Pocketride - AI Fraud Detection: Expected Outliers

1. Unusual Transaction Patterns

- Multiple rides in a short period: A user booking an abnormally high number of rides within a short timeframe could be a sign of fraud.
- Excessive cancellations or no-shows: Frequent ride cancellations or rides where the driver or rider doesn't show up could indicate abuse or manipulation.
- Unusual ride timings: Rides booked at odd hours, such as very late at night or early morning, especially in low-demand areas.
- Ride duration or distance outliers: Rides that are either much longer or shorter than typical patterns for a given route or location.

2. Abnormal Payment Behavior

- Multiple payment methods on one account: A single user switching between several different credit cards or payment methods might signal fraud.
- Failed payment attempts: A high number of declined payments or attempted transactions before a successful one.
- Unusual discounts or promotions: Users exploiting promotional codes or discounts far more frequently than typical riders.

3. Geographical Outliers

- Geolocation anomalies: Frequent changes in the rider's or driver's location within a short period.
- Rides starting and ending in unusual areas: Rides consistently starting or ending in very remote, unsafe, or high-risk areas can raise red flags.
- Driver-rider proximity issues: When a driver or rider frequently appears to be much farther apart than they claim to be in the app.

4. User Account Behavior

- New account with high activity: New users exhibiting abnormally high usage of the platform within a short time, which could signal fake or fraudulent accounts.
- Multiple accounts from the same device/IP: Users creating multiple accounts from the same IP address or device may indicate account farming or abusive behavior.
- Irregular login patterns: Unusual login times or frequent logins from different geographic locations for the same account.

5. Driver-Specific Outliers

- Unusually high earnings per trip: If a driver is earning significantly more than the average for similar routes or areas, it could be an indication of fraud or fare manipulation.
- Low trip acceptance rates: Drivers who consistently reject rides but manage to complete high-value trips might be manipulating the system to gain higher fares.
- Unusual trip requests: Drivers accepting or completing rides outside of normal working hours or during unusually low-traffic times.
- Frequent driver-rider matches: If the same rider is matched with the same driver frequently in a short period, it could indicate collusion.

6. Ride Behavior Anomalies

- Abnormal detours: Rides taking significantly longer or using different routes than expected, leading to higher charges.
- GPS spoofing: Using fake GPS locations to manipulate trip routes, times, or distances.
- Ghost rides: Fake rides that appear completed on the system but never actually took place.

7. Behavioral Outliers

- Unusual communication patterns: Overly frequent or inconsistent messaging between rider and driver.
- Device emulation or automation: Detecting patterns of automation tools or bots that mimic rider or driver behavior.

8. Suspicious Fare Adjustments

- Manipulation of dynamic pricing: Artificially inflating or reducing fare prices through unusual ride-hailing behaviors.
- Unexplained refunds or adjustments: Frequent fare adjustments or refunds processed for the same users or drivers.

9. High-Risk Identity and Profile Information

- Use of disposable emails/phone numbers: Users signing up with temporary or suspicious email domains or phone numbers.
- Fake identity details: Detection of fake or mismatched identity information.
- Stolen credentials: Accounts exhibiting behaviors common to identity theft or unauthorized use of another person’s account details.