भारतीय रिज़र्व बैंक
Reserve Bank of India

RBI/DoS/2026-27/420
DoS.CO.CSITEG.14/31.01.015/2026-27 July 31, 2026

Reserve Bank of India (Small Finance Banks – Digital Payment Security Controls) Directions, 2026 (Updated as on October 01, 2026)

Table of Contents

Chapter I - Preliminary 2

A. Short Title and Commencement 2

B. Applicability 2

C. Definitions 2

Chapter II - Role of the Board 5

A. Board Approved Policies 5

Chapter III - General Controls 6

A. Governance and Management of Security Risks 6

B. Other Generic Security Controls 10

C. Application Security Life Cycle 11

D. Authentication Framework 14

E. Fraud Risk Management 16

F. Reconciliation Mechanism 18

G. Customer Protection, Awareness and Grievance Redressal Mechanism. 18

Chapter IV - Internet Banking Security Controls 21

Chapter V - Mobile Payments Application Security Controls 22

Chapter VI - Card Payment Security Controls 26

Chapter VII - Repeal and Other Provisions 31

A. Repeal and Saving 31

B. Application of Other Laws Not barred 31

C. Interpretations 32

पर्यवेक्षण विभाग, भारतीय रिज़र्व बैंक, केंद्रीय कार्यालय, मेकर टावर-ई, 20वीं मंजिल, कफ परेड, कोलाबा, मुंबई-400 005
दूरभाष: 022-2216 1816 ई-मेल: csite@rbi.org.in

Department of Supervision, Reserve Bank of India, Central Office, Maker Tower-E, 20th floor, Cuffe Parade, Colaba, Mumbai- 400 005
Tel: 022- 2216 1816 Email: csite@rbi.org.in

हिंदी आसान है इसका प्रयोग बढ़ाइए

In exercise of the powers conferred by extant provisions of the Banking Regulation Act, 1949, Chapter IV of Payment and Settlement Systems Act, 2007, and all other provisions / laws enabling the Reserve Bank of India ('RBI') in this regard, RBI being satisfied that it is necessary and expedient in the public interest so to do, hereby issues Directions hereinafter specified.

Chapter I - Preliminary

A. Short Title and Commencement

1. These Directions shall be called the Reserve Bank of India (Small Finance Banks – Digital Payment Security Controls) Directions, 2026.

2. These Directions shall come into effect immediately upon issuance.

B. Applicability

3. These Directions shall be applicable to Small Finance Banks (hereinafter collectively referred to as 'banks' and individually as 'bank').

4. These Directions are applicable for digital payment products and services provided by the bank as detailed below:

   (1) Any digital payment product or service offered by the bank to customers for carrying out financial transactions or non-financial transactions such as balance enquiry, set / change Personal Identification Number (PIN), mobile banking registration, generation of one-time password (OTP), mini-statement, facility of checking transaction status, and option to the customer to raise dispute / grievance. Such digital payment products and services offered directly by the bank or through a system operated by RBI or a system operated by any of the RBI authorised Payment System Operators (PSOs), and the associated IT assets (applications, systems, infrastructure) shall be considered for the scope of these Directions.

C. Definitions

5. The following definitions are sourced from Financial Stability Board (FSB) Cyber Lexicon unless explicitly mentioned otherwise. In these Directions, unless the

context states otherwise, the terms herein shall bear the meanings assigned to them below.

(1) *'Availability'* - Property of being accessible and usable on demand by an authorised entity.

(2) *'Confidentiality'* - Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes, or systems.

(3) *'Cyber'* - Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.

(4) *'Cybersecurity'* - Preservation of confidentiality, integrity, and availability of information and / or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

(5) *'Cyber-attack'* - Malicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt, or gain unauthorised access to assets.

(6) *'Distributed Denial of Service (DDoS)'* - A denial of service that is carried out using numerous sources simultaneously.

(7) *'Framework'* - A framework is a structured set of strategies, policies, procedures, methods, and best practices that guides organisational activities, enables governance, and supports the achievement of defined objectives.

(*Source*: adapted from ISACA glossary)

(8) '*Information System*' - Set of applications, services, information technology assets, or other information-handling components, which includes the operating environment and networks.

(9) *'Integrity'* - Property of accuracy and completeness.

(10) *'Malware'* - Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.

(11) *'Penetration Testing'* - A test methodology in which assessors typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

(12) *'Phishing'* - A digital form of social engineering that attempts to acquire private or confidential information by pretending to be a trustworthy entity in an electronic communication.

(13) '*Vulnerability'* - A weakness, susceptibility, or flaw of an asset or control that can be exploited by one or more threats.

(14) '*Vulnerability Assessment (VA)*' - Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

6. All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Reserve Bank of India Act, 1934, or the Banking Regulation Act, 1949, or the Payment and Settlement Systems Act, 2007, or the Information Technology Act, 2000, or the Companies Act, 2013, or any statutory modification or re-enactment thereto or other regulations issued by the RBI or the Glossary of Terms published by the RBI or as used in commercial parlance as used in RBI Directions, as the case may be.

