**Design Thinking Project Workbook**

**Team Name: PromoShield**

**Team Members:**

* **M.M.S. Chandra Nagu - 2320030206**
* **A. Subash - 2320030207**
* **G. Nikitha Chowdary - 2320030102**

**1. Problem/Opportunity Domain**

* **Domain of Interest:** Artificial Intelligence and Machine Learning (AIML) – Fraud Detection
* **Description:** This project focuses on detecting promo code abuse within online payment gateways. Many companies offer promotional codes to attract users or encourage usage, but certain individuals attempt to exploit these offers by creating multiple accounts or using fake credentials. These actions not only result in financial losses but also impact the fairness and integrity of promotional campaigns.

The system identifies such abusers by analysing user behaviour using statistical techniques and unsupervised learning algorithms. Key indicators include multiple accounts registered from the same IP address, mismatch in address details, and use of gibberish names or contact numbers.

* **Why Chosen:**Promo code abuse is a growing problem in the digital economy. As businesses become more reliant on digital transactions and online offers, they are increasingly vulnerable to fraudulent activities. By addressing this issue through machine learning, we can help organizations minimize losses, optimize promotional strategies, and improve the trustworthiness of their platforms. The project also provides practical exposure to handling real-world fraud detection scenarios using AIML techniques, making it both socially impactful and technically enriching.

**2. Problem/Opportunity Statement**

**Problem Statement:** To detect and prevent promo code abuse by identifying fraudulent user behavior in an online payment gateway system using statistical and unsupervised machine learning techniques.

**Problem Description:**

Online payment platforms often offer promo codes as marketing tools to encourage user registration and engagement. However, some users exploit these promotions by creating fake accounts, using false credentials, or manipulating system loopholes. These fraudulent activities lead to financial losses, misuse of company resources, and skewed customer data.

**Context:** The rise of digital transactions and e-commerce has made it easier for fraudsters to abuse systems anonymously. Businesses must find ways to detect and counter such misuse without affecting genuine customers. Machine learning offers the ability to spot hidden patterns and anomalies that could indicate fraud, even in the absence of labeled data.

**Alternatives:**

* Manual account verification
* Rule-based fraud detection systems
* Third-party fraud monitoring services

**Customers:**

* FinTech companies
* E-commerce platforms
* Online service providers
* Digital marketing teams

**Emotional Impact:**

Customers feel cheated when abusers manipulate systems meant for everyone’s benefit. Businesses suffer frustration and loss of trust. Employees may also experience pressure in addressing increasing fraudulent activity manually.

**Quantifiable Impact:**

* Financial losses due to repeated use of promo codes
* Increase in the number of fake user accounts
* Misleading user engagement and campaign performance metrics

**Alternative Shortcomings:**

* Manual verification is time-consuming and inefficient at scale
* Rule-based systems are rigid and often bypassed by evolving fraud patterns
* Third-party solutions can be expensive and may not align with business-specific requirements

**Any Video or Images to showcase the problem:**

sdvhkchskdcsdhskjckjsdc

**3. Addressing SDGs**

**Relevant SDGs:**

* SDG 9: Industry, Innovation and Infrastructure
* SDG 16: Peace, Justice and Strong Institutions

**How Addressed:** **SDG 9 – Industry, Innovation and Infrastructure:**  
The project promotes innovation in digital infrastructure by leveraging AI and machine learning for fraud detection. It contributes to the development of smarter and more secure financial technologies, enhancing the trust and efficiency of online payment systems.

**SDG 16 – Peace, Justice and Strong Institutions:**  
By combating fraudulent activities like promo code abuse, the system supports strong digital governance and ethical use of resources. It promotes fairness and reduces exploitation, creating a more transparent and accountable digital economy.

