

# Fraud Detection ML Pipeline Report

## Comprehensive Analysis and Insights

Generated: 2025-08-06 09:07:42

## Table of Contents

Executive Summary	3
Quality Score Analysis	4
Risk Analysis	6
Anomaly Detection Results	8
Traffic Similarity Analysis	10
Model Performance Metrics	12
Recommendations	13

# Executive Summary

## TL;DR - Key Findings

Key Metrics	
Total Channels Analyzed	21,330
High-Risk Channels	3,241 (15.2%)
Channels with Anomalies	170 (0.8%)
Average Quality Score	3.44/10
Average Bot Rate	2.3%
Total Traffic Volume	1,487,379

## Critical Findings

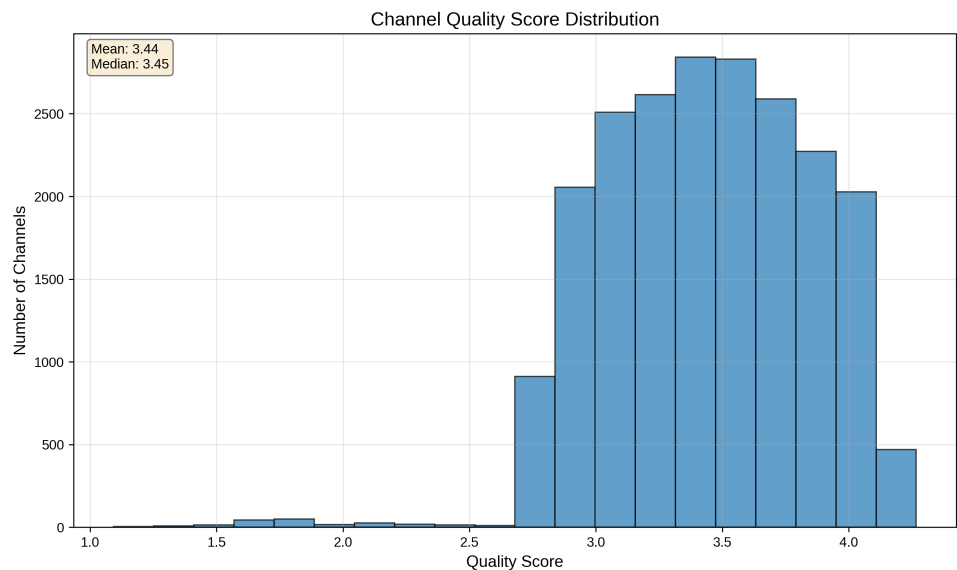
- **High Risk:** 3241 channels (15.2%) classified as high-risk

## Action Items

1. Immediately investigate top 50 high-risk channels
2. Review 100 channels with multiple anomalies
3. Implement automated filtering for channels with quality score < 3.0
4. Set up real-time alerts for new fraud patterns

# Quality Score Analysis

## Channel Quality Distribution



**What this shows:** This histogram displays how channels are distributed across different quality score ranges. The x-axis shows quality scores (0-10), and the y-axis shows the number of channels in each range.

**How to interpret:** Look for concentration patterns: A right-skewed distribution (more channels with high scores) indicates overall good traffic quality. Left-skewed suggests widespread quality issues. Bimodal distributions may indicate distinct channel groups.

## Quality Score vs Traffic Volume



**What this shows:** This scatter plot correlates channel quality scores with traffic volume. Each point represents a channel, with position indicating its quality (y-axis) and traffic volume (x-axis, log scale).