Chapter II - Role of the Board

A. Board Approved Policies

7. The Board of Directors shall approve the policies related to digital payment products and services. The Board may delegate the review of such policies to the Board-level IT Strategy Committee (ITSC). Material amendments thereto shall be approved by the Board. The review shall be undertaken at least annually.[1]

[1] Substituted w.e.f. October 1, 2026, consequent to Reserve Bank of India (Small Finance Banks - Governance) Amendment Directions, 2026.

Chapter III - General Controls

A. Governance and Management of Security Risks

8. The bank shall formulate a policy for digital payment products and services with the approval of its Board. The contours of the policy, while discussing the parameters of any 'new product' including its alignment with the overall business strategy and inherent risk of the product, risk management / mitigation measures, compliance with regulatory instructions, and customer experience, shall explicitly cover payment security requirements from Functionality, Security and Performance (FSP) angles such as:

   (1) necessary controls to protect the confidentiality of customer data and integrity of data and processes associated with the digital product / services offered;

   (2) availability of requisite infrastructure such as human resources and technology with necessary backup;

   (3) assurance that the payment product is built in a secure manner offering robust performance ensuring safety, consistency, and rolled out after necessary testing for achieving desired FSP;

   (4) capacity building and expansion with scalability (to meet the growth for efficient transaction processing);

   (5) minimal customer service disruption with high availability of systems / channels (to have minimal technical declines);

   (6) efficient and effective dispute resolution mechanism and handling of customer grievance; and

   (7) adequate and appropriate review mechanism followed by swift corrective action, in case any one of the above requirements is hampered or having high potential to get hampered.

9. The Board and Senior Management shall be responsible for implementation of this policy. The policy shall be reviewed at least annually. The bank may

formulate this policy separately for its different digital products / services or include the same as part of its overall product policy.

10. The policy shall require that every digital payment product / service offered addresses the mechanics, clear definition of starting point, critical intermittent stages / points and end point in the digital payment cycle, security aspects, validations till the digital payment is settled, clear pictorial representation of digital path, exception handling, signing off of the above requirements, mechanism for carrying out User Acceptance Tests (UAT) in multiple stages before roll-out, sign off from multiple stakeholders [post User Acceptance Test (UAT)], and data archival requirements.

11. The bank shall clearly articulate the need for an external assessment of the entire process including the logic, build, and security aspects of the application(s) supporting the digital product or service.

12. The bank shall incorporate appropriate processes into its governance and risk management programs for identifying, analysing, monitoring, and managing the specific risks, including compliance risk and fraud risk, associated with the portfolio of digital payment products and services on a continual basis and in a holistic manner.

13. The Senior Management of the bank shall have appropriate performance monitoring systems / key performance indicators for assessing whether the product or service offered through digital payment channels meets operational and security norms. As part of this process, the bank shall define product-level limits on the level of acceptable security risk, document specific security objectives, and performance criteria including quantitative benchmarks for:

    (1) evaluating the success of the security built into the digital payment product or service;

    (2) comparing actual results with projections and qualitative benchmarks on a periodic basis to detect and address adverse trends or concerns in a timely manner; and

(3) modifying the business plan / strategy involving the product or service, when appropriate, based on its security performance.

(Note: Limits may be qualitative or quantitative in nature. Illustrative examples of such limits include, inter alia, parameters derived from multiple fraud risk indicators; defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO); key performance indicators such as transaction failure rates and system uptime or availability; customer complaint metrics; third-party or supply chain risk factors; and financial losses incurred by the bank or customers due to cyber-attacks on the payment product or service. With respect to product-level limits, the bank shall be guided by its internal risk assessment.)

14. The bank shall have trained resources with necessary expertise to manage the digital payment infrastructure. Wherever the bank is dependent on third-party service providers, adequate oversight, and controls for monitoring the activities of the third-party personnel, shall be put in place.

15. The bank shall conduct risk assessments with regard to the safety and security of digital payment products / services and associated processes as well as suitability and appropriateness of the same vis-à-vis the target users, both prior to establishing the service(s) and regularly thereafter. The risk assessment shall factor in:

(1) the technology stack and solutions used;

(2) known vulnerabilities at each of the touchpoints of the digital product / service and the remedial action taken by the bank;

(3) dependence on third-party service providers and oversight over such providers;

(4) risk arising out of integration of digital payment platform with other systems both internal and external to the bank, including core systems, and systems of PSOs;

(5) customer experience, convenience, and technology adoption required to use such products / services;

(6) reconciliation process;

(7) interoperability aspects;

(8) data storage, security, and privacy protection as per extant laws / instructions;

(9) operational risk including fraud risk;

(10) business continuity and service availability;

(11) compliance with extant cybersecurity requirements; and

(12) compatibility aspects.

