Bank Transaction Dataset for Fraud Detection

Data-Driven Insights into Suspicious Banking Activities

Contents

Author: Lajos Almasi

Date: 2025. 05. 07.

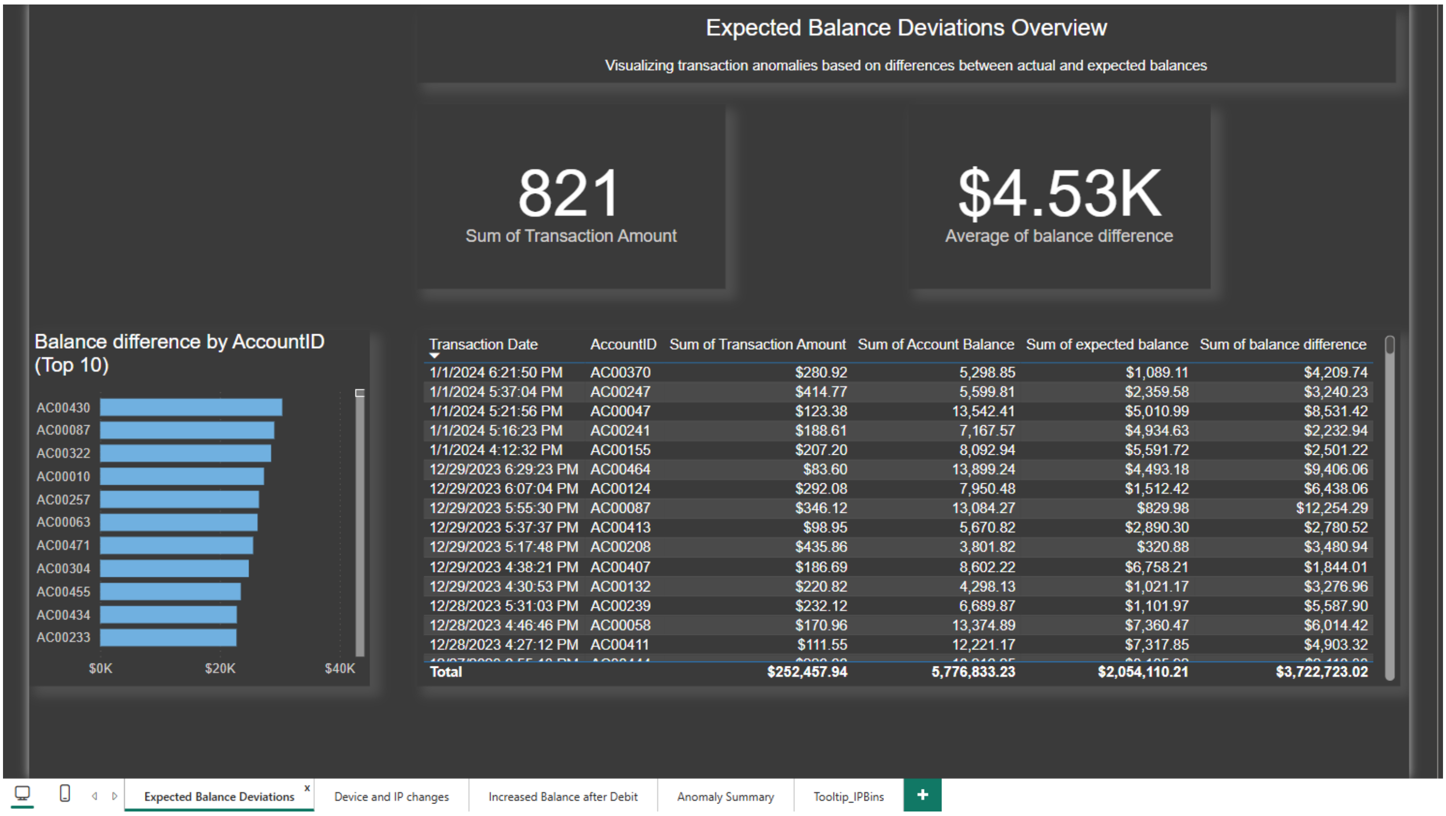
Dashboard Overview

This report analyzes bank transaction data for detecting potential fraud. The dataset was downloaded from Kaggle.com and contains transactional records that were cleaned, transformed, and analyzed using PostgreSQL and Table Plus, then visualized with Power BI.

Tools Used: PostgreSQL, Table Plus, Power BI, Excel.

Page 1: Expected Balance Deviations

The first dashboard page highlights discrepancies between expected and actual account balances. A total of **821** transactions show a combined balance deviation of over **$3.7** million. The average deviation is **$4.53K** per transaction. The top 10 accounts with the highest deviations are visualized, revealing specific accounts with recurring anomalies.



Expected Balance Deviations Overview

Visualizing transaction anomalies based on differences between actual and expected balances

