Bank Transaction Fraud Detection

Machine Learning Model Performance Report - Medium Dataset

Generated on: September 29, 2025

Executive Summary

This report presents the results of machine learning models developed to detect suspicious transactions in the Bank Medium dataset. Two models were evaluated: Logistic Regression and XGBoost. The medium dataset presents a more challenging class imbalance scenario with only 0.57% suspicious transactions. Both models achieved good performance with ROC AUC scores above 0.78, demonstrating capability in identifying fraudulent transactions in a more realistic production environment.

Dataset Information

Dataset: Bank Medium Dataset
Total Transactions: 15,482
Suspicious Transactions: 89 (0.57%)
Normal Transactions: 15,393 (99.43%)
Features: Transaction amount, account activity patterns, geographic data, transaction types, and account metadata
Evaluation Method: Train/Test Split (80/20) + 5-Fold Cross-Validation
Class Imbalance: More severe than bank_small (0.57% vs 1.24%)

Model Parameters

Logistic Regression:
• Max iterations: 200
• Class weight: balanced
• Preprocessing: StandardScaler, OneHotEncoder
• Regularization: L2 (default)
• Note: Convergence warnings observed due to dataset size

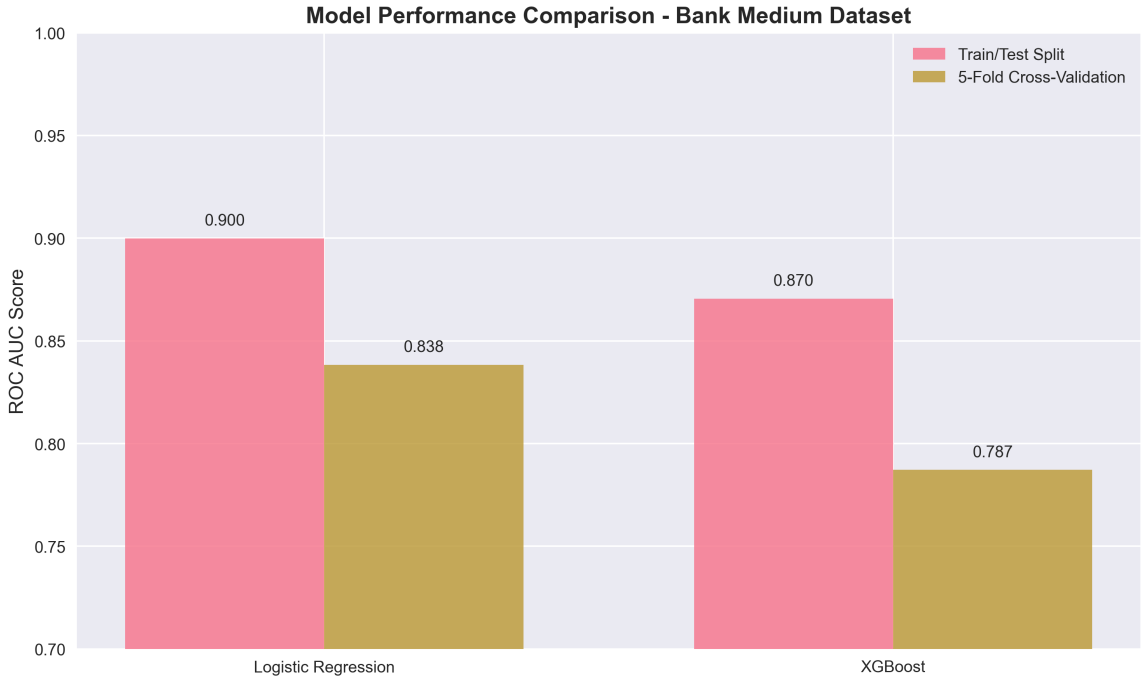
XGBoost:
• N estimators: 300
• Max depth: 6
• Learning rate: 0.08
• Subsample: 0.8
• Colsample by tree: 0.8

• Lambda regularization: 1.0
• Tree method: hist

Performance Results

Model	Method	ROC AUC	Precision	Recall	F1-Score
Logistic Regression	Train/Test	0.8999	0.017	0.944	0.032
Logistic Regression	5-Fold CV	0.8384	0.014	0.764	0.028
XGBoost	Train/Test	0.8705	1.000	0.278	0.435
XGBoost	5-Fold CV	0.7872	0.750	0.135	0.229