**4. Stakeholders**

* **Roles:** The stakeholders involved in this project include the development team (students), mentors or faculty guides, online payment gateway companies, and their end-users. The development team is responsible for designing and implementing the machine learning model. Mentors guide the team with technical and domain-specific insights. Companies act as the beneficiaries of the system, while end-users are indirectly affected by the improved fraud detection.
* **Interests/Concerns:** Stakeholders are primarily interested in ensuring that the system accurately identifies fraudulent users without falsely flagging legitimate ones. Concerns include model accuracy, ethical data usage, and the efficiency of implementation. Businesses are particularly focused on minimizing losses and improving the integrity of promotional campaigns.
* **Influence:** Payment platforms have a high level of influence as their needs and data directly shape the model's features and focus. Mentors influence the technical decisions and project scope, while the development team executes the actual work. End-users have indirect influence through the behavioral patterns that the model learns from.
* **Engagement:** Engagement is achieved through regular team discussions, mentor meetings, and feedback loops. Any stakeholder input, especially from potential real-world users (e.g., fintech companies), is considered in refining the approach and features used for detection.
* **Communication:** Communication between team members and mentors is maintained through weekly updates, meetings, and progress reports. Documentation, presentations, and visual representations such as flowcharts and model outputs are used to clearly communicate ideas, progress, and results with all stakeholders.

**5. Power Interest Matrix of Stakeholders**

**High Power, High Interest:**

* **Mentors/Faculty Guides** – They have a strong influence on project direction and are highly interested in its success.
* **Company Decision Makers (if involved)** – Their interest in preventing fraud and their authority in integrating the solution make them key stakeholders.

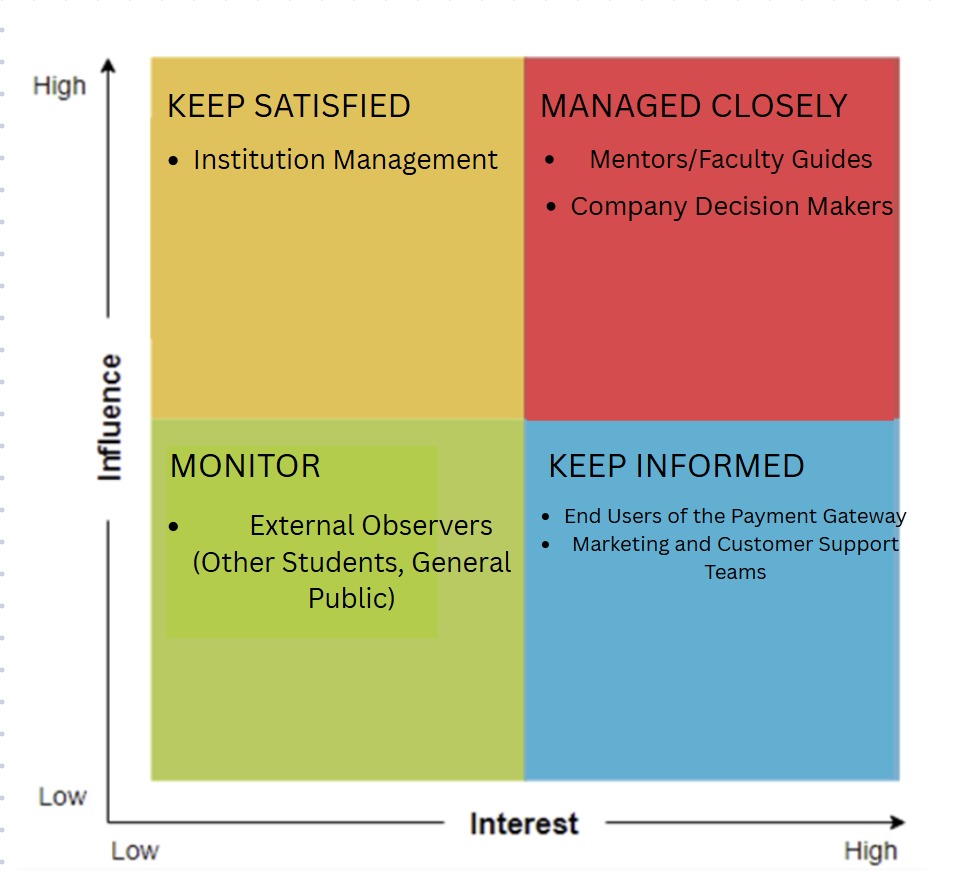
**High Power, Low Interest:**

* **Institution Management** – They provide resources and support but may not be deeply involved in technical execution.