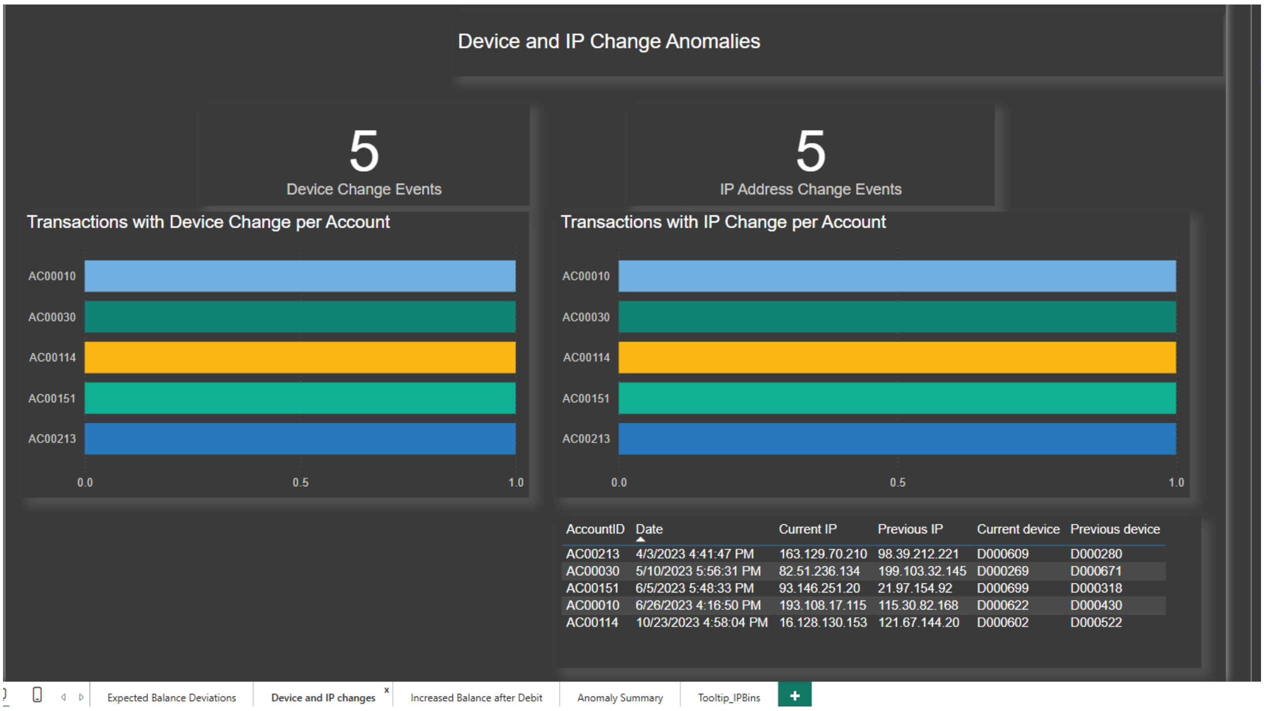
821
Sum of Transaction Amount

$4.53K
Average of balance difference

Transaction Date	AccountID	Sum of Transaction Amount	Sum of Account Balance	Sum of expected balance	Sum of balance difference
1/1/2024 6:21:50 PM	AC00370	$280.92	5,298.85	$1,089.11	$4,209.74
1/1/2024 5:37:04 PM	AC00247	$414.77	5,599.81	$2,359.58	$3,240.23
1/1/2024 5:21:56 PM	AC00047	$123.38	13,542.41	$5,010.99	$8,531.42
1/1/2024 5:16:23 PM	AC00241	$188.61	7,167.57	$4,934.63	$2,232.94
1/1/2024 4:12:32 PM	AC00155	$207.20	8,092.94	$5,591.72	$2,501.22
12/29/2023 6:29:23 PM	AC00464	$83.60	13,899.24	$4,493.18	$9,406.06
12/29/2023 6:07:04 PM	AC00124	$292.08	7,950.48	$1,512.42	$6,438.06
12/29/2023 5:55:30 PM	AC00087	$346.12	13,084.27	$829.98	$12,254.29
12/29/2023 5:37:37 PM	AC00413	$98.95	5,670.82	$2,890.30	$2,780.52
12/29/2023 5:17:48 PM	AC00208	$435.86	3,801.82	$320.88	$3,480.94
12/29/2023 4:38:21 PM	AC00407	$186.69	8,602.22	$6,758.21	$1,844.01
12/29/2023 4:30:53 PM	AC00132	$220.82	4,298.13	$1,021.17	$3,276.96
12/28/2023 5:31:03 PM	AC00239	$232.12	6,689.87	$1,101.97	$5,587.90
12/28/2023 4:46:46 PM	AC00058	$170.96	13,374.89	$7,360.47	$6,014.42
12/28/2023 4:27:12 PM	AC00411	$111.55	12,221.17	$7,317.85	$4,903.32
Total		**$252,457.94**	**5,776,833.23**	**$2,054,110.21**	**$3,722,723.02**

Page 2: Device and IP Changes

This section tracks anomalies based on device and IP address changes. There are five cases each of device and IP changes occurring in quick succession, which could indicate fraudulent access attempts. Each change is broken down by account, highlighting those affected multiple times. The detailed log provides transparency into the specific events and values.



Device and IP Change Anomalies

5

Device Change Events

5

IP Address Change Events

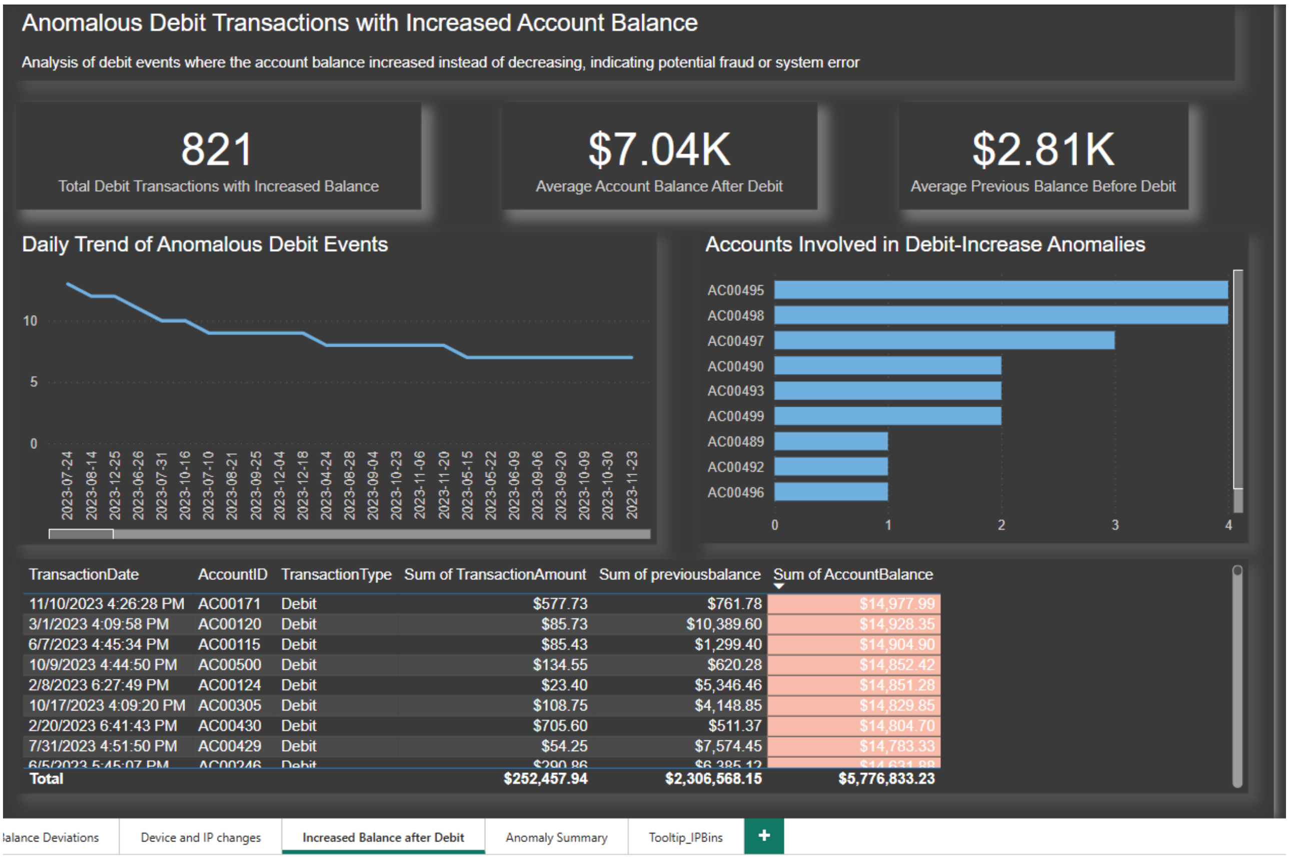
Transactions with Device Change per Account

Transactions with IP Change per Account

AccountID	Date	Current IP	Previous IP	Current device	Previous device
AC00213	4/3/2023 4:41:47 PM	163.129.70.210	98.39.212.221	D000609	D000280
AC00030	5/10/2023 5:56:31 PM	82.51.236.134	199.103.32.145	D000269	D000671
AC00151	6/5/2023 5:48:33 PM	93.146.251.20	21.97.154.92	D000699	D000318
AC00010	6/26/2023 4:16:50 PM	193.108.17.115	115.30.82.168	D000622	D000430
AC00114	10/23/2023 4:58:04 PM	16.128.130.153	121.67.144.20	D000602	D000522

Page 3: Increased Balance After Debit

Anomalies where account balances increased after a debit transaction are visualized here. This counterintuitive behaviour suggests either a system fault or manipulation. The dashboard shows a timeline of these events, identifies key affected accounts, and summarizes the transactional details contributing to this anomaly.



Anomalous Debit Transactions with Increased Account Balance

Analysis of debit events where the account balance increased instead of decreasing, indicating potential fraud or system error

