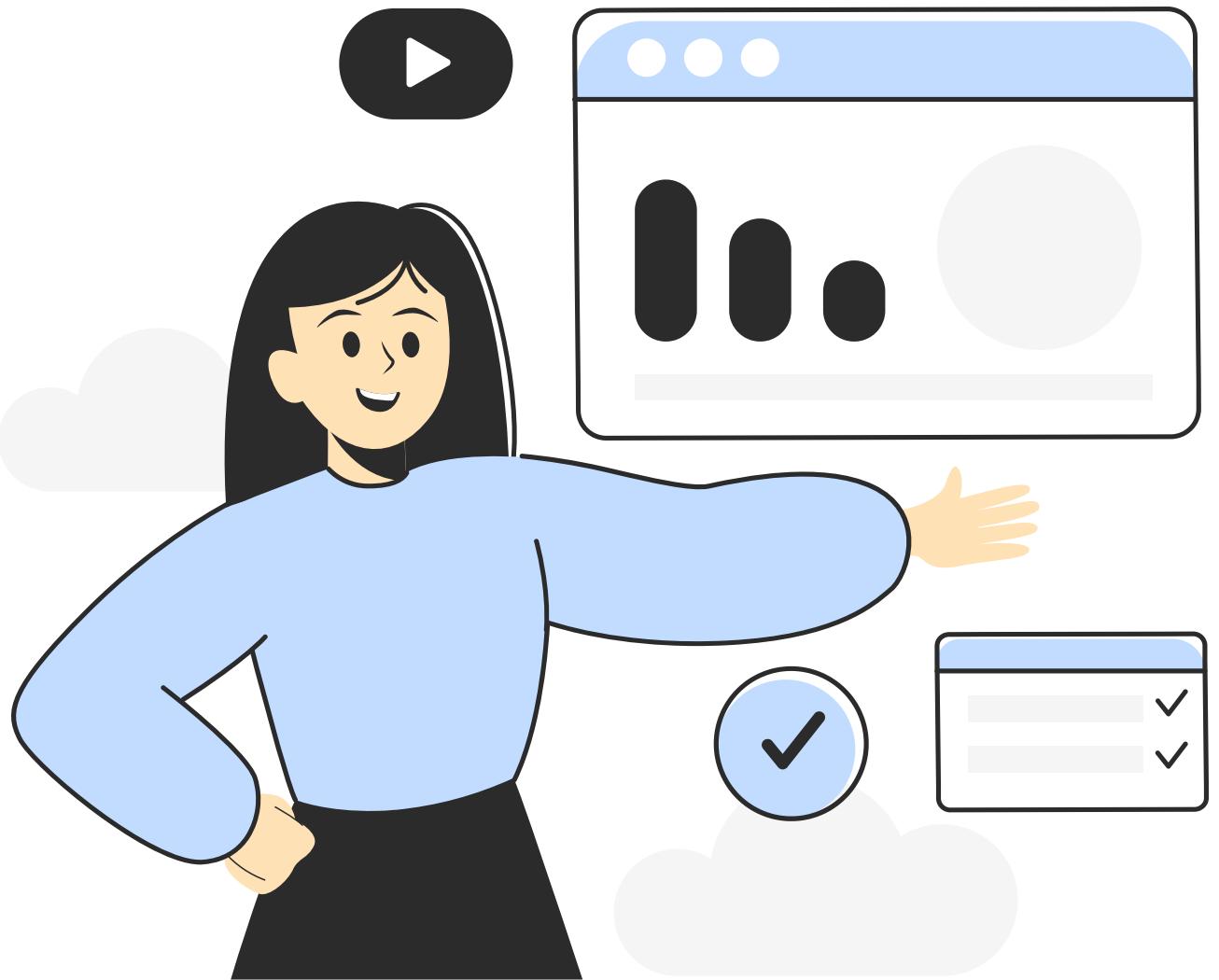
```
select
    t.card_id,
    t.transaction_id,
    t.transaction_datetime,
    t.is_fraud,
    max(case when is_fraud = 0 then transaction_datetime end)
        over (
            partition by card_id
            order by transaction_datetime
            rows between unbounded preceding and 1 preceding
        ) as last_legit_datetime,
    round(
        (t.transaction_datetime -
        max(case when is_fraud = 0 then transaction_datetime end)
        over (
            partition by card_id
            order by transaction_datetime
            rows between unbounded preceding and 1 preceding
        ))
        , 0
    ) as dormant_days
from transactions t
order by t.card_id, t.transaction_datetime;
```