**Low Power, High Interest:**

* **End Users of the Payment Gateway** – They are directly affected by fraud prevention measures but have no control over the project.
* **Marketing and Customer Support Teams** – Interested in the results for campaign improvement but not involved in decision-making.

**Low Power, Low Interest:**

* **External Observers (Other Students, General Public)** – May be aware of the project but are not directly impacted or interested.  **6.Empathetic Interviews**

|  |  |  |
| --- | --- | --- |
| **I need to know**  **(thoughts, feelings, actions)** | **Questions I will ask**  **(open questions)** | **Insights I hope to gain** |
| Thoughts | |  | | --- | | What do you think about how promo codes are being used today? |  |  | | --- | |  | | Whether users see promo codes as a reward or an exploitable feature. |
|  | |  | | --- | | How do you perceive online fraud in payment apps or offers? |  |  | | --- | |  | | |  | | --- | | Understand awareness levels and user definition of "fraud." |  |  | | --- | |  | |
|  | What comes to your mind when you see "exclusive offer" or "first-time user offer"? | Gauge the mindset and intent behind using such features. |
| Feelings | How do you feel when someone misuses promo codes and gains more benefit than you? | |  | | --- | | Understand feelings of unfairness or indifference among regular users. |  |  | | --- | |  | |
|  | |  | | --- | | Do you trust the way current platforms handle fraud? Why or why not? |  |  | | --- | |  | | |  | | --- | | Insight into user trust and expectations from the system. |  |  | | --- | |  | |
|  | |  | | --- | | How would you feel if you were wrongly flagged as a fraud user? |  |  | | --- | |  | | |  | | --- | | Emotional impact of false positives – fear, anger, or anxiety. |  |  | | --- | |  | |
| actions | |  | | --- | | What do you do when you see someone using multiple accounts to claim offers? |  |  | | --- | |  | | |  | | --- | | Real-life examples of witnessing fraud and actions taken. |  |  | | --- | |  | |
|  | |  | | --- | | Have you ever tried using a promo code multiple times? Why? |  |  | | --- | |  | | |  | | --- | | Capture motivations behind borderline fraudulent behavior. |  |  | | --- | |  | |
|  | |  | | --- | | What would you suggest companies do to stop misuse of promo codes? |  |  | | --- | |  | | User-driven ideas to strengthen the system; feature suggestions. |

****

**SKILLED INTERVIEW REPORT**

|  |  |  |
| --- | --- | --- |
| **User/Interviewee** | **Questions Asked** | **Insights gained (NOT THEIR ANSWERS)** |
| |  | | --- | | Rahul S., Tech Student |  |  | | --- | |  | | |  | | --- | | What do you think about people using fake accounts for promo offers? |  |  | | --- | |  | | |  | | --- | | Many users are aware of such practices but think it’s common and not a big deal. |  |  | | --- | |  | |
| |  | | --- | | Anjali T., Online Shopper |  |  | | --- | |  | | |  | | --- | | How would you feel if someone abused the promo system and got more offers than you? |  |  | | --- | |  | | |  | | --- | | Some users feel it's unfair and demotivating when others exploit the system. |  |  | | --- | |  | |
| |  | | --- | | Praveen K., App Developer |  |  | | --- | |  | | |  | | --- | | What do you believe is the biggest challenge in detecting fraud in promo codes? |  |  | | --- | |  | | |  | | --- | | Developers believe that evolving fraud patterns and lack of labeled data make it hard to detect abuse. |  |  | | --- | |  | |
| |  | | --- | | Meena R., Homemaker |  |  | | --- | |  | | |  | | --- | | Have you ever felt tempted to use a promo code multiple times using different accounts? Why? |  |  | | --- | |  | | Some users admitted they were tempted due to attractive offers, even if they didn’t do it. |
|  |  |  |

**Empathy Map**



They hear complaints from teams and users about unfair promo use and hear competitors adopting smarter solutions.