821
Total Debit Transactions with Increased Balance

$7.04K
Average Account Balance After Debit

$2.81K
Average Previous Balance Before Debit

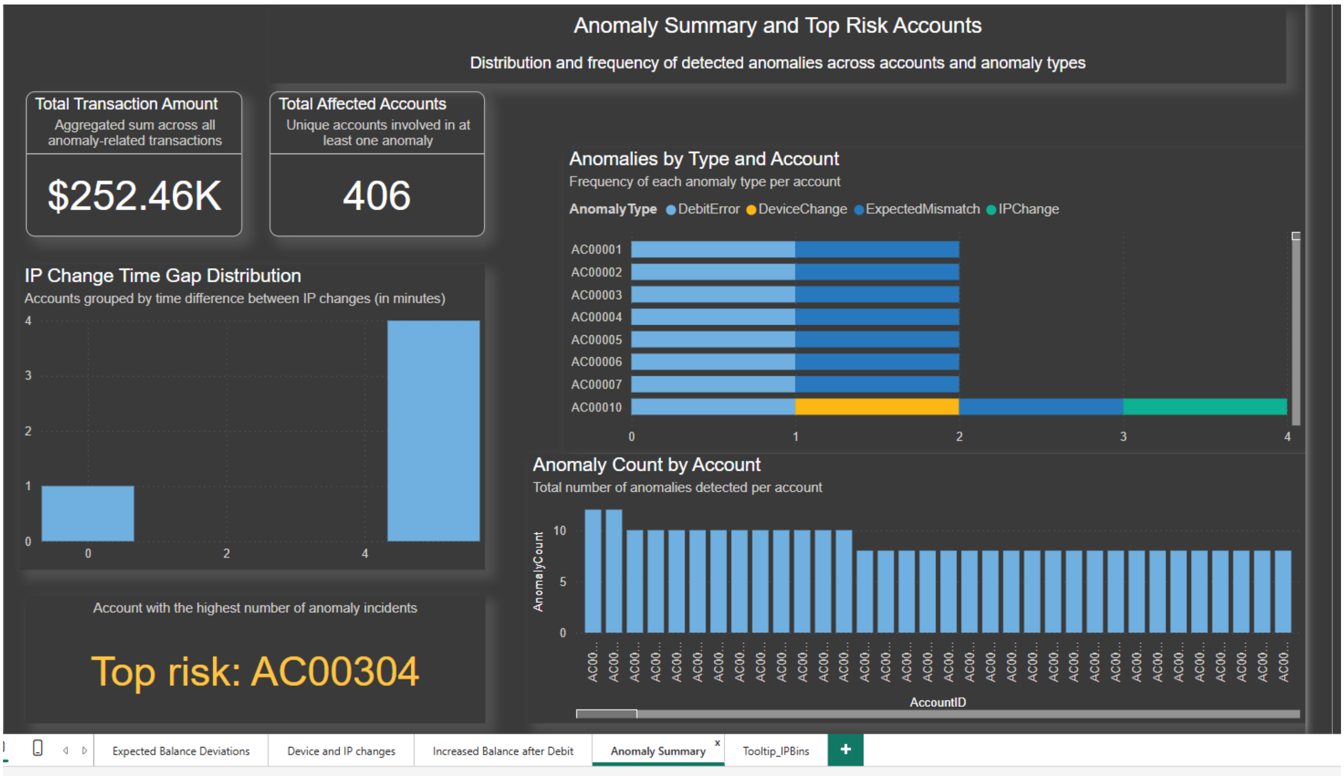
Daily Trend of Anomalous Debit Events

Accounts Involved in Debit-Increase Anomalies

TransactionDate	AccountID	TransactionType	Sum of TransactionAmount	Sum of previousbalance	Sum of AccountBalance
11/10/2023 4:26:28 PM	AC00171	Debit	$577.73	$761.78	$14,977.99
3/1/2023 4:09:58 PM	AC00120	Debit	$85.73	$10,389.60	$14,928.35
6/7/2023 4:45:34 PM	AC00115	Debit	$85.43	$1,299.40	$14,904.90
10/9/2023 4:44:50 PM	AC00500	Debit	$134.55	$620.28	$14,852.42
2/8/2023 6:27:49 PM	AC00124	Debit	$23.40	$5,346.46	$14,851.28
10/17/2023 4:09:20 PM	AC00305	Debit	$108.75	$4,148.85	$14,829.85
2/20/2023 6:41:43 PM	AC00430	Debit	$705.60	$511.37	$14,804.70
7/31/2023 4:51:50 PM	AC00429	Debit	$54.25	$7,574.45	$14,783.33
6/5/2023 5:45:07 PM	AC00246	Debit	$290.86	$6,385.12	$14,631.88
Total			**$252,457.94**	**$2,306,568.15**	**$5,776,833.23**

Page 4: Anomaly Summary and Top Risk Accounts

This summary view consolidates all detected anomalies. A total transaction volume of $252.46K was flagged, affecting 406 unique accounts. IP time gap distribution shows most anomalies clustered in a narrow time frame. The top-risk account (AC00304) had the highest number of incidents. Bar charts illustrate anomaly frequency and type per account.



Anomaly Summary and Top Risk Accounts

Distribution and frequency of detected anomalies across accounts and anomaly types

Total Transaction Amount

Aggregated sum across all anomaly-related transactions

$252.46K

Total Affected Accounts

Unique accounts involved in at least one anomaly

406

IP Change Time Gap Distribution

Accounts grouped by time difference between IP changes (in minutes)

Account with the highest number of anomaly incidents

Top risk: AC00304

Anomalies by Type and Account

Frequency of each anomaly type per account

Anomaly Count by Account

Total number of anomalies detected per account

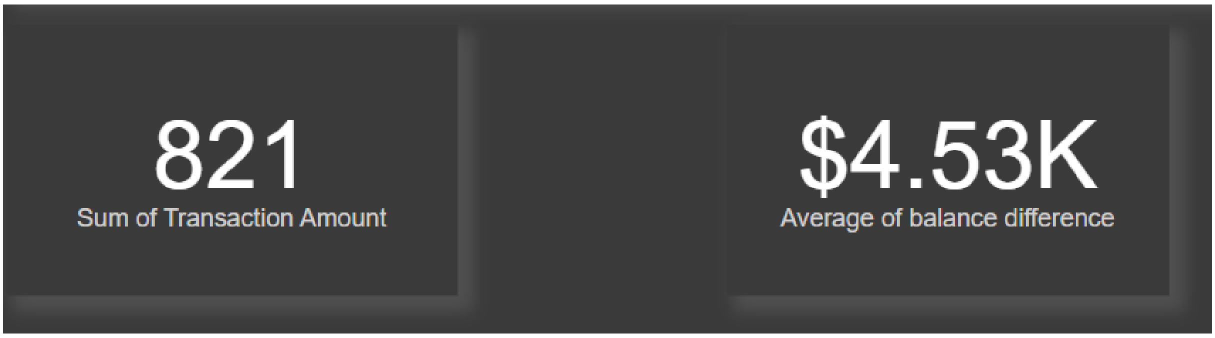
Visualizations

1. **Sum of Transaction Amount**

A total of 821 transactions were analyzed in relation to expected balance deviations. This metric reflects the volume of potentially anomalous or notable transactions within the dataset.

2. **Average of Balance Difference**

The average gap between expected and actual account balances is approximately **$4,530**. This suggests substantial discrepancies that could indicate calculation errors or suspicious activities.

