Product Requirements Document (PRD)

By - Aryaraj Singh

Razorpay AI-Powered Fraud Detection System

1. Introduction

This document outlines the product requirements for Razorpay's new AI-powered Fraud Detection System. This system aims to provide a comprehensive solution to address the growing concerns around fraud in the Indian digital payments landscape, with a particular focus on UPI fraud prevention. By leveraging AI and machine learning, this system will enhance Razorpay's existing fraud prevention capabilities and provide merchants with real-time protection, advanced analytics, and customizable fraud rules.

2. Market Context

2.1 Indian Digital Payments Market

The Indian digital payments market is experiencing rapid growth, driven by factors such as increased smartphone penetration, government initiatives promoting digital transactions, and the rise of e-commerce. In 2023, the market size reached US$320 billion and is projected to reach US$624 billion by 2032, exhibiting a CAGR of 7.7% [1]. Furthermore, the market size is projected to reach $10.15 billion by 2025 [2]. UPI has emerged as a dominant force in this ecosystem, with transaction volumes growing from 92 crore in FY 2017-18 to 13,116 crore in FY 2023-24 [3]. Notably, UPI frauds constitute a significant portion of these incidents, highlighting the need for robust UPI-specific fraud prevention measures [4].

2.2 Razorpay's Market Position

Razorpay has established itself as a leading player in the Indian digital payments market. The company has achieved an annualized Total Payment Volume (TPV) of $150 billion, securing a majority market share in the digital payments processing category [5]. This strong market position provides a solid foundation for the launch of a new AI-powered fraud detection system.

2.3 Key Competitors

Razorpay faces competition from other payment gateway providers in India, including:

- **Pine Labs:** Pine Labs offers a range of payment solutions, including POS terminals, online payment gateways, and fraud detection tools. They focus on providing secure payment processing and fraud prevention for in-store and online transactions [6]. They utilize real-time transaction monitoring to identify suspicious patterns, such as multiple email IDs associated with the same customer [7].
- **Stripe:** Stripe is a global payment gateway provider that has expanded its presence in India. They offer a comprehensive suite of fraud prevention solutions, including machine learning-based fraud detection and customizable risk rules [8]. Their partnerships with major card networks and banks, including Visa, Mastercard, and American Express, provide them with access to valuable data sources like TC40s and SAFE reports for enhanced fraud detection [8].
- **PayU:** PayU is another major player in the Indian digital payments market, offering a variety of payment solutions for businesses of all sizes. They provide fraud prevention tools and security features to protect merchants and customers [9].

2.4 Regulatory Landscape

The Reserve Bank of India (RBI) has introduced regulations for payment aggregators and payment gateways to ensure secure and transparent payment processing. These regulations include requirements for licensing, governance, KYC/AML compliance, and data security [10]. These regulations also include stipulations on the settlement and maintenance of escrow accounts to safeguard customer funds [11]. Razorpay's new fraud detection system must comply with all relevant RBI guidelines, including PCI DSS and PA/PG regulations.

2.5 RBI's Digital Payments Intelligence Platform

The Reserve Bank of India (RBI) is proposing the establishment of a Digital Payments Intelligence Platform to combat the rising incidence of fraud in the digital payments ecosystem [12]. This platform aims to collect and analyze data from various sources to identify fraud trends, assess risks, and develop proactive fraud prevention measures. This initiative highlights the RBI's commitment to strengthening the security of the digital payments landscape in India.

3. Razorpay Ecosystem

3.1 Existing Product Suite

Razorpay offers a comprehensive suite of products that cater to the diverse needs of businesses in the Indian market. These products include:

- **Payment Gateway:** Razorpay's core offering allows businesses to accept payments online through various methods, including credit cards, debit cards, net banking, UPI, and wallets [13].

- **RazorpayX:** A neo-banking platform that provides businesses with current accounts, payroll processing, vendor payments, and other financial management tools [14].
- **Magic Checkout:** A checkout solution designed to improve conversion rates and reduce return-to-origin (RTO) rates by providing a faster and more seamless checkout experience [15].
- **Route:** A payment routing and reconciliation solution that enables businesses to optimize payment success rates and manage complex payment flows [16].
- **RAY:** An AI-powered assistant that provides businesses with insights and support for payments and payroll management [17].

