Pioneer Trust Bank

SQL-Based Fraud Detection in Banking

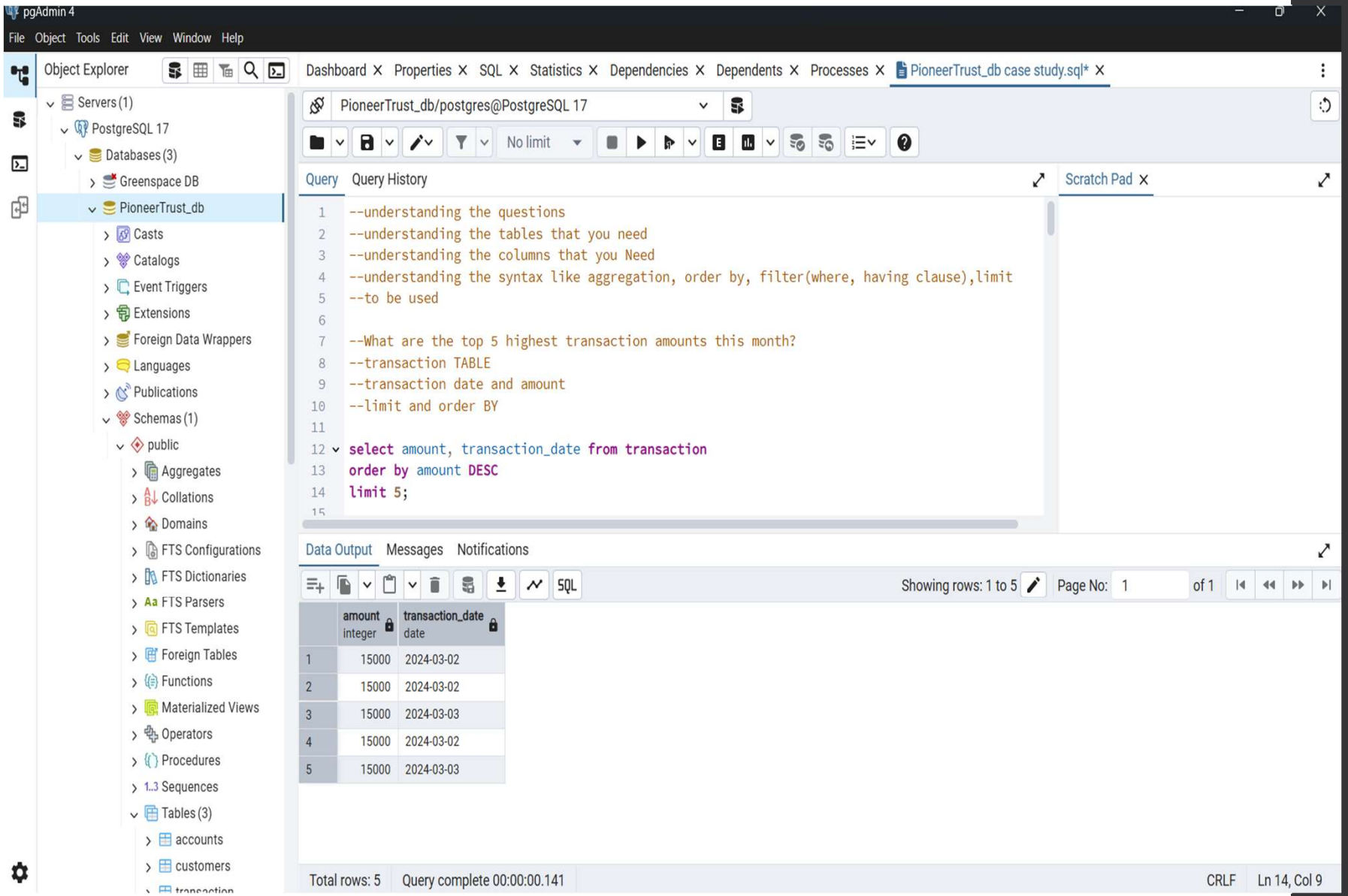
Osaroh Ekhoragbon

May 19, 2025

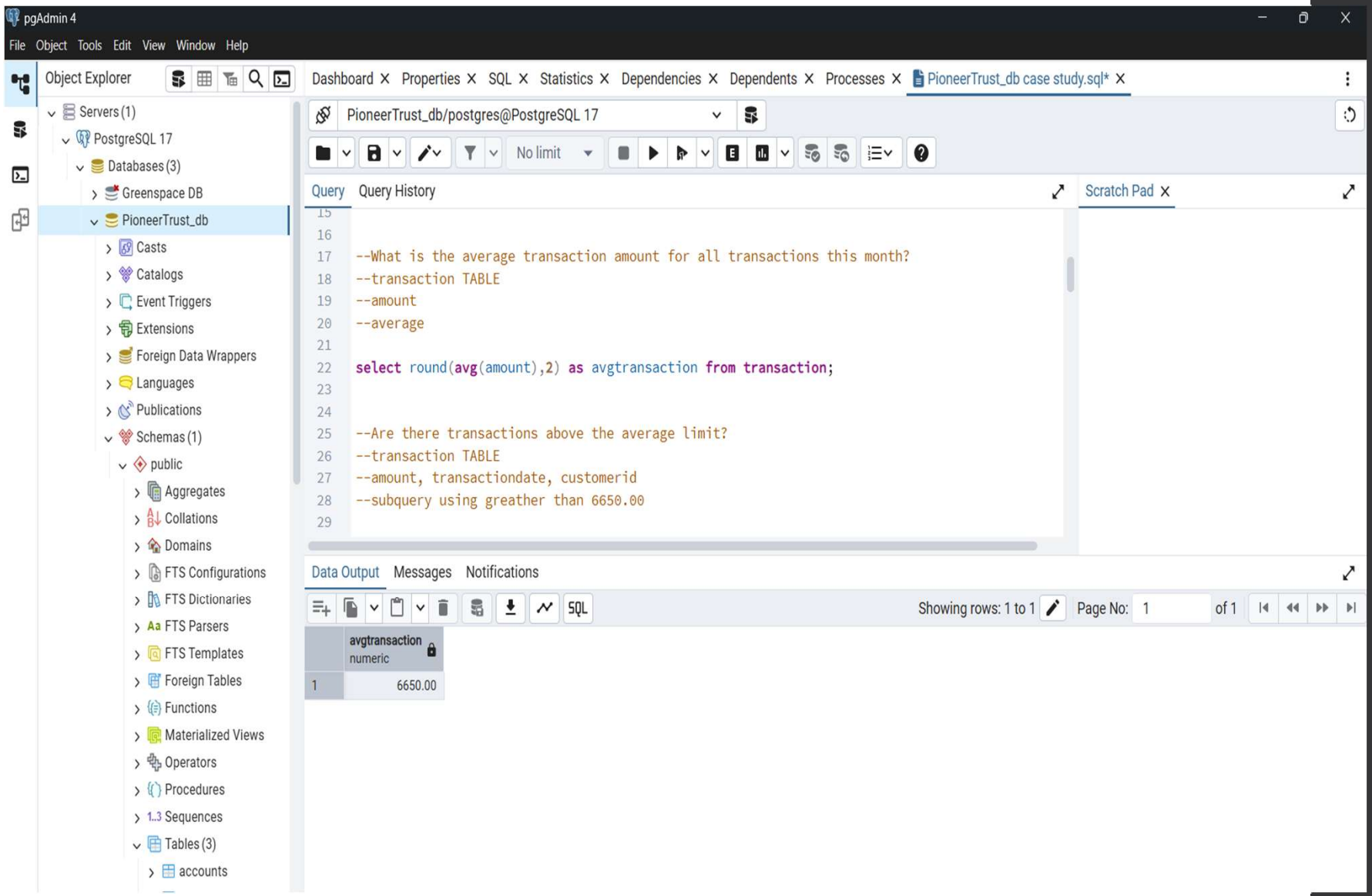
Business Overview

- **Pioneer Trust Bank is a financial institution facing a surge in fraudulent activities across customer transactions. The existing fraud detection system is inadequate for real-time analysis, leading to financial loss and reduced customer trust.**
- **This project applies SQL-based analytics on historical transaction data to identify high-risk activities and deliver strategic insights for fraud prevention.**
- **This demonstrates the potential of structured SQL analysis in driving actionable risk mitigation strategies for the banking industry.**