16. The risk assessment shall cover the surrounding ecosystem as well and address the need to protect and secure payment data (such as customer data, customer and beneficiary account details, payment credentials, and transaction data) and evaluate the resilience of systems. The internal Risk and Control Self-Assessment (RCSA) exercise shall cover the risks (inherent) and controls vis-à-vis the probability and impact of threats to arrive at residual risk. The bank shall maintain database of all systems and applications storing customer data in the payment ecosystem and compliance with applicable Payment Card Industry (PCI) standards in each of the systems (notwithstanding mandatory requirements of certification / standard accreditation). The periodicity of RCSA may be determined by the bank based on changes in the scope of the risk assessment. In case of vendors, the bank shall evaluate the RCSA conducted by the vendor.

17. The bank shall evaluate the risks associated with the chosen technology platforms, application architecture, both on the server and client side. Further, the bank shall undertake a review of the risk scenarios and existing security measures based on incidents affecting its services, before any major change to the infrastructure or procedures, or whenever any new threats are identified

through risk monitoring activities. Further, unused, or unwanted features of the platform shall be closely controlled to minimise risk.

18. The bank shall develop sound internal control systems and take into account the operational risk before offering digital payment products and related services. This shall include ensuring adequate safeguards to protect integrity of data, customer confidentiality, and security of data.

19. The bank shall ensure that its digital payment architecture is robust and scalable, commensurate with the transaction volumes and customer growth. The Information Technology (IT) strategy of the bank shall ensure that a robust capacity management plan is in place to meet evolving demand. The bank shall also put in place a mechanism to review its IT / IT security architecture and technology platform overhaul on a periodic basis based on the Board-approved policy.

20. The bank shall have necessary capacity, systems, and procedures in place to periodically test backed-up data and applications pertaining to digital products / services to ensure recovery without loss of transactions or audit-trails. These facilities shall be tested at least on a half-yearly basis.

B. Other Generic Security Controls

21. The communication protocol in the digital payment channels (especially over internet) shall adhere to a secure standard. An appropriate level of encryption and security shall be implemented in the digital payment ecosystem.

22. Web applications providing the digital payment products and services shall not store sensitive information in Hyper-Text Mark-up Language (HTML) hidden fields, cookies, or any other client-side storage to avoid any compromise in the integrity of the data.

23. The bank shall implement Web Application Firewall (WAF) solution and DDoS mitigation techniques to secure the digital payment products and services offered over internet.

24. The key length (for symmetric / asymmetric encryption, hashing), algorithms (for encryption, signing, exchange of keys, creation of message digest, random number generators), cipher suites, digital certificates, and applicable protocols used in transmission channels, processing of data, and for authentication purposes shall be strong. The bank shall adopt internationally accepted and published standards that are not deprecated / demonstrated to be insecure / vulnerable and shall ensure that the configurations involved in implementing such controls are compliant with extant laws and regulatory instructions.

25. The bank shall renew its digital certificates used in the digital payment ecosystem well in time.

26. The mobile application (mobile banking / mobile payment applications of the bank) and internet banking application shall have effective logging and monitoring capabilities to track user activity, security changes, and identify anomalous behaviour and transactions.

C. Application Security Life Cycle

27. The bank shall implement multi-tier application architecture, segregating application, database and presentation layer in the digital payment products and services.

28. The bank shall follow a ‘secure by design’ approach in the development of digital payment products and services. The bank shall ensure that digital payment applications are inherently more secure by embedding security within their development lifecycle.

29. The bank shall explicitly define security objectives (including protection of customer information / data) during

    (1) requirements gathering;

    (2) designing;

    (3) development;

    (4) testing including source code review;

(5) implementation, maintenance, and monitoring; and

(6) decommissioning phases of the digital payment applications.

30. The bank (including those partnering with other entities to co-brand / co-develop applications) shall adopt and incorporate a threat modelling approach during application lifecycle management into its policies, processes, guidelines, and procedures.

31. For digital payment applications licensed by a third-party vendor, the bank shall put in place a source code escrow arrangement or other arrangements for ensuring continuity of services in case the vendor defaults or is unable to provide services.

32. The bank shall conduct security testing including review of source code, Vulnerability Assessment (VA) and Penetration Testing (PT) of its digital payment applications to assure that the application is secure for putting through transactions while preserving confidentiality and integrity of the data that is stored and transmitted. Such testing shall invariably cover compliance with various standards like Open Worldwide Application Security Project (OWASP). In those cases, where the source code is not owned by the bank, the bank shall obtain a certificate from the application developer stating that the application is free of known vulnerabilities, malware, and any covert channels in the code. Further, the bank shall ensure the following:

(1) The VA shall be conducted at least on a half-yearly basis; PT shall be conducted at least annually. In addition, VA / PT shall be conducted as and when any new IT infrastructure or digital payment application is introduced or when any major change is performed in the application or infrastructure.