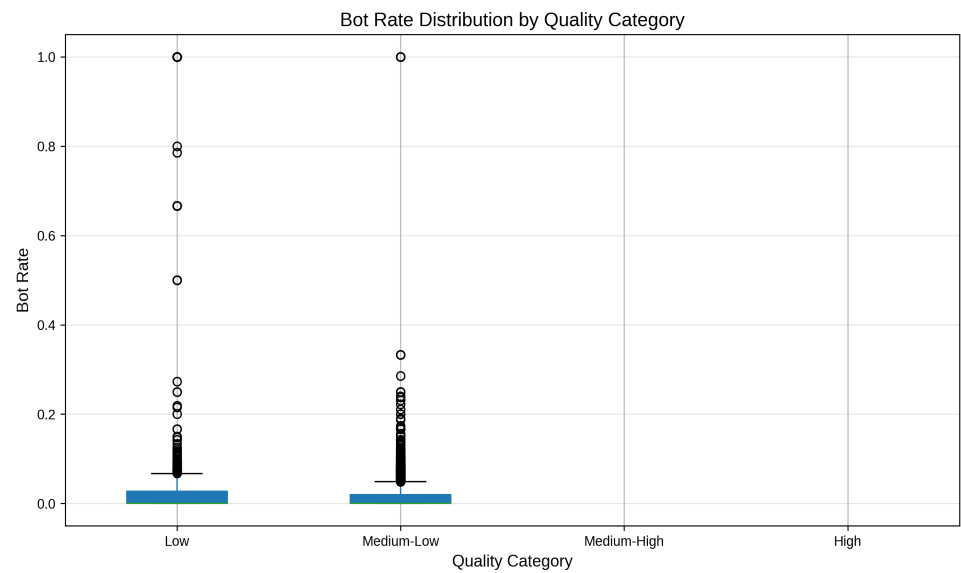
**How to interpret:** Ideal channels appear in the top-right (high quality, high volume). Bottom-right channels (low quality, high volume) pose the highest risk. Top-left channels (high quality, low volume) may be underutilized opportunities.

## Top Performing Channels

Channel ID	Quality Score	Bot Rate	Volume
20341...	4.27	2.3%	263
9529...	4.24	4.3%	46
18372...	4.24	2.3%	44
8622...	4.21	0.0%	7
18110...	4.19	0.0%	2

# Risk Analysis

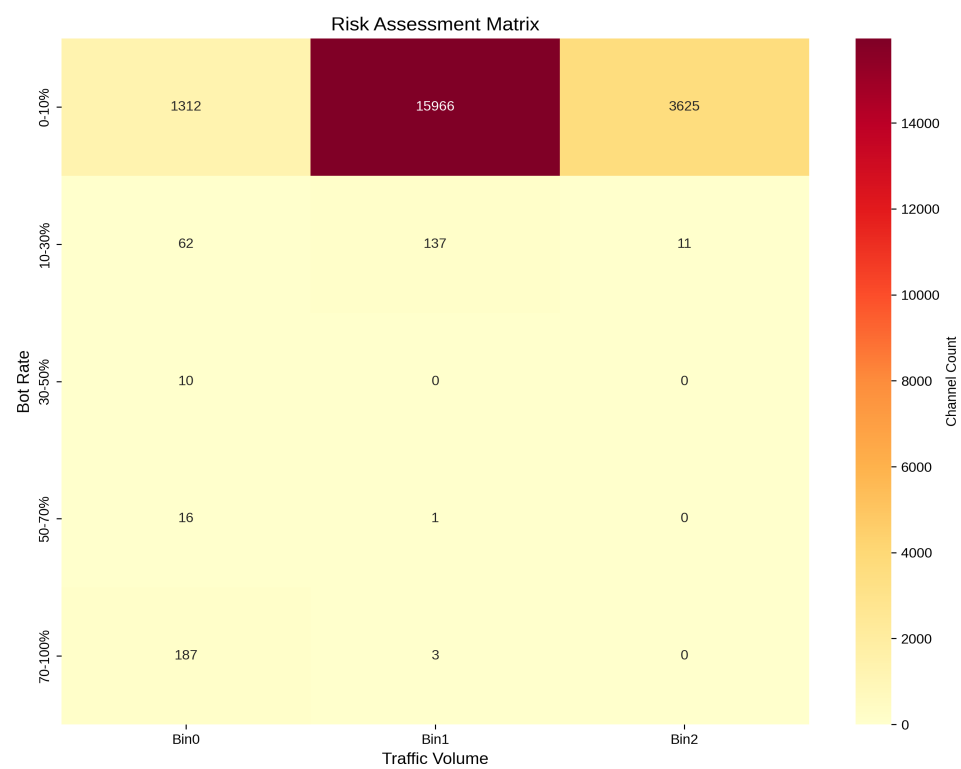
## Bot Rate Analysis by Quality Category



**What this shows:** This box plot shows the distribution of bot rates within each quality category. The boxes show quartiles, whiskers show the range, and dots indicate outliers.

