Ideation Phase

Empathize & Discover

Date	18th October 2023
Team ID	Team-592416
Project Name	Online Payments Fraud Detection Using ML
Maximum Marks	4 Marks

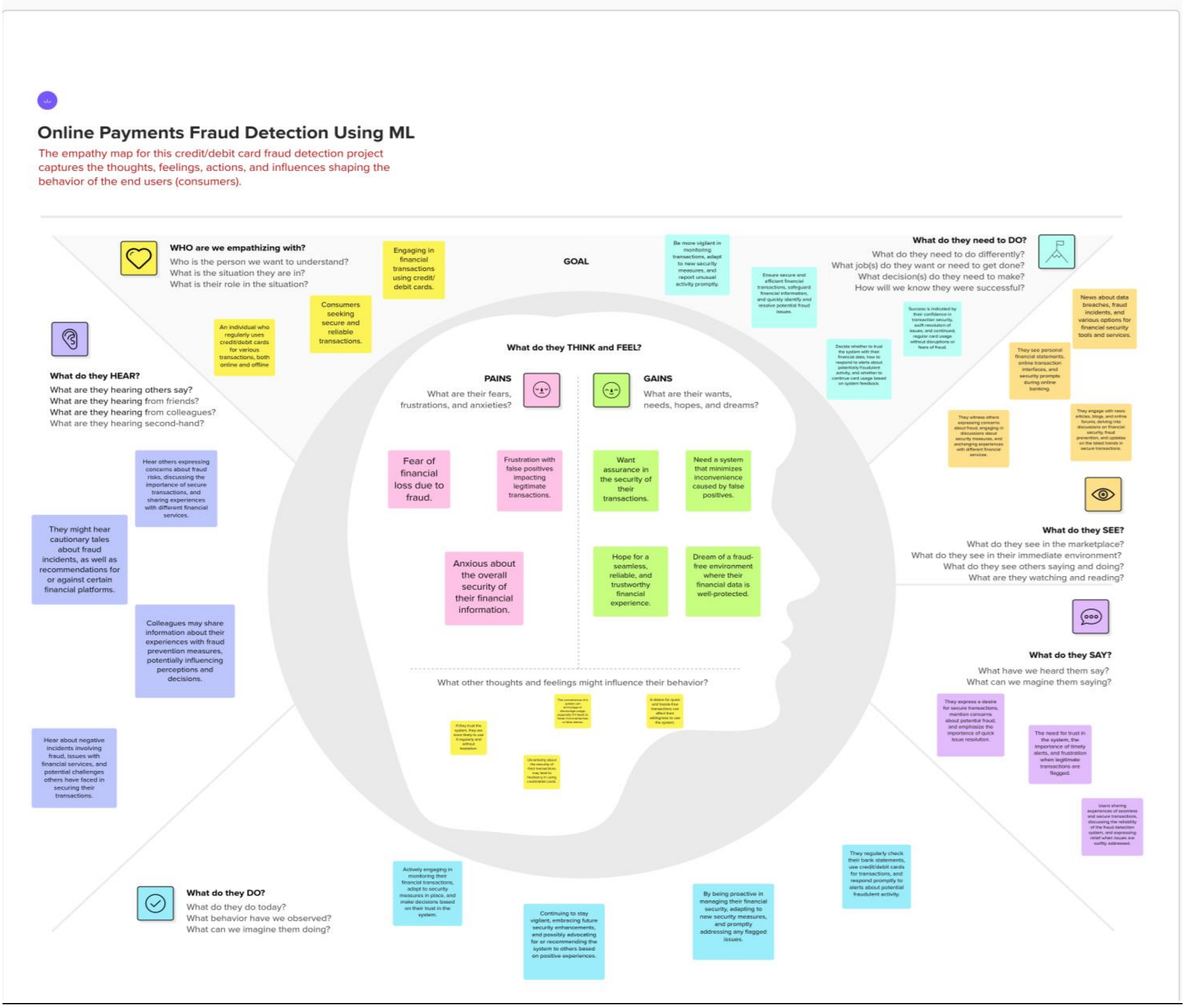
EMPATHY MAP CANVAS

The empathy map illuminates end users' observations, expressions, actions, and influences in the context of credit/debit card fraud detection. It reveals a landscape of observed and imagined behaviours, verbalized concerns, and emotional responses. Users actively engage in monitoring transactions, seek assurance, and harbour hopes for a seamless and secure financial experience. Influenced by trust, experiences, and external factors, the map informs user-centric decisions crucial for the project's success.

