Financial Crime Analysis

CUSTOMER_ID

All

10.00K

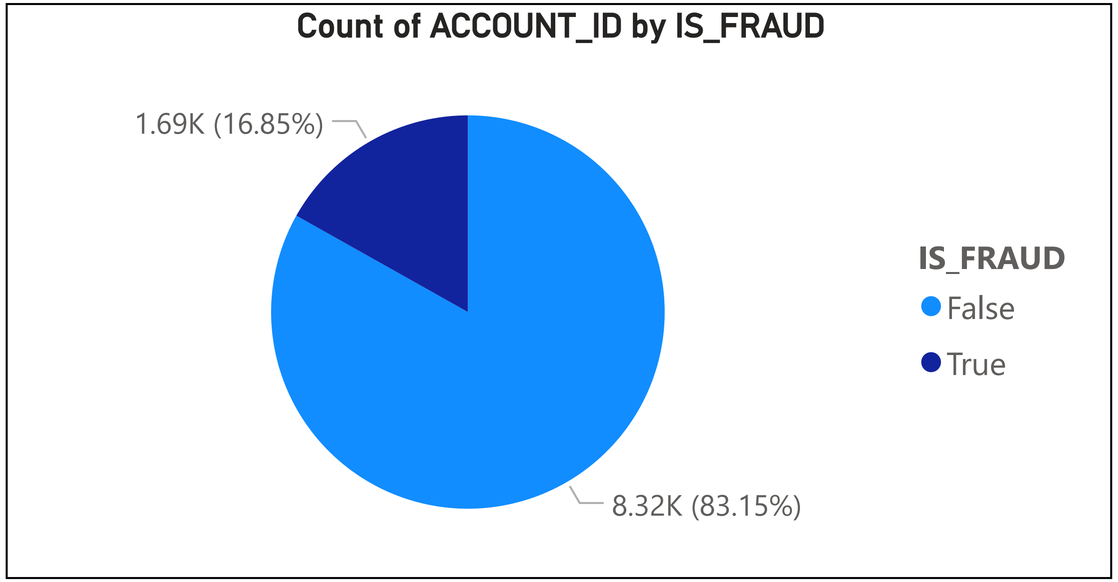
Total Bank Account

I

Account Type

US

COUNTRY

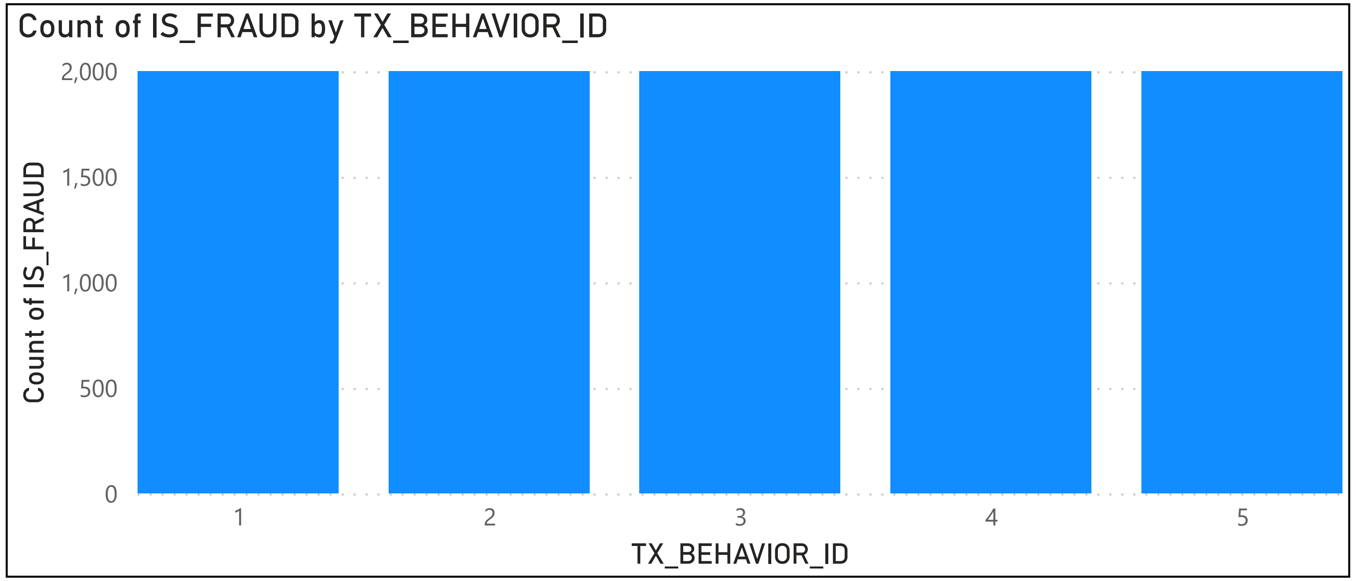

Count of ACCOUNT_ID by IS_FRAUD

Account Table Analysis

From the Dashboard we can see the total information about all the bank accounts whose transactions are monitored.

We can also see the Total No Of Fraud Accounts in the Bar Graph.

Also we can search by the customer ID to get the details about its account.

