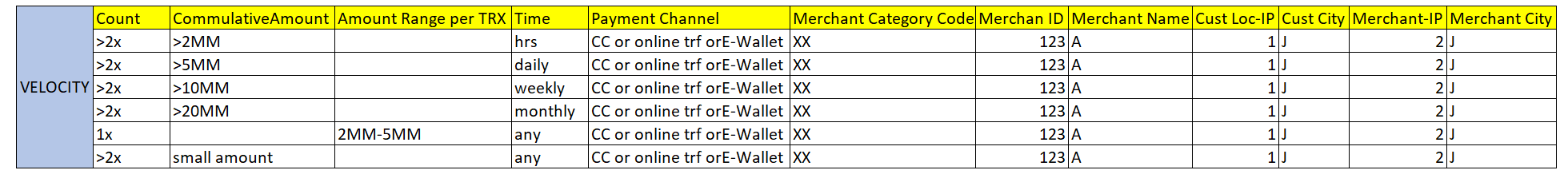
## Fraud Parameters Samples

### Velocity-Payment Channel

The following parameters are created from the Payment Channel - Customer perspective. In the following example, 6 parameters are expanded to 18 parameters depending on the number of payment channels available.



Rules row #1 - #4, Possibilities of fraud types; Account Take Over, Skimming Electronic/Counterfeiting, Lost-Stolen, Fraud application.

Payment more than 2 times in hours/daily/weekly/monthly using the payment channel CC or online transfer or E wallet with cumulative amount > Idr 2millions in the specific merchant would be captured by fraud parameter.

Rules row #5, Possibilities of fraud types; Account Take Over, Skimming Electronic/Counterfeiting, Lost-Stolen, Fraud application.

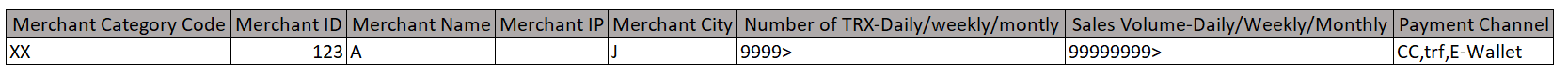
Single amount (depend on characteristic merchant and or payment channel) would be captured by fraud parameter.

Rules row #6, test card, Possibilities of fraud types; Skimming Electronic/Counterfeiting,

Small amount (depend on characteristic merchant and or payment channel) would be captured by fraud parameter.

### Velocity-Payment Acceptance

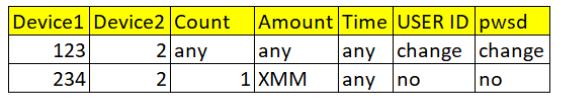
The following parameters are from the Payment Acceptance Merchant perspective. From 1 parameter this is expanded to 3 parameters depending on the number of payment channels are available. This data becomes a reference for machine learning where the Merchant ID or Merchant Category has a high risk of fraud.



Rules, Possibilities of fraud types: Account take Over, Lost-Stolen, Skimming Electronic/Counterfeiting Fraud Application and merchant as syndicates. The system will generate an alert for the sales volume based on the merchant characteristics and experience within a certain period of time. Machine learning algorithms will decisively determine if the pattern is suspicious or not based on a scoring system.

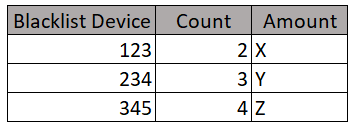
### Demographic-Customer Device

The following Demographic Parameters for device replacement.



Rules, Possibilities of fraud types: Account take Over, Lost-Stolen and Skimming Electronic/Counterfeiting. Changing customer device would be trigger as an alert with specific condition such as changing or no changing password and or UserID and transaction in certain amount high.

Parameters to block devices that have been confirmed as fraud.



Any devices are identified as fraud, the series put into storage to be declined in the future transaction.