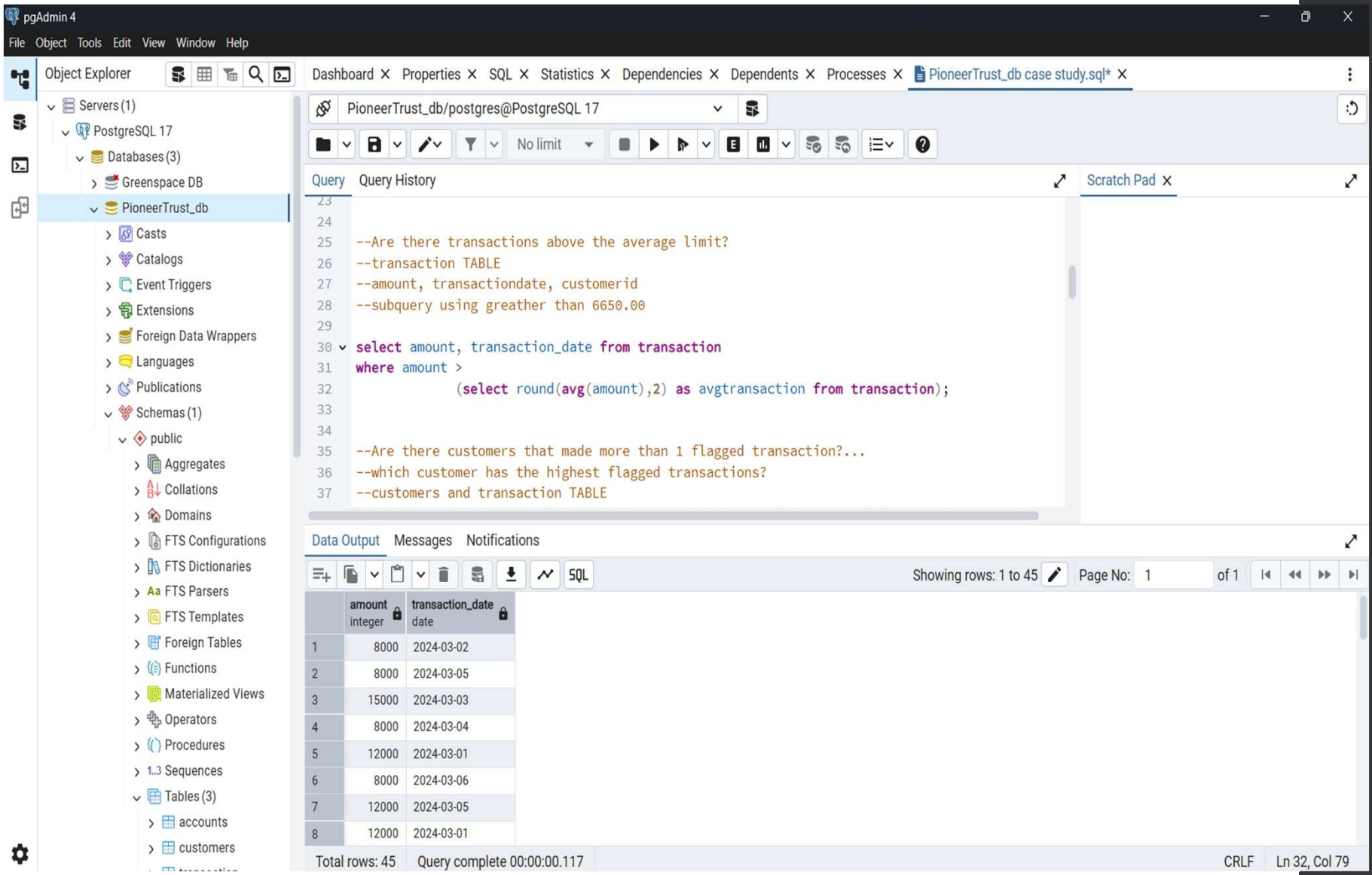
High Transaction Amounts



High Transaction Amounts



High Transaction Amounts



Insight: High Transaction Amounts

Objectives: Identify unusually large transactions to detect potential fraudulent behavior.

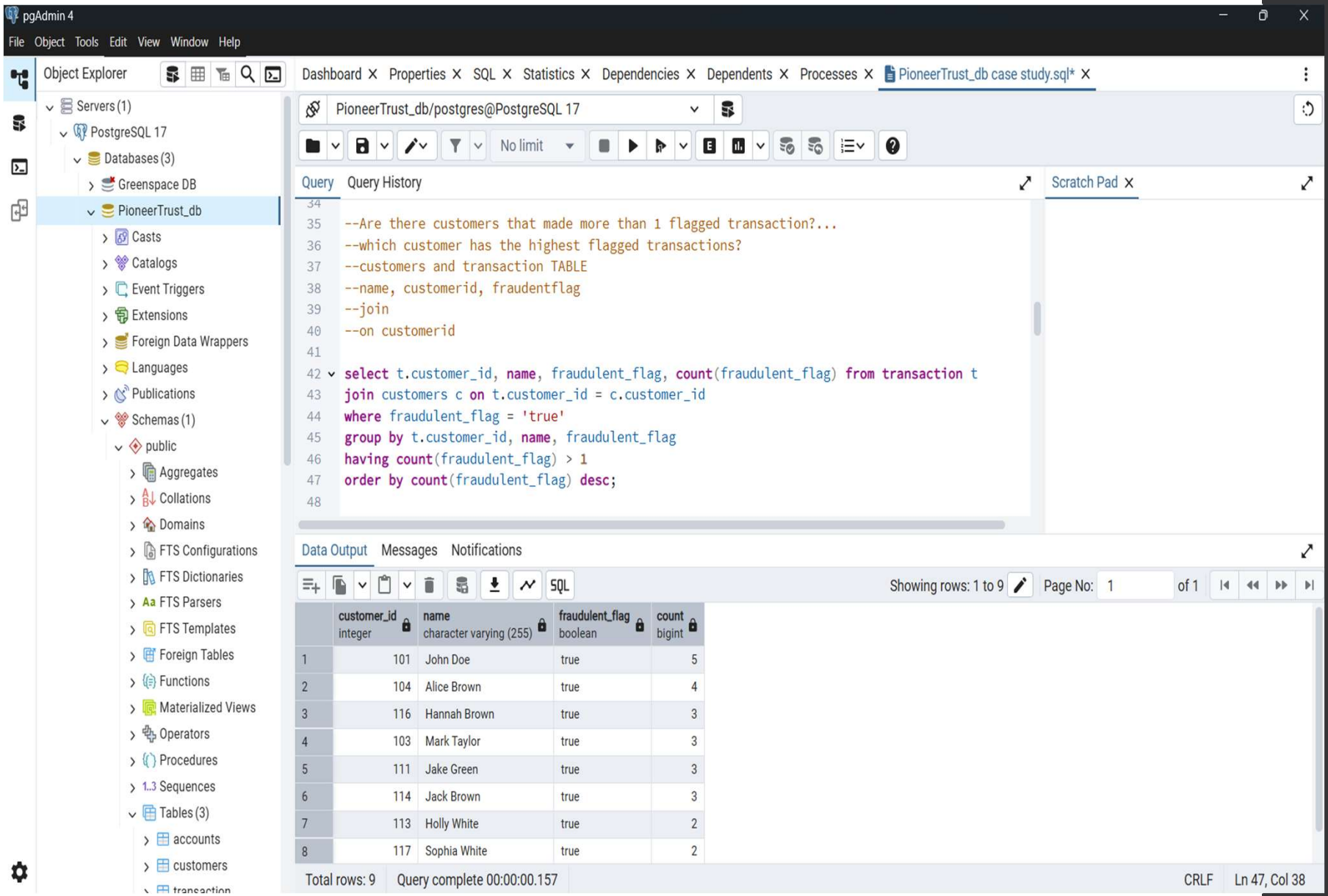
Findings:

- **The top 5 transactions, each valued at ₦15,000, revealed repeated high-value activities.**
- **The average transaction was ₦6,650 – transactions above this were flagged.**
- **Several transactions exceeded the average transaction limit, indicating high-value outliers.**

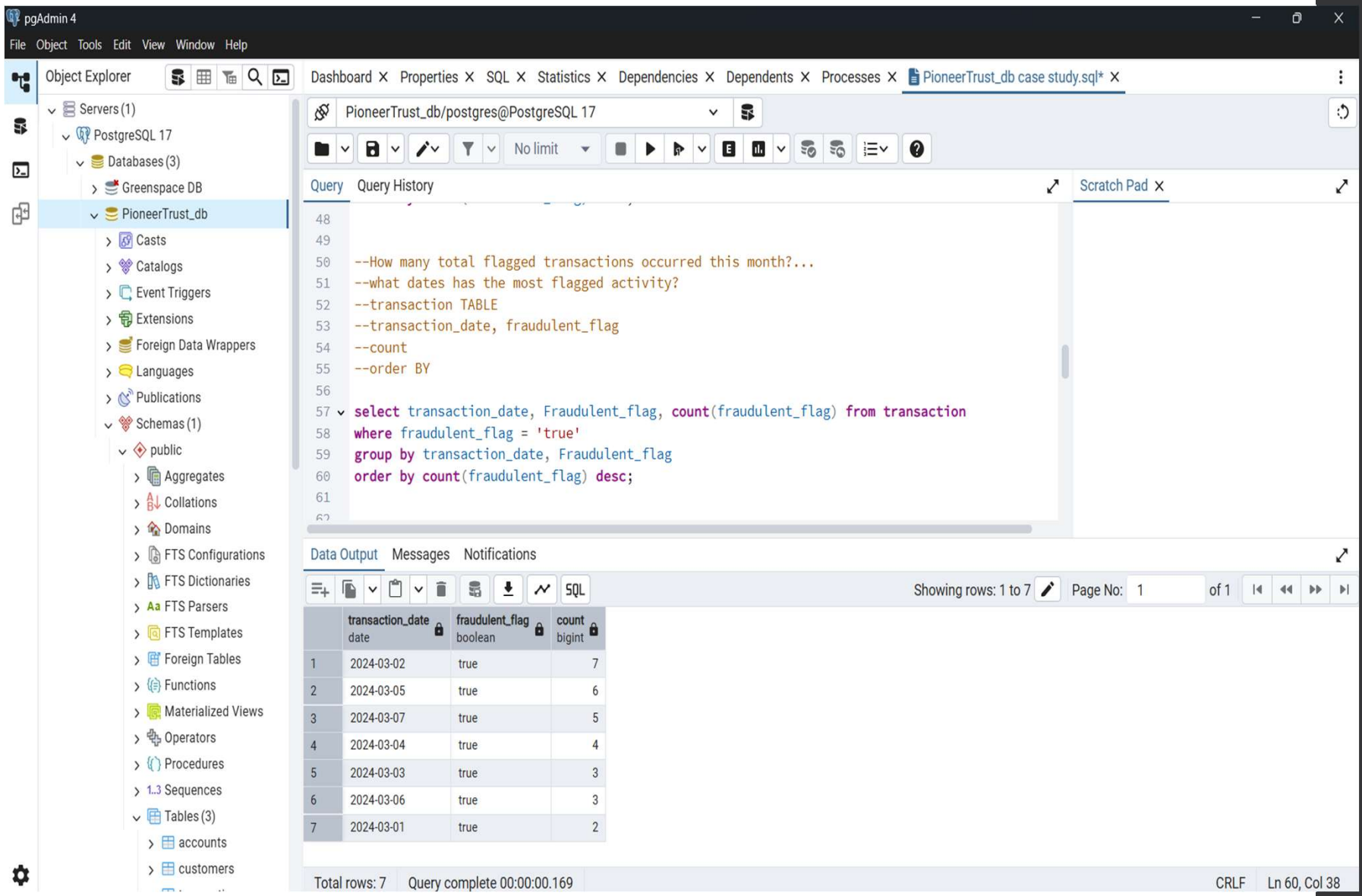
Recommendation:

- **Set automated alerts for transactions exceeding the 2x average threshold.**
- **These thresholds can be tailored to customer type and account profile.**

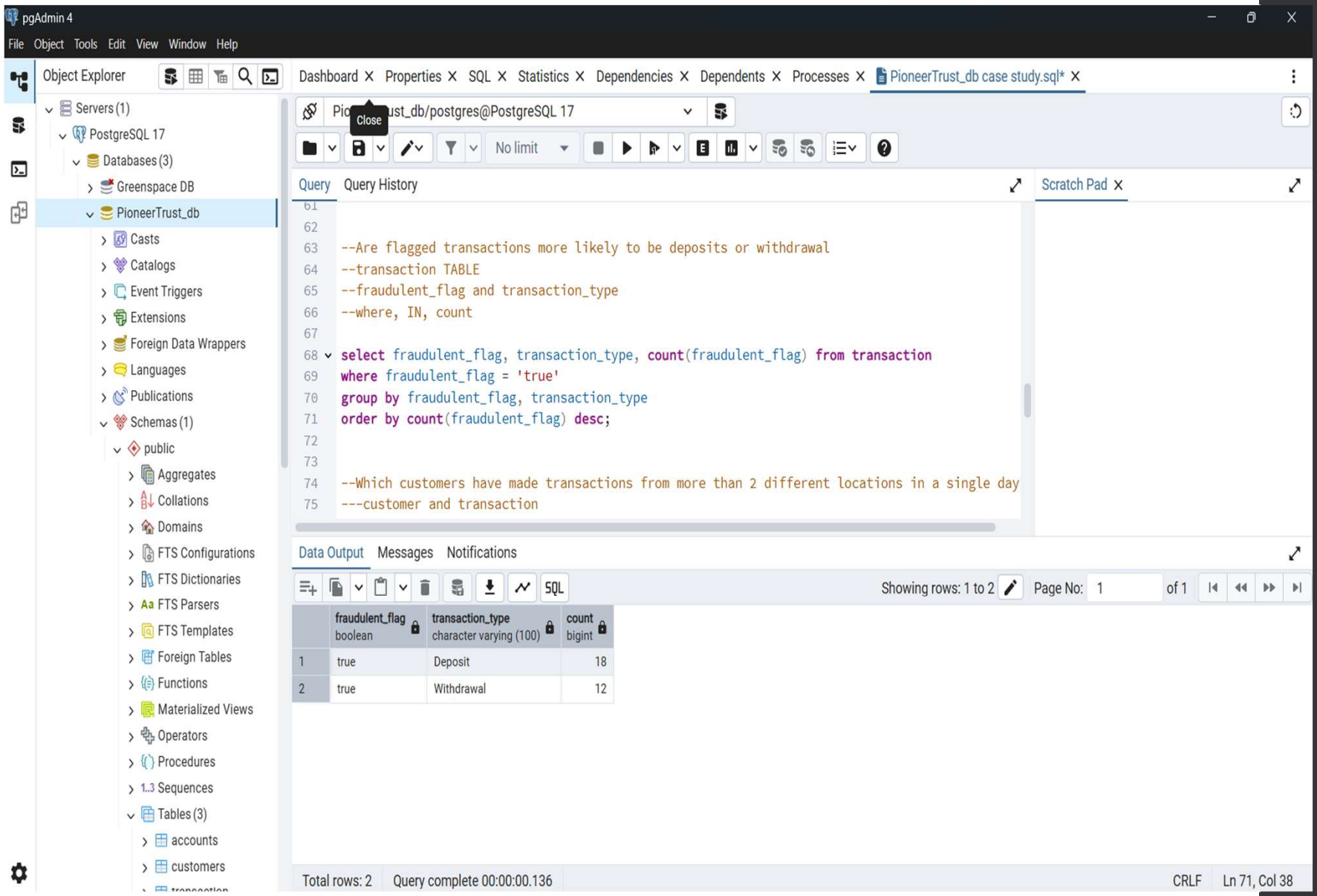
Repeat Offenders



Repeat Offenders



Repeat Offenders



Insight: Repeat Offenders

Objectives: Detect customers with multiple flagged transactions.