We are empathizing with genuine users of payment apps and platform administrators who are concerned about promo code exploitation.

Who is your Customer Segment: Online Payment Gateway Platforms and Regular App Users

Idea/Innovation Title: Promo Code Abuse Detection System

Designed By:Nandini

Date of Submission: 25/03/25

They are frustrated with the repeated financial losses due to promo code misuse and the inefficiency of manual detection methods.

They hope to implement a system that ensures fairness, reduces abuse, and improves campaign success.

They feel pressure to protect brand reputation and maintain user trust, which motivates their search for smarter, data-driven fraud detection.

They need to detect and prevent fraudulent behavior without affecting legitimate users.

They see increasing misuse of promo codes through fake accounts and repeated registrations.

They say that promo code abuse is becoming common and existing systems are not enough.

They attempt to track suspicious activity manually or with simple rule-based checks.

**7.Empathy Map**

**a.Who is your Customer?**

**Description:** Aditya

**Key points:**

1.  21 years old, a frequent user of online payment apps
2.  Notices that some users unfairly exploit promo codes using fake accounts
3.  We introduced him to our Promo Code Abuse Detection system, and he sees how it could help platforms ensure fairness and reduce misuse

**b.Who are we empathizing with?**

1. Description:  
    Users who are frustrated when others misuse promotional offers and gain unfair advantage
2. Business teams and developers who are anxious about the financial loss and system abuse due to fake accounts and repeated registrations
3. Admins who are overwhelmed by the limitations of manual checks and rule-based systems in catching evolving fraud techniques

**Key points:**

* The customer is honest, detail-oriented, and values fairness in digital services
* Prefers smart, automated systems that can detect suspicious behavior without affecting genuine users
* Needs a reliable and easy-to-integrate tool that can identify fraud while preserving a smooth user experience

**8. Persona of Stakeholders**

Stakeholder Name: Aditya

Demographics: 28 years old, lives in a metropolitan city, works as a fraud analyst in a fintech company.

Goals: To minimize financial losses due to promo code abuse, maintain campaign fairness, and improve customer trust in promotional strategies.

Challenges: Difficulty in identifying evolving fraud techniques, high volume of user data, and inefficiency of manual or rule-based detection systems.

Aspirations: Implement an AI-powered system that detects promo abusers automatically and provides actionable insights to optimize campaigns.

Needs: A scalable, real-time fraud detection tool using behavioral data analysis and unsupervised learning models.

Pain Points: Repeated misuse of promo codes by fake accounts, wasted marketing budget, and the risk of flagging genuine users incorrectly.

**9. Look for Common Themes, Behaviours, Needs, and Pain Points among the Users**

**Common Themes:** Key themes identified include the need for secure promotional campaigns, user authenticity, automated fraud detection, real-time results, behavioural pattern analysis, and protection against promo abuse.

**Common Behaviours:** Users often register with multiple accounts to exploit first-time user offers, use fake or gibberish names, mask their IP or location, and reuse promo codes across different phone numbers or emails.

**Common Needs:**

* Accuracy – High precision in detecting fraudulent behavior without flagging genuine users.
* Speed – Real-time detection and flagging of suspicious activity.
* Clarity – Transparent reports explaining why a user was flagged.
* **Scalability** – Ability to handle a large volume of users across campaigns.