# Nəticə:

CARD_ID	TRANSACTION_ID	TRANSACTION_DATETIME	IS_FRAUD	LAST_LEGIT_DATETIME	DORMANT_DAYS
1	1	112746 07-OCT-24	0 (null)	(null)	
2	1	137477 10-NOV-24	0 07-OCT-24		35
3	1	101858 24-NOV-24	0 10-NOV-24		14
4	1	116120 25-NOV-24	0 24-NOV-24		1
5	1	116016 30-MAR-25	0 25-NOV-24		125
6	1	117921 01-APR-25	0 30-MAR-25		2
7	1	129562 03-APR-25	0 01-APR-25		2
8	1	110724 24-JUN-25	0 03-APR-25		82
9	1	116709 09-JUL-25	0 24-JUN-25		15
10	1	134646 29-JUL-25	0 09-JUL-25		21
11	1	114676 21-AUG-25	0 29-JUL-25		23
12	1	105540 22-AUG-25	0 21-AUG-25		1
13	1	117153 22-SEP-25	0 22-AUG-25		31

## Yekun Dəyərləndirmə

- Bank baxımından:**
  - Bu analiz göstərir ki, bir çox kartlar uzun müddət yuxuda qaldıqdan sonra yenidən aktivləşir.
  - Belə kartların fırıldaqçılıq ehtimalı daha yüksəkdir.
- Strateji nəticə:**
  - Bank "Dormant Card Alert" qaydası tətbiq edə bilər:
    - Əgər kart son 90 gündə istifadə olunmayıbsa və birdən aktivləşirsə → əməliyyatı "riskli" kimi işarələmək.
    - Əlavə təsdiq (SMS və ya tətbiq bildiriş) istəmək.
- Fraud komandası üçün:**
  - "Dormant period" göstəricisi real vaxt risk modellərində "trigger" kimi istifadə oluna bilər.



# Xərcləmə Sürəti Anomaliyası

Fırıldaqçılıq əməliyyatlarını normal əməliyyatlardan fərqləndirən ani xərcləmə partlayışlarını müəyyən etmək növbəti addımımızdır. Hər bir tranzaksiya üçün window funksiyaları ilə son 24 saatlıq hərəkətli xərcləmə cəmi və son 3 tranzaksiyanın hərəkətli ortalaması hesablanır. Bu göstəricilər real-zaman rejimində izlənilə bilər. Əgər bir kart üçün bu dəyərlər qəfildən kəskin artsa, bu, əməliyyatın dərhal bloklanması və ya əlavə yoxlamaya göndərilməsi üçün bir siqnal (trigger) ola bilər.

## SQL sorğusu:

```
select
    t.transaction_id,
    t.card_id,
    t.transaction_datetime,
    t.transaction_amount,
    t.is_fraud,
    round(
        (select sum(t2.transaction_amount)
         from transactions t2
         where t2.card_id = t.card_id
           and t2.transaction_datetime between t.transaction_datetime - 1 and t.transaction_datetime
        ), 2
    ) as rolling_24h_sum,
```

# Notice:

	TRANSACTION_ID	CARD_ID	TRANSACTION_DATETIME	TRANSACTION_AMOUNT	IS_FRAUD	ROLLING_24H_SUM	MOVING_AVG_LAST_3
1	112746	1	07-OCT-24	120.32	0	120.32	120.32
2	137477	1	10-NOV-24	276.89	0	276.89	198.61
3	101858	1	24-NOV-24	3110.43	0	3110.43	1169.21
4	116120	1	25-NOV-24	177.52	0	3287.95	1188.28
5	116016	1	30-MAR-25	23.24	0	23.24	1103.73
6	117921	1	01-APR-25	27.75	0	27.75	76.17
7	129562	1	03-APR-25	39.22	0	39.22	30.07
8	110724	1	24-JUN-25	13.9	0	13.9	26.96
9	116709	1	09-JUL-25	145.16	0	145.16	66.09
10	134646	1	29-JUL-25	46.72	0	46.72	68.59
11	114676	1	21-AUG-25	174.02	0	174.02	121.97
12	105540	1	22-AUG-25	15.21	0	189.23	78.65