(2) Testing related to review of source code / certification shall be conducted / obtained and shall be continued annually, if changes / upgrades have been made to the application during the year.

(3) Testing / Certification shall address the objective that the product / version / module(s) functions only in a manner that it is intended for, is developed as

per the best secure design / coding practices and standards, addressing known flaws / threats due to insecure coding.

(4) Penal provisions are included in third-party contractual arrangements for any non-compliance by the application provider.

33. The bank may also run automated VA scanning tools on a continuous / more frequent basis to automatically scan all systems on the network that are critical, public facing or store customer sensitive data.

34. The bank shall compare the results from earlier vulnerability scans to verify / ascertain that vulnerabilities are addressed either by patching, implementing a compensating control, or documenting and accepting the residual risk with necessary approval and that there is no recurrence of the known vulnerabilities. The identified vulnerabilities shall be fixed in a time-bound manner.

35. The bank shall ensure that vulnerability scanning is performed in authenticated mode either with agents running locally on the system to analyse the security configuration or with remote scanners that are given administrative rights on the system being tested.

36. The bank shall verify and thoroughly test the functionality (to validate whether the system meets the functional requirements / specifications) and security controls of payment products and services before their launch / moving to the production environment.

37. The bank shall institute a mechanism to actively monitor for non-genuine / unauthorised / malicious applications (with similar name / features) on popular app-stores and the web and respond appropriately to bring them down.

38. The server at the bank's end shall have adequate checks and balances to ensure that no transaction is carried out through non-genuine / unauthorised digital payment products / applications and the authentication process is robust, secure, and centralised.

39. The security controls for digital payment applications shall focus on how these applications handle, store, and protect payment data. The Application

Programming Interfaces (APIs) for secure data storage and communication shall be implemented and used correctly in order to be effective. The bank shall refer to standards such as OWASP-Mobile Application Security Verification Standard (OWASP-MASVS), OWASP-Application Security Verification Standard (OWASP-ASVS), and other relevant OWASP standards, security and data protection guidelines in ISO 12812, threat catalogues and guides developed by National Institute of Standards and Technology (NIST) (including for Bluetooth and Long-Term Evolution (LTE) security), for application security, and other protection measures. Such testing shall necessarily verify for vulnerabilities including, but not limited to OWASP / OWASP Mobile Top 10, application security guidelines / requirements developed / shared by operating system providers / Original Equipment Manufacturers (OEMs).

40. The bank shall redact / mask customer information such as account numbers / card numbers / other sensitive information when transmitted via SMS / emails (including attachments).

D. Authentication Framework

41. The bank shall implement, except where explicitly permitted / relaxed, multi-factor authentication for payments through electronic modes and fund transfers, including cash withdrawals from ATMs / micro-ATMs / business correspondents, through digital payment applications. At least one of the authentication methodologies shall be dynamic or non-replicable. [e.g., Use of OTP, mobile devices (device binding and Subscriber Identification Module (SIM)), biometric / Public Key Infrastructure (PKI) / hardware tokens, 'Europay, Mastercard, and Visa' (EMV) chip card (for Card Present Transactions) with server-side verification could be termed either in dynamic or non-replicable methodologies].

42. The bank shall ensure to design and implement robust multi-factor authentication methods to:

    (1) act as a strong fraud deterrent;

    (2) be more difficult to compromise;

(3) protect the confidentiality of payment data; and

(4) enhance confidence in digital payment by effectively addressing various cyber-attack mechanisms like phishing, keylogging, spyware / malware, and other internet-based frauds targeted at the bank and its customers.

43. The bank may also adopt adaptive authentication to select the right authentication factors depending on risk assessment, user risk profile, and behaviour.

44. The implementation of appropriate authentication methods shall be based on an assessment of the risks posed by the bank's digital payment products and services. The risks shall be evaluated in light of the type of customer (e.g., retail / corporate / commercial), the customer transactional requirements / pattern (e.g., bill payment, fund transfer), the sensitivity of customer information and the volume, value of transactions involved.

45. The authentication methods shall take into consideration, inter alia, customer acceptance, ease of use, reliable performance, scalability to accommodate growth, customer profile, location, transaction, and interoperability with other systems.

46. The bank shall implement multi factor authentication and alerts (through channels such as SMS and email) for all payment transactions (including debits and credits), creation of new account linkages (addition / modification / deletion of beneficiaries), change in account details or revision to fund transfer limits. In devising these security features, the bank shall take into account their efficacy and differing customer preferences for additional online protection.

47. The alerts and OTPs received by the customer for online transactions shall identify the merchant name, wherever applicable, rather than the payment aggregator through which the transaction was effected.

48. As an integral part of the multi factor authentication architecture, the bank shall also implement appropriate measures to minimise exposure to middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-

the browser (MITB) attack or man-in-the application attack. The bank shall, inter alia, ensure, that the data in transit is secured and the transactions are authenticated only by genuine / authorised source / process.