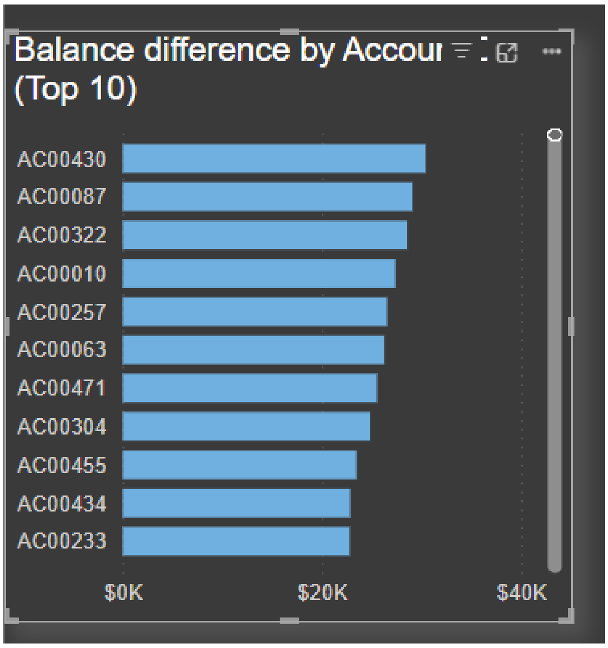


821
Sum of Transaction Amount

$4.53K
Average of balance difference

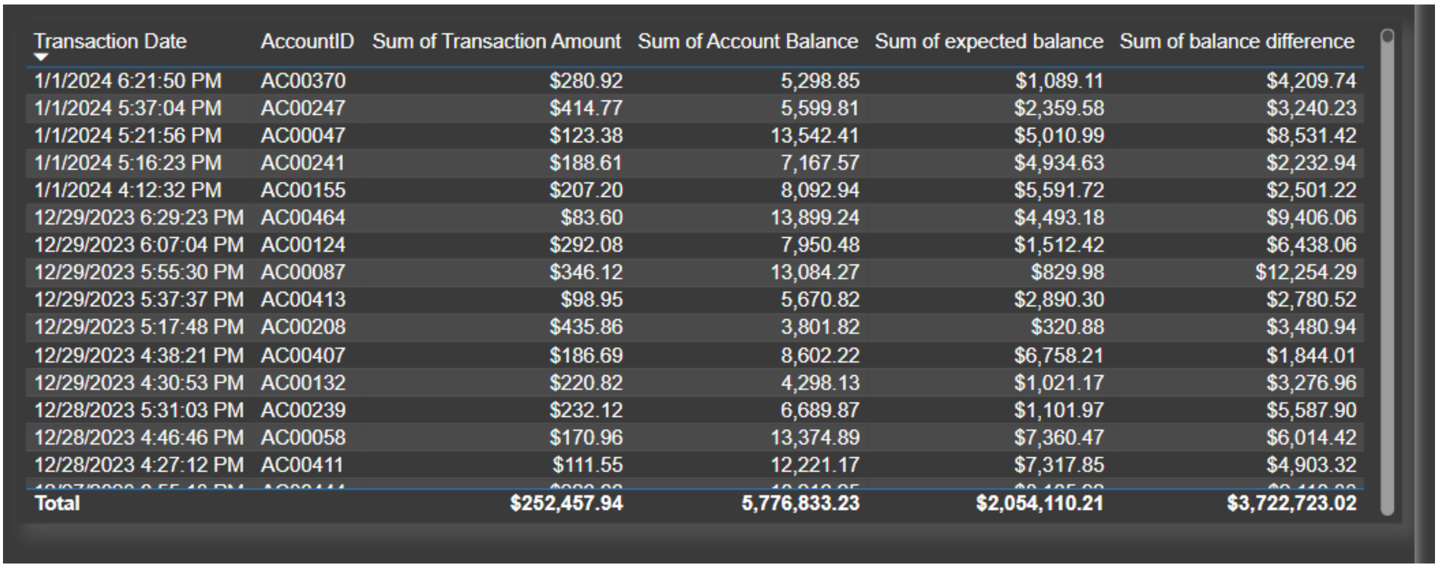
1. **Balance Difference by Account (Top 10) – Summary (Stacked Bar Chart)**

- The chart highlights the 10 accounts with the largest discrepancies between actual and expected balances.
- Account AC00430 shows the highest total deviation, exceeding $35K.
- All listed accounts have discrepancies above $20K, indicating repeated or high-impact anomalies.
- These deviations could result from transaction recording issues or be signs of fraudulent behaviour requiring further investigation.



2. Detailed Transaction and Deviations – Summary

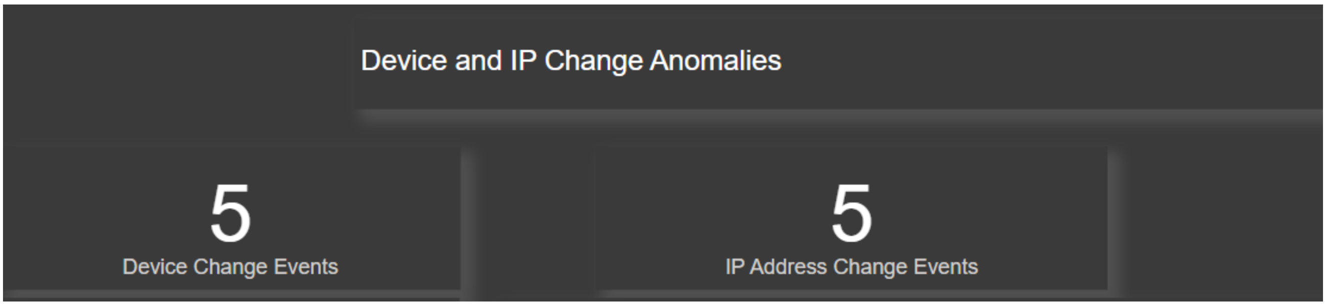
- The table presents individual transactions with discrepancies between the actual account balance and the expected value.
- Several accounts, such as **AC00087** and **AC00304**, exhibit balance differences exceeding **$10K**, raising potential red flags.
- Total anomalies amount to **$3.72M** in cumulative balance difference across all accounts.
- These gaps suggest the need for targeted review of transaction logic or monitoring for fraudulent activity.



Transaction Date	AccountID	Sum of Transaction Amount	Sum of Account Balance	Sum of expected balance	Sum of balance difference
1/1/2024 6:21:50 PM	AC00370	$280.92	5,298.85	$1,089.11	$4,209.74
1/1/2024 5:37:04 PM	AC00247	$414.77	5,599.81	$2,359.58	$3,240.23
1/1/2024 5:21:56 PM	AC00047	$123.38	13,542.41	$5,010.99	$8,531.42
1/1/2024 5:16:23 PM	AC00241	$188.61	7,167.57	$4,934.63	$2,232.94
1/1/2024 4:12:32 PM	AC00155	$207.20	8,092.94	$5,591.72	$2,501.22
12/29/2023 6:29:23 PM	AC00464	$83.60	13,899.24	$4,493.18	$9,406.06
12/29/2023 6:07:04 PM	AC00124	$292.08	7,950.48	$1,512.42	$6,438.06
12/29/2023 5:55:30 PM	AC00087	$346.12	13,084.27	$829.98	$12,254.29
12/29/2023 5:37:37 PM	AC00413	$98.95	5,670.82	$2,890.30	$2,780.52
12/29/2023 5:17:48 PM	AC00208	$435.86	3,801.82	$320.88	$3,480.94
12/29/2023 4:38:21 PM	AC00407	$186.69	8,602.22	$6,758.21	$1,844.01
12/29/2023 4:30:53 PM	AC00132	$220.82	4,298.13	$1,021.17	$3,276.96
12/28/2023 5:31:03 PM	AC00239	$232.12	6,689.87	$1,101.97	$5,587.90
12/28/2023 4:46:46 PM	AC00058	$170.96	13,374.89	$7,360.47	$6,014.42
12/28/2023 4:27:12 PM	AC00411	$111.55	12,221.17	$7,317.85	$4,903.32
Total		**$252,457.94**	**5,776,833.23**	**$2,054,110.21**	**$3,722,723.02**

3. Device and IP Change Anomalies – KPI Summary

- There are **5 recorded device change events**, indicating user access from a new or altered device.
- Additionally, **5 IP address change events** were identified, which may suggest unusual access behaviour or possible account misuse.
- The equal count across both metrics implies a strong overlap and may warrant further investigation of simultaneous device and location shifts.