Finding:

Multiple customers triggered repeated fraud flags. Notably, one customer (John Doe) had 5 flagged transactions, showing a pattern of repeated suspicious activity.

Flagged transactions were more frequent on specific dates, notably March 2nd.

Deposits were more commonly flagged than withdrawals—highlighting where monitoring should be stricter.

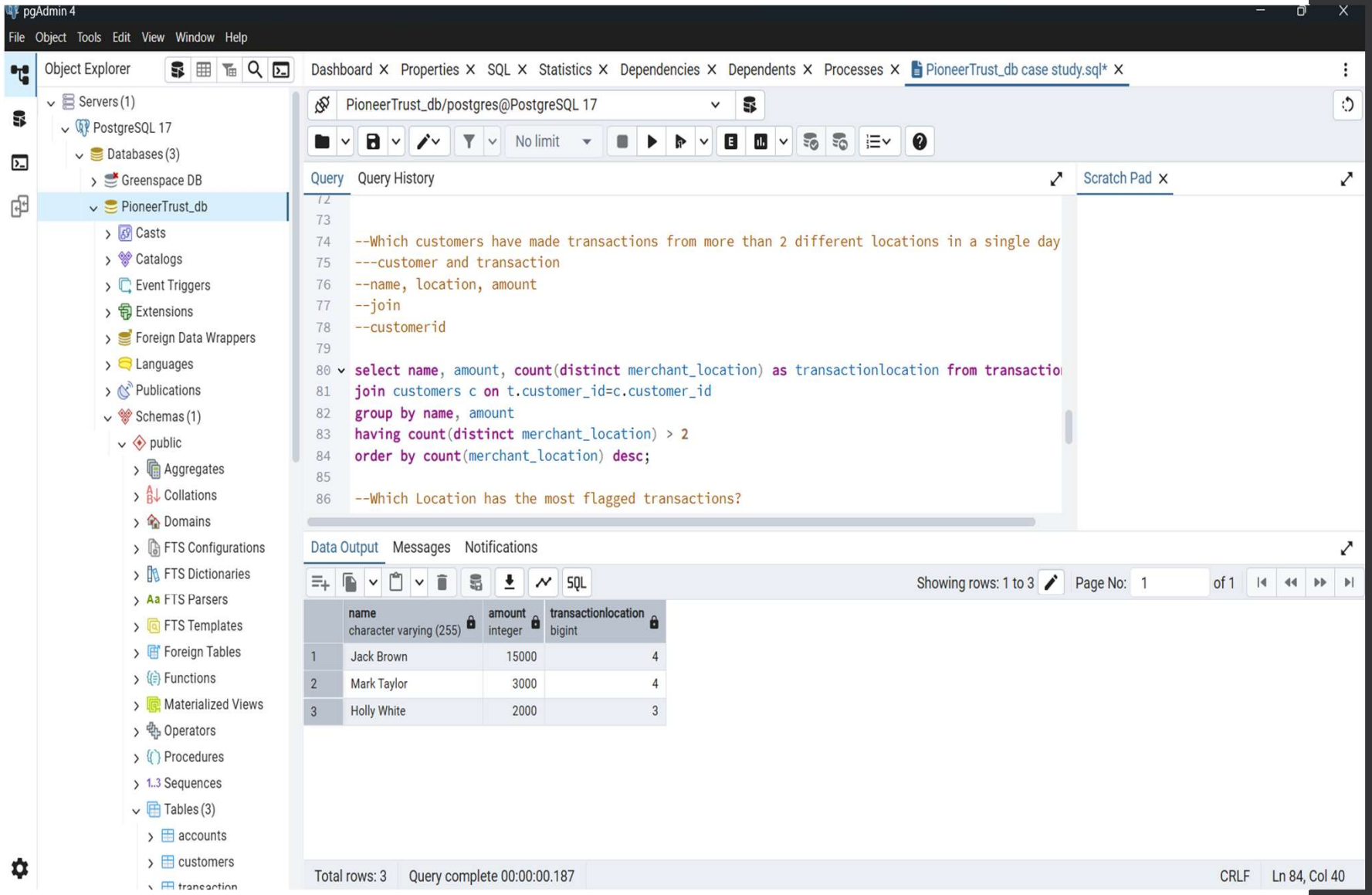
Recommendation:

Monitor high-frequency fraud customers with enhanced scrutiny.

