**Digital Banking**

|  |  |
| --- | --- |
| **Sr. No.** | **RBI Notifications** |
| 1 | Bharat Bill Payment System – Addition of Biller Category |
| 2 | Usage of Automated Teller Machines / Cash Recycler Machines – Review of Interchange Fee and Customer Charges |
| 3 | Customer Due Diligence for transactions in Virtual Currencies (VC) |
| 4 | Relaxation in timeline for compliance with various payment system requirements |
| 5 | Prepaid Payment Instruments (PPIs) – (i) Mandating Interoperability; (ii) Increasing the Limit to ₹2 lakh for Full-KYC PPIs; and (iii) Permitting Cash Withdrawal from Full-KYC PPIs of Non-Bank PPI Issuers |
| 6 | Master Direction on Levy of Penal Interest for Delayed Reporting / Wrong Reporting / Non-Reporting of Currency Chest Transactions and Inclusion of Ineligible Amounts in Currency Chest Balances |
| 7 | Master Direction on “Currency Distribution & Exchange Scheme (CDES)” for bank branches including currency chests based on performance in rendering customer service to members of public |
| 8 | Master Circular – Scheme of Penalties for bank branches including Currency Chests based on performance in rendering customer service to the members of public |
| 9 | Master Circular – Detection and Impounding of Counterfeit Notes |
| 10 | Master Circular – Facility for Exchange of Notes and Coins |
| 11 | Framework for processing of e-mandates for recurring online transactions |
| 12 | Guidelines on Regulation of Payment Aggregators and Payment Gateways |
| 13 | Extension of Cheque Truncation System (CTS) across all bank branches in the country |
| 14 | Master Direction on Digital Payment Security Controls |
| 15 | Introduction of Legal Entity Identifier for Large Value Transactions in Centralised Payment Systems |
| 16 | Operationalisation of Payments Infrastructure Development Fund (PIDF) Scheme |
| 17 | Booklet on Payment Systems in India |

1**. Bharat Bill Payment System – Addition of Biller Category**

RBI/2021-22/54
CO.DPSS.POLC.No.S188/02-27-020/2021-2022

June 14, 2021

The Chairman and Managing Director / Chief Executive Officer
Scheduled Commercial Banks including RRBs /
Urban Co-operative Banks / State Co-operative Banks /
District Central Co-operative Banks / Payment Banks / Small Finance Banks /
NPCI Bharat BillPay Ltd. / Bharat Bill Payment System Providers /
System Participants and prospective Bharat Bill Payment Operating Units

Madam / Dear Sir,

**Bharat Bill Payment System – Addition of Biller Category**

This has reference to the guidelines on Bharat Bill Payment System (BBPS) issued by the Reserve Bank of India vide [circular DPSS.CO.PD.No.940/02.27.020/2014-2015 on November 28, 2014](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=9368&Mode=0). BBPS, started as an interoperable platform for repetitive bill payments, which covered bills of five categories viz. Direct to Home (DTH), Electricity, Gas, Telecom and Water. The system provided standardised bill payment experience, centralised customer grievance redressal mechanism, prescribed customer convenience fee and ensured availability of a bouquet of anytime, anywhere digital payment options. The scope and coverage of BBPS was expanded vide [circular DPSS.CO.PD.No.605/02.27.020/2019-20 dated September 16, 2019](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11686&Mode=0) to include all categories of billers which raise recurring bills (except mobile prepaid recharges) as eligible participants, on a voluntary basis.

2. With consistent growth in different biller categories and to facilitate mobile prepaid customers with more options to recharge, it has been decided to permit ‘mobile prepaid recharges’ as a biller category in BBPS, on a voluntary basis. This will be implemented on or before August 31, 2021.

3. This directive is issued under Section 10 (2) read with Section 18 of the Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

**2. Usage of Automated Teller Machines / Cash Recycler Machines – Review of Interchange Fee and Customer Charges**

**RBI/2021-22/52DPSS.CO.OD.No.S-182/06.07.011/2021-22 June 10, 2021**

*The Chairman and Managing Director / Chief Executive Officer, All Scheduled Commercial Banks including RRBs / Urban Co-operative Banks / State Co-operative Banks / District Central Co-operative Banks / Authorised ATM Network Operators / Card Payment Network Operators / White Label ATM Operators*

The Reserve Bank of India had constituted a Committee in [June 2019](https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=47270) under the Chairmanship of the Chief Executive, Indian Banks’ Association to review the entire gamut of Automated Teller Machine (ATM) charges and fees with particular focus on interchange structure for ATM transactions.

2. The recommendations of the Committee have been comprehensively examined. It is also observed that the last change in interchange fee structure for ATM transactions was in August 2012, while the charges payable by customers were last revised in August 2014. A substantial time has thus elapsed since these fees were last changed. Accordingly, given the increasing cost of ATM deployment and expenses towards ATM maintenance incurred by banks / white label ATM operators, as also considering the need to balance expectations of stakeholder entities and customer convenience, it has been decided as under :

1. Allow increase in interchange fee per transaction from ₹15 to ₹17 for financial transactions and from ₹5 to ₹6 for non-financial transactions in all centres. This shall be effective from August 1, 2021.
2. Customers are eligible for five free transactions (inclusive of financial and non-financial transactions) every month from their own bank ATMs. They are also eligible for free transactions (inclusive of financial and non-financial transactions) from other bank ATMs viz. three transactions in metro centres and five transactions in non-metro centres. Beyond the free transactions, the ceiling / cap on customer charges is ₹20 per transaction, as prescribed vide [circular DPSS.CO.PD.No.316/02.10.002/2014-2015 dated August 14, 2014](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=9170&Mode=0). To compensate the banks for the higher interchange fee and given the general escalation in costs, they are allowed to increase the customer charges to ₹21 per transaction. This increase shall be effective from January 1, 2022.
3. Applicable taxes, if any, shall be additionally payable.
4. These instructions shall also apply, mutatis mutandis, to transactions done at Cash Recycler Machines (other than for cash deposit transactions).

3. This directive is issued under Section 10(2) read with Section 18 of the Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

**3. Customer Due Diligence for transactions in Virtual Currencies (VC)**

**RBI/2021-22/45 DOR. AML.REC 18 /14.01.001/2021-22 May 31, 2021**

*All Commercial and Co-operative Banks / Payments Banks/ Small Finance Banks /
NBFCs / Payment System Providers*

It has come to our attention through media reports that certain banks/ regulated entities have cautioned their customers against dealing in virtual currencies by making a reference to the [RBI circular DBR.No.BP.BC.104/08.13.102/2017-18 dated April 06, 2018](https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=11243&fn=2&Mode=0). Such references to the above circular by banks/ regulated entities are not in order as this  circular was set aside by the Hon’ble Supreme Court on March 04, 2020 in the matter of Writ Petition (Civil) No.528 of 2018 (Internet and Mobile Association of India v. Reserve Bank of India). As such, in view of the order of the Hon’ble Supreme Court, the circular is no longer valid from the date of the Supreme Court judgement, and therefore cannot be cited or quoted from.