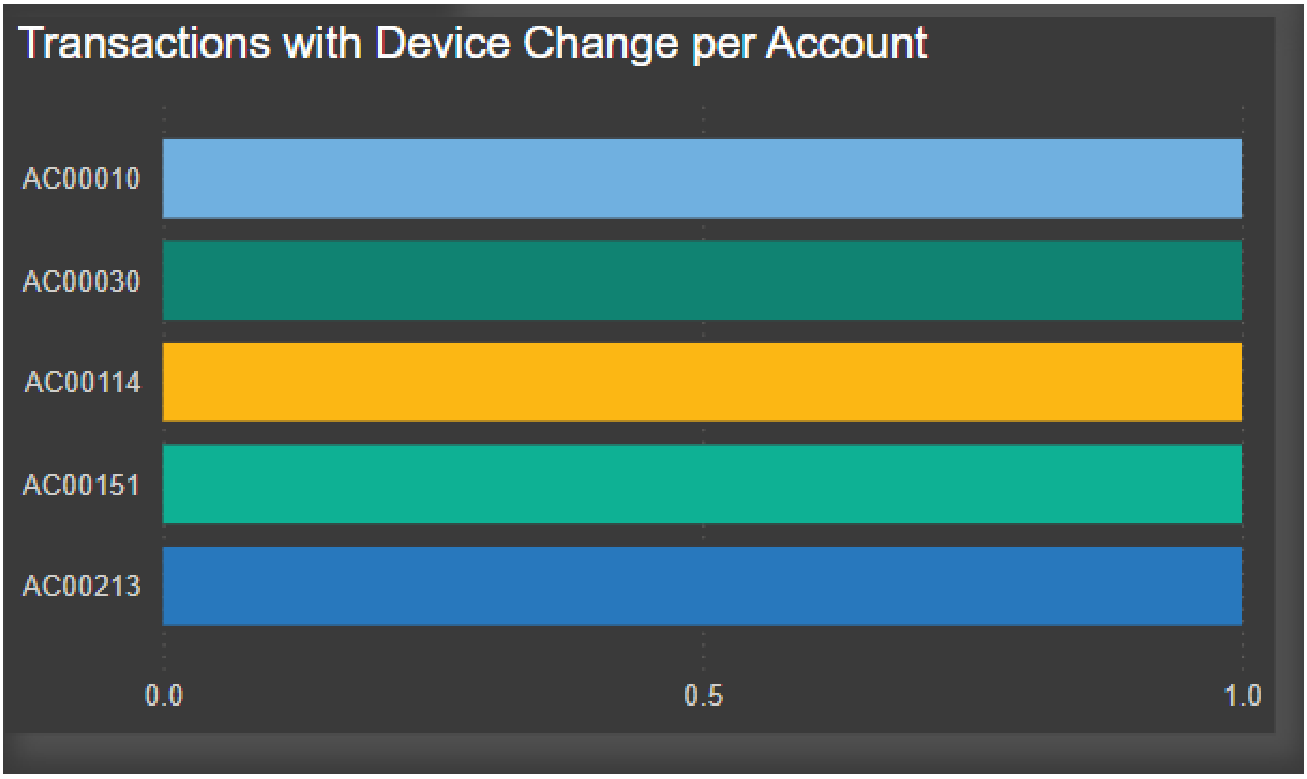
Device and IP Change Anomalies

5
Device Change Events

5
IP Address Change Events

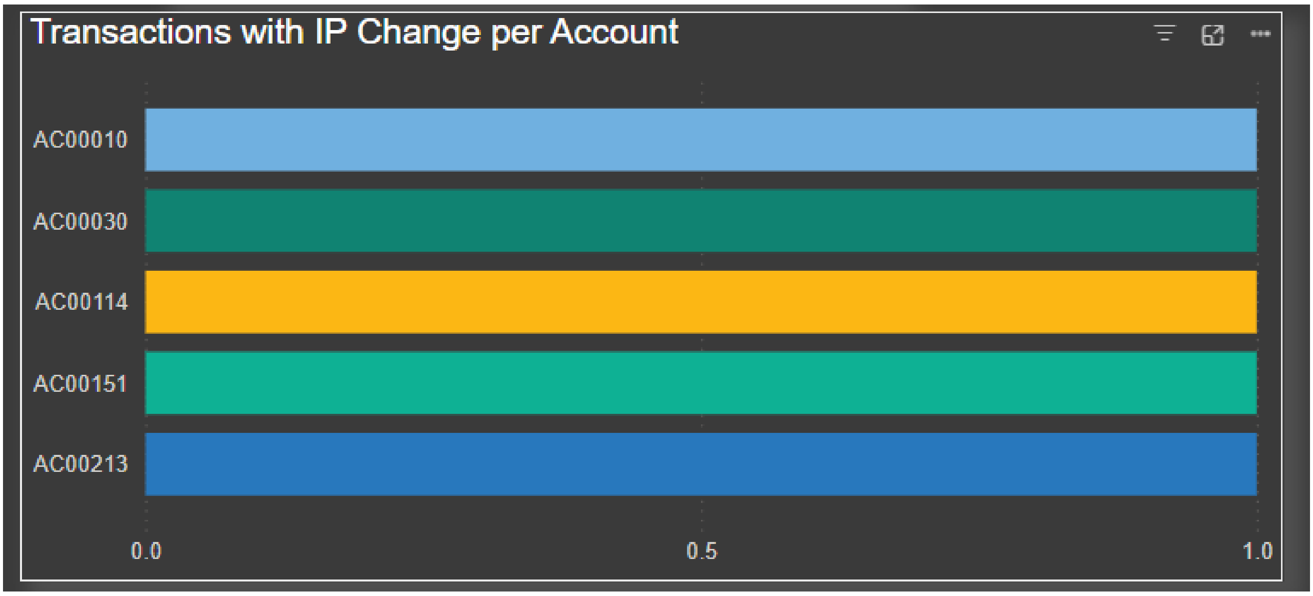
4. Transactions with Device Change per Account – Summary

- Each of the five listed accounts experienced exactly **one device change event**, suggesting isolated but notable shifts in user access patterns.
- The uniform bar lengths indicate consistent anomaly frequency across the accounts, rather than repeated or excessive switching.
- This uniformity may point to coordinated behaviour or a system-wide trigger prompting device changes across multiple users.
- Accounts **AC00114**, **AC00213**, and **AC00030** should be reviewed further if linked to other anomaly types.



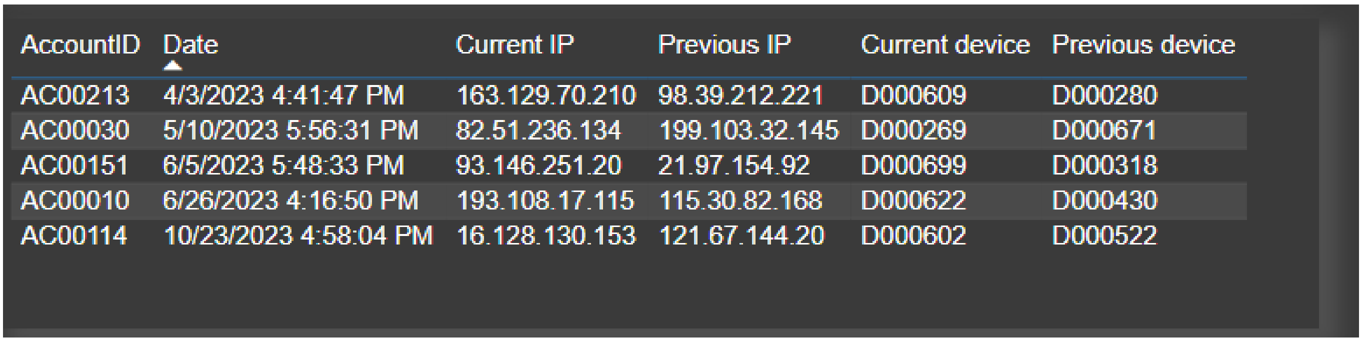
5. **Transactions with IP Change per Account – Summary**

   - All five accounts (**AC00010**, **AC00030**, **AC00114**, **AC00151**, **AC00213**) recorded **exactly one IP address change event**, mirroring the device change anomaly pattern.
   - The uniform count suggests these were singular occurrences rather than repeated location shifts but still warrant attention.
   - Combined device and IP changes in the same accounts may indicate potentially suspicious login behaviour or compromised access.
   - These changes could result from user travel, VPN usage, or fraudulent attempts—further contextual investigation is recommended.



6. Detailed Device and IP Change Log – Summary

- Each of the five flagged accounts shows a simultaneous change in both device ID and IP address during a single transaction.
- The IP address changes span various ranges, suggesting possible location shifts or the use of anonymization tools.
- Device ID transitions (e.g., from D000522 to D000602) reflect new hardware or re-registrations, which could be benign or indicative of account compromise.
- Timestamp alignment of changes further supports the need for correlation analysis to distinguish between user behaviour and potential fraud.