3.2 Integration with Existing Products

The new fraud detection system will be seamlessly integrated with Razorpay's existing product suite. This integration will enable the system to leverage data from various sources, such as payment transactions, customer profiles, and risk assessments, to provide a holistic view of fraud risk.

Product	Integration Points	Benefits
Payment Gateway	Real-time transaction monitoring, risk scoring, fraud alerts	Enhanced fraud prevention during payment processing [18]
RazorpayX	KYC/AML data integration, risk assessment for payouts	Improved fraud detection for business banking operations
Magic Checkout	Fraud checks during checkout, risk-based authentication	Reduced fraud risk and improved conversion rates
Route	Fraud monitoring for payment routing, risk-based routing decisions	Optimized payment success rates and reduced fraud losses
RAY	AI-powered insights and recommendations for fraud prevention	Enhanced fraud detection capabilities and user experience

3.3 Current Fraud Prevention Capabilities

Razorpay currently employs various fraud prevention measures, including:

- **Tokenization:** Securely storing sensitive card details in the form of tokens to protect against data breaches [19].
- **Encryption:** Encrypting payment information during transmission to ensure data confidentiality [20].
- **Authentication:** Implementing strong authentication methods, such as OTPs and 3D Secure, to verify user identity [20].
- **Risk Monitoring:** Monitoring payment and refund patterns to identify suspicious activities [19].
- **KYC/AML Verification:** Conducting background checks and KYC verification to mitigate fraud risk [19].
- **Razorpay FraudShield:** An AI-ML powered risk engine that analyzes payment data, tracks customer disputes, and helps mitigate chargebacks in international payments [21].

3.4 Areas for Improvement

While Razorpay has existing fraud prevention measures in place, there are areas for improvement:

- **Limited AI/ML Capabilities:** The current system relies primarily on rule-based fraud detection, which may not be effective in identifying sophisticated fraud patterns. For example, the current system might struggle to identify "man-in-the-middle" attacks where fraudsters intercept and manipulate payment information.
- **Lack of Real-time Analytics:** Merchants have limited access to real-time fraud analytics and insights to make informed decisions. This can hinder their ability to proactively identify and respond to emerging fraud trends.
- **Inadequate UPI Fraud Prevention:** Specific features for preventing UPI fraud, such as Virtual Address Verification (VAV) and real-time transaction monitoring, are lacking. This leaves merchants vulnerable to UPI-specific fraud attacks.
- **Limited International Payment Monitoring:** Cross-border fraud detection and currency exchange rate monitoring capabilities are limited. This can expose businesses to financial losses from international fraud schemes.

4. Problem Statement

4.1 Impact of Fraud on Razorpay and Merchants

Fraudulent activities pose a significant threat to Razorpay and its merchants.

Impact of Fraud on Razorpay:

- **Financial Losses:** Fraudulent transactions result in direct financial losses for Razorpay.
- **Reputational Damage:** Fraud incidents can damage the reputation of Razorpay, leading to customer distrust and loss of business.

Impact of Fraud on Merchants:

- **Financial Losses:** Fraudulent transactions and chargebacks directly impact merchants' revenue and profitability. In FY 2023-24, digital payment fraud in India reached $175 million [22].
- **Chargebacks:** Merchants face chargebacks and associated fees when customers dispute fraudulent transactions. Chargebacks can cause losses of 2-3% of total revenue [23].
- **Reputational Damage:** Fraud incidents can damage the reputation of merchants, leading to customer distrust and loss of business.
- **Operational Inefficiencies:** Investigating and resolving fraud cases consume valuable time and resources for merchants.
- **Payment Declines:** Payment declines, often a consequence of overly strict fraud prevention, impact a significant portion of customers (33%), leading to a poor customer experience and potential loss of revenue [23].
- **Manual Fraud Management Costs:** Globally, manual fraud management is estimated to consume 5-15% of revenue annually, highlighting the need for efficient, automated solutions [23].