2. Banks, as well as other entities addressed above, may, however, continue to carry out customer due diligence processes in line with regulations governing standards for Know Your Customer (KYC), Anti-Money Laundering (AML), Combating of Financing of Terrorism (CFT) and obligations of regulated entities under Prevention of Money Laundering Act, (PMLA), 2002 in addition to ensuring compliance with relevant provisions under Foreign Exchange Management Act (FEMA) for overseas remittances.

**4. Relaxation in timeline for compliance with various payment system requirements**

**RBI/2021-22/41 CO.DPSS.POLC.No.S-106/02-14-003/2021-2022 May 21, 2021**

*The Chairman / Managing Director / Chief Executive Officer, All Scheduled Commercial Banks, including Regional Rural Banks / Urban Co-operative Banks / State Co-operative Banks, District Central Co-operative Banks / Payments Banks / Small Finance Banks / Local Area Banks / Non-Bank PPI Issuers / Authorised Payment System Operators / Participants*

A reference is invited to Reserve Bank of India instructions – (a) [DPSS.CO.PD.No.1164/02.14.006/2017-18 dated October 11, 2017](https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142) (as updated from time to time) on Master Direction on Issuance and Operation of Prepaid Payment Instruments (PPI-MD); (b) [DPSS.CO.PD.No.629/02.01.014/2019-20 dated September 20, 2019](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11693&Mode=0) on Harmonisation of Turn Around Time (TAT) and Customer Compensation for Failed Transactions using Authorised Payment Systems; (c) DPSS.CO.OD.No.1325/06.11.001/2019-20 dated January 10, 2020 on Scope and Coverage of System Audit of Payment Systems; (d) [DPSS.CO.PD.No.1810/02.14.008/2019-20 dated March 17, 2020](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0) on Guidelines on Regulation of Payment Aggregators (PAs) and Payment Gateways (PGs); and (e) [DPSS.CO.PD.No.1897/02.14.003/2019-20 dated June 4, 2020](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11910&Mode=0) on Extension of Timeline for Compliance with Various Payment System Requirements.

2. Keeping in view the resurgence of the COVID-19 pandemic and the representations received from various bank and non-bank entities, it has been decided to extend the timeline prescribed for compliance in respect of a few areas detailed in the [Annexure](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12095&Mode=0#AN).

3. This directive is issued under Section 10(2) read with Section 18 of the Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

**Annexure**

|  |  |  |  |
| --- | --- | --- | --- |
| **SN** | **Instruction / Circular** | **Present Timeline** | **Revised Timeline** |
| 1. | All existing non-bank PPI issuers (at the time of issuance of PPI-MD) to comply with the minimum positive net-worth requirement of Rs.15 crore for the financial position as on March 31, 2020 (audited balance sheet). | Financial position as on March 31, 2021 | Financial position as on September 30, 2021 |
| 2. | Harmonisation of TAT and customer compensation for failed transactions using authorised Payment Systems – “Calendar days” to be read as “Working days”. | Working days until December 31, 2020 (Calendar days from January 1, 2021) | Working days – Prospective – Until September 30, 2021 |
| 3. | Authorised Payment System Operators (PSOs) are required to furnish System Audit Report conducted by CERT-IN empanelled auditors or a Certified Information Systems Auditor registered with Information Systems Audit and Control Association or by a holder of a Diploma in Information System Audit qualification of the Institute of Chartered Accountants of India, on an annual basis within two months of close of their respective financial year. | By May 31, 2021 | By September 30, 2021 |
| 4. | Existing non-bank entities offering PA services shall apply for authorisation on or before June 30, 2021. | By June 30, 2021 | By September 30, 2021\* |

\* Extension provided vide [circular CO.DPSS.POLC.No.S33/02-14-008/2020-2021 dated March 31, 2021](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12050&Mode=0) to enable payment system providers and participants to put in place workable solutions to comply with the provisions of Paragraphs 7.4 and 10.4 of the [circular dated March 17, 2020](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0) will not be impacted.

**5. Prepaid Payment Instruments (PPIs) – (i) Mandating Interoperability; (ii) Increasing the Limit to ₹2 lakh for Full-KYC PPIs; and (iii) Permitting Cash Withdrawal from Full-KYC PPIs of Non-Bank PPI Issuers**

**RBI/2021-22/40 DPSS.CO.PD.No.S-99/02.14.006/2021-22 May 19, 2021**

*All Bank and Non-Bank Prepaid Payment Instrument Issuers, System Providers and System Participants*

This has reference to paragraphs 10 and 11 of the [Statement on Developmental and Regulatory Policies dated April 07, 2021](https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=51382) wherein it was announced that (a) PPI interoperability shall be made mandatory, (b) the limit for full-KYC PPIs shall be increased from ₹1 lakh to ₹2 lakh, and (c) cash withdrawal shall be permitted using full-KYC PPIs of non-bank PPI issuers.

2. A reference is also invited to the [Master Direction DPSS.CO.PD.No.1164/02.14.006/2017-18 dated October 11, 2017](https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142) on Issuance and Operation of PPIs (as amended from time to time) and [Circular DPSS.CO.PD.No.808/02.14.006/2018-19 dated October 16, 2018](https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11393&Mode=0) on PPIs – Guidelines for Interoperability.

3. Accordingly, the following are advised –

1. It shall be mandatory for PPI issuers to give the holders of full-KYC PPIs (KYC-compliant PPIs) interoperability through authorised card networks (for PPIs in the form of cards) and UPI (for PPIs in the form of electronic wallets);
2. Interoperability shall be mandatory on the acceptance side as well;
3. The interoperability shall be enabled by March 31, 2022; and
4. PPIs for Mass Transit Systems (PPI-MTS) shall remain exempted from interoperability while Gift PPI issuers have the option to offer interoperability.

4. The maximum amount outstanding in respect of full-KYC PPIs (KYC-compliant PPIs) has been increased from ₹1 lakh to ₹2 lakh. All other conditions mentioned under paragraphs 9.1 (ii) and 9.2 of the [Master Direction on PPIs dated October 11, 2017](https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142) shall continue to be applicable.