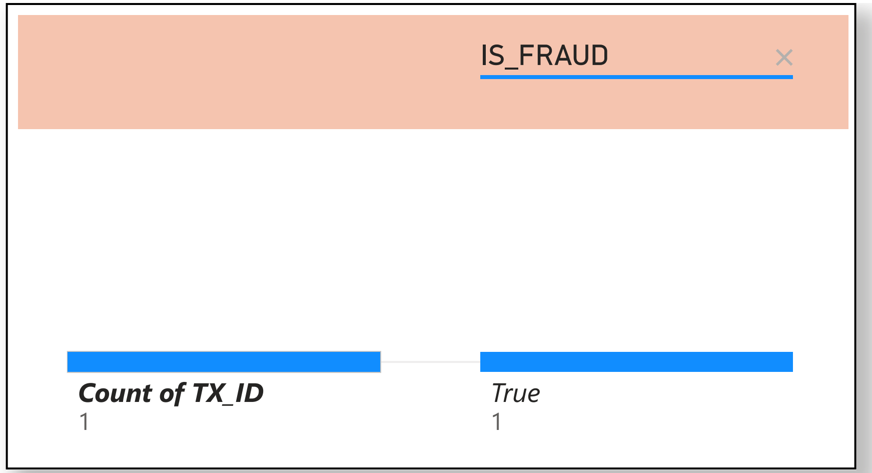

Count of IS_FRAUD by TX_BEHAVIOR_ID

Transaction & Alert Table Analysis

Select the Transaction ID

82

In this Dashboard we can select the Transaction ID and get the entire details of the transaction.



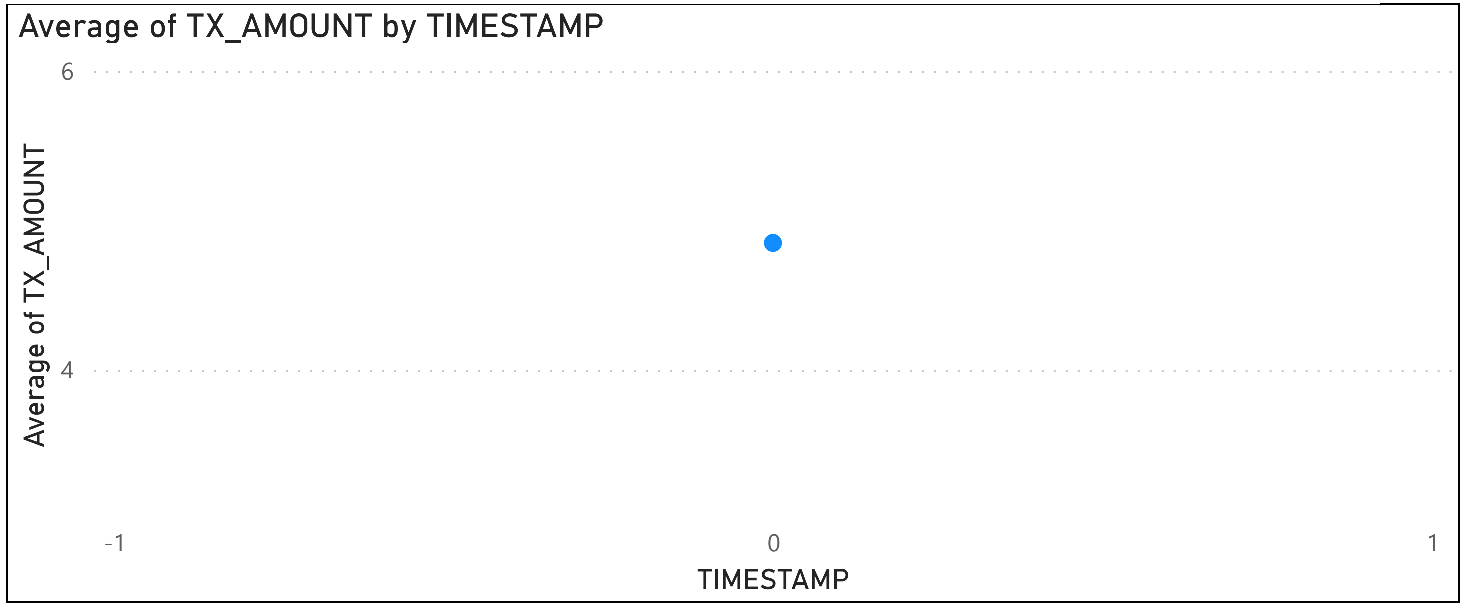
SENDER_ACCOUNT_ID
□ 6976

RECEIVER_ACCOUNT_ID
□ 9739

4.85

Total TX_AMOUNT

We can also see the sender & Receiver Account Id on the basis of transaction Id.



ALERT_TYPE	TX_TYPE	ALERT_ID	TII
fan_in	TRANSFER	193	

We shows that Transaction is Fraud or Not. If it's Fraud then its Alert Id & Alert Type is also displayed.

Ways to identify or mitigate financial crime.

1. Understand current state of play

This is crucial for determining what is working and what is not. Companies should undertake a full audit of all internal processes, technology, stored and third-party data and coordination between departments. This will help to determine the weak spots within the current KYC setup and prioritise actions.

2. Categorise your key issues and find appropriate solutions to address each.

According to Richard Kayley, Financial Crime Delivery Manager for Legal & General, it is important to understand where the bulk of the issues lie; is it strategy, policy or technology and data?

- **Strategy**: Companies must ensure that they have a robust strategy for mitigating financial crime risk.
- **Policy**: Fine-tuning internal policies on a regular basis is important to ensure compliance with new legislation and ensure they are embedded at every level of the business.
- **Technology**: Organisations should evaluate their current technology stack to understand if it is using outdated or ineffective technology. They should consider whether they can utilise their current technology further.
- **Data**: Stale or inaccurate third-party data are a common cause of non-compliance. Reviewing third party data sources, data collection and cleansing methods on a regular basis can help to reduce risk, eradicate false positives and improve the accuracy of KYC decision-making.

3. Ensure your KYC and AML framework is fit for purpose, especially if scaling into global markets

The next stage is to build out robust policies, processes and AML framework. It’s critical that this includes regular monitoring of new legislation and regulatory guidance and companies should aim to automate this process wherever possible to improve efficiency.