4.2 Merchant Pain Points

Merchants experience various pain points due to fraud:

- **Financial Losses:** Fraudulent transactions and chargebacks directly impact merchants' revenue and profitability [24]. Studies indicate that the total cost to a merchant for accepting one fraudulent transaction can be more than double the transaction value itself [25].
- **Operational Burden:** Managing fraud cases and disputes requires significant time and effort, diverting resources from core business activities [26].
- **Reputational Damage:** Fraud incidents can erode customer trust and negatively impact brand image [25].
- **Limited Control:** Merchants often lack the tools and insights to effectively prevent and manage fraud [27].

4.3 Competitive Analysis

Competitor	Strengths	Weaknesses
Pine Labs	Strong focus on in-store payment security, wide network of POS terminals	Limited AI/ML capabilities for online fraud detection
Stripe	Advanced machine learning-based fraud detection, global expertise	Pricing may be higher for some merchants

4.4 Market Opportunity

The market opportunity for an AI-powered fraud detection system in India is significant. The fraud detection and prevention market in India is projected to grow at a CAGR of 21.2% during 2024-2032 [28]. This growth is driven by the increasing adoption of digital payments, the rising sophistication of fraud techniques, and the need for real-time fraud prevention solutions.

5. Product Specifications

5.1 Core AI/ML Capabilities

The new fraud detection system will leverage the following AI/ML capabilities:

- **Real-time Anomaly Detection:** The system will continuously analyze transaction data in real-time to identify anomalies and suspicious patterns that deviate from expected behavior [29]. A key advantage of these AI/ML capabilities is their ability to adapt to new and evolving fraud patterns, ensuring the system remains effective against emerging threats [30].
- **Behavioral Biometrics:** The system will analyze user behavior, such as typing speed, mouse movements, and device interactions, to identify and prevent account takeover attempts [31].
- **Device Fingerprinting:** The system will create unique device fingerprints based on various attributes, such as device type, operating system, and browser information, to identify potentially risky devices [30].
- **Machine Learning Models:** The system will utilize advanced machine learning models trained on vast datasets to predict and prevent fraud with high accuracy [32].

5.2 Integration with Razorpay Dashboard

The new system will be seamlessly integrated with the existing Razorpay Dashboard, providing merchants with:

- **Real-time Fraud Alerts:** Merchants will receive real-time alerts for suspicious transactions, enabling them to take immediate action [18].
- **Detailed Analytics:** The system will provide merchants with detailed fraud analytics, including fraud trends, chargeback rates, and risk scores, to gain insights into their fraud exposure [33].
- **Customizable Fraud Rules:** Merchants will be able to define and customize fraud rules based on their specific business needs and risk tolerance [34].

5.3 UPI Fraud Prevention

The system will incorporate specific features for preventing UPI fraud:

- **Virtual Address Verification (VAV):** The system will verify the authenticity of virtual payment addresses (VPAs) to prevent fraudsters from using fake or compromised VPAs [35].
- **Risk Scoring:** The system will assign risk scores to UPI transactions based on various factors, such as transaction amount, user history, and device information, to identify high-risk transactions [36].
- **Real-time Transaction Monitoring:** The system will monitor UPI transactions in real-time to detect and prevent fraudulent activities [37].

5.4 International Payment Monitoring

The system will address the need for international payment monitoring by:

- **Cross-border Fraud Detection:** The system will utilize machine learning models trained on global datasets to identify and prevent cross-border fraud [38].
- **Currency Exchange Rate Monitoring:** The system will monitor currency exchange rates to detect and prevent fraudulent activities related to currency manipulation [39].

5.5 RBI Compliance

The system will be designed and implemented to comply with all relevant RBI guidelines, including:

- **PCI DSS Compliance:** The system will adhere to the Payment Card Industry Data Security Standard (PCI DSS) to ensure the secure handling of cardholder data [11].
- **PA/PG Regulations:** The system will comply with the RBI's regulations for payment aggregators and payment gateways, including KYC/AML requirements and data security standards [40].

6. Technical Requirements

6.1 System Integration

The new system will need to integrate with Razorpay's existing infrastructure, including:

- **APIs:** The system will utilize APIs to exchange data with Razorpay's payment gateway, RazorpayX platform, and other products.
- **Databases:** The system will need to access and process data from Razorpay's transaction databases, customer databases, and other relevant data sources.
- **Dashboards:** The system will integrate with the Razorpay Dashboard to provide merchants with real-time alerts, analytics, and fraud management tools.