5. The feature of cash withdrawal shall be permitted in respect of full-KYC PPIs issued by non-bank PPI issuers as well. The following conditions shall, however, be applicable –

1. Maximum limit of ₹2,000 per transaction with an overall limit of ₹10,000 per month per PPI;
2. All cash withdrawal transactions performed using a card / wallet, shall be authenticated by an Additional Factor of Authentication (AFA) / PIN;
3. Any PPI issuer offering this facility shall put in place proper customer redressal mechanisms. Complaints in this regard shall fall under the ambit of the respective ombudsmen schemes and instructions on limiting liability of customers; and
4. PPI issuers shall put in place suitable cooling period for cash withdrawal upon opening the PPIs or loading / re-loading of funds into PPIs to mitigate the risk of fraudulent use of PPIs.

6. The cash withdrawal limit from Points of Sale (PoS) terminals using debit cards and open system prepaid cards issued by banks in India advised vide [circular DPSS.CO.PD.No.449/02.14.003/2015-16 dated August 27, 2015](https://rbi.org.in/Scripts/NotificationUser.aspx?Id=10004&Mode=0) has also been rationalised to ₹2,000 per transaction within an overall monthly limit of ₹10,000 across all locations (Tier 1 to 6 centres). The requirement of submission of data to RBI mentioned at paragraph 6 of the circular has been dispensed with. All other provisions shall, however, continue to be applicable.

7. The [Master Direction on Issuance and Operation of PPIs dated October 11, 2017](https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142) (as amended from time to time) is being modified to reflect the above.

8. These instructions are issued under Section 18 read with Section 10(2) of the Payment and Settlement Systems Act, 2007.

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12094&Mode=0>

**6. Master Direction on Levy of Penal Interest for Delayed Reporting / Wrong Reporting / Non-Reporting of Currency Chest Transactions and Inclusion of Ineligible Amounts in Currency Chest Balances**

RBI/2021-22/77 Master Direction DCM (CC) No.G-4/03.35.01/2021-22 April 01, 2021

*The Chairman/ Managing Director/Chief Executive Officer, (All Banks having Currency Chests)*

In terms of the Preamble, under Section 45 of the RBI Act, 1934 and 35 A of the Banking Regulation Act, 1949, the Bank issues guidelines / instructions for realising the objectives of our Clean Note Policy. With a view to sustain these efforts and to ensure discipline among the banks on timely and accurate reporting of currency chest transactions, we have issued instructions on the subject. The Master Direction enclosed incorporates updated guidelines / circulars on the subject. The Direction will be updated from time to time as and when fresh instructions are issued.

**1. Penal interest for Delayed Reporting / Wrong Reporting / Non-Reporting of Currency Chest Transactions**

**1.1 Reporting of Currency Chest Transactions**

The minimum amount of deposit into / withdrawal from currency chest will be ₹ 1,00,000 and thereafter, in multiples of ₹ 50,000.

**1.2 Time limit for Reporting**

**1.2.1** The currency chests should invariably report all transactions through CyM – CC portal on the same day by **7 pm**.

**1.2.2 Relaxation in respect of strike period in banks**

Relaxation in the reporting period on account of strike situation will be considered on case-to-case basis.

**1.3 Levy of penal interest –**

**1.3.1 Delay in Reporting -**

In the event of delay in reporting currency chest transactions, penal interest at the rate indicated in paragraph 3 of this circular will be levied on the **amount due** from the chest holding bank for the period of delay. Penal interest will be calculated on T+0 basis i.e. penal interest will be levied in respect of transactions not reported by currency chests to the Issue Office on the same business day within the time limit prescribed above.

**1.3.2 Wrong reporting**

Penal interest will be levied in respect of cases of wrong reporting in the same manner till the date of receipt of corrected advice by Reserve Bank. As debits/credits to banks' current accounts are raised on the basis of the transactions reported by the currency chests, penal interest will invariably be levied in all cases of wrong reporting by the currency chests. It is expected that currency chests would ensure the correctness of figures reported on the CyM - CC portal. Particular care should be taken to ensure that remittances of fresh notes/notes to the currency chests are not reported as 'deposit' transactions on the portal.

**1.3.3 Penal interest for inclusion of ineligible amounts in the currency chest balances**

(i) Penal interest will be levied in all cases where the bank has enjoyed 'ineligible' credit in its current account with Reserve Bank on account of wrong reporting / delayed reporting / non-reporting of transactions. Penal measures will also be taken in cases of shortages in chest balances / remittances, shortages due to pilferage / frauds, counterfeit banknotes detected in chest balances / remittances as per the prevailing “Scheme of Penalties”.

(ii) Further, only cash held in the custody of joint custodians and 'freely available' to them is eligible for inclusion in the chest balances. Thus, cash kept for safe custody in sealed covers for whatever reasons/cash in trunks/bins under the lock and key of any official/s other than the Joint Custodians or bearing a third lock put by any official in addition to the two locks of the Joint Custodians is not eligible for being included in the chest balances. If such amounts are included in the chest balances, these will be treated as instances of wrong reporting and will attract penal interest at the rate specified in Para 3.

(iii) In all the above cases (excepting shortages in chest balances / remittances, shortages due to pilferage / frauds, counterfeit banknotes detected in chest balances / remittances), penal interest will be levied from the date of inclusion of 'ineligible' amounts in chest balances till the exclusion of such amounts from chest balances. Penal measures for shortages in chest balances / remittances, shortages due to pilferage / frauds, counterfeit banknotes detected in chest balances / remittances will be taken on the basis of prevailing “Scheme of Penalties”.

**2 Levy of penalty**

**2.1 Reporting of Soiled note remittances to RBI**

Soiled note remittances to RBI should not be shown as withdrawal by chest/s. In case such remittances to RBI are wrongly reported as 'withdrawals', a penalty of ₹ 50,000 will be levied irrespective of the value of remittance and period of such wrong reporting.

**2.2 Reporting of diversions in CyM – CC portal**

All currency chest diversions (both between chests of the same bank and between chests of different banks) have to be reported through ‘Diversion Module’ of CyM-CC Portal. The CC sending the diversion should initiate the diversion entry. The receiving CC should acknowledge the same. Diversions must not be reported as Deposit/Withdrawal. A penalty of ₹ 50,000 will be levied for such wrong reporting.

**2.3 Delayed reporting where currency chests had “Net Deposit”**

Penal interest at the prevailing rate for delayed reporting of the instances where the currency chest had reported “net deposit” may not be charged. However, in order to ensure proper discipline in reporting currency chest transactions, a flat penalty of ₹ 50,000 may be levied on the currency chests for delayed reporting irrespective of the value of net deposit.

