A COMPARATIVE ANALYSIS OF PSP FRAMEWORKS AND ECOSYSTEM CHALLENGES IN INDIA AND UZBEKISTAN

Rajesh Gajjar
Dual Degree Master's LL.M. Student
National Forensic Sciences University,
India and Tashkent State University of Law, Uzbekistan
https://doi.org/10.5281/zenodo.21187150

=

Abstract

Payment Services Providers (PSPs) have become indispensable to digital financial ecosystems, enabling secure, interoperable, and real-time transactions across domestic and international markets. India and Uzbekistan, two rapidly digitizing economies have witnessed significant expansion in digital payments driven by regulatory modernization, fintech innovation, and consumer adoption. However, PSPs in both jurisdictions face complex challenges relating to regulatory compliance, cybersecurity, digital forensics, operational risks, and cross-border governance. This article provides a doctrinal and comparative analysis of PSP frameworks in India and Uzbekistan, examining statutory regimes, cybercrime vulnerabilities, forensic constraints, and systemic barriers. It concludes with policy recommendations aimed at strengthening PSP resilience, regulatory clarity, and cyber-forensic readiness.

Keywords

Payment Services Providers (PSP), Digital Payments, Central Bank of Uzbekistan, Data Localization, Cross-Border Payments

1. Introduction

Digital payments have transformed financial governance, economic participation, and national security. PSPs comprising banks, fintech companies, payment gateways, wallet providers and cross-border remittance platforms operate at the intersection of finance, technology and law. Their role is particularly significant in emerging economies such as India and Uzbekistan, where digital transformation is accelerating.

India's digital payments revolution, led by the Unified Payments Interface (UPI), Aadhaar enabled systems, and robust regulatory oversight by the Reserve Bank of India (RBI), has created one of the world's largest real-time payment infrastructures. Uzbekistan, meanwhile, is undergoing rapid modernization through the Central Bank's digital transformation agenda, expansion of online banking, and integration of domestic and international PSPs.

Despite progress, PSPs in both jurisdictions face substantial challenges: regulatory fragmentation, cybercrime escalation, data protection constraints, interoperability gaps, and cross-border compliance complexities. These challenges are particularly relevant for cybercrime law and digital forensics, where PSPs serve as critical nodes for evidence collection, fraud detection, and financial investigation.

2. Regulatory Framework Governing PSPs

2.1 India

India's digital payment ecosystem is a sophisticated framework designed to balance rapid innovation with systemic stability. At its core, the **Payment and Settlement Systems Act, 2007 (PSS Act)** serves as the primary legislation, granting the RBI absolute authority to

oversee all clearing and settlement systems. This ensures that every transaction is backed by a legal mandate for finality.

The **2020 RBI Guidelines for Payment Aggregators (PAs)** represented a major shift, bringing intermediaries under direct regulation. These rules mandate strict capital adequacy (initially ₹15 crore) and the use of escrow accounts to ensure that merchant funds are never co-mingled with a provider's operational cash. Similarly, **PPI Regulations** govern "stored value" systems like wallets, categorizing them by KYC levels to mitigate money laundering risks.

While the RBI handles the macro-legalities, the **NPCI** manages the operational rules for **UPI**, focusing on real-time interoperability and fraud management. Finally, the **IT Act** and **2022 CERT-In Directions** provide the cybersecurity backbone, requiring entities to report security breaches within six hours—a critical requirement in a high-volume financial environment.

Digital Personal Data Protection Act, 2023 – Consent, data fiduciary obligations, cross-border data transfer restrictions.

India's regulatory approach is characterized by **high compliance intensity**, **real-time supervision**, and **stringent licensing norms**, especially for fintech PSPs.

2.2 Uzbekistan

Uzbekistan's PSP ecosystem is defined by a state-centric model prioritizing financial stability and local control. The **Law on Payments and Payment Systems (2019)** acts as the primary pillar, establishing licensing and operational standards for all providers. Oversight of digital wallets and online banking is managed via **Central Bank Regulations**, while the **Law on Personal Data** mandates strict data localization.

Security is handled by the **Ministry of Digital Technologies**, which enforces a cybersecurity framework for incident reporting. For international players, the **Regulations for Foreign PSPs** require local partnerships, reflecting Uzbekistan's focus on domestic sovereignty over global digital platforms.