## Yekun Dəyərləndirmə

### 1. Normal əməliyyatlarda balanslı göstəricilər görünür.

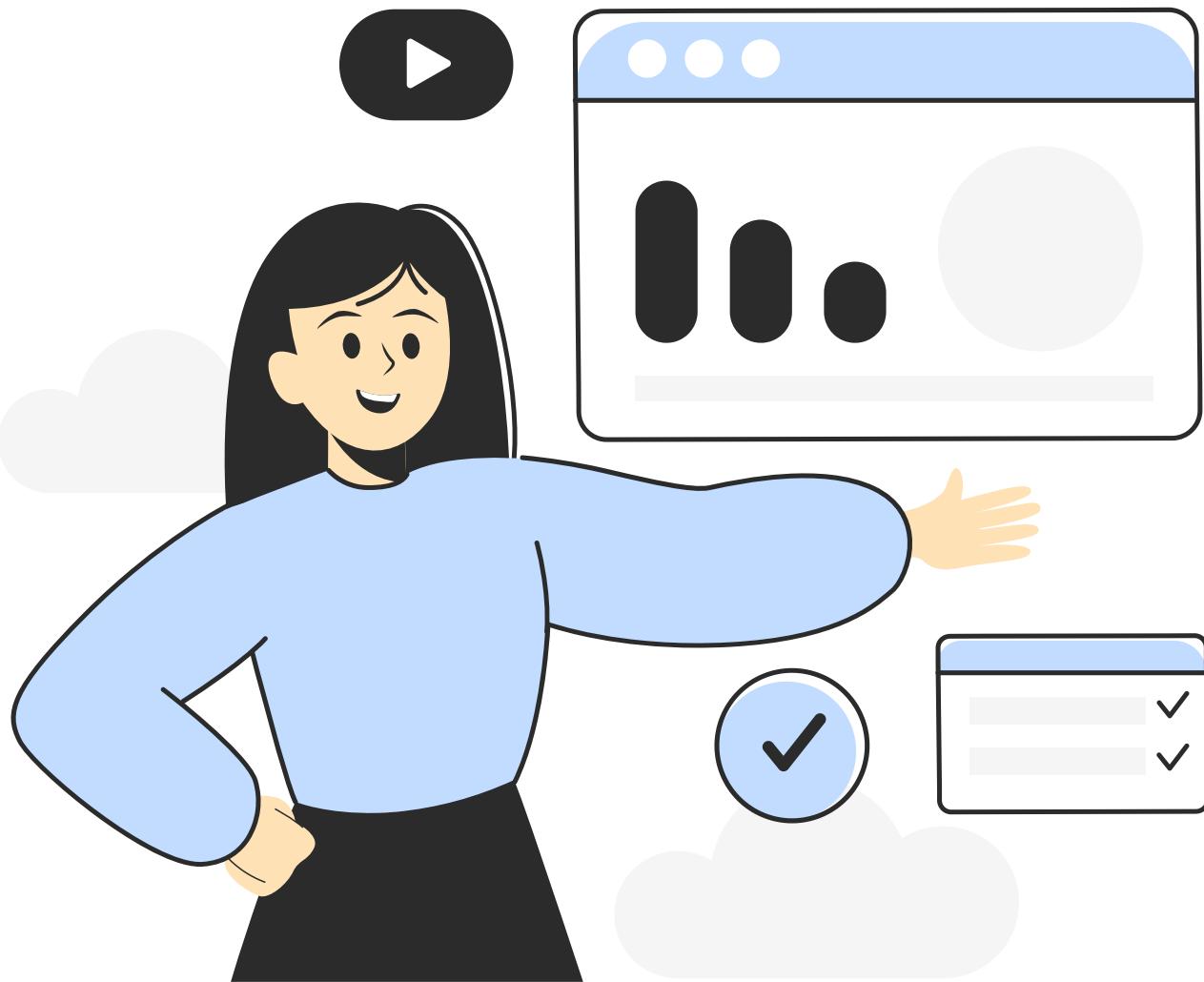
- Məsələn, transaction\_amount 120–300 AZN cıvarında olanda həm 24 saatlıq cəm, həm də son 3 əməliyyatın ortası bir-birinə yaxındır.
- Bu, müştərinin xərcləmə vərdişlərinin sabit və təbii olduğunu göstərir.

