Here's how the SQL schema can be utilised for fraud detection:

Cardholder Information: The "card_holder" table stores information about cardholders, including their names and unique IDs. This data can be used to verify the identity of the cardholders during transactions and for tracking their transaction histories.

Credit Card Information: The "credit_card" table contains credit card information, including the card numbers and the corresponding cardholders' IDs. This table can be used to identify and validate the cards used in transactions.

Merchant Information: The "merchant" table stores information about merchants, including their names, unique IDs, and merchant categories. This data is essential for categorizing transactions and identifying potentially suspicious merchants.

Merchant Categories: The "merchant_category" table defines the various merchant categories. Assigning merchants to specific categories can aid in detecting unusual transaction patterns based on the types of merchants involved.

Transaction Information: The "transaction" table contains details about individual transactions, including the transaction IDs, transaction dates, transaction amounts, associated credit cards, and corresponding merchant IDs. This table forms the core of the fraud detection process.

Fraud detection involves analysing transaction data to identify potentially fraudulent activities. Several strategies can be employed using the provided SQL schema:

a. Anomaly Detection: By monitoring transaction patterns, such as transaction amounts, locations, and merchant types, it is possible to detect anomalies. Unusual or out-of-pattern transactions can raise red flags for potential fraud.

b. Transaction Frequency: Monitoring the frequency of transactions for each credit card can help identify abnormal behavior, such as a sudden increase in transactions or multiple transactions from different locations within a short period.

c. Merchant Behavior Analysis: Analyzing the transaction history of each merchant can help identify deviations from their usual behavior. Unusual merchant activities or sudden changes in their transaction patterns may indicate potential fraud.

d. Geographical Analysis: Tracking the geographical locations of transactions can help detect suspicious transactions made from distant or uncommon locations.

e. Cardholder Behaviour Analysis: Monitoring cardholders' transaction histories can reveal any significant deviations from their usual spending patterns or transaction locations.

f. Transaction Aggregation: Aggregating transactions based on various parameters like cardholder, merchant, or location can help identify trends and patterns associated with fraudulent activities.

g. Machine Learning Models: The data stored in the database can be utilized to train machine learning models that can predict fraud based on historical transaction data and other features.

Overall, the SQL schema provided lays the foundation for storing and organizing transaction data, cardholder information, and merchant details, which are essential components for implementing effective fraud detection strategies in a financial system. The actual fraud detection logic and algorithms would be implemented in application code, querying the database using SQL to retrieve the necessary information for analysis and decision-making.