**3. Rate of penal interest**

Penal interest shall be levied at the rate of 2% over the prevailing Bank Rate for the period of delayed reporting/wrong reporting/non-reporting /inclusion of ineligible amounts in chest balances.

**4. Representations**

**4.1** As the sole criterion for levy of penal interest for **delayed reporting** is the number of days of delay, there should ordinarily be no occasion for banks to request for reconsideration of the Reserve Bank's decision in individual cases. However, representations, if any, on account of genuine difficulties faced by chests especially in hilly/remote areas and those affected by natural calamities, etc., may be made to the Issue Office concerned through the Head / Controlling office of the bank concerned within a month from the date of debit of the bank concerned.

**4.2** In the case of **wrong reporting** representations for waiver will not be considered. {cf. para 1.3.2 above}.

**4.3** As the intention behind the levy of penal interest is to inculcate discipline among banks so as to ensure prompt/correct reporting, pleas by banks for waiver of penal interest on grounds that delayed/wrong/non-reporting did not result in utilization of the Reserve Bank's funds or shortfall in the maintenance of CRR/SLR or that they were the result of clerical mistakes, unintentional or arithmetical errors, first time error, inexperience of staff etc., will **not** be considered as valid grounds for waiver of penal interest. Further, we will take a serious view of all such lapses.

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12056&Mode=0>

**7. Master Direction on “Currency Distribution & Exchange Scheme (CDES)” for bank branches including currency chests based on performance in rendering customer service to members of public**

**RBI/2021-22/76 Master Direction DCM (CC) No.G-2/03.41.01/2021-22 April 01, 2021**

*The Chairman/Managing Director/Chief Executive Officer, All Banks*

In terms of the Preamble, under Section 45 of the RBI Act, 1934 and 35 A of the Banking Regulation Act, 1949, the Bank issues guidelines / instructions for realising the objectives of Clean Note Policy. With a view to sustaining these objectives, the Bank has formulated a scheme of incentives titled Currency Distribution and Exchange Scheme (CDES) in order to ensure that all bank branches provide better customer services to members of public.

1. The Currency Distribution & Exchange Scheme (CDES) for bank branches including currency chests has been formulated in order to ensure that all bank branches provide better customer service to members of public with regard to exchange of notes and coins, in keeping with the objectives of Clean Note Policy.

**2. Incentives**

As per the scheme, banks are eligible for the following financial incentives for providing facilities for exchange of notes and coins:

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Nature of Service** | **Particulars of Incentives** |
| i) | Opening of and maintaining currency chests at centres having population of less than 1 lakh in under banked States | **a. Capital Cost:** Reimbursement of 50% of capital expenditure subject to a ceiling of ₹ 50 lakh per currency chest. In the North Eastern region up to 100% of capital expenditure is eligible for reimbursement subject to the ceiling of ₹ 50 lakh.**b. Revenue cost:** Reimbursement of 50% of revenue expenditure for the first 3 years. In the North Eastern region 50% of revenue expenditure will be reimbursed for the first 5 years. |
| ii) | Exchange of soiled notes/ adjudication of mutilated banknotes over the counter at bank branches | **a. Exchange of soiled notes –** ₹ 2 per packet for exchange of soiled notes up to denomination ₹ 50**b. Adjudication of mutilated notes –**₹ 2 per piece |
| iii) | Distribution of coins over counter | i. ₹ 25 per bag for distribution of coins over the counter.ii. The incentives would be paid on the basis of withdrawal from currency chest, without waiting for claims from banks.iii. Banks may put in place a system of checks and balances to ensure that coins are distributed to retail customers in small lots and not to bulk customers.iv. The distribution of coins shall be verified by RBI Regional Offices through inspection of currency chest / incognito visits to branches etc. |

**3. Operational Guidelines to avail performance-based incentives –**

1. The incentives will be paid on the soiled notes actually received in the Issue Office of the RBI. Banks need not submit a separate claim in this regard. Currency chest branch will have to pass on the incentive to the linked branches for the soiled notes tendered / coins distributed by them on a pro-rata basis.
2. ii) Similarly, incentive will be paid in respect of the adjudicated notes received along with the soiled note remittances / sent separately by registered / insured post in a sealed cover to the RBI. No separate claim is required to be made.

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12055&Mode=0>

**8. Master Circular – Scheme of Penalties for bank branches including Currency Chests based on performance in rendering customer service to the members of public**

**RBI/2021-22/03 DCM (CC) No. G-3/03.44.01/2021-22 April 01, 2021**

*The Chairman/Managing Director/Chief Executive Officer, All Banks*

Please refer to the Circular DCM (CC) No. G-1/03.44.01/2020-21 dated July 1, 2020 on the scheme of penalties. A revised and updated version on the subject is annexed for information and necessary action.

1. The Scheme of Penalties for bank branches including currency chests has been formulated in order to ensure that all bank branches provide better customer service to members of public with regard to exchange of notes and coins, in keeping with the objectives of Clean Note Policy.

2. Penalties

Penalties to be imposed on banks for deficiencies in exchange of notes and coins/remittances sent to RBI/operations of currency chests etc. are as follows:

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Nature of Irregularity** | **Penalty** |
| i. | Shortages in soiled note remittances and currency chest balances | **For notes in denomination up to ₹ 50**₹ 50/- per piece in addition to the loss**For notes in denomination of ₹ 100 & above**Equal to the value of the denomination per piece in addition to the loss.In case of shortage in soiled note remittances/chest balances, the amount of shortage/loss thereof will be recovered immediately.Penalty will be levied immediately on detection of shortage in soiled note remittances/chest balances, irrespective of the number of pieces detected. |
| ii. | Counterfeit notes detected in soiled note remittances and currency chest balances. | Penalty on account of detection of counterfeit notes by RBI from soiled note remittance of banks and in currency chest balances shall be levied in terms of the instructions issued by DCM (FNVD) No.G-1/16.01.05/2021-22 dated April 01, 2021. |
| iii. | Mutilated notes detected in soiled note remittances and currency chest balances | ₹ 50/- per piece irrespective of the denominationIn case of mutilated notes detected in soiled note remittances and currency chest balances, the amount of loss thereof will be recovered immediately.Penalty will be levied immediately on detection of mutilated notes in soiled note remittances / currency chest balances, irrespective of the number of pieces detected. |
| iv. | Non-compliance with operational guidelines by currency chests detected by RBI officialsa) Non-functioning of CCTVb) Branch cash/documents kept in strong roomc) Non-utilization of NSMs for sorting of notes (NSMs not used for sorting of high denomination notes received over the counter or not used for sorting notes remitted to chest/RBI) | Penalty of ₹ 5000 for each irregularity.Penalty will be enhanced to ₹ 10,000 in case of repetition.Penalty will be levied immediately. |
| v. | Violation of any term of agreement with RBI (for opening and maintaining currency chests) or deficiency in service in providing exchange facilities, as detected by RBI officials e.g.a) Non-issue of coins over the counter to any member of public despite having stock.b) Refusal by any bank branch to exchange soiled notes / refusal by any currency chest branch to adjudicate mutilated notes tendered by any member of publicc) Non conduct of surprise verification of chest balances, at least at bimonthly intervals, by officials unconnected with the custody thereof and by the officials from the Controlling Office once in six months.d) Denial of facilities/services to linked branches of other banks.e) Non acceptance of lower denomination notes (i.e. denomination of ₹ 50 and below) tendered by members of public and linked bank branches.f) Detection of mutilated /counterfeit notes in re-issuable packets prepared by the currency chest branches. | ₹ 10,000 for any violation of agreement or deficiency of service. ₹ 5 lakh in case there are more than 5 instances of violation of agreement/deficiency in service by the branch. The levy of such penalty will be placed in public domain.Penalty will be levied immediately. |

3. Operational Guidelines on levy of penalties –

3.1 Competent Authority –

The Competent Authority to decide the nature of irregularity will be the Officer-in-Charge of the Issue Department of the Regional Office under whose jurisdiction the defaulting currency chest/bank branch is located.

3.2 Appellate Authority -

1. Appeal against the decision of the Competent Authority may be made by the Controlling Office of the currency chest/branch to the Regional Director/Chief General Manager/Officer-in-Charge of the Regional Office concerned, within one month from the date of debit, who may decide whether the same can be accepted/ rejected.
2. Appeals for waiver of penalty made on grounds such as staff being new/untrained, lack of awareness of staff, corrective action having been taken/will be taken, etc. will not be considered.

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12054&Mode=0>

**9. Master Circular – Detection and Impounding of Counterfeit Notes**

**RBI/2021-22/02 DCM (FNVD) G–1/16.01.05/2021-22 April 1, 2021**

*The Chairman/ Managing Director /Chief Executive Officer, All Banks and Director of Treasuries of all States*

Please refer to the [Master Circular DCM (FNVD) G-2/16.01.05/2020-21 dated July 1, 2020](https://www.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=11931) consolidating the instructions issued till July 1, 2020, relating to Detection and Impounding of Counterfeit Notes. The [Master Circular](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12053&Mode=0#MC) has since been updated by incorporating the instructions issued till date.

**Detection and Impounding of Counterfeit Notes**

**Para 1- Authority to Impound Counterfeit Notes**

The Counterfeit Notes can be impounded by

1. All Banks
2. All Treasuries and Sub-Treasuries.
3. Issue Offices of Reserve Bank of India.

**Para 2 - Detection of Counterfeit Notes**

Banknotes tendered over the counter should be examined for authenticity through machines.

Similarly, banknotes received directly at the back office / currency chest through bulk tenders should also be examined through machines.

No credit to customer’s account is to be given for Counterfeit Notes, if any, detected in the tender received over the counter or at the back-office / currency chest.

In no case, the Counterfeit Notes should be returned to the tenderer or destroyed by the bank branches / treasuries. Failure of the banks to impound Counterfeit Notes detected at their end will be construed as wilful involvement of the bank concerned in circulating Counterfeit Notes and penalty will be imposed.

**Para 3 - Impounding of Counterfeit Notes**

Notes determined as counterfeit shall be stamped as "COUNTERFEIT NOTE" and impounded in the prescribed format ([Annex I](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12053&Mode=0#Annex_I)). Each such impounded note shall be recorded under authentication, in a separate register.

**Para 4 - Issue of Receipt to Tenderer**

When a banknote tendered at the counter of a bank branch / back office and currency chest or treasury is found to be counterfeit, an acknowledgement receipt in the prescribed format ([Annex II](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12053&Mode=0#Annex_II)) must be issued to the tenderer, after stamping the note as in Paragraph 3 ibid. The receipt, in running serial numbers, should be authenticated by the cashier and tenderer. Notice to this effect should be displayed prominently at the offices / branches for information of the public. The receipt is to be issued even in cases where the tenderer is unwilling to countersign it.

**Para 5 - Detection of Counterfeit Notes - Reporting to Police and other bodies**

The following procedure should be followed while reporting incidence of detection of Counterfeit Note to the Police:

For cases of detection of Counterfeit Notes up to 4 pieces, in a single transaction, a consolidated report in the prescribed format ([Annex III](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12053&Mode=0#Annex_III)) should be sent by the Nodal Bank Officer to the police authorities or the Nodal Police Station, along with the suspect Counterfeit Notes, at the end of the month.

For cases of detection of Counterfeit Notes of 5 or more pieces, in a single transaction, the Counterfeit Notes should be forwarded immediately by the Nodal Bank Officer to the local police authorities or the Nodal Police Station for investigation by filing FIR in the prescribed format ([Annex IV](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12053&Mode=0#Annex_IV)).

A copy of the monthly consolidated report / FIR shall be sent to the Forged Note Vigilance Cell constituted at the Head Office of the bank (only in the case of banks), and in the case of the treasury, it should be sent to the Issue Office of the Reserve Bank concerned.

Acknowledgement of the police authorities concerned has to be obtained for note/s forwarded to them both as consolidated monthly statement and for filing of FIR. If the Counterfeit Notes are sent to the police by insured post, acknowledgement of receipt thereof by the police should be invariably obtained and kept on record. A proper follow-up of receipt of acknowledgement from the police authorities is necessary. In case any difficulty is faced by the Offices / Branches due to reluctance of the police to receive monthly consolidated statement / file FIRs, the matter may be sorted out in consultation with the Nodal Officer of the police authority designated to coordinate matters relating to investigation of Counterfeit Banknotes cases. The list of Nodal Police Stations may be obtained from the Regional Office concerned of the Reserve Bank of India.

In order to facilitate identification of people abetting circulation of Counterfeit Notes, banks are advised to cover the banking hall / area and counters under CCTV surveillance and recording and preserve the recording.

Banks should also monitor the patterns / trends of such detection and suspicious trends / patterns should be brought to the notice of RBI / Police authorities immediately.