### 2. Kəskin sıçrayışlar anomaliyadır.

- Məsələn, transaction\_amount = 3110.43 olan əməliyyatda ROLLING\_24H\_SUM = 3110.43, amma əvvəlki 3 əməliyyatın ortası cəmi ~1169 AZN-dir.
- Burada birdən-birə çox böyük xərcləmə olub → bu potensial risk siqnalı ola bilər.

### 3. Xüsusilə ardıcıl iri məbləğlər risklidir.

- Əgər bir kart qısa vaxt ərzində (24 saat ərzində) bir neçə iri əməliyyat edirsə, rolling sum kəskin artır.
- Bu, fraudçuların tez bir zamanda maksimum pul çıxarma davranışına uyğundur.



Bir kart üzrə ilk fırıldaqcılıq baş verdikdən sonra fırıldaqların nə qədər sürətlə hərəkət etdiyini və qısa müddətdə nə qədər zərər vurduğunu ölçürük. Hər oğurlanmış kart üçün ilk fırıldaqcılıq əməliyyatı tapılır və ondan sonrakı 1 saat ərzində edilən digər fırıldaqcılıqların sayı və ümumi məbləği hesablanır. Bu analiz, şübhəli bir əməliyyat aşkarlandıqdan sonra kartın dərhal bloklanması nə qədər kritik olduğunu rəqəmlərlə sübut edir və bankın reaksiya müddətinin optimallaşdırılmasının vacibliyini vurğulayır.

## "İlk Hükum" Analizi

## SQL sorğusu:

```
with first_fraud as (
    select
        card_id,
        min(transaction_datetime) as first_fraud_time
    from transactions
    where is_fraud = 1
    group by card_id
)
select
    f.card_id,
    to_char(f.first_fraud_time, 'YYYY-MM-DD HH24:MI:SS') as first_fraud_time,
    count(t.transaction_id) as fraud_count_within_1h,
    coalesce(sum(t.transaction_amount), 0) as fraud_amount_within_1h
    from first_fraud f
```

# Notice:

CARD_ID	FIRST_FRAUD_TIME	FRAUD_COUNT_WITHIN_1H	FRAUD_AMOUNT_WITHIN_1H
1	10 2024-10-22 13:40:20	1	1
2	23 2025-02-03 06:46:06	1	4213.7
3	49 2025-07-26 02:58:19	1	2.08
4	52 2024-10-18 00:56:48	1	348.21
5	54 2024-11-07 16:32:50	1	4555.56
6	73 2025-02-26 06:51:31	1	2341.72
7	90 2024-09-30 18:56:23	1	1.06
8	117 2025-02-15 05:44:35	1	1.13
9	128 2024-10-01 20:25:49	1	2374.19

## Yekun Dəyərləndirmə

1. Əksər kartlarda ilk hücumdan sonra əlavə əməliyyat olmayıb.

- FRAUD\_COUNT\_WITHIN\_1H = 1 deməkdir ki, 1 saat ərzində yalnız bir fırıldaq əməliyyat olub.
- Bu, o deməkdir ki, hücumlar çox qısa və hədəfli şəkildə həyata keçirilib.