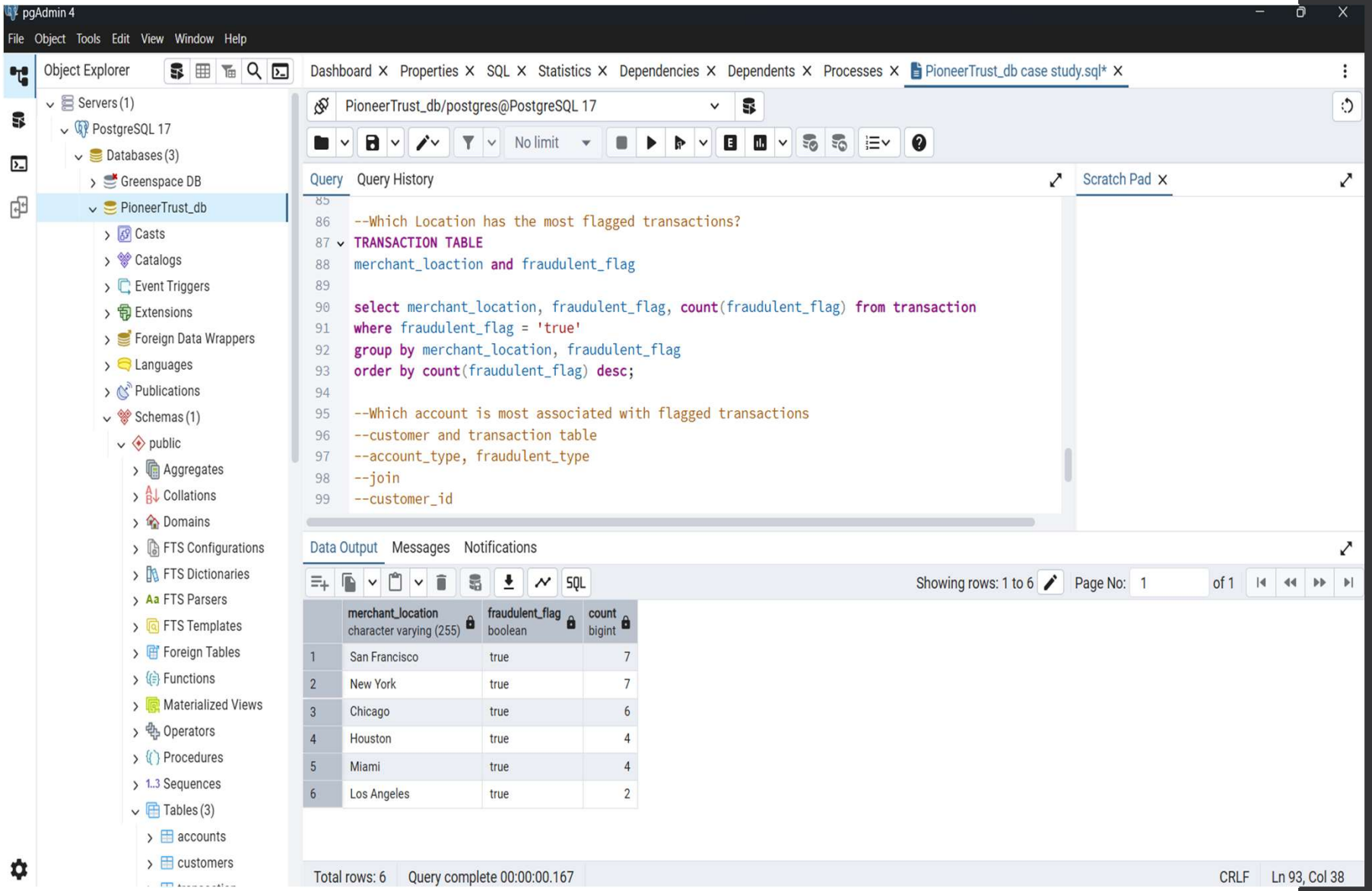
Implement profiling of frequent offenders with real-time blocking triggers.

Review KYC data and transaction histories of flagged deposits and withdrawals.