The progress made by banks in detection and reporting of Counterfeit Notes to Police, RBI, etc. and problems thereof, should be discussed regularly in the meetings of various State Level Committees viz. State Level Bankers’ Committee (SLBC), Standing Committee on Currency Management (SCCM), State Level Security Committee (SLSC), etc.

The data on detection of counterfeit Indian notes at bank branches and treasuries should be included in the monthly returns forwarded to the Reserve Bank Issue Offices as indicated in [para 10](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12053&Mode=0#C10) below.

The definition of 'counterfeiting' in the Indian Penal Code covers currency notes issued by a foreign government authority as well. In case of suspected foreign currency note received for opinion from the police and government agencies, etc., they should be advised to forward the case to the Interpol Wing of the CBI, New Delhi after prior consultation with them.

The Government of India has framed Investigation of High Quality Counterfeit Indian Currency Offences Rules, 2013 under Unlawful Activities (Prevention) Act (UAPA), 1967. The Third Schedule of the Act defines High Quality Counterfeit Indian Currency Note. Activity of production, smuggling or circulation of High Quality Counterfeit Indian Notes has been brought under the ambit of UAPA, 1967.

**Para 6 - Examination of the Banknotes before Issuing over Counters, Feeding ATMs and Remitting to Issue Offices of the Reserve Ban**k

The banks should re-align their cash management in such a manner so as to ensure that cash receipts in the denominations of ₹100 and above are not put into re-circulation without the notes being machine processed for authenticity. The said instructions shall be applicable to all bank branches, irrespective of the volume of daily cash receipt. Any non-compliance will be construed as violation of the [Directive No.3158/09.39.00 (Policy)/2009-10 dated November 19, 2009](https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=5376&Mode=0#M) issued by the Reserve Bank.

In order to obviate complaints regarding receipt of Counterfeit Notes through ATMs, and to curb circulation of counterfeits, it is imperative to put in place adequate safeguards / checks before loading ATMs with notes. Dispensation of Counterfeit Notes through the ATMs would be construed as an attempt to circulate the Counterfeit Notes by the bank concerned.

Detection of counterfeits in chest remittances is also liable to be construed as wilful involvement of the chest branches concerned in circulating Counterfeit Notes and may attract special investigation by police authorities, and other action like suspending the operation of the chest concerned.

Penalty at 100% of the notional value of Counterfeit Notes, in addition to the recovery of loss to the extent of the notional value of such notes, will be imposed under the following circumstances:

a) When Counterfeit Notes are detected in the soiled note remittance of the bank.

b) If Counterfeit Notes are detected in the currency chest balance of a bank during Inspection / Audit by RBI.

In terms of [DPSS.CO.OD.No.1916/06.07.011/2018-19 dated March 7, 2019](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11495&Mode=0), all guidelines, safeguards, standards and control measures applicable to banks relating to (a) currency handling, and (b) cyber-security framework for ATMs, shall also be applicable to the WLA Operators.

**Para 7 - Designating Nodal Bank Officer**

Each bank should designate a Nodal Bank Officer, district-wise and notify the same to the Regional Office of RBI concerned and Police Authorities. All cases of reporting of Counterfeit Note detection as indicated in [Para 5](https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=10517&fn=2753&Mode=0#5) should be done through the Nodal Bank Officer. The Nodal Bank Officer will also serve as the contact point for all Counterfeit Note detection related activities.

**Para 8 - Establishment of Forged Notes Vigilance Cell at Head Office of Bank**

Each bank shall establish at its Head Office, a Forged Note Vigilance (FNV) Cell to undertake the following functions:

1. Dissemination of instructions issued by the Reserve Bank on Counterfeit Notes to bank’s branches. Monitoring the implementation of these instructions. Compilation of data on detection of Counterfeit Notes, and its submission to Reserve Bank, FIU-IND and National Crime Records Bureau (NCRB) as per extant instructions. Follow-up of cases of Counterfeit Notes, with police authorities / designated nodal officer.
2. Sharing of the information thus compiled with bank’s CVO and report to him / her all cases of acceptance / issue of Counterfeit Notes over the counters.
3. Conducting periodic surprise checks at currency chests where shortages / defective / Counterfeit Notes etc. are detected.
4. Ensuring operation of Note Sorting Machines of appropriate capacity at all the currency chests / back offices and closely monitoring the detection of Counterfeit Notes and maintaining the record of the same. Ensuring that only properly sorted and machine examined banknotes are fed into the ATMs / issued over the counters and to put in place adequate safeguards, including surprise checks, both during the processing and in transit of notes.

FNV Cell shall submit status report on a quarterly basis covering the aforesaid aspects to the Chief General Manager, Department of Currency Management, Reserve Bank of India, Central Office, Amar Building, Fourth Floor, Sir P. M. Road, Fort, Mumbai 400 001 / to (email) and to the Issue office of the Regional office of Reserve Bank under whose jurisdiction the FNV Cell is functioning, within a fortnight from the conclusion of the quarter under report. The said report should be sent by e-mail. No hard copy need be sent.

In order to update the record of the addresses of the FNV Cells, the bank shall furnish by e-mail, in the prescribed format ([Annex V](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12053&Mode=0#Annex_V)), the particulars to the Reserve Bank every year, as on 1st April. No hard copy need be sent.

**Para 9 - Provision of Ultra-Violet Lamp and Other Infrastructure**

With a view to facilitating the detection of Counterfeit Notes, all bank branches / identified back offices should be equipped with ultra-violet lamps / other appropriate banknote sorting / detection machines. In addition, all currency chest branches should be equipped with verification, processing and sorting machines and should be used to their optimum capacity. Such machines should conform to the guidelines on '[Note Authentication and Fitness Sorting Parameters' prescribed by the Reserve Bank](https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=5671&Mode=0#A).

The banks shall maintain a daily record of the notes processed through the Note Sorting machines, including the number of counterfeits detected.

The banks should also consider providing at least one counting machine (with dual display facility) for public use at the counter.

**Para 10 - Reporting of Data to RBI / NCRB / FIU-IND**

By All Bank branches

Data on Counterfeit Notes detected by all the branches of the bank shall be reported in the prescribed format, on a monthly basis. A statement ([Annex VI](https://rbidocs.rbi.org.in/rdocs/content/pdfs/02MC01042021_AVI.pdf)) showing the details of Counterfeit Notes detected in the bank branches during the month shall be compiled and forwarded to the Issue Office of Reserve Bank concerned so as to reach them by 7th of the next month. A “nil “report may be sent in case no counterfeit note has been detected during the month.