2. Bəzi hallarda zərər çox yüksəkdir.

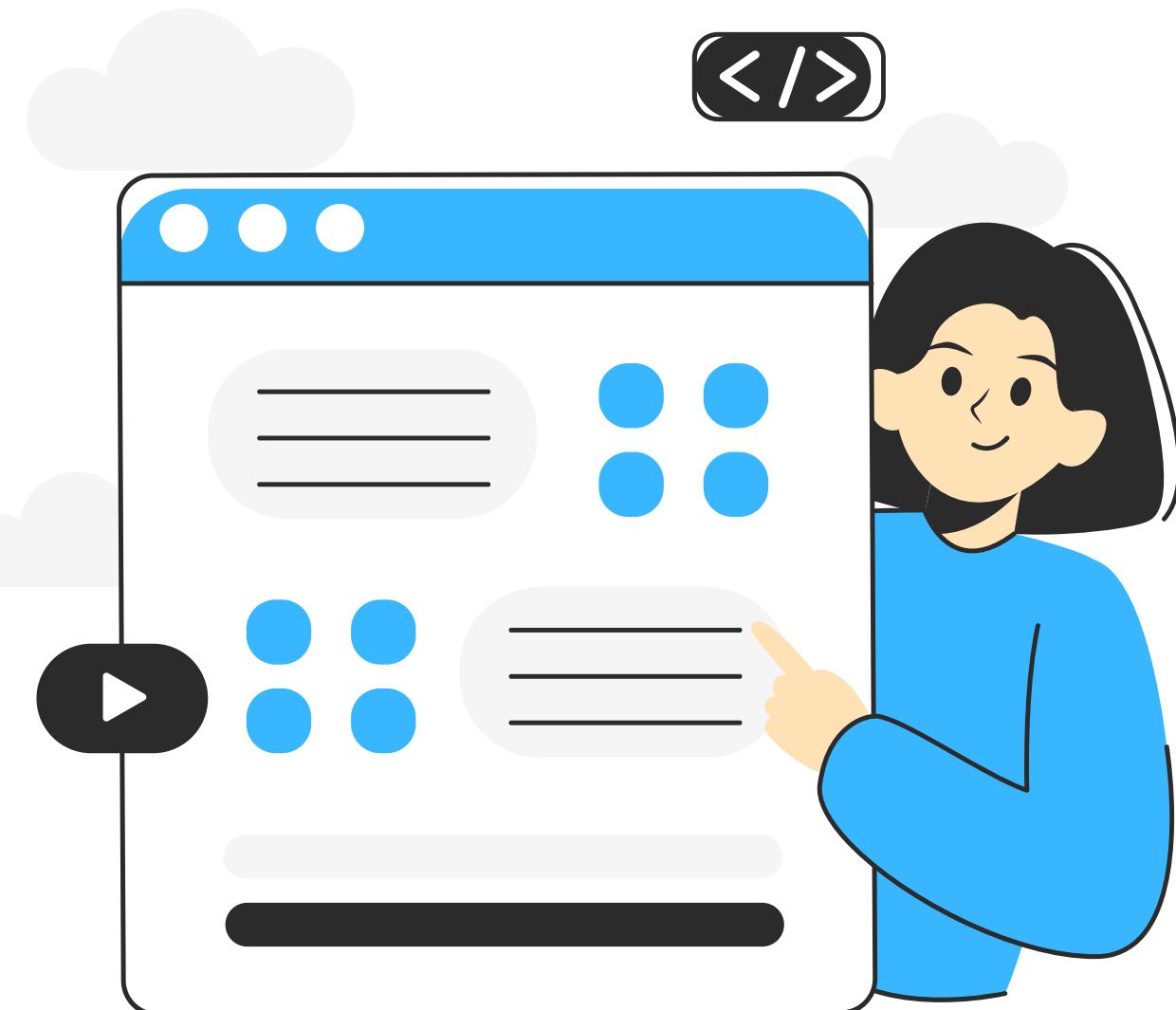
- Məsələn, CARD\_ID = 5 üçün 1 saat içində 4555.56 AZN,
- CARD\_ID = 2 üçün 4213.70 AZN,
- Bu, göstərir ki, fırıldaqçılar bir əməliyyatda maksimum zərəri vurmağa çalışırlar.

3. Kiçik məbləğli hücumlar da var, məsələn 1–2 AZN cıvarında.

- Bu tip əməliyyatlar çox vaxt test tranzaksiyaları olur.
- Fırıldaqçılar əvvəlcə kiçik məbləğlə sistemin reaksiya verib-vermədiyini yoxlayır.

4. Zaman baxımından tendensiya:

- Hücumlar müxtəlif aylarda baş verir, amma bir çoxu gecə və səhər erkən saatlarda həyata keçirilib (məsələn, 00:56:48, 02:58:19, 05:44:35).
- Bu, aşağı nəzarət saatlarında hücum strategiyasını göstərir.



Fırıldaqçılıq əməliyyatlarının hansı satıcılarda (merchant) cəmləşdiyini müəyyən etməliyik. Bir saat ərzində 1-dən çox fərqli oğurlanmış kartdan əməliyyat qəbul edən "qaynar nöqtə" satıcılar müəyyən edilir. Bu, banka kompromitə edilmiş POS terminalları və ya onlayn ödəmə sistemləri haqqında məlumat verir. Bank bu satıcılarla aparılan əməliyyatlara daha sərt nəzarət tətbiq edə və ya həmin satıcılarla əməkdaşlığı dayandırıra bilər.