49. The bank shall ensure that an authenticated session, together with its encryption protocol, shall remain intact throughout the interaction with the customer. In the event of interference or in case of closure of the application by the customer, the session shall be terminated, and the affected transactions shall be resolved or reversed out. The customer shall be promptly notified about the status of the transaction by email, SMS, or other means.

50. The bank shall set down the maximum number of failed login or authentication attempts after which access to the digital payment product / service is blocked.

51. The bank shall have a secure procedure in place to re-activate the access to blocked product / service. The bank shall notify the customer of failed login or authentication attempts.

E. Fraud Risk Management

52. The bank shall document and implement the configuration requirements for identifying suspicious transactional behaviour, including rules, preventive and detective controls, mechanism to alert the customers in case of failed authentication attempts, and the applicable time frames.

53. The bank shall parameterise and monitor system alerts in terms of various applicable parameters. Such parameters, as applicable could include: Transaction velocity (e.g., fund transfers, cash withdrawals, payments through electronic modes, and adding new beneficiaries) in a short period, more so in the accounts of customers who have never used mobile app / internet banking / card (depending upon the type of payment channel), high risk merchant category codes (MCC) parameters, counterfeit card parameters (e.g., String of Invalid Card Verification Value (CVV) / PINs indicates an account generation attack), new account parameters (excessive activity on a new account), time zones, geo-locations, IP address origin (in respect of unusual patterns, prohibited zones / rogue IPs), behavioural biometrics, transaction origination from point of

compromise, transactions to mobile wallets / mobile numbers / Virtual Payment Address (VPAs) on whom vishing fraud or other types of fraud is / are registered / recorded, declined transactions, and transactions with no approval code.

54. The bank shall conduct fraud analysis to identify the reason for fraud occurrence and determine mechanism to prevent such frauds.

55. The bank shall educate the staff, especially in the fraud control function, about frauds and train them in the following skills and areas of expertise:

    (1) fraud control tools and their usage;

    (2) investigative techniques and procedures;

    (3) cardholder and merchant education techniques to prevent fraud;

    (4) scheme / card operating regulations;

    (5) data processing and analysis, liaising or communicating with law enforcement agencies; and

    (6) the requisite skills required to (i) set and update appropriate rules, (ii) monitor the exceptions thrown based on the rules on a continuous basis and take necessary actions promptly, (iii) communicate / escalate wherever required to appropriate authorities, and (iv) differentiate false positives from the rest.

56. The bank shall maintain updated contact details of service providers, intermediaries, external agencies, and other stakeholders for coordination in incident response. The bank shall put in place a mechanism with the stakeholders to update and verify such contact details. The bank shall also formulate specific Standard Operating Procedures (SOPs) to handle incidents related to payment ecosystem to mitigate the loss either to the customer or the bank.

F. Reconciliation Mechanism

57. A real-time / near-real-time [not later than 24 hours from the time of receipt of settlement file(s)] reconciliation framework for all digital payment transactions between the bank and all other stakeholders such as payment system operators, business correspondents, card networks, payment system processors, payment aggregators, payment gateways, third-party technology service providers, and other participants, shall be put in place for better detection and prevention of suspicious transactions. The bank shall also have a mechanism to monitor the implementation and effectiveness of such framework.

G. Customer Protection, Awareness and Grievance Redressal Mechanism

58. The bank shall incorporate secure, safe, and responsible usage guidelines and training materials for end users within the digital payment applications. The bank shall make it mandatory (i.e., not providing any option to circumvent / avoid the material) for the customer to go through secure usage guidelines (in the customer's preferred language) while obtaining and recording confirmation during the on-boarding procedure in the first instance and first use after each update of the digital payment application or after major updates to secure and safe usage guidelines.

59. The bank shall incorporate a section in the digital payment application clearly specifying the process and procedure (including relevant forms and contact information) to lodge customer grievances. A mechanism shall be put in place to keep this information periodically updated. The reporting facility on the application shall provide an option for registering a grievance. Customer dispute handling, reporting, and resolution procedures, including the expected timelines for the bank's response, shall be clearly defined.

60. The bank shall be guided by RBI/2020-21/21 DPSS.CO.PD No.116/02.12.004/2020-21 dated August 6, 2020 on 'Online Dispute Resolution (ODR) System for Digital Payments' updated from time to time, for putting in place system(s) for online dispute resolution for resolving disputes and grievances of customers pertaining to digital payments.

61. The bank shall educate customers about the need to maintain the physical and logical security of their devices accessing digital payment products and services. This shall include but not be limited to recommending secure and regular installation of operating system and application updates, downloading applications only from authorised sources, and having anti-malware / anti-virus applications on devices.