**Common Pain Points:**

* **False Positives/Negatives** – Incorrectly classifying genuine users or missing fraud cases.
* **Manual Burden** – Time-consuming and inefficient manual review of accounts.
* **Lack of Insights** – Difficulty in interpreting fraud indicators from data.
* **Data Privacy** – Concerns over handling sensitive user data during analysis.

**10. Define Needs and Insights of Your Users**

**User Needs:**

* **Accurate Detection** – Precisely identify fraudulent users exploiting promo codes without misclassifying genuine ones.
* **Real-Time Analysis** – Detect and respond to suspicious activities instantly during user registration or promo code redemption.
* **Automation Support** – Reduce the need for manual reviews by using intelligent unsupervised learning algorithms.
* **Privacy Protection** – Ensure user data is securely processed without misuse or unauthorized access.
* **User-Friendly Interface** – Provide a simple, dashboard-based system for admins to view alerts, reports, and trends easily.

**User Insights:**

* **Value Accuracy** – Stakeholders prioritize fraud detection systems that are reliable and produce minimal false results.
* **Need for Intelligent Systems** – Users and admins prefer AI-based tools that evolve and adapt to new fraud patterns.
* **Concern About Data Privacy** – Users expect platforms to handle personal information (IP, phone, address) responsibly.
* **Appreciate Simplicity** – Admins value clear visualizations and concise explanations for fraud scores and decisions.
* **Expect Integration** – Businesses prefer fraud detection tools that can be integrated into existing systems like CRM or user onboarding pipelines.

**13. POV Statements**

|  |  |  |
| --- | --- | --- |
| PoV Statements | Benefit, Way to Benefit,  Job TBD,  Need (more/less) | PoV Questions  (At least one per statement) |
| |  | | --- | | Fraud analysts need a way to detect promo abusers because manual tracking is inefficient. |  |  | | --- | |  | | |  | | --- | | Need more automation |  |  | | --- | |  | | |  | | --- | | What can we design to reduce manual effort in fraud detection? |  |  | | --- | |  | |
| |  | | --- | | Admins need a way to identify suspicious users in real-time because financial losses are increasing. |  |  | | --- | |  | | |  | | --- | | Need real-time alerts |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | How can we design a system that prevents misuse of promo codes? |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Businesses need a way to protect promo budgets because abusers are exploiting first-time offers. |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Need better control |  |  | | --- | |  | |  |  | | --- | |  | | |  | | --- | | How can we ensure fair usage of promo offers across users? |  |  | | --- | |  | |
| |  | | --- | | Users need fair access to offers because abuse by others feels unfair. |  |  | | --- | |  | | |  | | --- | | Need fairness |  |  | | --- | |  | | How might we scan and compare online sources for unauthorized use of content? |
| |  | | --- | | Developers need adaptable models because fraud patterns keep evolving. |  |  | | --- | |  | | |  | | --- | | Need adaptable algorithms |  |  | | --- | |  | | |  | | --- | | How can we build ML models that learn and evolve with user behavior? |  |  | | --- | |  | |
| |  | | --- | | Marketers need clearer reports because they can’t interpret raw data well. |  |  | | --- | |  | | |  | | --- | | Need clear dashboards |  |  | | --- | |  | | |  | | --- | | What can we design to show fraud detection insights in a clear way? |  |  | | --- | |  | |
| Support teams need fewer false positives because wrongly flagged users complain. | |  | | --- | | Need more precision |  |  | | --- | |  | | |  | | --- | | How can we reduce false alerts in the fraud detection system? |  |  | | --- | |  | |
| |  | | --- | | Data privacy officers need secure processing because user trust is critical. |  |  | | --- | |  | | |  | | --- | | Need data protection |  |  | | --- | |  | | |  | | --- | | What design ensures fraud detection respects data privacy? |  |  | | --- | |  | |