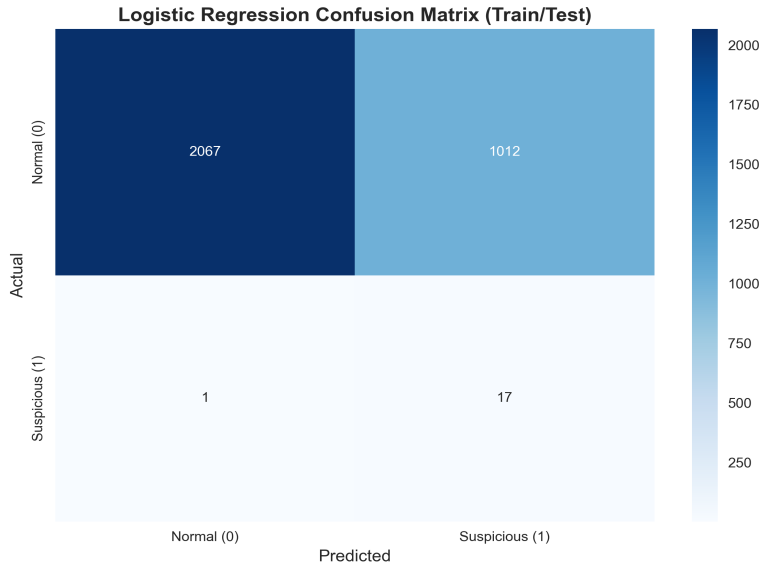
Model Performance Comparison



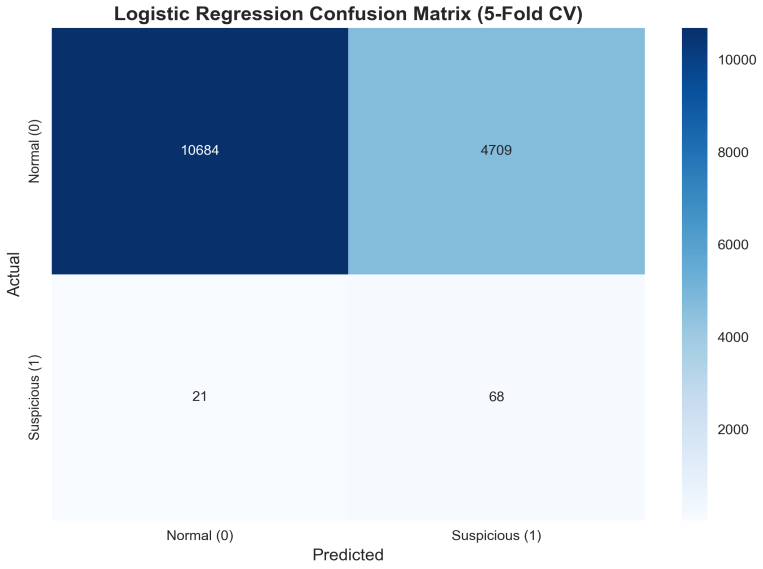
Precision-Recall Analysis

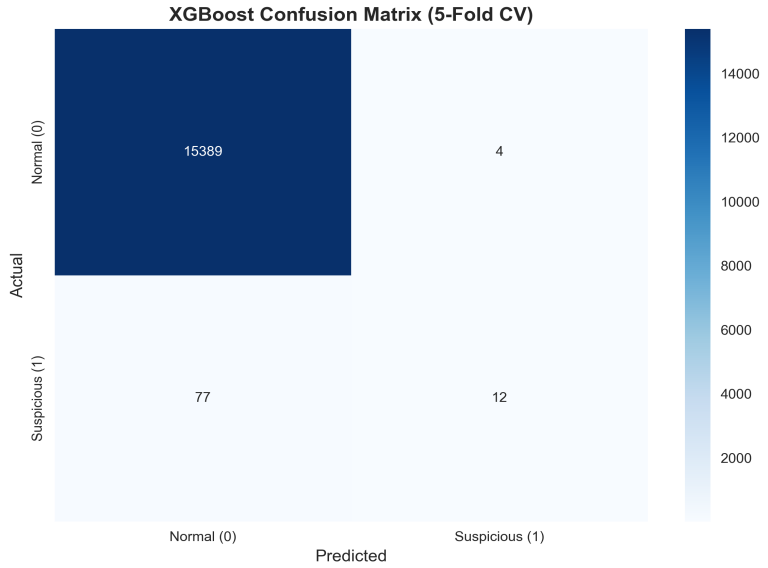
Confusion Matrices

Train/Test Split Results



5-Fold Cross-Validation Results





Detailed Anomaly Analysis

Suspicious Transaction Patterns

Pattern Type Breakdown:
• Fan-in Pattern: 40 transactions (44.9%) - Multiple accounts sending money to same destination
• Cycle Pattern: 49 transactions (55.1%) - Circular money flow patterns

Top Destination Accounts (Fan-in Pattern):
• Account 4: 5 suspicious incoming transactions
• Account 72: 5 suspicious incoming transactions
• Account 31: 5 suspicious incoming transactions
• Account 17: 5 suspicious incoming transactions
• Account 3: 4 suspicious incoming transactions

