Ideation Phase
Empathise & Discover

Date	Monday 16 October 2023
Team ID	SI-GuidedProject-591292-1697128137
Project Name	Online Payments Fraud Detection Using ML
Maximum Marks	4 M

Guided Project Smart Interns

Online Payments Fraud Detection Using ML

The growth in internet and e-commerce appears to involve the use of online credit/debit card transactions.

The increase in the use of credit / debit cards is causing an increase in fraud. The frauds can be detected through various approaches, yet they lag in their accuracy and its own specific drawbacks.

If there are any changes in the conduct of the transaction, the frauds are predicted and taken for further process. Due to large amount of data credit / debit card fraud detection problem is rectified by the proposed method.

Originally created by Dave Gray at

XPLANE®

Share template feedback

Develop shared understanding and empathy

Stakeholders involved in online payment transactions are navigating a complex landscape where security and fraud prevention are paramount. Their behaviors, wants, and concerns are influenced by a combination of factors as **Behavior, Wants and Needs, Hopes and Dreams & Thoughts and Feelings.** These factors collectively shape their actions and strategies in response to the challenges and opportunities presented by online payment transactions, reflecting a dynamic and ever-evolving industry.

WHO are we empathizing with?

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

The "person" here refers to anyone involved in online transactions customers, merchants, or financial institutions who would benefit from a more secure online payment system.

Rising Online Transactions: The increase in online and e-commerce transactions using credit/debit cards.

Growing Fraud: The accompanying rise in fraudulent activities and attempts, which is a consequence of the increased use of credit/debit cards for online payments.

Need for Detection: The need for a reliable system to detect and prevent fraudulent transactions to safeguard customers, merchants, and financial institutions.

GOAL

Enhanced Vigilance: Customers may need to be more vigilant about reviewing their card statements and reporting any suspicious transactions promptly.

Use of Secure Platforms: Choosing to do business with online merchants and platforms that have robust security measures in place.

Implementing Security Measures: Learning and implementing personal security measures, such as using strong and unique passwords and enabling two-factor authentication.

What do they need to DO?

What job(s) do they want or need to get done?
What decision(s) do they need to make?

Monitoring Transactions: Customers should regularly monitor their card statements and report any suspicious transactions to their bank.

Selecting Payment Methods: Customers may choose between different payment methods and decide which one is most secure and convenient for their needs.

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?

Industry Best Practices:
They hear about best practices in online payment security, such as encryption methods, secure payment gateways, and authentication techniques from industry experts and peers.

Emerging Threats:
Stakeholders often receive information about new and evolving fraud tactics and cybersecurity threats. They learn about emerging trends in online payment fraud from sources like cybersecurity experts and industry reports.

Regulatory Changes:
They hear about changes in regulations and compliance requirements related to online payments and data security from industry associations, government agencies, and legal experts.

Case Studies:
Industry players share case studies and success stories on how they have effectively tackled online payment fraud, offering insights into successful strategies.

Security Practices:
Colleagues share information about security best practices, such as secure payment gateways, encryption methods, and multi-factor authentication.

Fraud Trends:
Colleagues discuss and share insights about emerging fraud trends, including common tactics used by fraudsters and methods to detect and prevent fraud.

Competitor Strategies:
Insights into the strategies adopted by competitors in the industry to enhance online payment security and customer trust.

Collaborative Efforts:
News about collaborative initiatives among financial institutions, merchants, and industry associations to share information and combat fraud collectively.

Educational Resources:
Information about training programs, webinars, and resources offered by industry associations and organizations on online payment security and fraud prevention.

Market Analysis:
Market analyses and insights on the growth of e-commerce, mobile payments, and digital wallets that impact the online payment landscape.

What do they THINK and FEEL?

PAINS

What are their fears, frustrations, and anxieties?

Unauthorized Transactions: Fear of unauthorized or fraudulent transactions on their credit/debit cards, resulting in financial losses.

Data Breaches: Concerns about their personal and financial data being exposed in a data breach, potentially leading to identity theft.

Complex Security: Frustration with complex security measures that can make online transactions less convenient.

Trust Issues: Anxieties about trusting online merchants and platforms with their financial information.

Lack of Control: Frustration over the limited control they have in preventing fraud.

GAINS

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

Security: Customers want their online payments to be secure and free from fraudulent activity to protect their financial assets.

