# Capstone Project

Charmaine Neo

# Problem

Bank is concern on the increasing number of credit card fraud transaction and wants to implement measures to prevent their customers from bring a credit card fraud victim.

# Data Acquisition & Cleansing

Obtained from Kaggle in csv format:
https://www.kaggle.com/kartik2112/fraud-detection?select=fraudTest.csv

It contains data of more than 500,000 cases of credit card fraud detected from June 2020 to December 2020.

The columns include:

- Transaction Date
- Credit Card Number
- Merchant Name
- Category of Merchant
- First Name of Holder
- Last Name of Holder
- Gender of Holder
- Amount of Transaction
- City Population
- Job of Holder
- Street, City, State, Zip of Holder
- Latitude, Longitude location of Holder
- City Population
- Date Of Birth of Holder
- Age of Holder
- Transaction Number
- Fraud Flag
- Latitude, Longitude location of Merchant

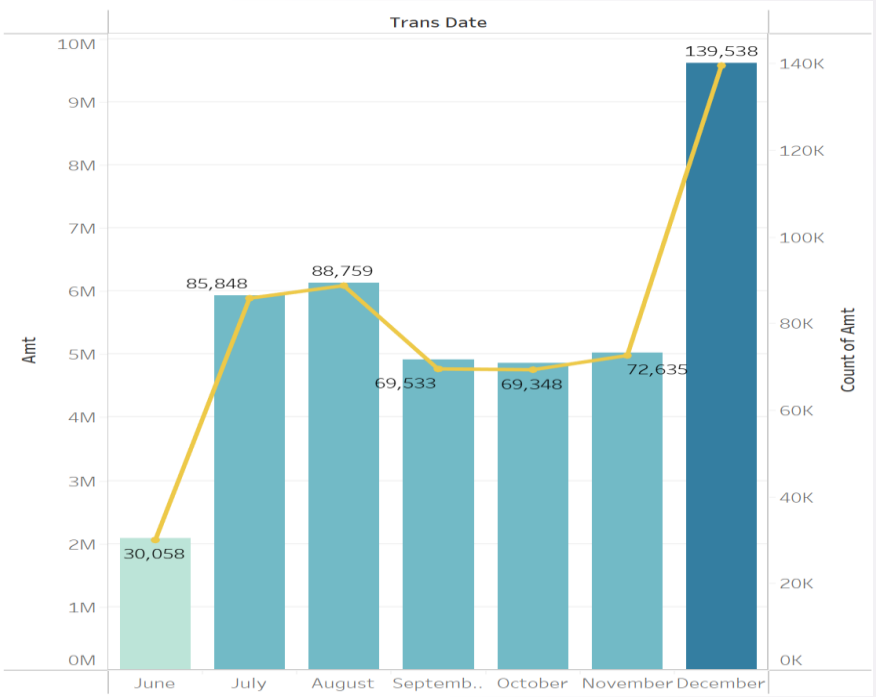
# Tableau - Story Board

Capstone Project - Charmaine Neo | Tableau Public

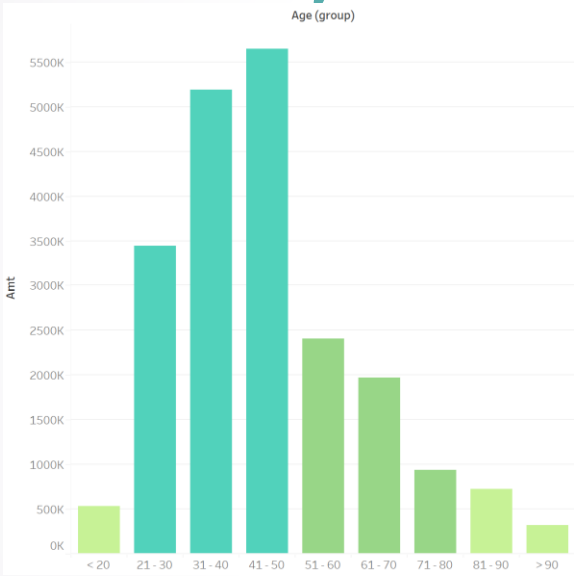
# Data Insights & Analysis

As per Tableau graph, noted an overall increasing trend of credit card fraud transactions from June 2020 to December 2020.

Reason: Based on expert reports, this increase is mainly due to the Covid-19 as there is an increase in spending online through credit cards.