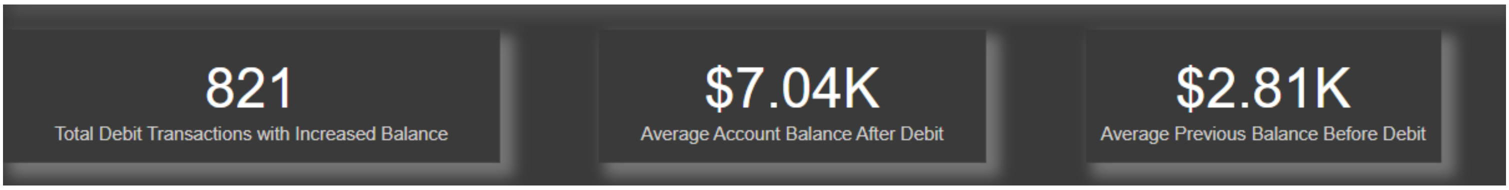


AccountID	Date	Current IP	Previous IP	Current device	Previous device
AC00213	4/3/2023 4:41:47 PM	163.129.70.210	98.39.212.221	D000609	D000280
AC00030	5/10/2023 5:56:31 PM	82.51.236.134	199.103.32.145	D000269	D000671
AC00151	6/5/2023 5:48:33 PM	93.146.251.20	21.97.154.92	D000699	D000318
AC00010	6/26/2023 4:16:50 PM	193.108.17.115	115.30.82.168	D000622	D000430
AC00114	10/23/2023 4:58:04 PM	16.128.130.153	121.67.144.20	D000602	D000522

7. KPI Cards – Anomalous Debit Transactions with Increased Balance (Page 3)

- **821 anomalous debit transactions** were identified where the account balance *increased* rather than decreased, contrary to expected behavior.

- The **average post-debit account balance** across these events is approximately **$7.04K**, indicating high-value accounts.
- Surprisingly, the **average pre-debit balance** is much lower at **$2.81K**, which further supports the presence of unusual or potentially fraudulent activity.

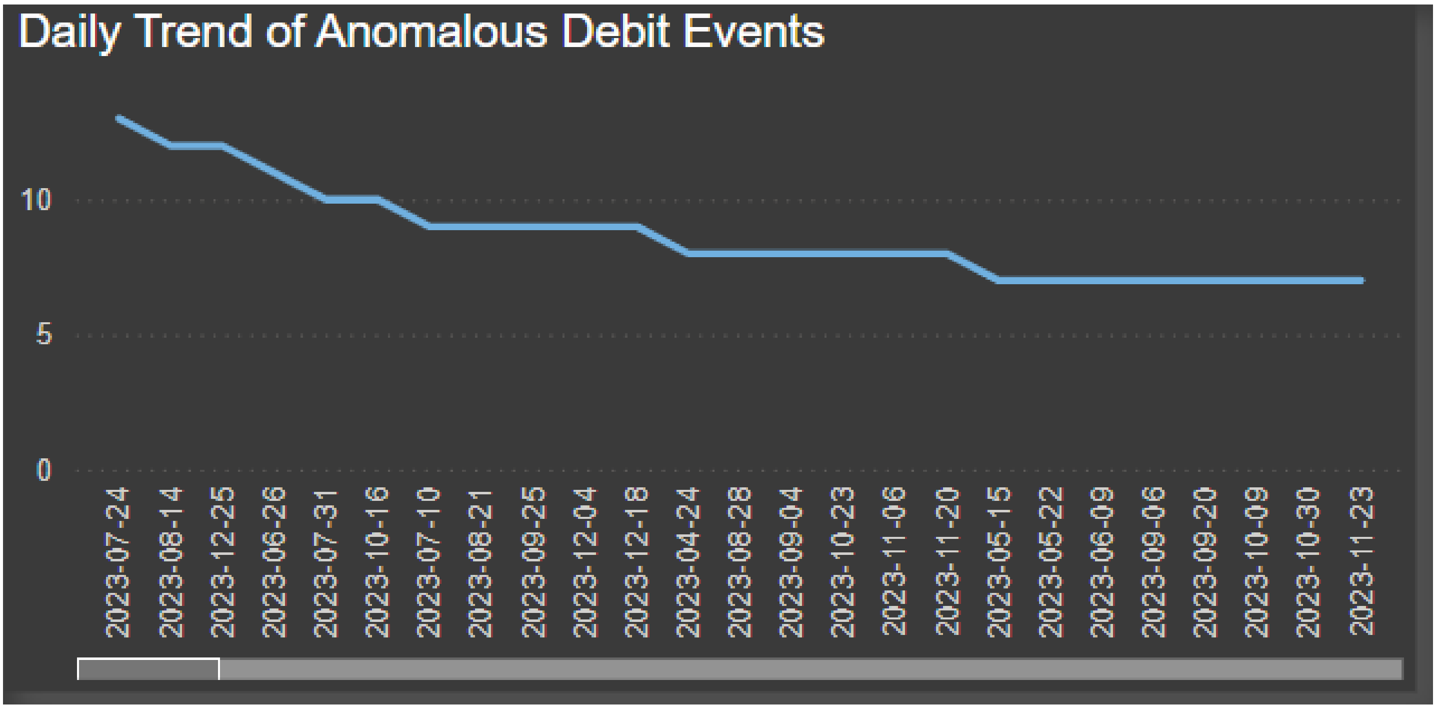


821
Total Debit Transactions with Increased Balance

$7.04K
Average Account Balance After Debit

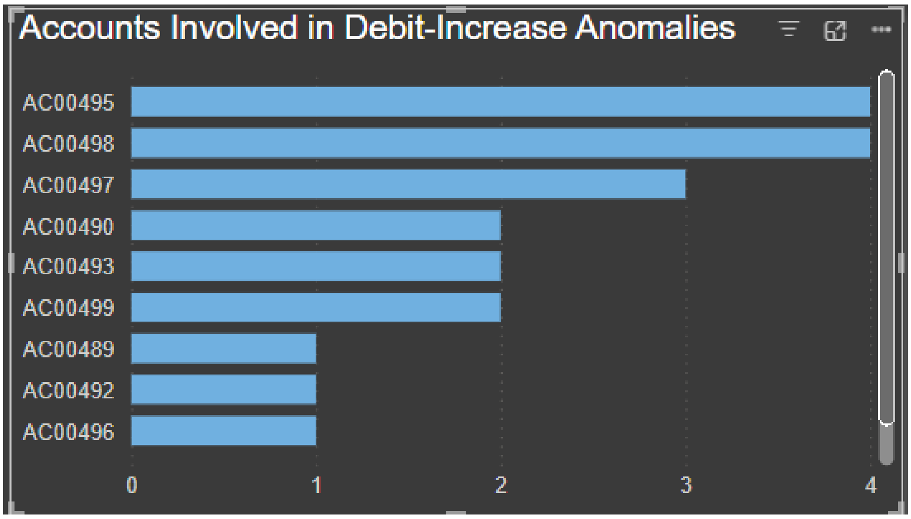
$2.81K
Average Previous Balance Before Debit

8. **Line Chart: Daily Trend of Anomalous Debit Events**
    - The number of anomalous debit transactions shows a **gradual decline over time**, suggesting reduced occurrence or improved controls.
    - Initial peak activity was observed around **July 2023**, with **12+ events per day**, dropping to **7 events** by late 2023.
    - The **flat tail** in recent months may indicate stabilization or consistent detection efforts.
    - This trend can reflect seasonal behaviour or the impact of anomaly detection interventions.