Under Rule 8 (1) of Prevention of Money Laundering (Maintenance of Records) Amendment Rules, 2013, Principal Officers of banks are also required to report information on cash transactions where forged notes have been detected to The Director, FIU-IND, Financial Intelligence Unit- India, 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi-110021, by the 15th day of the succeeding month, **by uploading the information on the FINnet Portal**. Similarly, data on Counterfeit Note detection is also to be uploaded on the web-enabled software of National Crime Records Bureau, New Delhi **at their website**.

**Para 11- Preservation of Counterfeit Notes Received from Police Authorities**

All Counterfeit Notes received back from the police authorities / courts may be carefully preserved in the safe custody of the bank and a record thereof be maintained by the branch concerned. FNV Cell of the bank shall also maintain a branch-wise consolidated record of such Counterfeit Notes.

These Counterfeit Notes at branches should be subjected to verification on a half-yearly basis (on 31st March and 30th September) by the Officer-in-Charge of the bank office concerned. They should be preserved for a period of three years from the date of receipt from the police authorities.

Counterfeit Notes, which are the subject matter of litigation in the court of law should be preserved with the branch concerned for three years after conclusion of the court case.

After the preservation period, such notes may be sent to the Issue Office of Reserve Bank of India concerned with full details.

**Para 12 - Detection of Counterfeit Notes - Training of Staff**

It is necessary to ensure that the cash handling staff in banks and treasuries / sub-treasuries are fully conversant with the security features of a banknote.

With a view to educating the branch staff on detection of Counterfeit Notes, the design and security features of all the banknotes shown in [Annex VII](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12053&Mode=0#Annex_VII) have been supplied to all the banks / treasuries with instructions to display them prominently at the branches for information of the public. Details of security features of the New Design banknotes of ₹2000, ₹500, ₹200, ₹100, ₹50, ₹20 and ₹10 are available at the link [https://paisaboltahai.rbi.org.in](https://paisaboltahai.rbi.org.in/).

Details of other banknotes are also available under ‘Know your Banknotes’ at the above link.

The Controlling Offices / Training Centers should also organise / conduct training programmes on the security features of banknotes for members of staff to enable detection of Counterfeit Notes at the point of receipt itself. The banks should ensure that all bank personnel handling cash are trained on features of genuine Indian bank notes. These trainings should cover detection, impounding and reporting of Counterfeit Notes. The Reserve Bank will also provide faculty support and training materials.

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12053&Mode=0>

**10. Master Circular – Facility for Exchange of Notes and Coins**

**RBI/2021-22/01 DCM (NE) No.G-4/08.07.18/2021-22 April 01, 2021**

*The Chairman/ The Managing Director/The Chief Executive Officer, All Banks*

Please refer to the [Master Circular DCM (NE) No.G-3/08.07.18/2020-21 dated July 01, 2020](https://www.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=11932) containing instructions on the facility for exchange of notes and coins. A revised version of [Master Circular](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12052&Mode=0#MC) on the subject is annexed for your information and necessary action.

**1. Facility for Exchange of Notes and Coins at Bank Branches**

**(a)** All branches of banks in all parts of the country are mandated to provide the following customer services, more actively and vigorously to the members of public so that there is no need for them to approach the RBI Regional Offices for this purpose:

1. Issuing fresh / good quality notes and coins of all denominations,
2. Exchanging soiled / mutilated / defective notes,

\*Small Finance Banks and Payment Banks may exchange mutilated and defective notes at their option.

and

1. Accepting coins and notes either for transactions or exchange.

It will be preferable to accept coins, particularly, in the denominations of ₹1 and ₹2, by weighment. However, accepting coins packed in sachets of 100 each would perhaps be more convenient for the cashiers as well as the customers. Such sachets may be kept at the counters and made available to the customers.

**(b)** All branches should provide the above facilities to members of public without any discrimination on all working days. The scheme of providing exchange facility by a few select currency chest branches on one of the Sundays in a month will remain unchanged. The names and addresses of such bank branches should be available with the respective banks.

**(c)** The availability of the above-mentioned facilities at the bank branches should be given wide publicity for information of the public at large.

**(d)** None of the bank branches should refuse to accept small denomination notes and / or coins tendered at their counters. All coins in the denomination of 50 paise, ₹1, ₹2, ₹5, ₹10 and ₹20 of various sizes, theme and design issued from time to time by the Government of India continue to be legal tender.

**2. Reserve Bank of India (Note Refund) Rules, 2009 [as Amended by Reserve Bank of India (Note Refund) Amendment Rules, 2018] - Delegation of Powers**

**(a)** In terms of Section 28 read with Section 58 (2) of Reserve Bank of India Act, 1934, no person is entitled as a right to recover from the Government of India or RBI the value of any lost, stolen, mutilated or imperfect currency note of the GOI or banknote. However, with a view to mitigating the hardship to the public in genuine cases, it has been provided that the RBI may, with the previous sanction of the Central Government, prescribe the circumstances in, and the conditions and limitations subject to which, the value of such currency notes or banknotes may be refunded as a matter of grace.

**(b)** With a view to extending the facility for the benefit and convenience of public, all branches of banks have been delegated powers under Rule 2(j) of Reserve Bank of India (Note Refund) Rules, 2009 [as Amended by Reserve Bank of India (Note Refund) Amendment Rules, 2018] (hereinafter referred to as NRR, 2009) for exchange of mutilated / defective notes free of cost.

**(c)** The NRR, 2009 were amended to enable the public to exchange mutilated notes in Mahatma Gandhi (New) series, which are smaller in size compared to the earlier series. The minimum area of the single largest undivided piece of the note required for payment of full value for notes of rupees fifty and above denominations were also revised. The Reserve Bank of India (Note Refund) Amendment Rules, 2018 have since been notified in the Gazette of India on September 6, 2018.

**3. Liberalized Definition of a Soiled Note**

In order to facilitate quicker exchange facilities, the definition of soiled note has been expanded. A ‘soiled note’ means a note which has become dirty due to normal wear and tear and also includes a two piece note pasted together wherein both the pieces presented belong to the same note and form the entire note with no essential feature missing. These notes should be accepted over bank counters in payment of Government dues and for credit to accounts of the public maintained with banks. However, in no case, these notes should be issued to the public as re-issuable notes and shall be deposited in currency chests for onward transmission to RBI offices as soiled note remittances for further processing.