3. Challenges Faced by PSPs in India and Uzbekistan

3.1 Regulatory and Licensing Challenges

India

High compliance burden due to capital adequacy norms, escrow requirements, and periodic audits. Frequent regulatory updates create uncertainty for fintech startups. Restrictions on credit-based payments limit innovation in BNPL and micro-credit PSP models. Data localization mandates increase operational costs for foreign PSPs.

Uzbekistan

Complex licensing procedures, especially for foreign PSPs. Regulatory ambiguity due to rapid digital transformation. Limited sandbox environments slow fintech experimentation. Restrictions on foreign digital payment platforms limit cross-border expansion.

3.2 Cybersecurity and Digital Forensics Challenges

India

High volume of cyber fraud: UPI phishing, QR-code scams, SIM-swap attacks, mule accounts. CERT-In's strict 6-hour incident reporting requirement strains PSP compliance. Weak consumer cyber hygiene increases fraud exposure. Digital forensics complexity due to encrypted transactions and distributed ledgers.

Uzbekistan

Growing sophistication of cybercrime: card-skimming, account takeover attacks. Limited forensic capacity compared to India. Dependence on foreign technology creates infrastructure vulnerabilities. Challenges in evidence preservation due to server distribution and localization rules.

3.3 Operational and Technological Challenges

India

Interoperability issues between legacy banking systems and modern PSP platforms. High transaction volumes strain infrastructure during peak periods. Merchant onboarding risks due to fake or fraudulent merchants. Competition with state-backed platforms reduces profitability for private PSPs.

Uzbekistan

Limited digital literacy among rural populations. Infrastructure gaps affect PSP performance. Slow adoption of advanced fintech tools such as tokenization and AI-based fraud detection. Strong dependence on cash economy reduces PSP penetration.

3.4 Cross-Border and AML Compliance Challenges

India

Strict AML/KYC norms under PMLA and RBI guidelines. High risk of cross-border money laundering through digital wallets and crypto-linked PSPs. Complex compliance requirements for foreign PSPs due to data localization.

Uzbekistan

AML enforcement still developing; PSPs face inconsistent compliance expectations. Cross-border remittance restrictions complicate migrant worker payments. Limited integration with global AML databases increases fraud exposure.

4. Comparative Analysis

A comparative analysis of the regulatory frameworks governing Payment Service Providers (PSPs) in India and Uzbekistan reveals two distinct approaches to managing digital financial ecosystems, shaped by their respective market maturities and strategic priorities. India has established a mature, highly sophisticated, and innovation-driven landscape anchored by the Payment and Settlement Systems Act (2007). The Reserve Bank of India (RBI) operates with intense compliance oversight, mandating strict capital adequacy, escrow isolation for payment aggregators, and an aggressive six-hour cybersecurity breach reporting window via CERT-In. Conversely, Uzbekistan operates a developing, state-centric model governed by its 2019 Law on Payments and Payment Systems. While India focuses on scaling real-time interoperability (via the NPCI and UPI) while mitigating macro-systemic risks, Uzbekistan prioritizes domestic sovereignty, financial stability, and local control, actively requiring foreign platforms to secure local partnerships to operate.

Furthermore, the operational and cybersecurity challenges faced by PSPs in both jurisdictions reflect their varying stages of fintech adoption. Indian PSPs grapple with the side effects of massive transaction volumes, including sophisticated UPI phishing, infrastructure strain during peak hours, and complex digital forensics over distributed ledgers. In contrast, Uzbekistani providers face foundational hurdles, such as navigating a heavily cash-dependent economy, addressing digital literacy gaps among rural populations, and operating with limited domestic forensic capacity. Both nations enforce strict data localization, India through the Digital Personal Data Protection Act (2023) and Uzbekistan through its Law on Personal Data yet their execution differs; India uses localization to safeguard a highly interconnected, open fintech ecosystem, whereas Uzbekistan treats it as a

buffer to secure domestic infrastructure against foreign technological dependencies. Ultimately, India presents a high-velocity, high-compliance environment focused on systemic resilience, while Uzbekistan offers a protective, evolving framework centred on infrastructural transition and sovereign risk management.