62. The bank shall ensure that its customers are provided information about the risks, benefits, and liabilities of using digital payment products and related services before they subscribe to them. The bank shall also inform the customers clearly and precisely on their rights, obligations and responsibilities on matters relating to digital payments, and any problems that may arise from its service unavailability, processing errors, and security breaches. The terms and conditions including customer privacy and security policy applying to digital payment products and services shall be readily available to customers within the product. All digital channels shall be offered on express willingness of customers and shall not be bundled without their knowledge.

63. The bank shall provide clear and effective communication, along with sufficient instructions, to enable customers to properly utilise any new operating features or functions, particularly those relating to security, integrity, and authentication, introduced to online delivery channels.

64. The bank may continuously create public awareness on the types of threats and attacks used against the customers while using digital payment products and precautionary measures to safeguard against the same. The bank shall caution the customers against commonly observed threats including phishing, vishing, reverse phishing, remote access of mobile devices, and educate them to secure and safeguard their account details, credentials, PIN, card details, devices and other authentication information.

65. The bank shall provide digital payment products and services to a customer only at their option based on a specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions.

66. The bank shall provide a mechanism on its mobile and internet banking application for its customers, with necessary authentication, to identify / mark a transaction as fraudulent for seamless and immediate notification to the bank. On such notification by the customer, the bank shall endeavour to build the capability for seamless / instant reporting of fraudulent transactions to the corresponding beneficiary / counterparty's entity. The bank may also have a mechanism to receive such fraudulent transactions reported from other entities.

Chapter IV - Internet Banking Security Controls

67. In addition to the controls prescribed in **Chapter III**, the following instructions are applicable to the bank offering / intending to offer internet banking facility to its customers:

(1) The bank, based on its risk / vulnerability assessment on authentication-related attacks such as brute force / Denial of Service (DoS) attacks, shall implement additional levels of authentication to internet banking websites such as adaptive authentication, strong CAPTCHA (with anti-bot features) with server-side validation, in order to plug the vulnerability and prevent its exploitation.

(2) The bank shall take appropriate measures to prevent Domain Name System (DNS) cache poisoning attacks and for secure handling of cookies.

(3) A virtual keyboard option shall be made available.

(4) An online session shall be automatically terminated after a fixed period of inactivity.

(5) The bank shall ensure secure delivery of password for login purpose. The password generated and dispatched by the bank shall be valid for a limited period from the date of its creation. If the password is generated and dispatched by the bank, then the user shall be compulsorily required to change the password, on the first login.

(6) When the internet banking application is accessed through external websites (e.g., in case of payment of taxes, e-commerce transactions), the procedure for authentication and the appearance / look / feel of the bank's internet banking site shall be made uniform as far as possible.

Chapter V - Mobile Payments Application Security Controls

68. In addition to the controls prescribed in **Chapter III**, the following instructions are applicable to the bank offering / intending to offer mobile banking / mobile payments facility to its customers through mobile application:

(1) On detection of any anomalies or exceptions for which the mobile application was not programmed, the customer shall be directed to remove the current copy / instance of the application and proceed with installation of a new copy / instance of the application. The bank shall be able to verify the version of the mobile application before the transactions are enabled.

(2) The bank shall ensure implementation of the following specific controls for mobile applications:

(i) device policy enforcement [allowing the installation / execution of applications only after baseline requirements defined based on the bank's risk assessment, are met. The baseline requirements shall include but not be limited to checks for vulnerable operating system, vulnerable or malicious applications, and insecure Wi-Fi configurations];

(ii) application secure download / install;

(iii) deactivating older application versions in a phased but time-bound manner (not exceeding six months from the date of release of newer version) i.e., maintaining only one version (excluding the overlap period while phasing out older version) of the mobile application on a platform / operating system;

(iv) ability to identify remote access applications (to the extent possible) and prohibit login access to the mobile application;

(v) storage of customer data;

(vi) device or application encryption (to prevent compromise of sensitive customer information stored on the device);

(vii) ensuring minimal data collection / app permissions;

(viii) application sandbox / containerisation; and

(ix) code obfuscation.

[Note: The paragraphs 68(2)(v) to 68(2)(ix) provide an illustrative list of controls to ensure confidentiality and integrity of the data / application stored / processed at the customer end (e.g., mobile device). The bank may, however, adopt alternate / compensating controls, strictly ensuring meeting of such control objectives.]

(3) The bank may perform validation on the security and compatibility condition of the device / operating system and the mobile application to ensure that activities relating to the account are put through the mobile application in a safe and secure manner.

(4) The bank may explore the feasibility of implementing a code that checks if the device is rooted / jailbroken prior to the installation of the mobile application and disallow the mobile application to install / function if the phone is rooted / jailbroken.

(5) The bank shall host the checksum of current active version of its mobile application on public platform so that users can verify the same. A checksum may be treated as a unique mechanism for identifying the bank's mobile application and for distinguishing it from unauthorised or rogue mobile applications. Where the mobile application is made available exclusively through mobile platform app store, compliance with this control may be achieved by providing, on the bank's website, a direct link or Quick Response (QR) code to enable customers to access or download only the authorised mobile application of the bank.