Convenience: They hope for convenient and seamless online payment experiences without complex security measures.

Trust: Customers dream of having complete trust in online merchants and payment platforms to protect their personal and financial information.

Swift Resolution: They need swift and hassle-free resolution of any issues related to unauthorized or fraudulent transactions.

Privacy: Customers want their privacy to be respected and their personal data kept secure.

What other thoughts and feelings might influence their behavior?

Reputation and Brand Image:
Businesses are concerned about their reputation and brand image, as incidents of fraud or data breaches can harm customer trust and loyalty.
Cost Considerations:
The cost of implementing security measures and managing chargebacks can influence behavior, especially for merchants.
Regulatory Compliance:
Adherence to regulations and data protection laws is a significant driver of behavior, as non-compliance can result in legal and financial consequences.

Trust and Confidence:
The level of trust and confidence they have in online payment systems, merchants, and financial institutions can greatly influence their willingness to engage in online transactions.

Fear and Anxiety:
Fears of fraud, data breaches, and financial loss can make individuals and organizations more cautious in their online payment behavior.

Convenience vs. Security:
Balancing the desire for convenience in online payments with the need for robust security measures often leads to trade-offs and decisions.

What do they SEE?

What do they see in the marketplace?
What are they watching and reading?

Industry News and Publications:
They may follow industry-specific news websites, journals, and publications that cover topics like online payments, cybersecurity, and fraud prevention.

Regulatory Updates:
Keeping an eye on government and regulatory updates related to online payments and data security, such as new laws or guidelines affecting the industry.

Cybersecurity Reports:
Reviewing cybersecurity reports and studies published by organizations and security firms to understand the latest threats and vulnerabilities.

Evolution of E-commerce: The marketplace is witnessing a continuous growth in e-commerce, with more businesses and consumers engaging in online transactions. This growth presents both opportunities and challenges for all stakeholders.

Increasing Payment Options: Customers have a wide range of payment options, including credit/debit cards, digital wallets, and various online payment gateways. This diversity of payment methods offers convenience but also creates more avenues for potential fraud.

Rising Cybersecurity Threats: With the increasing use of technology, the marketplace has seen a rise in cybersecurity threats. Fraudsters are becoming more sophisticated in their tactics, making it necessary to adapt fraud detection methods accordingly.

What do they SAY?

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

- "I'm worried about the security of my credit card information when shopping online."
- "I've had unauthorized charges on my card, and it was a hassle to resolve."
- "I prefer to use payment methods with strong security features."
- "I wish online stores would provide better information on their security measures."

What do they DO?

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

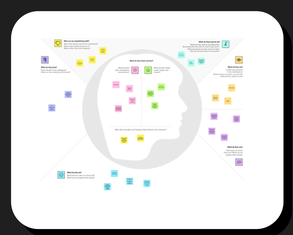
- Actively monitoring their credit card statements and transactions for any signs of unauthorized or fraudulent activity.
- Using secure and reputable online marketplaces and e-commerce websites for their shopping needs.
- Adopting two-factor authentication (2FA) and other security measures to enhance the safety of their online accounts.
- Providing feedback and reviews about their online payment experiences to raise awareness and share insights with others.

Increased Emphasis on Security:
Customers are increasingly cautious about the security of their online transactions and are often willing to adopt additional security measures like two-factor authentication.

Adoption of Multi-Layered Security:
Merchants and financial institutions are implementing multi-layered security approaches that include encryption, tokenization, and fraud detection systems to protect transactions.

Shift Toward Real-Time Fraud Detection:
Financial institutions are moving away from batch processing to real-time fraud detection, enabling immediate action upon detecting suspicious transactions.

- **Secure Account Management**: Customers often manage their online accounts with care, using strong passwords and enabling security features like two-factor authentication.
- **Regularly Monitor Transactions**: They review their credit/debit card statements and online transaction history regularly to spot any unauthorized or suspicious activity.
- **Use Reputable Merchants**: Customers tend to shop from reputable online merchants with established security measures and positive reviews.
- **Report Suspicious Transactions**: If they notice suspicious transactions, they promptly report them to their financial institution for investigation and resolution.



Need some inspiration?

See a finished version of this template to kickstart your work.

Open example

Anurag I Aayushi I Yashraj