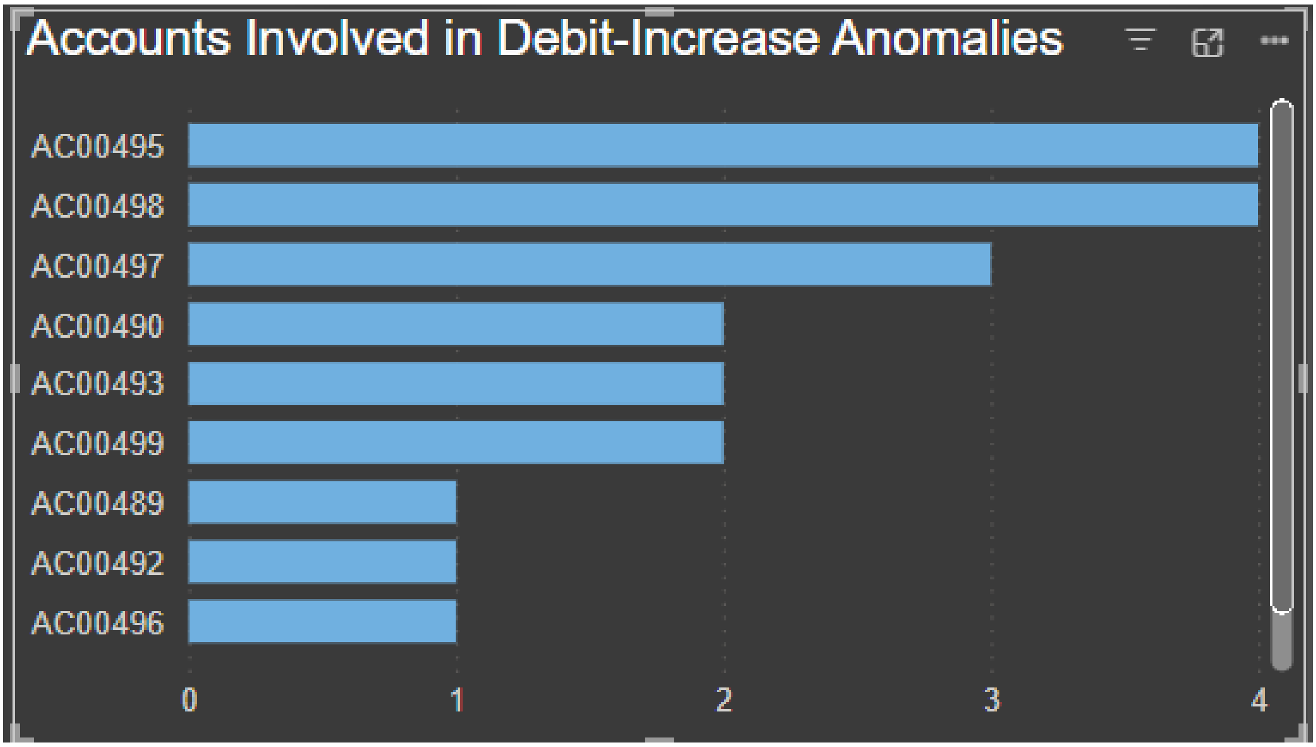
9. Bar Chart: Accounts Involved in Debit-Increase Anomalies

- The chart highlights accounts most frequently involved in suspicious debit transactions where balances increased post-transaction.
- **AC00495** and **AC00498** are the most affected accounts, each associated with 4 anomaly cases.
- The top five accounts collectively contribute to a significant portion of the irregular activity, signalling a need for targeted investigation.
- These patterns can help prioritize audit and fraud analysis efforts on high-risk users.



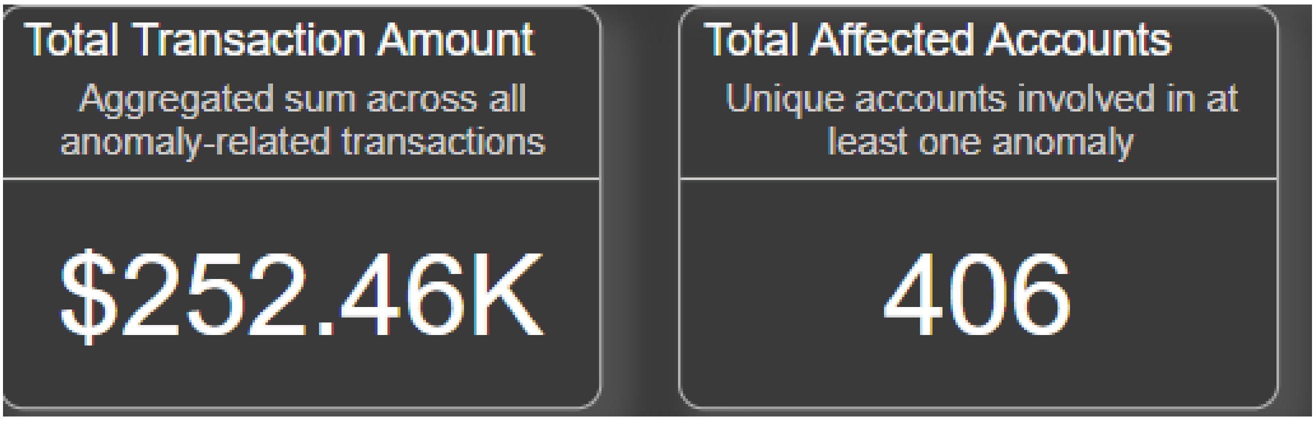
10. Detailed Log of Debit Anomalies (Table)

- This table shows **individual debit transactions** where the **account balance increased** after the transaction - an unexpected behaviour for debits.
- For example, on 11/10/2023, account **AC00171** had a debit of **$577.73**, yet the balance increased from **$761.78 to $14,977.99**.
- Several other accounts (e.g., **AC00120**, **AC00430**) exhibit similar unusual jumps in balance post-debit.
- The total post-debit balance across all entries is over **$5.77** million, compared to a pre-debit total of **$2.3** million, reinforcing the severity of these anomalies.



11. KPI Cards – Anomaly Summary (Page 4)

- The total value of transactions flagged with anomalies amounts to **$252.46K**, highlighting the potential financial exposure.
- **406** unique accounts have been involved in at least one anomaly, indicating a relatively wide distribution of issues across the dataset.
- These metrics help quantify both the monetary impact and account-level spread of anomalous activity within the dataset.