**How to interpret:** Lower bot rates in higher quality categories validate the scoring model. Wide boxes indicate high variability within a category. Many outliers suggest inconsistent patterns that need investigation.

## Risk Assessment Matrix

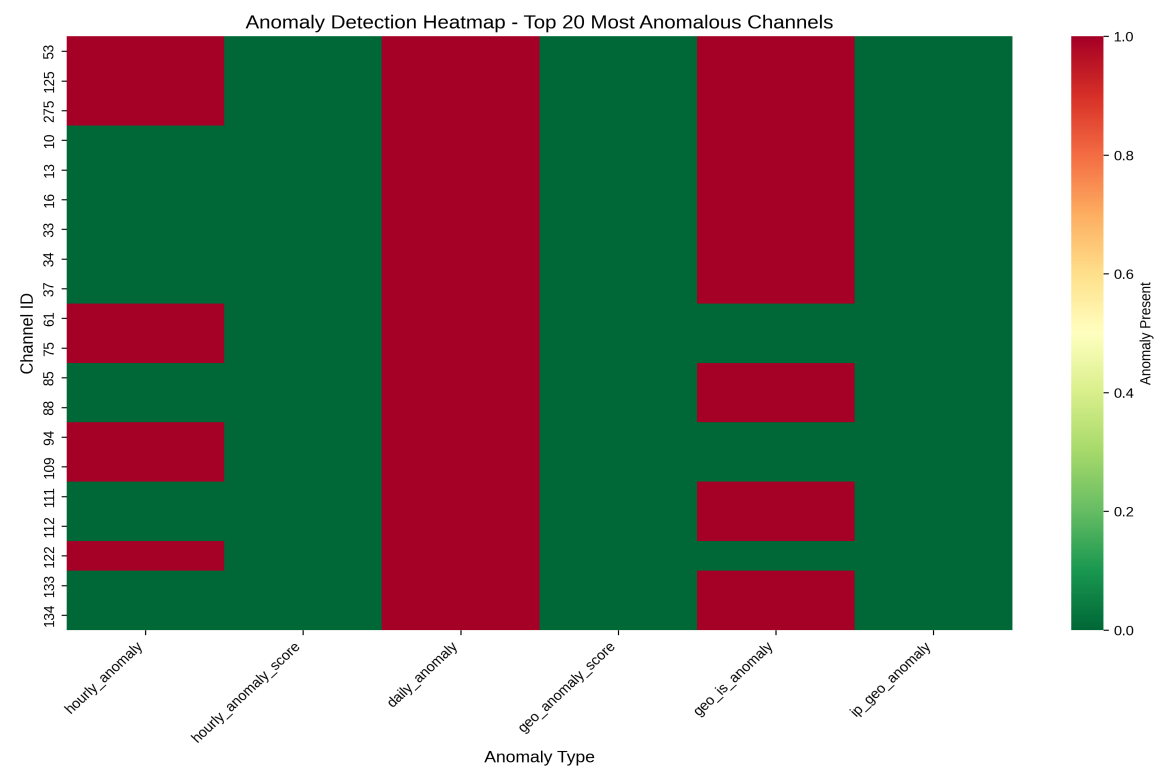


**What this shows:** This 2D heatmap maps channels by bot rate (y-axis) and volume (x-axis), with color intensity showing the number of channels in each zone.

**How to interpret:** Red zones (high bot rate + high volume) require immediate action. The darker the color, the more channels in that risk zone. Focus on reducing channels in the upper-right quadrant.