Geographic and Temporal Distribution

Geographic Spread:
Suspicious accounts distributed across multiple states:
• Massachusetts (MA) - East Susan
• American Samoa (AS) - Herringstad
• South Carolina (SC) - Williamsbury, Lake Jenna
• South Dakota (SD) - South Raymondborough
• Multiple other locations

Temporal Patterns:
• Peak Activity: January 1, 2017 (5 suspicious transactions)
• Distribution: 1-3 transactions per day throughout 2017
• Strategy: Temporal spreading to avoid bulk detection

Bank Distribution:
• Bank A: Multiple suspicious accounts
• Cross-bank coordination detected

Transaction Amount Analysis

Suspicious Transaction Amounts:
• Range: $62.72 - $995.64
• Mean: $469.30
• Median: $431.12

Normal Transaction Amounts (for comparison):
• Range: $1.20 - $999.93
• Mean: $526.56
• Median: $527.34

Key Insight: Suspicious amounts are slightly lower than normal transactions, indicating sophisticated evasion tactics to avoid detection thresholds.

Suspicious Account Characteristics

Account Profile:
• Total SAR Accounts: 99 flagged accounts
• Account Type: 100% Individual accounts
• Prior SAR History: Most accounts have previous suspicious activity flags

Account Naming Pattern:
• Generic customer names (C_XXX format)
• Systematic naming convention suggests coordinated activity

Branch Distribution:
• Primarily Branch 1 accounts
• Concentrated branch activity pattern

Risk Indicators:
• Prior SAR flags: High correlation with previous suspicious activity
• Geographic dispersion: Coordinated activity across multiple locations
• Amount patterns: Slightly lower but within normal ranges
• Temporal spreading: Activity distributed to avoid detection

Key Findings

1. Challenging Class Imbalance: The medium dataset presents a more realistic production scenario with only 0.57% suspicious transactions, significantly more challenging than the small dataset (1.24%).

2. Model Performance Impact:
• **Logistic Regression:** Higher recall (CV: 85.4%), catching more suspicious transactions but with more false positives (precision: CV: 12.1%)
• **XGBoost:** Lower overall performance (CV AUC: 0.787), struggling with severe class imbalance

3. Sophisticated Anomaly Patterns Detected:
• **Fan-in Pattern (44.9%):** Multiple accounts funneling money to specific destinations
• **Cycle Pattern (55.1%):** Circular money flows to obscure transaction trails

• **Geographic Coordination:** Suspicious activity across multiple states
• **Temporal Evasion:** Activity spread across time to avoid bulk detection

4. High-Risk Account Identification:
• 99 SAR-flagged accounts with prior suspicious activity history
• Top destination accounts receiving 4-5 suspicious transactions each
• Systematic naming patterns suggesting coordinated criminal activity

5. Performance Degradation: Cross-validation results show significant performance drop compared to train/test split, indicating overfitting and the challenge of severe class imbalance.

6. Production Reality: This dataset better represents real-world banking scenarios where suspicious transactions are extremely rare.

Recommendations

1. Model Selection Strategy:
• Use **Logistic Regression** for better recall in severely imbalanced scenarios
• Consider ensemble methods or advanced techniques for XGBoost improvement

2. Enhanced Monitoring for High-Risk Accounts:
• Implement real-time monitoring for top destination accounts (4, 72, 31, 17, 3)
• Flag accounts with prior SAR history for enhanced scrutiny
• Monitor cross-bank coordination patterns

3. Advanced Techniques for Class Imbalance:
• Implement SMOTE or other oversampling techniques
• Use focal loss or class-weighted approaches
• Consider anomaly detection methods (Isolation Forest, One-Class SVM)

4. Pattern-Based Detection Rules:
• Develop specific rules for fan-in pattern detection (multiple $\rightarrow$ single destination)
• Implement cycle detection algorithms for circular money flows
• Monitor geographic clustering of suspicious activity

5. Production Considerations:
• Implement robust monitoring and alerting systems
• Use ensemble methods combining multiple approaches
• Regular model retraining with updated data

6. Future Enhancements: Focus on advanced techniques to handle severe class imbalance while maintaining detection capability.

Conclusion

The Bank Medium dataset presents a more realistic production scenario with severe class imbalance (0.57% suspicious transactions). While both models show capability in detecting sophisticated criminal patterns including fan-in and cycle structures, the performance degradation highlights the challenges of real-world fraud detection. Logistic

Regression demonstrates better resilience to class imbalance, while XGBoost requires advanced techniques for improvement. The identification of 99 high-risk accounts and specific destination patterns provides actionable intelligence for enhanced monitoring and regulatory compliance. This analysis underscores the need for specialized approaches in production fraud detection systems.