# Fırıldaqçılıq Zəncirinin Xəritələnməsi

## SQL sorğusu:

```
select
    m.merchant_name,
    count(*) as fraud_count,
    count(distinct t.card_id) as unique_cards
from transactions t
join merchants m on t.merchant_id = m.merchant_id
where t.is_fraud = 1
group by m.merchant_name, trunc(t.transaction_datetime, 'hh24')
order by fraud_count desc
```

# Nəticə:

MERCHANT_NAME	FRAUD_COUNT	UNIQUE_C...
1 Wolt	1	1
2 YouTube Premium	1	1
3 Azergold	1	1
4 Google Play	1	1
5 Aliexpress	1	1
6 Azpetrol	1	1
7 Uber Eats	1	1
8 Əsgərov Hacızadə QSC	1	1

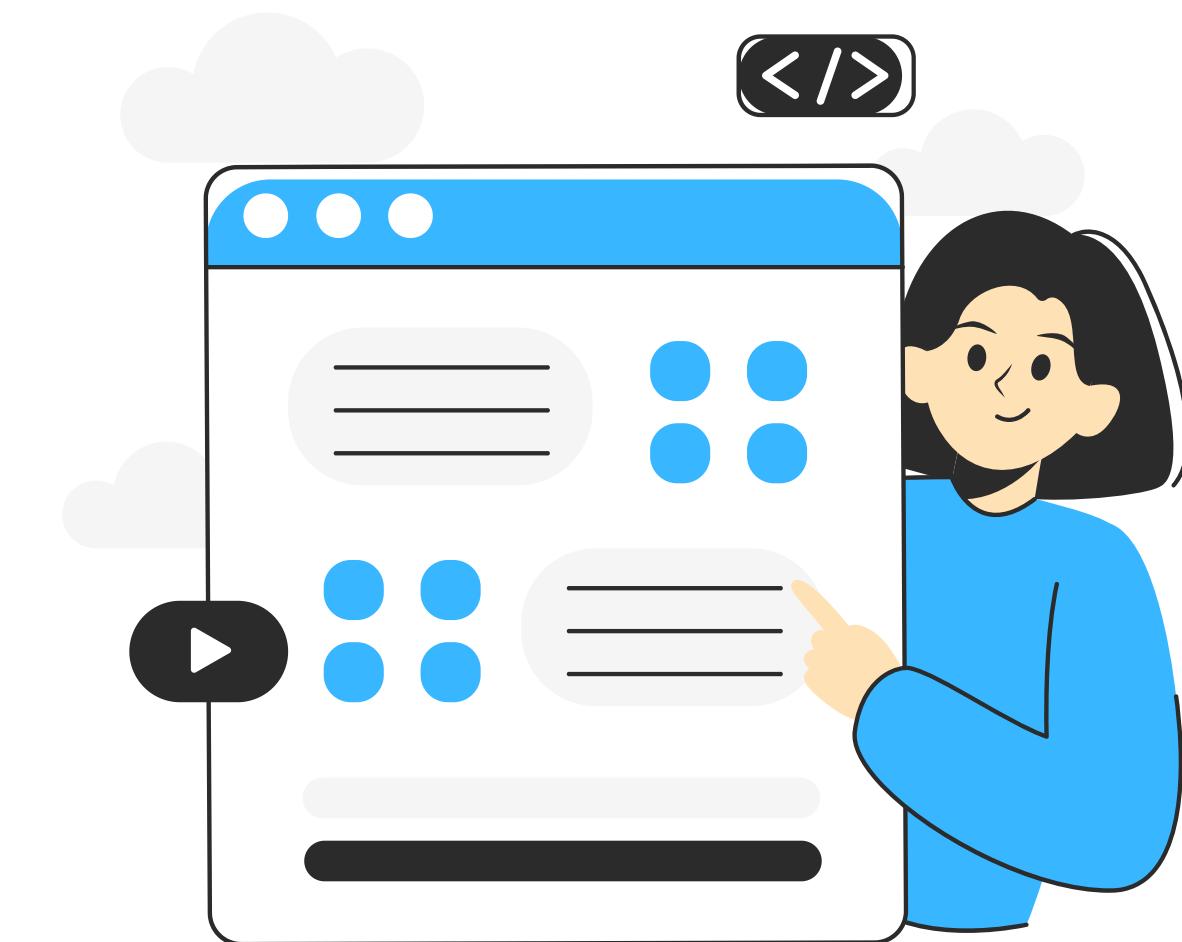
## Yekun Dəyərləndirmə

Aparılan analiz nəticəsində heç bir satıcıının (merchant) eyni bir saat ərzində 5-dən çox fərqli kartdan fırıldaqçılıq əməliyyatı qəbul etmədiyi müəyyən edildi.