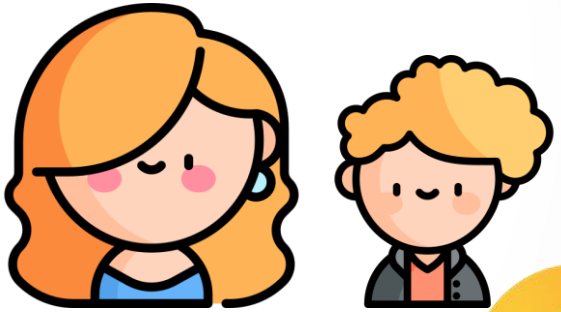


# Data Insights & Analysis



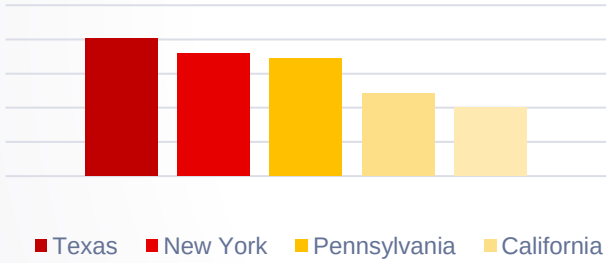

**54.9%** of the victims are woman.

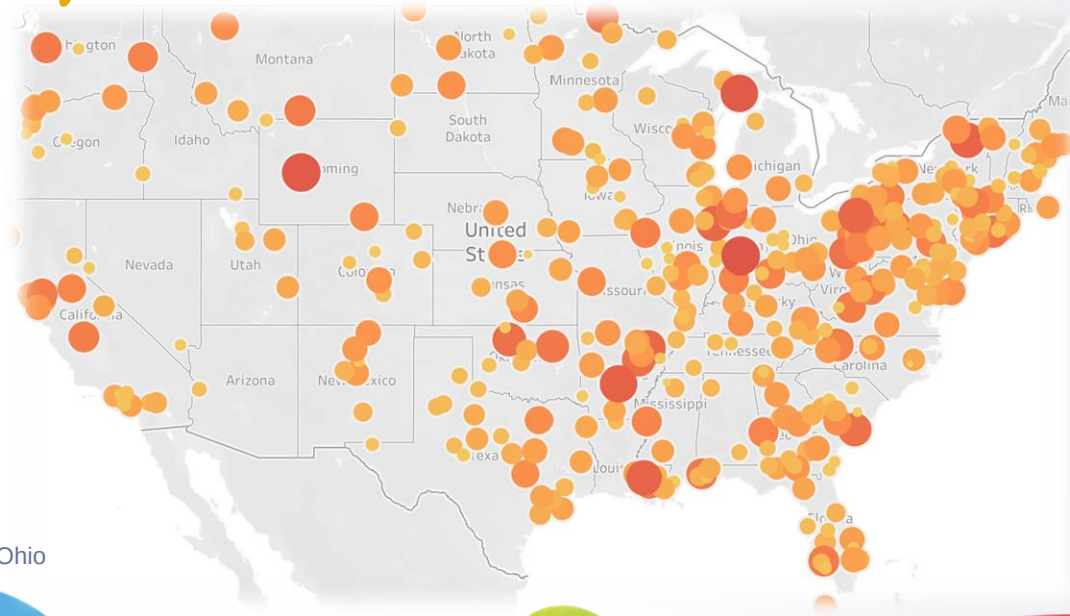
The most common age group vulnerable is from 21 to 50.



# Data Insights & Analysis

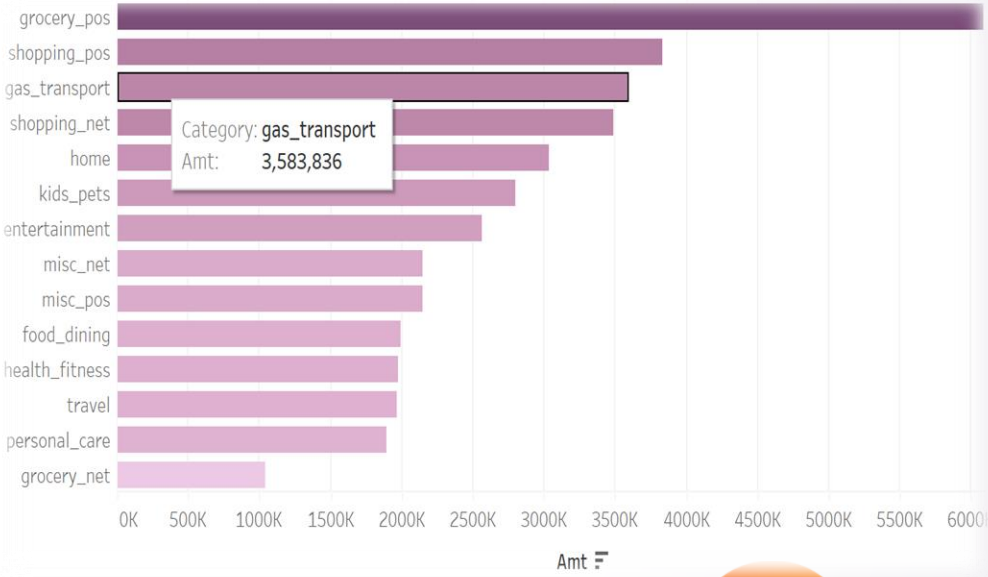
As per Tableau map, noted a wide spread of cases in different city. But most are crowded in the East side of United States.



# Data Insights & Analysis

As per Tableau map, noted the category with the highest transaction amounts are grocery and shopping which are both high in client flow and exposes details easily when using physical card and pin.



# Mitigations

- **Mandatory transaction alerts**

Noted that many transactions are only detected after a long period of time. Hence, to ensure that users are aware of all transactions performed with their credit cards, financial institutions should make payment transaction alerts mandatory instead of being optional to allow early or prompt detection of fraudulent transactions.

- **Educate users on traits of phishing emails and scams**

Noted that many card details are stolen through phishing emails and scams where users are prompted to reveal credit card details knowingly or unknowingly. Hence, credit card issuers should educate users on such traits (e.g. Directed to click on unknown links, emails requiring payment made on suspicious platforms). Furthermore, financial institutions should also ensure that those traits educated would not appear in their own emails.

# Mitigations

- **Encourage merchants to leverage on the use of contactless payment**

Noted that many card details are stolen through having physical contact with the credit card. Hence by leveraging on contactless payment through GooglePay / ApplePay or even through the tapping of card would reduce the risk of card details being stolen by both the merchant, skimmers and others who looks over shoulders at checkout.

- **Educate users on methods to protect card details online**

Now that online shopping is common especially in the younger generation, financial institutions should educate credit card users on moves to protect their card details online. E.g. by not saving card information for convenience, being mindful to cookie's acceptance as such moves will expose their card details during cyber attacks.

# Thanks!

Capstone Project - Charmaine Neo | Tableau Public