# Anomaly Detection Results

## Anomaly Detection Heatmap

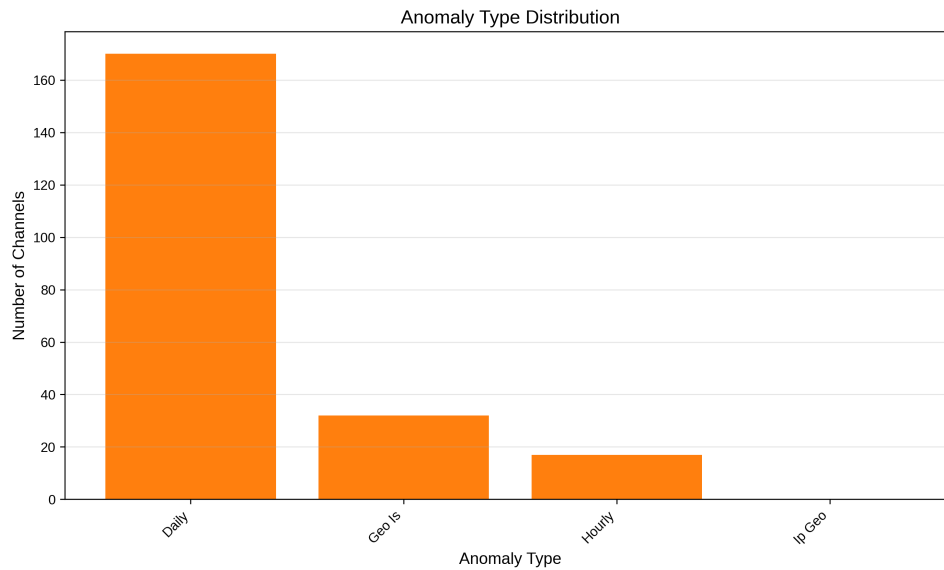


**What this shows:** This heatmap visualizes which channels (rows) have which types of anomalies (columns). Dark cells indicate the presence of an anomaly.

**How to interpret:** Channels with multiple dark cells across the row have multiple anomaly types and need priority investigation. Columns with many dark cells indicate common anomaly patterns affecting many channels.

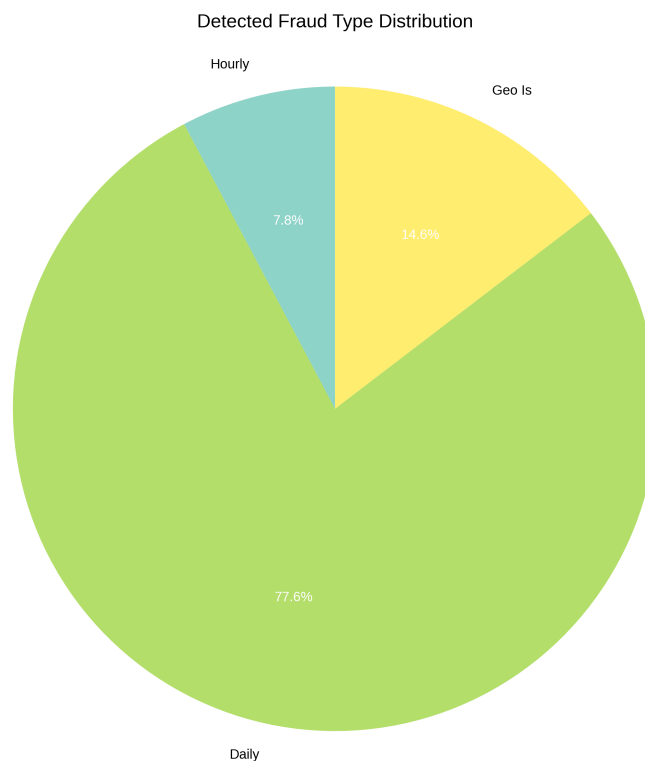
## Anomaly Type Distribution





**What this shows:** This bar chart shows how many channels are affected by each type of anomaly, helping prioritize which anomaly patterns to address first.

**How to interpret:** Focus on anomaly types with the highest counts first, as they affect the most channels. Types with very low counts might indicate rare but potentially serious issues.

