BSmart Case Study Competition

Mastercard's regulatory failure in India: lessons on data localisation and compliance

Uploaded By: Abhishek Chatterjee

Departments : MBA General,Marketing,Business Analytics,Healthcare,Finance,International Business,Digital Marketing,Human Resource Management

Published on - 13 Nov 2025, 1:22 pm

Closing Date - 27 Nov 2025, 1:20 pm

No. of Questions - 3

Total Marks - 30

Authors: Dr Mallika Ahuja & Abhinav Anand

Problem Statement

There has been a massive explosion in the amount of data generated by connected internet users in India, leading to subsequent data breaches. Data breaches are an unfortunate consequence. As a result, in July 2021, the RBI barred Mastercard from issuing new debit and credit cards to Indian customers. This case study examines the Reserve Bank of India's (RBI) regulatory action against Mastercard over its failure to comply with India's payment data localisation norms.

This regulatory action disrupted several partner banks, strained customer trust, and caused reputational damage to the company. The case details the context and implications of the ban on issuing new cards, the evolving data localisation regime, operational disruptions, and the broader regulatory environment for multinational digital service providers. The discussion highlights compliance-related challenges, legal interpretations, and strategic lessons for global payment networks operating in India and other emerging markets with stringent data policies.

Please go through the Guiding Note attached below before diving into the caselet for better understanding.

Context

In April 2018, the RBI mandated that all payment system providers store the whole end-to-end transaction and related data for Indian customers only on servers physically located in India. This data localisation policy was aimed at enhancing data privacy and security, as well as regulatory oversight. RBI allowed foreign payment operators to process data abroad for certain transactions but required that any such data be deleted from overseas servers within 24 hours and stored solely in India. Operators were also required to submit board-approved audit reports from a CERT-IN-empanelled auditor confirming compliance with the norms.

Localisation norms in India already existed through diverse laws and policies before the discussions in the Draft Personal Data Protection Bill, 2018, and subsequently in the Personal Data Protection Bill, 2019. The significant reasons backing data localisation measures in India broadly stem from privacy, security and

protectionist ends. RBI's 2018 data localisation directive cited security and monitoring as key motivations, whereas the erstwhile data localisation measures in the draft National Policy Framework for E-Commerce in India were seen as a way to protect domestic companies, including data centres and digital payments groups. India is at a crucial juncture regarding its data regulation policies.

As part of the procedural steps to strengthen localisation measures, RBI exercised its powers under the Payment and Settlement Systems Act, 2007. It imposed a ban on Mastercard and others in July 2021. The action followed similar restrictions imposed earlier that year on American Express and Diners Club. The credit card companies argued that the data localisation would prevent them from doing business in India. But the RBI did not entertain this argument.

Discussion

1. Regulatory Requirements and Mastercard's Failures

Data Localisation Mandate: The RBI's April 2018 circular required all payment system operators (PSOs) to store payment data (including customer information, payment credentials, and transaction details) only in India. The norms provided a six-month window to comply and submit an audit report by a CERT-IN-empanelled auditor. Operators could process data outside India but had to delete foreign copies within 24 hours. The introduction of data localisation restrictions, however, is sometimes considered counterproductive. Precisely for some of the ultimate goals of regulatory supervision and law enforcement. By limiting the internal sharing of information across jurisdictions, data localisation requirements may be detrimental to financial institutions' ability to maintain a —golden source of datall and comprehensive risk management systems.

Non-compliance Issues:

- Mastercard maintained "dual records," with some transaction data continuing to reside outsi de India or being processed for fraud checks overseas beyond allowed timelines.
- Mastercard reportedly delayed submitting the required audit reports, favouring overseas aud itors, contrary to RBI's specifications for domestic CERT-IN-approved firms.
- While Mastercard localised some data segments, the RBI wanted "end-to-end" data stored domestically, including for fraud and risk analysis.
- Mastercard's stance contrasted with that of other major players, such as Visa, which proacti vely engaged with the RBI and sought to comply rapidly.