Team Members

1. **Aryan Sharma (21BBS0106)**
2. **Arjun Malhotra (21BBS0110)**
3. **Pranav Singh Mahara (21BBS0188)**
4. **Kanishak Khanna (21BCI0147)**

Link for the Empathy Map→
https://app.mural.co/t/kanishak3745/m/kanishak3745/1697550397494/3c8a4b9534771377e36f73bdcc7d31a6eee95ad2?sender=uf9cd485c67db74999d5a6095



Online Payments Fraud Detection Using ML

The empathy map for this credit/debit card fraud detection project captures the thoughts, feelings, actions, and influences shaping the behavior of the end users (consumers).

WHO are we empathizing with?

Who is the person we want to understand?
What is the situation they are in?
What is their role in the situation?

- Engaging in financial transactions using credit/debit cards.
- Consumers seeking secure and reliable transactions.
- An individual who regularly uses credit/debit cards for various transactions, both online and offline

GOAL

What do they need to DO?

What do they need to do differently?
What job(s) do they want or need to get done?
What decision(s) do they need to make?
How will we know they were successful?

- Be more vigilant in monitoring transactions, adapt to new security measures, and report unusual activity promptly.
- Ensure secure and efficient financial transactions, safeguard financial information, and quickly identify and resolve potential fraud issues.
- Decide whether to trust the system with their financial data, how to respond to alerts about potentially fraudulent activity, and whether to continue card usage based on system feedback.
- Success is indicated by their confidence in transaction security, swift resolution of issues, and continued, regular card usage without disruptions or fears of fraud.

What do they THINK and FEEL?

PAINS

What are their fears, frustrations, and anxieties?

- Fear of financial loss due to fraud.
- Frustration with false positives impacting legitimate transactions.
- Anxious about the overall security of their financial information.

GAINS

What are their wants, needs, hopes, and dreams?

- Want assurance in the security of their transactions.
- Need a system that minimizes inconvenience caused by false positives.
- Hope for a seamless, reliable, and trustworthy financial experience.
- Dream of a fraud-free environment where their financial data is well-protected.

What other thoughts and feelings might influence their behavior?

- If they trust the system, they are more likely to use it regularly and without hesitation.
- The convenience of a system can encourage or discourage usage, especially if it leads to fewer inconveniences or false alarms.
- A desire for quick and hassle-free transactions can affect their willingness to use the system.
- Uncertainty about the security of their transactions may lead to hesitancy in using credit/debit cards.

What do they HEAR?

What are they hearing others say?
What are they hearing from friends?
What are they hearing from colleagues?
What are they hearing second-hand?

- Hear others expressing concerns about fraud risks, discussing the importance of secure transactions, and sharing experiences with different financial services.
- They might hear cautionary tales about fraud incidents, as well as recommendations for or against certain financial platforms.
- Colleagues may share information about their experiences with fraud prevention measures, potentially influencing perceptions and decisions.
- Hear about negative incidents involving fraud, issues with financial services, and potential challenges others have faced in securing their transactions.

What do they SEE?

What do they see in the marketplace?
What do they see in their immediate environment?
What do they see others saying and doing?
What are they watching and reading?

- News about data breaches, fraud incidents, and various options for financial security tools and services.
- They see personal financial statements, online transaction interfaces, and security prompts during online banking.
- They witness others expressing concerns about fraud, engaging in discussions about security measures, and exchanging experiences with different financial services.
- They engage with news articles, blogs, and online forums, delving into discussions on financial security, fraud prevention, and updates on the latest trends in secure transactions.

What do they SAY?

What have we heard them say?
What can we magine them saying?

- They express a desire for secure transactions, mention concerns about potential fraud, and emphasize the importance of quick issue resolution.
- The need for trust in the system, the importance of timely alerts, and frustration when legitimate transactions are flagged.
- Users sharing experiences of seamless and secure transactions, discussing the reliability of the fraud detection system, and expressing relief when issues are swiftly addressed.

What do they DO?

What do they do today?
What behavior have we observed?
What can we imagine them doing?

- Actively engaging in monitoring their financial transactions, adapt to security measures in place, and make decisions based on their trust in the system.
- Continuing to stay vigilant, embracing future security enhancements, and possibly advocating for or recommending the system to others based on positive experiences.
- By being proactive in managing their financial security, adapting to new security measures, and promptly addressing any flagged issues.
- They regularly check their bank statements, use credit/debit cards for transactions, and respond promptly to alerts about potential fraudulent activity.