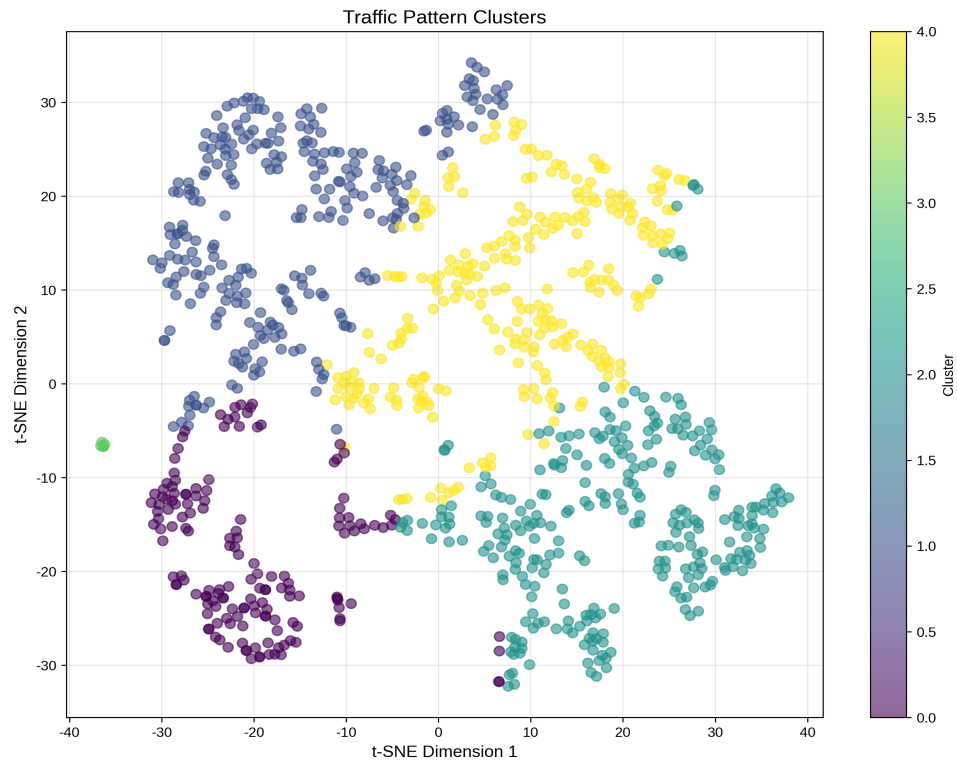


**What this shows:** This pie chart breaks down the proportion of different fraud types detected across all channels.

**How to interpret:** Large slices indicate prevalent fraud types requiring systematic solutions. Multiple small slices suggest diverse fraud tactics. Use this to prioritize anti-fraud measures.

# Traffic Similarity Analysis

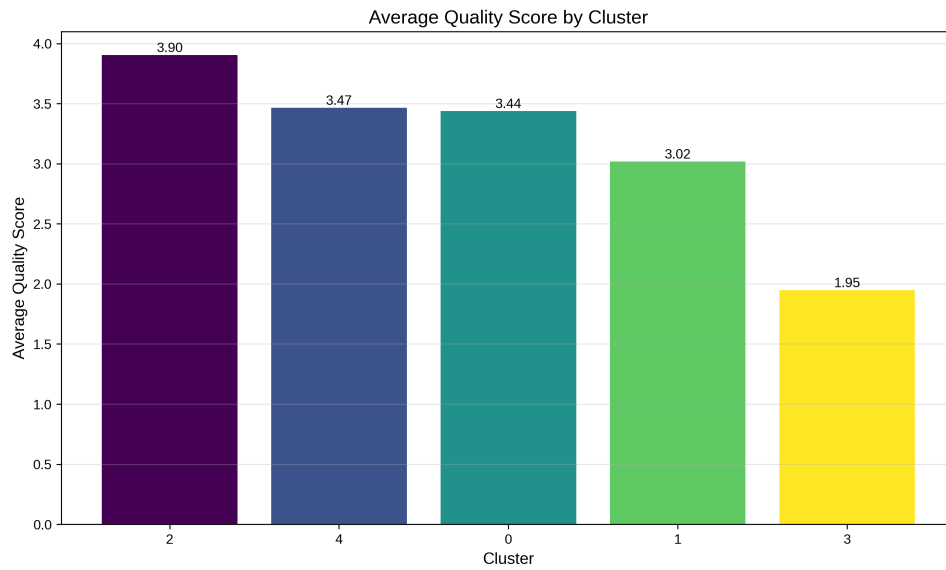
## Traffic Pattern Clusters



**What this shows:** This t-SNE plot shows how channels group into natural clusters based on their traffic patterns. Each point is a channel, colored by its cluster assignment.