6.2 Data Processing Capabilities

The system must have the capacity to handle large volumes of transaction data in real-time. This requires:

- **Scalable Infrastructure:** The system should be deployed on a scalable infrastructure that can handle increasing data volumes and transaction throughput.
- **Real-time Data Processing:** The system should utilize technologies such as stream processing and in-memory databases to process data in real-time. Real-time data processing is crucial for preventing fraud before it occurs, minimizing financial losses and enabling immediate intervention [41].
- **Efficient Data Storage:** The system should utilize efficient data storage solutions to manage large volumes of historical transaction data. This includes implementing robust data preprocessing techniques, such as data cleaning, normalization, and feature engineering, to ensure data quality and optimal model performance [42]. It's crucial to ensure high-quality data for training the AI/ML models, as data accuracy and comprehensiveness directly impact the system's performance [43].

6.3 Security Standards

The system must implement robust security standards and protocols to protect sensitive data. This includes:

- **Data Encryption:** Encrypting all sensitive data at rest and in transit using industry-standard encryption algorithms.
- **Access Control:** Implementing strict access control measures to limit access to sensitive data based on roles and permissions.
- **Regular Security Audits:** Conducting regular security audits and vulnerability assessments to identify and address potential security risks.

7. Success Metrics

The success of the new AI-powered Fraud Detection System will be measured based on the following metrics:

Metric	Target
Fraud Reduction	20% reduction in fraud transaction value within 6 months of launch
Chargeback Reduction	15% reduction in chargeback rate within 12 months of launch

Metric	Target
False Positive Rate	Maintain a false positive rate below 1%
Transaction Approval Rate	Achieve a transaction approval rate of 99% for legitimate transactions
Revenue Impact	10% increase in revenue from reduced fraud losses within 12 months of launch

8. Timeline and Resources

8.1 Timeline

The following is a tentative timeline for the development, testing, and launch of the new system:

- **Phase 1 (3 months):** Requirements gathering, system design, and development of core AI/ML capabilities.
- **Phase 2 (2 months):** System integration, testing, and pilot launch with select merchants.
- **Phase 3 (1 month):** Full-scale launch and ongoing monitoring and optimization.

These durations are based on internal estimates and previous project experience with similar AI-driven product development initiatives.

8.2 Resources

The project will require the following resources:

- **Personnel:** A dedicated team of data scientists, engineers, and product managers.
- **Budget:** Allocate budget for development, infrastructure, and ongoing maintenance.
- **Infrastructure:** Access to cloud computing resources and data storage solutions.

9. Go-to-Market Strategy

9.1 Target Audience Segmentation

The go-to-market strategy will focus on specific merchant segments to maximize adoption and impact. This includes:

- **High-risk Merchants:** Merchants in industries with high fraud rates, such as e-commerce

and online gaming.
- **Large Enterprises:** Large businesses with high transaction volumes and complex payment flows.
- **Merchants with International Transactions:** Businesses processing cross-border payments and dealing with multiple currencies.

9.2 Competitive Analysis

The go-to-market strategy will consider the competitive landscape and position the AI-powered Fraud Detection System as a superior solution. This includes:

- **Highlighting Key Differentiators:** Emphasizing the system's advanced AI/ML capabilities, real-time fraud detection, and seamless integration with Razorpay's existing product suite.
- **Competitive Pricing:** Offering competitive pricing plans that cater to the needs of different merchant segments.

9.3 Channel Strategy

A multi-channel approach will be used to reach target audiences and promote the new system:

- **Online Channels:** Utilizing Razorpay's website, blog, and social media platforms to create awareness and generate leads.
- **Direct Sales:** Leveraging Razorpay's sales team to reach out to target merchants and offer personalized solutions.
- **Partnerships:** Collaborating with industry partners and technology providers to expand reach and promote the system.

10. Conclusion

The development of an AI-powered Fraud Detection System is a strategic initiative for Razorpay to address the growing challenges of fraud in the Indian digital payments market. By leveraging AI and machine learning, this system will enhance Razorpay's existing fraud prevention capabilities, provide merchants with real-time protection, and contribute to a more secure and trustworthy payment ecosystem. This system will not only help reduce financial losses and operational burdens for merchants but also enhance customer trust and strengthen Razorpay's position as a leader in the digital payments industry.