(6) The bank shall ensure device binding of the mobile application. Device binding shall be implemented through a combination of hardware, software, and service information. In case, the bank allows multiple devices to be registered, then, (i) the user shall be notified of every new device

registration on multiple channels such as registered mobile number, email or phone call, and (ii) in relation to the mobile application, the bank shall maintain a record of all registered devices, providing the user a facility to disable a registered device.

(7) The bank may implement alternatives to SMS-based OTP authentication mechanisms.

(8) The mobile application shall require re-authentication whenever the device or application remains unused for a designated period and each time the user launches the application.

(9) The bank shall ensure that mobile applications are able to identify new network connections or connections from unsecured networks, such as unsecured Wi-Fi connections, and shall implement appropriate authentication / checks / measures to perform transactions under such circumstances.

(10) The mobile application shall not store / retain sensitive personal / customer authentication information such as user IDs, passwords, keys, hashes, and hard coded references, on the device and the application shall securely wipe all sensitive customer information from memory when the customer / user exits the application.

(11) The bank shall ensure that its mobile application limits writing of sensitive information into ‘temp’ files. The sensitive information written in such files shall be suitably encrypted / masked / hashed and stored securely.

(12) The bank may consider designing anti-malware capabilities into its mobile application.

(13) The bank shall ensure to:

(i) avoid usage of raw (visible) Structured Query Language (SQL) queries in mobile applications to fetch or update data from databases;

(ii) secure mobile applications from SQL injection type of vulnerabilities;

(iii) write sensitive information to the database in an encrypted form (database here refers to the database in the mobile application at client's end. The bank shall encrypt the sensitive data stored in the database used by the mobile application);

(iv) prevent loading web content, as part of the mobile application’s layout if errors are detected during Secure Sockets Layer (SSL) / Transport Layer Security (TLS) negotiation; and

(v) display certificate errors on account of the certificate not being signed by a recognised certificate authority or due to expiry / revocation of the certificate, to the user.

Chapter VI - Card Payment Security Controls

69. In addition to the controls prescribed in **Chapter III**, the following instructions are applicable to the bank issuing / intending to issue cards (credit / debit / prepaid) (physical or virtual) to its customers:

(1) The bank shall follow various payment card standards [over and above Payment Card Industry-Data Security Standard (PCI-DSS) and Payment Card Industry-Software Security Framework (PCI-SSF)] as per Payment Card Industry (PCI) prescriptions for comprehensive payment card security as per applicability / readiness of updated versions of the standards such as:

(i) Payment Card Industry-Personal Identification Number (PCI-PIN) - secure management, processing, and transmission of PIN data;

(ii) Payment Card Industry-PIN Transaction Security (PCI-PTS) - security approval framework addressing the logical and / or physical protection of cardholder and other sensitive data at point of interaction (POI) devices and hardware security modules (HSMs);

(iii) Payment Card Industry-Hardware Security Module (PCI-HSM) - securing cardholder-authentication applications and processes including key generation, key injection, PIN verification, secure encryption algorithm; and

(iv) Payment Card Industry-Point to Point Encryption (PCI-P2PE) - security standard that requires payment card information to be encrypted instantly upon its initial swipe and then securely transferred directly to the payment processor.

(2) With reference to paragraph 69(1), though formal certification may not be mandatory, the bank shall follow these standards holistically, as per applicability. The standards shall apply to the bank in its capacity as both issuer and acquirer. The scope of applicability shall vary depending on the outsourcing model adopted by the bank. The bank shall obtain appropriate

confirmation from the relevant third parties regarding compliance with these standards. The bank shall put up a status report on compliance with these standards to its IT Strategy Committee, as prescribed under Reserve Bank of India (Small Finance Banks – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026, for deliberation and appropriate action.

(3) The bank shall ensure that (i) terminals installed at the merchants for capturing card details for payments or otherwise are validated against the PCI-P2PE program to use PCI-approved P2PE solutions, (ii) Point of Sales (PoS) terminals with PIN entry installed at the merchants for capturing card payments (including the double swipe terminals) are approved by the PCI-PTS program. While deploying any new PoS terminals, the bank shall ensure that such terminals are certified in accordance with PCI-PTS requirements. PoS terminals already deployed may not be required to undergo re-certification upon expiry of the certification, provided that they were duly certified at the time of deployment. The bank may also consider mandating re-certification through its vendor, as deemed appropriate.

(4) The bank as an Acquirer shall secure its card payment infrastructure [Unique Key Per Terminal (UKPT) or Derived Unique Key Per Transaction - (DUKPT) / Terminal Line Encryption (TLE)].

(5) The bank shall implement the following controls at the HSMs:

(i) The HSMs shall have logging enabled and the logs must themselves be tamper proof.

(ii) The bank shall mitigate the risk of single point of failure at HSM by implementing ‘clustering’ for high availability and ensuring secure backups.