Bu o deməkdir ki, analiz dövründə eyni vaxt intervalında kütləvi və əlaqəli fırıldaqçılıq hallarına rast gəlinməyib.

Başqa sözlə, sistem üzrə fırıldaqçılıq fəaliyyəti daha çox fərdi və izolyasiya olunmuş əməliyyatlar şəklində baş verir.

Bu, hazırda koordinasiyalı və geniş miqyaslı fırıldaq şəbəkələrinin aktiv olmadığını göstərir.



# Proaktiv Qayda Simulyasiyası: "Ağıllı Limit" Təklifi

Əvvəlki mərhələlərdə əldə edilən biliklər əsasında yeni bir fırıldaqçılıqla mübarizə qaydası təklif etmək və onun keçmiş məlumatlar üzərində nə qədər effektiv olacağını yoxlayırıq. "Əgər bir tranzaksiyanın məbləği, kartın son 30 gündəki ən böyük legitim əməliyyatından 10 dəfə böyükdürsə və əməliyyat xaricdədirse, onu blokla."

Bu qaydaya əsasən bloklanacaq bütün tranzaksiyalar tapılır. Həmin tranzaksiyaların neçəsinin həqiqətən fırıldaqçılıq olduğunu (True Positive) və neçəsinin səhvən bloklanmış legitim əməliyyat olduğunu (False Positive) hesablayan bir sorğu yazılır. Bu son mərhələ, təhlilin nəticələrini konkret, ölçülə bilən bir biznes təklifinə çevirir. Bank bu qaydanın potensial fayda və zərərlərini (fırıldaqçılığın qarşısını almaq vs. müştəri narazılılığı) qiymətləndirərək onu tətbiq edib-etmək barədə məlumatlı bir qərar verə bilər.

## SQL sorğusu:

```
select
    sum(case when t.is_fraud = 1 then 1 else 0 end) as true_positive,
    sum(case when t.is_fraud = 0 then 1 else 0 end) as false_positive,
    count(*) as total_blocked
from transactions t
left join (
    select card_id, max(transaction_amount) as max_legit_amount
    from transactions
    where is_fraud = 0
        and transaction_datetime >= sysdate - 30
    group by card_id
) max_tx on t.card_id = max_tx.card_id
```

**Nəticə:**

	TRUE_POSITIVE	FALSE_POSITIVE	TOTAL_BLOCKED	
1	150	698	848	

### Yekun Dəyərləndirmə

Aparılan analiz nəticəsində, ümumilikdə 848 əməliyyat potensial riskli kimi bloklanmışdır.

Bunlardan:

- 150 əməliyyat həqiqətən fırıldaqçılıq olduğu üçün doğru pozitivlərdir (True Positive),
- 698 əməliyyat isə səhvən riskli kimi qiymətləndirilib (False Positive).

Bu nəticə göstərir ki, sistemin ümumi bloklama dəqiqliyi (precision) nisbətən aşağıdır – yəni, blokunan əməliyyatların böyük hissəsi əslində legitim (normal) olub.

- “10 dəfə yüksək məbləğ” və “xarici ölkə lokasiyası” meyarları çoxlu sayıda yanlış pozitivlərə səbəb olur.
- Lakin eyni zamanda sistem 150 real fırıldaqçılığı uğurla aşkar edib, bu da modelin riskli davranışları tutmaq qabiliyyətini təsdiqləyir.

Bu layihə kredit kartı əməliyyatları əsasında firildaqçılıq (fraud) davranışlarının dərin analizini həyata keçirmək məqsədilə hazırlanmışdır.

- Müştəri profili ilə risk arasında əlaqə var.
- Dormant (yatan) kartlar potensial təhlükə mənbəyidir.
- Bank sistemlərində real vaxt analitik monitoring tətbiq olunmalıdır.
- Əməliyyat davranışlarına əsaslanan ağıllı qaydalar (məs. "Smart Limit Rule") riskləri azaldar.
- Fraud hadisələrinin qarşısını almaq üçün yalnız texniki yox, həm də müştəri davranışına əsaslanan analitik modellər vacibdir.

*Thank  
You*

