KHAITAN &CO ADVOCATES SINCE 1911

4 October 2024

Cyber Resilience and Digital Payment Security Governance: A Step Towards Secured Payments Systems

INTRODUCTION

The Reserve Bank of India (RBI) on 30 July 2024 issued its 'Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-bank Payment System Operators' (Master Directions).

The RBI had indicated its intent to issue directions on cyber resilience and payment security controls for payment system operators through its '*Statement on Developmental and Regulatory Policies*' issued on 8 April 2022. Accordingly, a draft '*Master Directions on Cyber Resilience and Digital Payment Security Controls for nonbank Payment System Operators*' was released by RBI on 2 June 2023 (Draft Master Directions) for stakeholder comments. The Master Directions have been released post evaluation of the feedback received by the RBI on the Draft Master Directions.

1. APPLICABILITY AND IMPLEMENTATION OF THE MASTER DIRECTIONS

The Master Directions apply to all authorised non-bank payment system operators (PSOs) and their arrangement with unregulated entities (such as payment gateways and third-party service providers) in the digital payments ecosystem (Service Providers). PSOs are required to adopt a board approved policy setting out its framework for information security and cyber resilience and ensure that its Service Providers also adhere to the Master Directions.

The Master Directions would be implemented in a phase wise manner based on the below-mentioned classification of non-bank PSOs:

#	CATEGORY	ENTITIES	IMPLEMENTATION TIMELINE
1	Large PSOs	(i) Clearing Corporation of India Limited; (ii) National Payments Corporation of India (NPCI); (iii) NPCI Bharat Bill Pay Limited; (iv) Card Payment Networks; (v) Non-bank ATM Networks, White Label ATM Operators; (vi) Large PPI issuers; (vii) Trade Receivables Discounting System (TReDS) Operators; (viii) Bharat Bill Payment Operating Units (BBPOUs); and (ix) Payment Aggregators.	1 April 2025
2	Medium PSOs	(i) Cross-border (in-bound) Money Transfer Operators under Money Transfer Service Scheme (MTSS); and (ii) Medium PPI issuers.	1 April 2026

#	CATEGORY	ENTITIES	IMPLEMENTATION TIMELINE
3	Small PSOs	(i) Instant Money Transfer Operators; and (ii) Small PPI issuers.	1 April 2028

The Master Directions categorises prepaid payment issuer (PPI) issuers into three categories as per the 'Oversight Framework for Financial Market Infrastructure and Retail Payment Systems' released by the RBI in the following manner:

#	CATEGORY	APPLICABILITY
1	Large PPI issuers	(i) Number of outstanding PPIs is greater than 2 crores as on 31 March of the preceding year; or (ii) Total amount outstanding for all issued PPIs is greater than INR 50 crores as on 31 March of the preceding year; or (iii) Total value of all PPI transactions processed during the preceding financial year is greater than INR 5000 crores.
2	Medium PPI issuers	(i) Number of outstanding PPIs is between 10 lakhs and 2 crores as on 31 March of the immediately preceding year; or (ii) Total amount outstanding for all issued PPIs is between INR 10 lakhs and INR 50 crores as on 31 March of the immediately preceding year; or (iii) Total value of all PPI transactions processed during the preceding financial year is between INR 1,000 crores and INR 5,000 crores.
3	Small PPI issuers	(i) Number of outstanding PPIs is less than 10 lakhs as on 31 March of the immediately preceding year; or (ii) Total amount outstanding for all issued PPIs is less than INR 10 lakhs as on 31 March of the immediately preceding year; or (iii) Total value of all PPI transactions processed during the preceding financial year is less than INR 1,000 crores.

2. KEY REGULATORY COMPLIANCES

2.1. Governance Controls.

The table sets out below the key governance controls required to be implemented by a PSO.

#	PARTICULARS	ROLE / FUNCTION
1	Board of Directors (Board)	(i) Oversee information security risks, including cyber risk and resilience. (ii) Primary oversight may be delegated to a sub-committee of a board headed by a member experienced in information / cyber security.

#	PARTICULARS	ROLE / FUNCTION
		(iii) Approve and implement information security policy covering roles and responsibilities of the Board / sub-committees, senior management and key personnel. (iv) Approve and implement measures to identify, assess, manage and monitor cyber security risks, with security controls and training processes for employees / stakeholders. (v) Approve and implement a cyber crisis management plan in line with guidelines from agencies such as Indian Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre, or Institute for Development and Research in Banking Technology.
2	Chief Information Security Officer (CISO) or equivalent senior-level executive	(i) Implement information security policy and cyber resilience framework. (ii) Oversee action points while conducting cyber risk assessments for new products / services or major changes.
3	IT oversight sub-committee	Review the information technology assessment reports presented to it.

Comment:

The requirements outlined above place significant emphasis on the role of the Board and senior management in managing and mitigating cyber security risks.

PSOs will be required to invest in putting place a compliance framework by appointing CISO(s) or an equivalent executive, adhering to cyber security oversight requirements and implementing measures for incident response and reporting.

2.2. Baseline Information Security Measures / Controls.

The Master Directions require PSOs to strictly enforce the following security measures. The obligations range from record keeping, defining access controls, monitoring of fraudulent transactions and securing the network of the PSO.

#	PARTCULARS	COMPLIANCE OBLIGATION
1	Inventory management	(i) Retain records related to key roles, information assets, critical functions, processes, Service Providers, classifying their usage, criticality and business value. (ii) A comprehensive process flow diagram of network resources, inter-connections and data flows with third-party systems is required. (iii) Asset information should include identifiers, network addresses, asset locations, owner names and end of life support status.