2. Impact on Mastercard and the Payments Ecosystem

Operational Disruption:

- The RBI ban halted the onboarding of new customers, temporarily limiting the ability of Mast ercard-partnered banks (notably RBL Bank and YES Bank) to issue cards. Visa and RuPay, however, were unaffected, allowing banks to reroute new issuance to those networks.
- The ban did not affect existing Mastercard customers, who could continue to transact normal ly

Reputational and Market Share Effects:

- Mastercard risked losing its competitive position, given its roughly 33% market share in Indi a's card payments ecosystem.
- Private and public criticism affected perceptions of Mastercard's trustworthiness and adapta bility to Indian regulatory priorities.

Industry-wide Ramifications:

- Some saw the RBI's "sledgehammer" approach as a warning to all multinationals regarding I ndia's regulatory assertiveness.
- The disruptions highlighted the heightened importance of data localisation for all global digita l service and payments providers operating in India.

3. Legal Rationale and Policy Context for Data Localisation

Policy Objectives:

- The primary goals of India's data localisation policies are data privacy, enhanced supervisio n, and the ability to investigate and regulate domestic transactions efficiently. Additionally, pu blic authorities such as financial supervisors, tax agencies, Anti-Money Laundering bodies, o r criminal prosecutors can access relevant data on citizens and corporations, subject to appr opriate restrictions and safeguards that balance the rights of data subjects.
- The approach is supported by the fact that when the relevant information is located offshore, national public authorities are usually under constant fear that their capacity to access data may be limited by the territorial limits of their powers and potential discrepancies with the law s and authorities of the host countries.

Legal Framework:

- The Payment and Settlement Systems Act, 2007, empowers the RBI to supervise and regul ate payment operators, including the enforcement of data localisation requirements.
- Subsequent clarifications (2018, 2019) broadened the definition of "payment data," requiring not only transaction data but also customer identities, credentials (PINs, OTPs), and related metadata to be stored in India alone.

4. Compliance Strategy: Lessons for Multinational Operators

- **Local Engagement:** Engaging proactively with regulators, accepting domestic audits, and l obbying constructively are critical to securing timely compliance.
- **Technical Preparedness:** Firms must anticipate infrastructure and operational challenges —such as building or leasing local data centres—and factor them into strategic planning and investment decisions.
- **Legal Risk Awareness:** The persistent emphasis on local audits, data storage, and proces sing illustrates that enforcement risk is not merely theoretical in emerging markets like India.
- **Holistic Compliance:** Multinationals must ensure holistic ("end-to-end") compliance, coveri ng all data flows, auxiliary processes (like fraud detection), and third-party contractors—not j ust core transaction data.

Conclusion

Access by foreign governments (or para-governmental institutions) to sensitive information can be considered a threat to national security. The sensitivity of a particular category or set of data is not only relative but increasingly difficult to assess, given how new technologies such as Artificial Intelligence and Machine Learning can generate unforeseen insights from combining different data sources.

The Mastercard case underscores the high stakes of regulatory compliance in digital economies, especially regarding data localisation in large, fast-growing markets like India. Despite being aware of emerging legal risks, Mastercard's partial, delayed, or piecemeal compliance led to regulatory action that disrupted its business and sent a powerful signal to the industry. Multinational payments firms must view such requirements as top-priority, not optional or deferrable, and develop robust legal and operational strategies in collaboration with local regulators to avoid similar disruptions in other markets.

(Contributed by Global Risk Management Institute)

Attachments:

- https://s3.ap-south-1.amazonaws.com/stcontent.bslearning.in/global/case_study/535/GuidingNotesMastercard.pdf
- https://s3.ap-south-1.amazonaws.com/stcontent.bslearning.in/global/case_study/535/MastercardsRegulatoryFailureinIndiaLesso.pdf

Questions:

Question 1: What were the specific regulatory requirements that Mastercard failed to comply within India?(10 Marks)

Question 2: What operational and reputational impacts did the RBI's ban have on Mastercard, its partner banks, and the Indian payments industry?(10 Marks)

Question 3: How should multinational payment networks approach compliance with local data laws in emerging markets?(10 Marks)