PROBLEM STATEMENTS FOR OCP 2.0

The below focus area is not restricted, any other innovative solution closed to below focus areas may also be considered for evaluation.

S. No.	Focus Area	Description	What Expected
1.	Digital Financial Inclusion	Despite advancements in digital banking and payment solutions, a large section of the rural and semi-urban population in India still lacks access to basic financial services.	How might we design and deliver easy- to-use, low-cost fintech solutions that cater to the needs of the financially underserved or excluded, especially in regions with limited internet access and digital literacy?
2.	Fraud Detection & Cyber Security	Fintech platforms are increasingly becoming targets of sophisticated fraud and cyber attacks.	How might we develop real-time, AI- driven security solutions that can proactively detect and mitigate financial fraud and ensure data privacy without affecting user experience?
3.	KYC and Onboarding Efficiency	Lengthy and cumbersome KYC (Know Your Customer) processes lead to high dropout rates and delayed customer acquisition.	How might we streamline KYC processes using digital tools such as e- KYC, video verification, or blockchain to improve onboarding speed, accuracy, and compliance?
4.	Trust and Transparency	Many consumers still hesitate to use digital financial services due to a lack of trust and understanding of how their data and money are handled.	How might we build greater transparency, trust, and financial literacy into fintech platforms, especially among first-time digital users?
5.	Credit Scoring for the Underserved	Traditional credit scoring models exclude individuals with no formal credit history, preventing them from accessing loans or credit-based services.	How might we create alternative credit scoring systems using unconventional data (e.g., mobile usage, utility payments, behavioral data) to assess creditworthiness of new-to-credit customers?
6.	Cyber Fraud & Money Tracing Back to the Victim	Despite growing digital literacy and advanced cyber security tools, cyber fraud continues to rise rapidly, exploiting loopholes in financial systems, social engineering tactics, and digital payment ecosystems.	To design and implement a robust, scalable, and real-time mechanism that: · Enables seamless tracing of fraudulent digital financial transactions across multiple

		Victims, often unaware or helpless during the initial phase of the fraud, face immense difficulty in getting their lost money traced and recovered due to fragmented jurisdiction, lack of real-time coordination among banks and law enforcement, cross-border complexities, and limited digital forensics capabilities. The absence of a unified framework for end-to-end money trail analysis further delays or prevents restitution to victims.	platforms and intermediaries, · Facilitates secure coordination among banks, fintechs, and law enforcement agencies, · Ensures timely freezing and potential reversal of fraudulent transfers, and · Ultimately returns the stolen funds to the rightful owner, while maintaining compliance with data privacy and legal requirements. · The solution must address technological gaps, jurisdictional hurdles, and user awareness barriers to make recovery from cyber fraud more accessible, efficient, and victim-centric.

Note: Innovators, startups, fintech professionals, faculties, researchers, students & women entrepreneurs are also encouraged to develop innovative solutions and participate to the OCP.