**How to interpret:** Well-separated clusters indicate distinct traffic patterns. Channels far from any cluster center are outliers. Large clusters may represent common traffic patterns, while small clusters might be niche or suspicious.

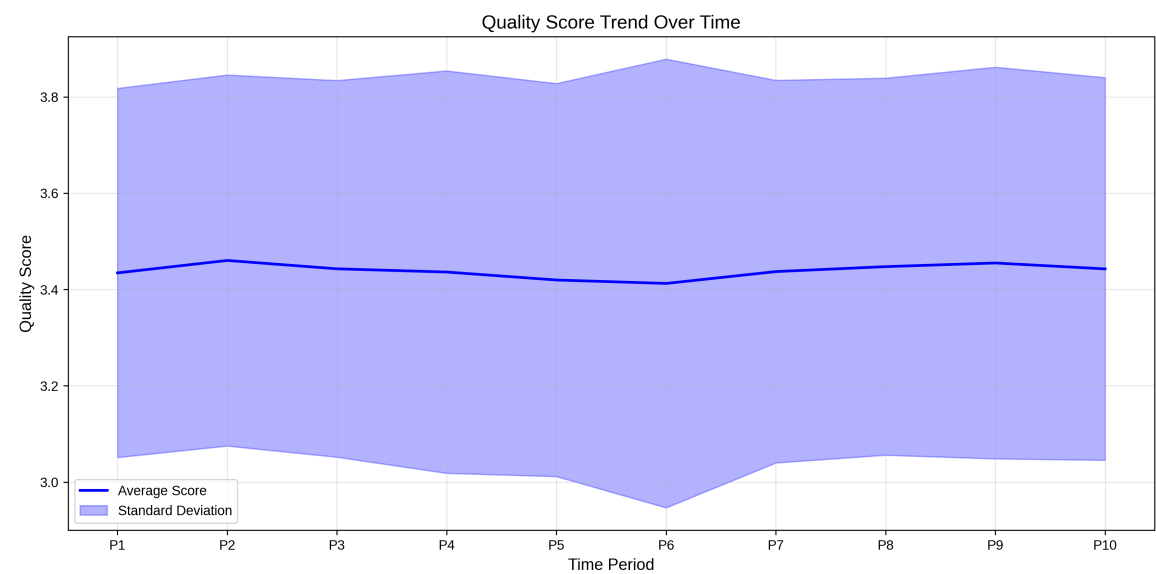
## Average Quality Score by Cluster



**What this shows:** This bar chart displays the average quality score for each traffic cluster, helping identify which traffic patterns correlate with quality.

**How to interpret:** Clusters with low average quality scores likely contain fraudulent or low-quality traffic patterns. High-scoring clusters represent desirable traffic patterns to encourage.

# Quality Score Analysis



**What this shows:** This line chart tracks quality score trends over time periods, revealing patterns and changes in traffic quality.

**How to interpret:** Upward trends indicate improving quality. Sudden drops may signal new fraud campaigns. Seasonal patterns help predict future quality fluctuations.

## Recommendations

### Immediate Actions Required

1. **Block/Investigate High-Risk Channels:** 3241 channels identified as high-risk with average bot rate of 7.7%
2. **Review Anomalous Patterns:** Focus on channels with multiple anomaly types
3. **Protect Revenue:** Potential revenue at risk: \$21394.30

### Short-term Improvements

1. **Quality Improvement:** Work with 18101 medium-low quality channels
2. **Pattern Monitoring:** Set up alerts for channels matching high-risk patterns
3. **Enforce Standards:** Require minimum quality score of 4.0 for new channels

### Long-term Strategy

1. **Model Enhancement:** Retrain models monthly with new data
2. **Process Optimization:** Automate channel blocking for scores < 2.0
3. **Dashboard:** Create real-time dashboard for ongoing monitoring
4. **ML Integration:** Implement real-time scoring for new channels