Works cited

1. India Digital Payment Market Size, Share & Growth, 2032 - IMARC Group, accessed January 14, 2025, https://www.imarcgroup.com/india-digital-payment-market
2. Curbing Frauds in Cross-Border Remittance - HyperVerge, accessed January 14, 2025, https://hyperverge.co/blog/curbing-frauds-in-cross-border-remittance/
3. with value of UPI transactions reaching ₹200 lakh crore in FY23-24 from ₹1 lakh crore in FY17-18 at CAGR of 138% UPI now seamlessly facilitates live transactions in 7 countries, including key markets such as UAE, Singapore, Bhutan, Nepal, Sri Lanka, France, and Mauritius - PIB, accessed January 14, 2025, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2057013
4. Payment Guide 6: Combating Payment Fraud | Worldline India, accessed January 14, 2025, https://worldline.com/en-in/home/main-navigation/resources/resources-hub/payment-guides/payment-guide-6-combating-payment-fraud
5. Razorpay records $150 bln in TPV, announces payment gateway 3.0, RAY & more - ET BFSI, accessed January 14, 2025, https://bfsi.economictimes.indiatimes.com/news/fintech/razorpay-records-150-bln-in-tpv-announces-payment-gateway-3-0-ray-more/107937080
6. Minimising payment fraud: Best practices for retailers - Pine Labs, accessed January 14, 2025, https://www.pinelabs.com/blog/minimising-payment-fraud-best-practices-for-retailers
7. Pine Labs, accessed January 14, 2025, https://www.pinelabs.com/media/Sunday-Guardian.pdf
8. Stripe Radar | Payment and Credit Card Fraud Prevention, accessed January 14, 2025, https://stripe.com/radar
9. 11 Best Payment Gateways in India (2025) - Aureate Labs, accessed January 14, 2025, https://aureatelabs.com/blog/best-payment-gateways-in-india/
10. stripe.com, accessed January 14, 2025, https://stripe.com/guides/rbi-guidelines-kyc-direction#:~:text=The%20Reserve%20Bank%20of%20India,and%20onboarding%2C%20the%20settlement%20and
11. strobes.co, accessed January 14, 2025, https://strobes.co/compliance/rbi-guidelines-for-payment-aggregators-payment-gateways/#:~:text=Payment%20Aggregators%20must%20ensure%20that,commingled%20with%20their%20operational%20funds.
12. RBI Proposes Digital Payments Intelligence Platform to Combat Rising Fraud, accessed January 14, 2025, https://www.outlookbusiness.com/corporate/rbi-proposes-digital-payments-intelligence-platform-to-combat-rising-fraud
13. Best Payment Gateway in India to Accept Online Payments - Razorpay, accessed January 14, 2025, https://razorpay.com/payment-gateway/
14. Simplify Your Business Finances with Automated Payments & Compliance - RazorpayX, accessed January 14, 2025, https://razorpay.com/x/
15. Razorpay Magic Checkout - Improve Conversions. Reduce RTOs ..., accessed January 14, 2025, https://razorpay.com/magic-checkout/
16. Route · Split and distribute payments, Automate vendor payouts, accessed January 14, 2025, https://razorpay.com/route/
17. Meet R.A.Y.- Your 24/7 On-Demand AI Concierge - Razorpay Blog, accessed January 14, 2025, https://razorpay.com/blog/meet-r-a-y-your-24-7-on-demand-ai-concierge/
18. Fraud Detection with Machine Learning and AI in 2025 - FOCAL, accessed January 14,