Category	India	Uzbekistan
Primary Legislation	Payment and Settlement Systems Act, 2007 (PSS Act); RBI Guidelines for Payment Aggregators (2020).	Law on Payments and Payment Systems (2019).
Primary Regulatory Authorities	Reserve Bank of India (RBI) for macro-legalities; National Payments Corporation of India (NPCI) for UPI operational rules.	Central Bank of Uzbekistan (via Central Bank Regulations).
Market Philosophy & Approach	Sophisticated framework balancing rapid innovation with systemic stability; high compliance intensity.	State-centric model prioritizing financial stability, domestic sovereignty, and local control.
Foreign Provider Entry	Face high operational costs due to data localization and strict licensing.	Mandates local partnerships; strict restrictions on foreign digital platforms.
Data Protection & Cybersecurity	Digital Personal Data Protection Act (2023) governs consent; IT Act and CERT-In require breach reporting within **6 hours**.	Law on Personal Data mandates strict data localization; Ministry of Digital Technologies handles incident reporting.
Regulatory & Licensing Challenges	High compliance burden (capital adequacy, escrow accounts), frequent policy updates, and credit restrictions (e.g., BNPL).	Complex licensing procedures, regulatory ambiguity, and limited sandbox environments for fintech experimentation.
Cybersecurity & Forensics Challenges	High volume of UPI phishing, QR scams, and SIM swaps; high strain from the 6-hour reporting window; weak consumer hygiene.	Growing card skimming and account takeovers; limited domestic forensic capacity; reliance on foreign technology infrastructure.

Category	India	Uzbekistan
Operational & Tech Hurdles	Legacy banking system interoperability issues; infrastructure strain during peak volumes; merchant onboarding fraud risks.	Limited digital literacy among rural populations; infrastructure gaps; high cash-dependence; slow adoption of AI/tokenization.
AML & Cross-Border Compliance	Strict AML/KYC norms under PMLA; high risk of cross-border laundering via crypto/wallets; complex data localization.	Developing AML enforcement with inconsistent expectations; remittance restrictions affecting migrant worker payments.

Table 1: A Comparative Analysis of PSP Frameworks of India and Uzbekistan

5. Cybercrime Law and Digital Forensics Implications

PSPs are central to cybercrime investigations, digital evidence collection, and financial forensics. Key implications include:

- Complex attribution challenges in cross- border fraud.
- Legal admissibility of digital payment records under Indian and Uzbek law.
- Need for harmonized cybercrime frameworks between India and Uzbekistan.
- Importance of AI- driven fraud detection and forensic automation.
- Challenges in accessing encrypted or tokenized transaction data.

6. Recommendations

India

Expand regulatory sandboxes for fintech innovation. Strengthen consumer cyber- awareness programs. Improve forensic access protocols for PSP data. Encourage AI- driven fraud detection systems.

Uzbekistan

Simplify licensing procedures for PSPs. Invest in national cybersecurity infrastructure. Expand digital literacy programs. Strengthen AML/KYC frameworks aligned with FATF standards.

7. Discussion

This comparative analysis reveals that while India and Uzbekistan are both driving digital financial transformation, they face distinct challenges shaped by their varying stages of regulatory maturity. India boasts a highly sophisticated, high-volume ecosystem anchored by the Unified Payments Interface (UPI). However, its payment service providers (PSPs) face intense operational pressure from strict compliance costs, mandatory data localization, and a highly targeted cyber threat landscape. Conversely, Uzbekistan is in a foundational phase, focused on building a secure regulatory framework through its Central Bank and the Law on Payments. While its cyber threat volume is lower, Uzbekistan is constrained by institutional bottlenecks, limited domestic competition, a shortage of digital forensic experts, and rural infrastructural gaps. Despite these differences, both nations face common hurdles in cross-border payment compliance and anti-money laundering (AML) detection. Ultimately, the study concludes that long-term resilience requires policymakers in both

jurisdictions to carefully integrate legal oversight, cybersecurity readiness, and adaptive regulations to successfully balance consumer protection with private-sector innovation.

