📊 Business Insights from Data Pre-Processing

🔷 **Zero-Amount Transactions as Potential Fraud Indicators**
✅ A significantly higher fraud rate (1.38%) in zero-amount transactions compared to non-zero (0.16%) suggests fraudsters may be using them for system probing—testing stolen cards before executing larger transactions.
✅ This "test transaction" pattern is common in fraud schemes, where small or zero-value transactions are attempted to check if the card is active before making high-value fraudulent purchases.

🔷 **Risk-Based Fraud Prevention Strategy**
✅ Financial institutions & merchants should flag or block zero-value transactions from unknown sources or require additional verification.
✅ Adaptive fraud detection models should weigh zero-amount transactions higher when assessing risk, as they have an 8.6x higher fraud likelihood.
✅ Transaction monitoring systems should trigger real-time alerts for repeated zero-value transactions from the same card, especially if followed by large transactions.

🔷 Policy Adjustments for Banks & Payment Processors
✅ Restricting zero-amount transactions unless explicitly permitted by the merchant can reduce fraud risk.
✅ Multi-factor authentication (MFA) for zero-value transactions can prevent fraudsters from successfully testing stolen cards.

📊 Business Insights from Fraud Timing Analysis

🔷 **Fraud Peaks at 2nd & 11th Transaction Hour**
✅ Fraud spikes during these hours suggest attackers may be strategically timing their transactions.
✅ Possible explanations:

- Exploiting system weaknesses during times when fraud monitoring is less active.
- High transaction volume periods, allowing fraud to blend in unnoticed.
  ✅ Business Actionable Insights:
- Banks & payment processors should increase fraud monitoring and flag transactions during these peak fraud hours.
- AI-based fraud detection models should assign a higher risk score to transactions made during these peak fraud periods.

🔷 **Low Fraud at 0th & 10th Hour**
✅ Fewer fraud attempts during these hours could mean:

- Fraudsters avoid midnight transactions (0th hour) when banking activity is minimal, making fraudulent activity more noticeable.
- The 10th hour could be a time when fraud detection systems are more effective.
  ✅ Business Recommendations:
- Banks should analyze fraud detection system logs during these hours to determine if their monitoring is more effective or if fraudsters avoid these times for other reasons.
- Introduce randomized fraud detection intensity throughout the day to prevent attackers from exploiting predictable monitoring weaknesses.

🔷 **Limitations: Weekday Analysis Not Useful**
✅ Since the dataset only covers two days, fraud by weekday analysis doesn't provide broader trends.
✅ Future Improvement:

- Analyzing transactions over a longer timeframe (weeks/months) could reveal weekend vs. weekday fraud patterns.
- Incorporating external factors like banking hours, holiday effects, or payday spikes may enhance fraud detection strategies.

📊 Business Insights from Fraud vs. Transaction Amount Analysis

🔷 **Fraud is Highest in Small Transactions (£) → 267 frauds**
✅ Fraudsters prefer small transactions, likely to avoid detection and bypass fraud monitoring systems.
✅ These transactions may be small enough not to trigger alerts, making them an ideal way for fraudsters to test stolen cards or exploit weaknesses.
✅ Business Actionable Insights:

- Implement dynamic fraud thresholds where multiple small transactions from the same account within a short time trigger alerts.
- Use AI-driven anomaly detection to spot suspicious patterns of frequent low-value transactions.

🔷 **Zero-Amount Transactions (£0) → 25 frauds**
✅ Zero-value frauds could indicate test transactions, where fraudsters check if a card is valid before making larger purchases.
✅ Possible Explanations:

- Fraudsters may be exploiting a loophole in transaction processing.

- Some merchants or banks may allow £0 pre-authorization transactions as part of their system.
  ✅ Business Recommendations:
- Monitor and flag £0 transactions—many payment systems don’t expect £0 values, making them a potential fraud signal.
- If £0 transactions serve a legitimate purpose, ensure they are logged and analyzed for unusual activity.

🔷 Moderate to High Fraud in Medium Transactions (££) → 99 frauds

✅ While not as frequent as small transactions, fraud still exists in mid-sized payments.
✅ Business Recommendations:

- Implement real-time verification for medium transactions, especially for new or high-risk accounts.

🔷 Fraud is Least in Very Large Transactions (££££) → 9 frauds

✅ Large transactions typically require additional verification, reducing fraud attempts.
✅ Takeaway: Fraudsters avoid high-value transactions due to stricter security protocols.
✅ Business Optimization Tip:

- Maintain multi-factor authentication for large transactions but streamline the process for legitimate users to reduce friction.

💰 Business Insights from Average Transaction Amount (Fraud vs. Non-Fraud)

🔷 Fraudulent Transactions Have a Higher Average Amount

✅ The average fraud transaction amount is £123.8, whereas the average non-fraud transaction amount is £88.41.
✅ This suggests that fraudsters strategically target higher-value transactions to maximize financial gain.

🔷 Key Takeaways for Fraud Prevention

✅ Fraud detection systems should assign higher risk scores to high-value transactions, especially when combined with other suspicious factors (e.g., multiple small transactions leading up to a big one).
✅ Real-time transaction monitoring should flag high-value purchases from new or unusual locations.
✅ Banks and merchants should implement stepped verification (e.g., OTP, biometric authentication) for high-value transactions to deter fraud attempts.