**14. Develop POV/How Might We (HMW) Questions to Transform Insights/Needs into Opportunities for Design**

|  |  |
| --- | --- |
| User Need/Insight | "How Might We" Question |
| |  | | --- | | Fraud detection teams need real-time identification of suspicious promo code activity. |  |  | | --- | |  | | |  | | --- | | **How might we enable instant detection and flagging of promo code abuse in real-time?** |  |  | | --- | |  | |
| |  | | --- | | Admins struggle with evolving fraud techniques that bypass traditional rules. |  |  | | --- | |  | | |  | | --- | | **How might we build adaptive models that evolve with new patterns of promo fraud?** |  |  | | --- | |  | |
| |  | | --- | | Businesses are losing revenue due to repeated misuse of first-time offers. |  |  | | --- | |  | | |  | | --- | | **How might we design a system that detects and prevents multi-account promo exploitation?** |  |  | | --- | |  | |
| |  | | --- | | Support teams deal with complaints from genuine users wrongly flagged as fraud. |  |  | | --- | |  | | |  | | --- | | **How might we reduce false positives while maintaining strong fraud detection?** |  |  | | --- | |  | |
| |  | | --- | | Stakeholders need interpretable insights from fraud detection systems. |  |  | | --- | |  | | |  | | --- | | **How might we design a dashboard that provides clear and actionable fraud insights?** |  |  | | --- | |  | |

**16. Crafting a Balanced and Actionable Design Challenge**

**Design Challenge Statement:**

*How might we design an AI-powered system that detects and prevents promo code abuse in real-time, ensuring fairness for genuine users while minimizing false positives and protecting user privacy?*

This statement is:

* **Balanced** – It considers both user experience and business security.
* **Actionable** – It points toward building an intelligent, responsive system.
* **Aligned with your AIML focus** – It integrates unsupervised learning, behavioral analysis, and scalability.

**17. Validating the Problem Statement with Stakeholders for Alignment**

**Validation Plan:**

Engage stakeholders through interviews, surveys, and demonstrations to confirm the relevance of the plagiarism checker. Key questions will evaluate the tool’s ability to detect similarity, support ethical writing, and reduce citation errors. Continuous feedback will help improve the system’s alignment with the needs of students, educators, publishers, and developers.

|  |  |  |  |
| --- | --- | --- | --- |
| Stakeholder/User | Role | Feedback on Problem Statement | Suggestions for Improvement |
| |  | | --- | | Honest Users |  |  | | --- | |  | | **End Users** | |  | | --- | | **Ensure the system does not wrongly flag genuine users and promotes fair promo distribution.** |  |  | | --- | |  | | |  | | --- | | **Add a trust score or appeal process for wrongly flagged accounts.** |  |  | | --- | |  | |
| |  | | --- | | Fraud Analysts |  |  | | --- | |  | | |  | | --- | | **End Users** |  |  | | --- | |  |  |  | | --- | |  | | |  | | --- | | **Confirm the system can catch evolving fraud techniques and patterns.** |  |  | | --- | |  | | |  | | --- | | **Include anomaly score explanations and fraud behavior breakdown.** |  |  | | --- | |  | |
| |  | | --- | | Business Stakeholders |  |  | | --- | |  | | |  | | --- | | **Decision Makers** |  |  | | --- | |  | | |  | | --- | | **Validate that the system can reduce financial loss from promo misuse.** |  |  | | --- | |  | | |  | | --- | | **Add financial impact estimates and ROI dashboards.** |  |  | | --- | |  | |
| |  | | --- | | Platform Admins |  |  | | --- | |  | | **Operations** | |  | | --- | | **Ensure integration is smooth and alerts are actionable.** |  |  | | --- | |  | | |  | | --- | | **Allow admin-customizable fraud thresholds and rule overrides.** |  |  | | --- | |  | |