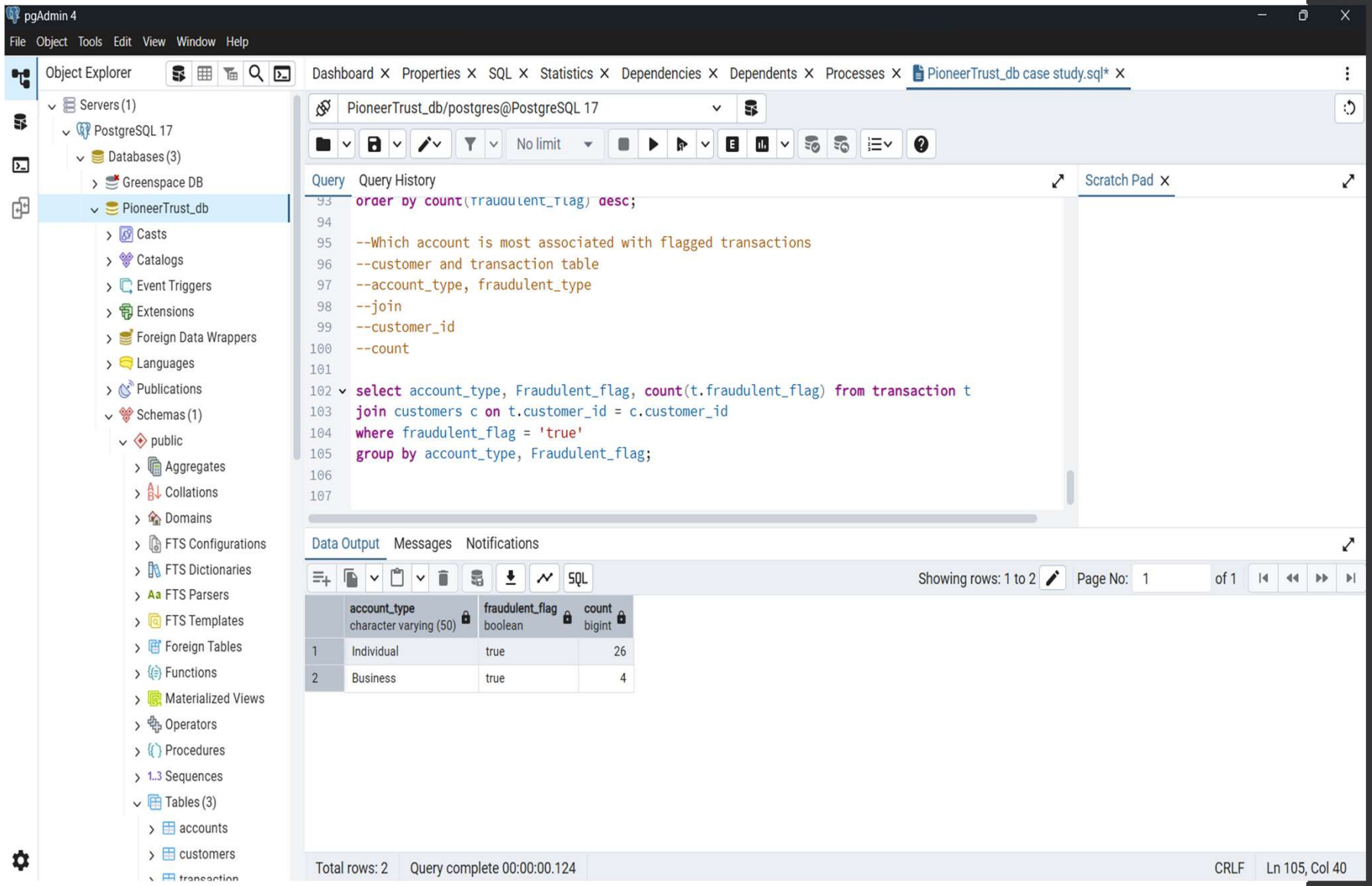
Transactions from Multiple Locations



Transactions from Multiple Locations



Transactions from Multiple Locations



Insight: Transactions from Multiple Locations

Objectives: Identify customers, account types, and transactions made from different geographical locations within short timeframes.

Finding:

- **Certain users (e.g., Jack Brown) made 4 transactions from different cities within one day.**
- **Locations like San Francisco and New York had the highest concentration of flagged transactions.**
- **Review KYC data and transaction histories of flagged Individuals.**

Recommendation:

- **Introduce geo-fencing and IP-location consistency checks.**
- **Alert system should flag abnormal travel-based transaction patterns.**
- **Introduce two-factor authentication for transactions occurring from distant or new locations.**

Conclusion & Recommendations

This project revealed critical insights using SQL on banking transaction data:

- High-value transactions often exceed normal patterns and require threshold-based alerts.
- Repeat offenders signal the need for automated profile-based blocking rules.
- Multi-location transactions suggest account compromise and warrant geographic checks.
- By combining these strategies, Pioneer Trust Bank can improve fraud detection, reduce losses, and restore customer trust.

Conclusion & Recommendations

The SQL-based analysis uncovered clear patterns of fraud risk:

- High-value and repeat transactions are key fraud indicators.
- Certain locations and individual account types are more fraud-prone.
- Time-based and behavior-based monitoring is crucial for proactive fraud detection.

Next Steps for Management

- Integrate automated alert systems for high-risk behaviors.
- Enhance fraud prevention systems using geolocation and behavioral analytics.
- Invest in staff training for fraud pattern recognition and anomaly detection.


FRAUD
PREVENTION