2025, https://www.getfocal.ai/blog/fraud-detection-with-machine-learning
19. Security For Customers | Razorpay Docs, accessed January 14, 2025, https://razorpay.com/docs/security/customers/
20. Payment Security Strategies in 2025 - Razorpay, accessed January 14, 2025, https://razorpay.com/blog/payment-security-types-explained/
21. Navigate payment risks, unlock the power of data with Razorpay's Shield Risk Engine, accessed January 14, 2025, https://razorpay.com/blog/navigate-payment-risks-with-razorpays-shield-risk-engine/
22. Facing a Surge in UPI Fraud, It's Time for India to Act - BankInfoSecurity, accessed January 14, 2025, https://www.bankinfosecurity.asia/blogs/facing-surge-in-upi-fraud-its-time-for-india-to-act-p-3634
23. Empowering Indian Businesses: How Razorpay SHIELD Secures International Payments, accessed January 14, 2025, https://razorpay.com/blog/razorpay-upticks-success-rates-razorpay-shield/
24. A comprehensive guide to payment fraud prevention for merchants - Signifyd, accessed January 14, 2025, https://www.signifyd.com/resources/fraud-101/payment-fraud-prevention-guide/
25. Understanding Merchant Liability in Credit Card and Payment Fraud - Signifyd, accessed January 14, 2025, https://www.signifyd.com/resources/fraud-101/merchant-liability-in-credit-card-fraud/
26. Merchant fraud 101: What businesses need to know - Stripe, accessed January 14, 2025, https://stripe.com/resources/more/merchant-fraud-101
27. Merchant Fraud | 5 New Types & How to Prevent Them - Zoot Enterprises, accessed January 14, 2025, https://zootsolutions.com/merchant-fraud/
28. India Fraud Detection and Prevention Market Report [2032] - IMARC Group, accessed January 14, 2025, https://www.imarcgroup.com/india-fraud-detection-prevention-market
29. AI & Machine Learning in Fraud Detection: What to Expect in 2024 - TrustDecision, accessed January 14, 2025, https://trustdecision.com/resources/blog/ai-machine-learning-fraud-detection-2024
30. What is AI/ML and why does it matter in fraud prevention? | Artificial Intelligence, accessed January 14, 2025, https://sift.com/blog/what-is-ai-ml-and-why-does-it-matter-in-fraud-prevention
31. How AI and Machine Learning Are Battling Global Financial Fraud, accessed January 14, 2025, https://insights.discoverglobalnetwork.com/insights/how-ai-and-machine-learning-are-battling-financial-fraud
32. Understanding AI Fraud Detection and Prevention Strategies | DigitalOcean, accessed January 14, 2025, https://www.digitalocean.com/resources/articles/ai-fraud-detection
33. UPI Fraud: Prevention Method for Customers & Businesses - Juspay, accessed January 14, 2025, https://juspay.io/blog/upi-fraud-protect-your-customers-and-your-business
34. How to Prevent UPI Frauds in India: Essential Tips and Best Practices for Secure Transactions - Sayyam Investments, accessed January 14, 2025, https://sayyaminvestments.in/prevent-upi-frauds-india.html
35. Understanding UPI frauds: Common scams and prevention tips, accessed January 14, 2025, https://www.pinelabs.com/blog/understanding-upi-frauds-common-scams-and-prevention-tips
36. What are UPI Frauds and Tips to Prevent it? - AU Small Finance Bank, accessed January 14, 2025, https://www.aubank.in/blogs/what-are-upi-frauds-and-tips-to-prevent-it
37. Cracking the code: How to master UPI fraud management? MintGenie explains | Mint,

accessed January 14, 2025, https://www.livemint.com/money/personal-finance/navigating-and-combatting-upi-frauds-by-mastering-fraud-management-digital-transactions-online-payments-phishing-11706511999468.html
38. How is cross-border payment fraud being tackled? - Sibos, accessed January 14, 2025, https://www.sibos.com/conference/hub/articles/how-cross-border-payment-fraud-being-tackled
39. Cross-border payments: fraud mitigation strategies - Financier Worldwide, accessed January 14, 2025, https://www.financierworldwide.com/cross-border-payments-fraud-mitigation-strategies
40. Understanding RBI guidelines: Navigating payment aggregators in India - Winvesta, accessed January 14, 2025, https://www.winvesta.in/blog/understanding-rbi-guidelines-navigating-payment-aggregators-in-india
41. Real-Time Fraud Detection - Everything You Need To Know - HyperVerge, accessed January 14, 2025, https://hyperverge.co/blog/real-time-fraud-detection/
42. The Power of AI in Fraud Detection: Techniques, Challenges, and Strategies - RTS Labs, accessed January 14, 2025, https://rtslabs.com/ai-in-fraud-detection
43. AI for Fraud Detection: Techniques and Implementation - RapidCanvas, accessed January 14, 2025, https://www.rapidcanvas.ai/blogs/ai-for-fraud-detection-techniques-and-implementation