(iii) The bank shall ensure access to the HSM through Access Control Lists (ACLs).

(iv) The bank shall maintain separate ACLs for each individual application to ensure application-level isolation.

(v) The bank shall manage and monitor access to HSM using a robust Privileged Identity and Access Management solution.

(vi) The bank shall ensure decryption and validation of keys, PIN at HSM.

(vii) The bank shall ensure card PIN generation and printing directly at system connected to HSM.

(viii) The bank shall ensure generation and validation of CVV at HSM.

(ix) The bank shall ensure that HSM is implemented with secure PIN block format with controls to disable outputting PIN block in weaker format.

(x) The bank shall ensure secure key management for HSMs including Local Master Keys (LMKs).

(xi) The bank shall ensure proper security for the maintenance of physical keys of the HSM.

(6) The bank shall ensure the following for improving the security posture of the ATM:

(i) implement security measures such as Basic Input / Output System (BIOS) password, disabling Universal Serial Bus (USB) ports, disabling auto-run facility, applying the latest patches of operating system and other software, terminal security solution, time-based admin access;

(ii) implement anti-skimming and whitelisting solution; and

(iii) upgrade all ATMs with supported versions of operating system.

(7) With regard to card transactions, the bank shall:

(i) ensure robust surveillance / monitoring of card transactions (especially overseas cash withdrawals) and setting up of rules and limits commensurate with its risk appetite;

(ii) take up with the card network and / or ATM network, to put in place transaction limits at card, Bank Identification Number (BIN) as well as at the bank level. Such limits shall be mandatorily set at the card network switch itself. Limits may be mandated for domestic as well as international transactions separately;

(iii) put in place transaction control mechanisms with necessary caps (restrictions on transactions), if any of the limits set as per the above requirement is breached. A periodic review mechanism of such limits set as per the risk appetite of the bank shall be put in place as per the Board-approved policy;

(iv) institute a mechanism to monitor breaches, if any, on a 24x7 basis, including weekends and holidays and put in place a robust incident response mechanism to mitigate the fraud loss, on account of suspicious transactions, if any;

(v) ensure that card details of the customers are not stored in plain text at the bank and its vendor(s) locations, systems, and applications; and

(vi) ensure that the processing of card details in readable format is performed in a secure manner to strictly avoid data leakage of sensitive customer information.

(8) The bank using card data scanning tools to identify unencrypted (clear text) payments card data in its ecosystem especially during audits, shall adhere to the following safety measures:

(i) any tool (procured by / from a third-party) for the purpose of scanning of unencrypted card data shall first be tested in a test environment to understand the scope and impact of the tool’s capabilities;

(ii) the scanning tool shall be installed only in the bank's premises on its devices;

(iii) card data scanning shall not be done remotely;

(iv) discovered data, if any, shall reside in the scanning tool;

(v) exportable card data shall be appropriately masked (no data, even masked, shall be taken out of the bank's premises / infrastructure); and

(vi) service providers shall be provided limited access to conduct the scan or analyse the data, and such access shall be provided only on the bank's devices.

Chapter VII - Repeal and Other Provisions

A. Repeal and Saving

70. With the issue of these Directions, the existing directions, instructions, and guidelines relating to Digital Payment Security Controls as applicable to Small Finance Banks stand repealed, as communicated vide circular no. DoS.CO.PPG.66/11.01.005/2026-27 dated July 31, 2026. The directions, instructions, and guidelines repealed prior to the issuance of these Directions shall continue to remain repealed.

71. Notwithstanding such repeal, any action taken or purported to have been taken, or initiated under the repealed directions, instructions, or guidelines shall continue to be governed by the provisions thereof. All approvals or acknowledgments granted under these repealed lists shall be deemed as governed by these Directions. Further, the repeal of these directions, instructions, or guidelines shall not in any way prejudicially affect:

(1) any right, obligation or liability acquired, accrued, or incurred thereunder;

(2) any penalty, forfeiture, or punishment incurred in respect of any contravention committed thereunder;

(3) any investigation, legal proceeding, or remedy in respect of any such right, privilege, obligation, liability, penalty, forfeiture, or punishment as aforesaid; and any such investigation, legal proceedings or remedy may be instituted, continued, or enforced and any such penalty, forfeiture or punishment may be imposed as if those directions, instructions, or guidelines had not been repealed.

B. Application of Other Laws Not barred

72. The provisions of these Directions shall be in addition to, and not in derogation of the provisions of any other laws, rules, regulations, or directions, for the time being in force.

C. Interpretations

73. For the purposes of giving effect to the provisions of these Directions or for removing any difficulties in their application or interpretation, RBI may, if it deems necessary, issue such clarifications as it considers appropriate in respect of any matter covered herein. The interpretation of any provision of these Directions by RBI shall be final and binding on all concerned entities.

(N. Suganandh)
Chief General Manager