

## Model Development Phase Template

Date	26 September 2024
Team ID	738309
Project Title	Online Payments Fraud Detection Using Machine Learning
Maximum Marks	5 Marks

## Feature Selection Report Template

In the forthcoming update, each feature will be accompanied by a brief description. Users will indicate whether it's selected or not, providing reasoning for their decision. This process will streamline decision-making and enhance transparency in feature selection.

Feature	Description	Selected (Yes/No)	Reasoning
<b>Transaction Features:</b>	<input type="checkbox"/> <b>Amount:</b> Dollar amount of the transaction. <input type="checkbox"/> <b>Time:</b> Date and time of the transaction. <input type="checkbox"/> <b>Location:</b> Merchant location (city, country) where the transaction occurred. (Consider privacy regulations when using this) <input type="checkbox"/> <b>Cardholder:</b> Information like billing address or zip code (limited due to privacy). <input type="checkbox"/> <b>Merchant:</b> Merchant category (e.g., grocery store, travel agency). <input type="checkbox"/> <b>Card Type:</b> Type of credit card used (e.g., Visa, Mastercard).	Yes	These features provide valuable information to the machine learning model for identifying fraudulent activities. Here's a quick recap of each feature:

<b>Frequency:</b>	Number of transactions per day/week/month by the user.	<b>Yes</b>	Analyzing the number of transactions per day/week/month can reveal anomalies. A sudden surge in transactions compared to the user's historical frequency might indicate a fraudulent attempt to exploit a stolen card.
<b>Average Transaction Amount</b>	Typical transaction amount for this user historically.	<b>Yes</b>	Significant deviations from the user's historical average transaction amount could be a sign of fraud. For instance, a series of small transactions followed by a large one might be a tactic used by fraudsters to bypass fraud detection systems that focus on large single transactions.