#	PARTCULARS	COMPLIANCE OBLIGATION
2	Identity and access management	(i) Adoption of policies and procedures to manage access privileges and rights of all individuals accessing the IT environment. (ii) Maintain and monitor user's digital identity. (iii) Follow the principle of 'least privilege' for system access, with privileged accounts utilising multi-factor authentication. (iv) Implement safeguards for removable media and portable devices, remote work precautions and session termination after pre-determined period of inactivity.
3	Network security	(i) Configure network devices and check periodically their compliance with the established security rules. (ii) Put in place security operations centre to provide centralised monitoring and management of security incidents, including automated systems that correlate all anomalous activities to prevent multi-faceted attacks. (iii) Implement anti-malware solutions and multi-layered boundary defences. (iv) Implement network segmentation based on data criticality and whitelisting solutions for applications and services. (v) Follow a secure-by-design approach like Secure-Software Development Life Cycle and implement a multi-tier application architecture. (vi) Conduct periodic security testing of applications, including source code review, vulnerability assessments, and penetration testing.
4	Vendor risk management and data security	(i) Adherence to RBI's *'Framework for Outsourcing of Payment and Settlement-related Activities by PSOs'* dated 3 August 2021. (ii) Implement measures to ensure security controls for preventing network infiltration from vendor environments. (iii) Adopt comprehensive data leak prevention policies, information security management systems and obtain PCI-DSS certification for storing card-data. (iv) Mitigate risks associated with insecure application programming interfaces by adhering to globally recognised standards.

#	PARTCULARS	COMPLIANCE OBLIGATION
		(v) Carry out periodic employee awareness and training programmes. (vi) Implement incident response mechanisms to ensure prompt notification and post-incident analysis, with cyber incident reporting to CERT-In. (vii) Develop robust business continuity plan. (viii) Include multi-factor authentication for transactions, secure IT-infrastructure configurations, real-time fraud monitoring and systematic audit log management. (ix) Maintain a manned facility to function on a 24x7x365 basis for facilitating swift resolution of unauthorised / fraudulent transactions and assisting law enforcement agencies.

Comment:

PSOs are now required to revisit their information security framework and analyse if the practices followed on the ground are aligned with the requirements under the Master Directions. PSOs are also required to ensure that their applicable vendors also ensure compliance with the above-mentioned requirements as part of their agreement with such vendors.

2.3. Digital Payment Security Measures / Controls.

#	PAYMENT TYPE	OBLIGATIONS
1	General	(i) Enable online alerts for transaction parameters, such as failed transactions, new account activity, geo-location, and IP address origin. (ii) Ensure that customer notifications are pushed after redacting sensitive information and financial data for online payments. (iii) Provide a feature for immediate marking of fraudulent transactions to customers.
2	Mobile payments	Maintain encryption during customer interactions, auto-terminating inactive sessions, limiting failed login attempts, and prohibit remote access applications during live sessions.
3	Card payments	(i) Validate merchant terminals against Payment Card Industry Point to Point Encryption (PCI-P2PE) and Payment Card Industry PIN Transaction Security (PCI-PTS) programs. (ii) Implement transaction limits and alert mechanisms for suspicious incidents. (iii) Store and process card details securely.

#	PAYMENT TYPE	OBLIGATIONS
4	Prepaid payment instruments	(i) Communicate OTP and transaction alerts in the user's preferred language, including vernacular languages. (ii) Implement a cooling period for funds transfer and cash withdrawal after electronic loading of funds.

Comment:

The digital payment security requirements under the Master Directions necessitate PSOs to make operational adjustments to enable online alerts and mark fraudulent transactions, which may require system upgrades or new technology investments. Mobile payment security practices will demand technological enhancements, potentially incurring additional costs and time efforts to ensure full compliance.

Merchant compliance with PCI-P2PE and PCI-PTS programs for card payments will necessitate training and support, potentially increasing operational expenses. Lastly, the requirement for PPI issuers to communicate in the user's preferred language will call for an enhancement in customer communication capabilities and investing in language translation technologies.

CONCLUDING REMARKS

The Master Directions stipulate mechanisms for identification, assessment, monitoring and management of information technology and information security risks, and prescribe certain baseline security measures for ensuring system resiliency as well as safe and secure digital payment transactions.

The introduction of the Master Directions is a significant step towards strengthening the security and resilience of India's digital payment systems. These guidelines are set to impact the business models of PSOs, necessitating complex and resource-intensive implementation across people, processes and technology. The challenge for such PSOs would be to balance delivery and risk management, particularly with the increasing adoption of cloud technology.

The enhanced security measures are expected to boost customer confidence, potentially increasing digital payment adoption and increasing transaction volumes. However, this necessitates a cultural shift towards a security-focused mindset, underlining the need for continuous training and awareness programs. While smaller PSOs may face operational challenges in meeting the stringent requirements, the RBI has acknowledged this with a phased implementation timeline based on size of the PSO.

The Master Directions will go a long way in fostering a secure digital payment ecosystem in India which would benefit consumers as well as businesses. This would pave the way for safe and sustainable growth and innovation in the digital payments sector, despite the initial complexities and challenges which applicable PSOs may face.

- *Prashanth Ramdas (Partner); Pritish Mishra (Principal Associate); Ishani Sahai (Associate) and Raj Shekhar (Associate)*

For any queries please contact: editors@khaitanco.com

AMBITION STATEMENT

"Our ambition is to be a respectable law firm providing efficient and courteous service, to act with fairness, integrity and diligence, to be socially responsible and to enjoy life. We should put greater emphasis on working in consonance with our aforesaid values than on maximizing earnings. Earn we should but with dignity and pleasure."

Khaitan & Co is a premier full-service Indian law firm with 25+ practice areas, over 1,000 lawyers, including 200+ partners. To know more about us, please visit www.khaitanco.com