**18. Ideation**

**Ideation Process:**

|  |  |  |  |
| --- | --- | --- | --- |
| Idea Number | Proposed Solution | Key Features/Benefits | Challenges/Concerns |
| Idea 1 | |  | | --- | | **AI-Based Behavioral Fraud Detection** |  |  | | --- | |  | | |  | | --- | | **Uses unsupervised learning to detect abnormal patterns like multiple logins, fake addresses, and repeat promo usage** |  |  | | --- | |  | | |  | | --- | | **Requires large dataset for effective training and tuning to minimize false positives** |  |  | | --- | |  | |
| Idea 2 | |  | | --- | | **Real-Time Promo Abuse Scoring System** |  |  | | --- | |  | | |  | | --- | | **Assigns a fraud probability score during each promo code usage or registration** |  |  | | --- | |  | | |  | | --- | | **Ensuring real-time performance without affecting user experience** |  |  | | --- | |  | |
| Idea 3 | |  | | --- | | **Admin Dashboard for Fraud Monitoring** |  |  | | --- | |  | | |  | | --- | | **Visual reports of flagged users, fraud signals, and promo code performance** |  |  | | --- | |  | | |  | | --- | | **Balancing simplicity and technical depth for different types of users** |  |  | | --- | |  | |
| Idea 4 | |  | | --- | | **Device/IP Address Clustering** |  |  | | --- | |  | | |  | | --- | | **Detects users registering multiple accounts from the same IP, device ID, or proxy network** |  |  | | --- | |  | | |  | | --- | | **Avoiding false flagging in cases like shared networks (e.g., hostels or families)** |  |  | | --- | |  | |
| Idea 5 | |  | | --- | | **Alert and Notification System** |  |  | | --- | |  | | |  | | --- | | **Sends instant alerts to admins and logs behavior patterns for investigation** |  |  | | --- | |  | | **Ensuring only significant and actionable alerts are sent to avoid overload** |

**Solution Concept Form**

**1. Problem Statement:**

* Promo code abuse leads to significant financial loss and unfair user experiences. Existing manual and rule-based systems are inefficient in detecting sophisticated fraudulent behaviors.

**2. Target Audience:**

* Online payment platforms, fraud analysts, marketing teams, and genuine app users who are affected by the misuse of promotional codes.

**3. Solution Overview:**

* A machine learning-based system that uses statistical signals and unsupervised learning to detect suspicious behavior patterns in real time, flagging fraudulent users and preventing repeated promo code abuse.

**4. Key Features:**

| **Feature** | **Description** |
| --- | --- |
| **Feature 1** | |  | | --- | | **Behavioral analysis using unsupervised learning to detect fraudulent patterns** |  |  | | --- | |  | |
| **Feature 2** | |  | | --- | | **Real-time fraud scoring system that flags suspicious users instantly** |  |  | | --- | |  | |
| **Feature 3** | Admin dashboard with detailed reports, alerts, and fraud heatmaps |

**5. Benefits:**

| **Benefit** | **Description** |
| --- | --- |
| **Benefit 1** | |  | | --- | | **Saves marketing costs by preventing repeated misuse of promotional codes** |  |  | | --- | |  | |
| **Benefit 2** | |  | | --- | | **Automatically detects fraud with minimal manual intervention** |  |  | | --- | |  | |
| **Benefit 3** | Enhances user trust and fairness in promotional campaigns |

**6. Unique Value Proposition (UVP):**

* Unlike static rule-based systems, this AI-powered solution adapts to new fraud patterns and delivers real-time detection while respecting user privacy—making it both effective and scalable.

**7. Key Metrics:**

| **Metric** | **Measurement** |
| --- | --- |
| **Metric 1** | **[What is the key metric to measure success?]** |
| **Metric 2** | **[What is another key metric for tracking progress?]** |

**8. Feasibility Assessment:**

* **[Provide a brief evaluation of how achievable or practical this solution is (consider resources, time, and technology).]**

**9. Next Steps:**

* **[Outline the next steps for further developing or prototyping this solution.]**