Total Transaction Amount

Aggregated sum across all anomaly-related transactions

$252.46K

Total Affected Accounts

Unique accounts involved in at least one anomaly

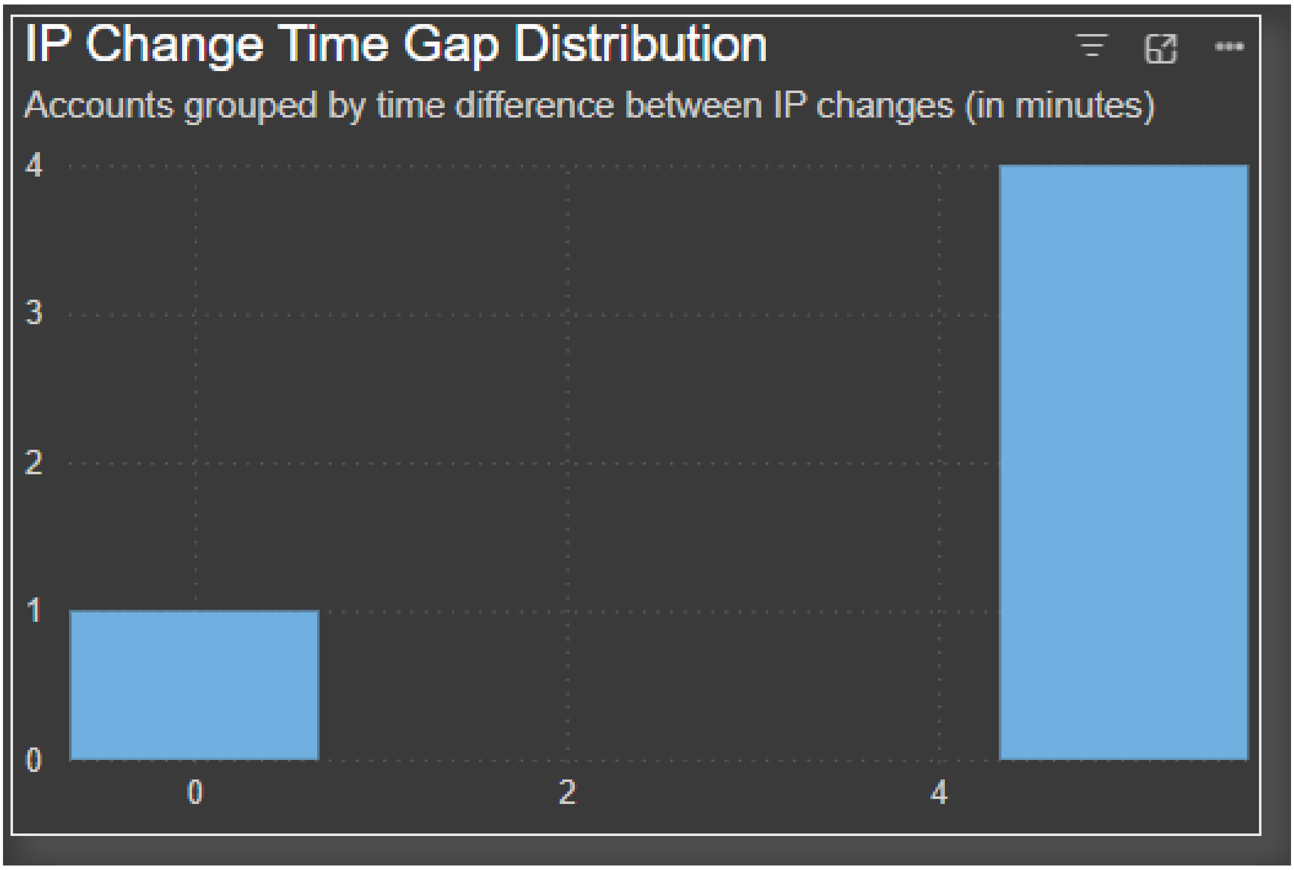
406

12. Anomalies by Type and Account

- This stacked bar chart shows the distribution of anomaly types across individual accounts.
- The most common anomaly types include **DebitError**, **ExpectedMismatch**, and **IPChange**.
- Account **AC0010** stands out, being affected by all four anomaly types, including a device change.
- This view helps prioritize investigation by highlighting both frequency and diversity of anomalies per account.

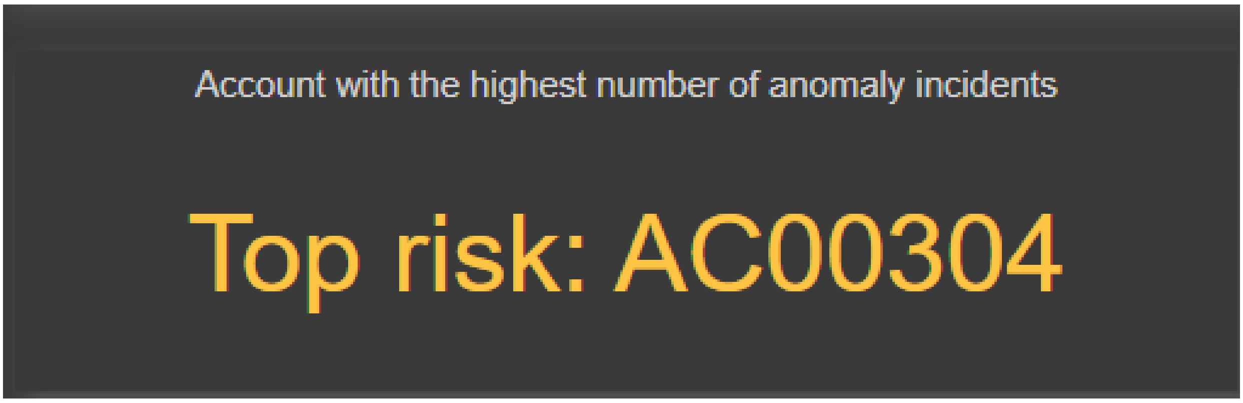
13. IP Change Time Gap Distribution (Histogram)

- This histogram visualizes how quickly IP address changes occurred between transactions for different accounts.
- Most accounts (4 out of 5) experienced an IP change within the **4–6**-minute range, which may indicate automated activity.
- One account had no delay (**0 minutes**) between IP changes, suggesting a possible simultaneous multi-IP login.
- This distribution can be useful in flagging unusual access patterns that merit further investigation.



14. Top Risk Account

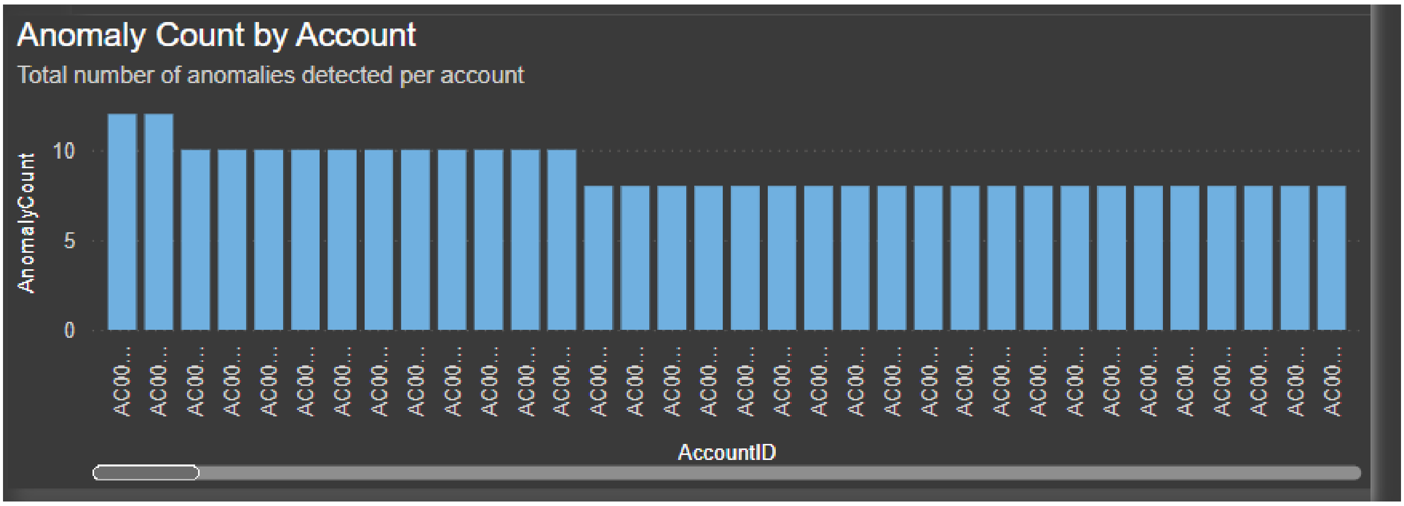
- Account **AC00304** was identified as the highest-risk profile.
- It recorded the largest number of anomaly incidents across all anomaly types.
- This account should be prioritized for manual review or investigation, as it may indicate fraudulent behaviour or system misuse.


Account with the highest number of anomaly incidents

Top risk: AC00304

15. Anomaly Count by Account

- The chart shows the total number of detected anomalies per account.
- Account AC00304 stands out with the highest count (12 anomalies), reinforcing its top-risk status.
- Most accounts show a consistent anomaly count between 7–10, suggesting systematic irregularities.
- A wider review of similarly high-count accounts is recommended to detect broader patterns or potential fraud networks.



Key Insights and Recommendations

- **Most anomalies are concentrated in a small subset of accounts**; targeted review of these could uncover fraud.
- **Unusual increases in balances post-debit** suggest system issues or potential insider manipulation.
- **Frequent device and IP changes** over short time intervals indicate unauthorized access attempts.
- We recommend implementing tighter security monitoring, real-time anomaly alerts, and automated validation checks to reduce risk.
- While multiple IP address changes may raise suspicion, they can also result from legitimate technical issues, such as device resets or network reassignments. Cross-verification is advised.