8. Conclusion

PSPs in India and Uzbekistan operate within dynamic digital ecosystems shaped by regulatory reforms, technological innovation, and rising cybercrime threats. India's mature digital payments environment contrasts with Uzbekistan's emerging but ambitious digital transformation. Yet, both jurisdictions face common challenges: cyber-fraud escalation, compliance burdens, data protection complexities, and cross-border regulatory fragmentation. Strengthening PSP resilience requires coordinated efforts across law, technology, cybersecurity, and international cooperation. For a dual-degree LL.M scholar specializing in Cyber Crime Law and Digital Forensics, the PSP landscape offers a critical domain for research, policy development, and professional engagement.

Bibliography

1. Central Bank of the Republic of Uzbekistan. (2020). *Regulation on electronic payment systems*.
2. Central Bank of Uzbekistan. (2021). *Rules for licensing payment service providers*.
3. Central Bank of Uzbekistan. (2022). *Digital payments development strategy 2022–2026*.
4. Central Bank of Uzbekistan. (n.d.). *Payment systems overview*. https://www.cbu.uz
5. Clough, J. (2020). *Principles of cybercrime*. Cambridge University Press.
6. Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).
7. Dubey, V. (2022). *Fintech law and regulation in India*. Oxford University Press.
8. Financial Action Task Force. (2023). *International standards on combating money laundering and the financing of terrorism & proliferation*. https://www.fatf-gafi.org
9. Financial Action Task Force. (n.d.). *Country mutual evaluation reports*. https://www.fatf-gafi.org
10. George, R. (2022). Regulating payment gateways in India: Challenges and prospects. *Indian Journal of Law & Technology*, *14*(1), 112.
11. Indian Computer Emergency Response Team. (2022). *Directions under section 70B of the IT Act*. Ministry of Electronics & IT, Government of India.
12. Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India).
13. International Monetary Fund. (2023). *India: Financial sector assessment program*.
14. Karimov, D. (2023). Digital payments and regulatory transformation in Uzbekistan. *Central Asian Economic Review*, *9*(4), 77.
15. Khasanov, A. (2023). *Financial technology and regulation in central Asia*. Tashkent Legal Press.
16. Law on Electronic Commerce, Law No. ZRU-707 (Republic of Uzbekistan 2021).
17. Law on Payments and Payment Systems, Law No. ZRU-573 (Republic of Uzbekistan 2019).
18. Law on Personal Data, Law No. ZRU-547 (Republic of Uzbekistan 2019) (as amended).
19. Ministry of Digital Technologies. (2022). *Cybersecurity requirements for digital financial infrastructure*. Republic of Uzbekistan.
20. Ministry of Economy and Finance. (2024). *Fintech growth and regulatory outlook*. Republic of Uzbekistan.
21. Ministry of Electronics & IT. (2023). *National cybersecurity strategy*. Government of India.
22. National Payments Corporation of India. (2024). *Unified Payments Interface procedural guidelines*.

23. National Payments Corporation of India. (n.d.). *UPI product specifications*. [suspicious link removed]
24. Payment and Settlement Systems Act, 2007, No. 51 of 2007, Acts of Parliament, 2007 (India).
25. Prevention of Money Laundering Act, 2002, No. 15 of 2003, Acts of Parliament, 2003 (India).
26. Reserve Bank of India. (2020). *Guidelines on regulation of payment aggregators and payment gateways*.
27. Reserve Bank of India. (2023a). *Annual report on payment systems*.
28. Reserve Bank of India. (2023b). *Master direction on prepaid payment instruments*.
29. Reserve Bank of India. (n.d.). *Payment systems statistics*. https://www.rbi.org.in
30. Sen, A. (2024). Cyber-fraud in UPI transactions: A forensic perspective. *National Law School Cyber Law Review*, *18*, 55.
31. Swaminathan, P. (2021). *Digital payments and cybersecurity in India*. Sage Publications.
32. Umarova, S. (2022). AML compliance challenges for fintech PSPs in Uzbekistan. *Uzbek Journal of Finance & Banking Law*, *6*(2), 41.
33. United Nations Office on Drugs and Crime. (2021). *Cybercrime and digital evidence guidelines*.
34. World Bank. (2022). *Uzbekistan digital economy diagnostic report*.