**4. Mutilated Notes – Presentation and Passing**

A mutilated note is a note of which a portion is missing or which is composed of more than two pieces. Mutilated notes may be presented at any of the bank branches. The notes so presented shall be accepted, exchanged and adjudicated in accordance with [NRR, 2009](https://www.rbi.org.in/Scripts/OccasionalPublications.aspx?head=RBI%20-%20Note%20Refund%20Rules).

**5. Extremely Brittle, Burnt, Charred, Stuck-Up Notes**

Notes which have turned extremely brittle or are badly burnt, charred or inseparably stuck up together and, therefore, cannot withstand normal handling, shall not be accepted by the bank branches for exchange. Instead, the holders may be advised to tender these notes to the Issue Office of Reserve Bank of India concerned where they will be adjudicated under a Special Procedure.

**6. Procedure for Exchange of Soiled/ Mutilated/ Imperfect Notes**

**6.1 Exchange of Soiled Notes**

**6.1.1 Notes presented in small number:** Where the number of notes presented by a person is up to 20 pieces with a maximum value of ₹5,000 per day, banks should exchange them over the counter, free of charge.

**6.1.2 Notes presented in bulk:** Where the number of notes presented by a person exceeds 20 pieces or ₹5,000 in value per day, banks may accept them, against receipt, for value to be credited later. Banks may levy service charges as permitted in Master Circular on Customer Service in Banks ([DBR.No.Leg.BC.21/09.07.006/2015-16 dated July 1, 2015](https://rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9862)). In case tendered value is above ₹50,000, banks are expected to take the usual precautions.

**6.2 Exchange of Mutilated and Imperfect Notes**

**6.2.1** While designated branches may continue to follow the procedure as laid down in Part III of NRR, 2009 ([www.rbi.org.in](https://www.rbi.org.in/)→Publications→Occassional) for exchanging mutilated and imperfect notes and issue receipt for the notes presented for adjudication, non-chest branches are required to follow the following procedure for notes presented in small numbers and in bulk.

**6.2.2 Notes presented in small number:** Where the number of notes presented by a person is up to 5 pieces, non-chest branches should normally adjudicate the notes as per the procedure laid down in Part III of NRR, 2009 and pay the exchange value over the counter. If the non-chest branches are not able to adjudicate the mutilated notes, the notes may be received against a receipt and sent to the linked currency chest branch for adjudication. The probable date of payment should be informed to the tenderers on the receipt itself and the same should not exceed 30 days. Bank account details should be obtained from the tenderers for crediting the exchange value by electronic means.

**6.2.3 Notes presented in bulk:** Where the number of notes presented by a person is more than 5 pieces not exceeding ₹5,000 in value, the tenderer should be advised to send such notes to nearby currency chest branch by insured post giving his / her bank account details (a/c no, branch name, IFSC, etc.) or get them exchanged thereat in person. All other persons tendering mutilated notes whose value exceeds ₹5,000 should be advised to approach nearby currency chest branch. Currency chest branches receiving mutilated notes through insured post should credit the exchange value to the account of sender by electronic means within 30 days of receipt of notes.

**6.3** Tenderers aggrieved with the service provided by the banks in this regard may approach Banking Ombudsman concerned, following the procedure as laid under Banking Ombudsman Scheme, 2006 with the bank/ postal receipts as proof for necessary action.

**7. Notes Bearing "PAY" / "PAID" / "REJECT" Stamps**

**(a)** Every Officer-in-charge of the branch i.e. the Branch Manager and every Officer-in-charge of the Accounts or Cash Wing of the Branch shall act as 'Prescribed Officer' in each branch to adjudicate the notes received at the branch for exchange in accordance with NRR, 2009. After adjudicating mutilated notes, the Prescribed Officer is required to record his order by subscribing his initials to the dated 'PAY'/ 'PAID'/ 'REJECT' stamp. The 'PAY' /'PAID' & 'REJECT' stamps should also carry the name of the bank and branch concerned and held under the custody of the 'Prescribed Officer' to avoid misuse.

**(b)** Mutilated / defective notes bearing 'PAY'/'PAID' (or 'REJECT') stamp of any RBI Issue Office or any bank branch, if presented for payment again at any of the bank branches should be rejected under Rule 6(2) of NRR, 2009 and the tenderer should be advised that the value of such note/s cannot be paid since the same has already been paid as is evident from the PAY/ PAID stamps affixed on it/ them. All bank branches have instructions not to issue notes bearing PAY/ PAID stamps to the public even through oversight. The branches should caution their customers not to accept such notes from any bank or anybody else.

**8. Notes with Slogans/ Scribbling/ Stain etc.**

**(a)** Notes with slogans, political or religious messages, scribbling, stain (including colour stain) etc. are unfit for usage and circulation and go against Clean Note Policy of RBI.

**(b)** Such notes received from members of public may not be reissued for circulation. They may be remitted to currency chest for onward remittance to RBI offices.

**(c)** Any note with slogans and message of a political or religious nature written across it ceases to be a legal tender and the claim on such a note will be rejected under Rule 6(3) (iii) of NRR, 2009. Similarly, notes which are disfigured may also be rejected under Rule 6(3) (ii) of [NRR, 2009](https://www.rbi.org.in/Scripts/OccasionalPublications.aspx?head=RBI%20-%20Note%20Refund%20Rules).

**(d)** All Bank notes with scribbling / stain (including colour stain) on them continue to be legal tender. Such notes can be deposited or exchanged in any bank branch.

**9. Deliberately Cut Notes**

The notes, which are found to be deliberately cut, torn, altered or tampered with, if presented for payment of exchange value should be rejected under Rule 6(3) (ii) of the NRR, 2009. Although it is not possible to precisely define deliberately cut notes, a close look at such notes will clearly reveal any deliberate fraudulent intention, as the manner in which such notes are mutilated will follow a broad uniformity in the shape/ location of missing portions of the notes, especially when the notes are tendered in large numbers. The details of the case such as the name of the tenderer, the number of notes tendered and their denominations should be reported thereafter to the DGM/ GM, Issue Department, Reserve Bank of India under whose jurisdiction the branch falls. The matter should also be reported to local police in case a large number of such notes are tendered.

**10. Training**

RBI Issue Offices conduct training programmes for 'Prescribed Officers' of bank branches on a priority basis. As the training programmes are intended to provide knowledge and instil confidence in the Prescribed Officers in the process of adjudication of defective notes, it is imperative that the Prescribed Officers of the branches are deputed for such programmes.

**11. Display of Notice Board**

All bank branches are required to display at their branch premises, at a prominent place, a board indicating the availability of note and coin exchange facility with the legend, "SOILED/ MUTILATED NOTES AND COINS ARE ACCEPTED AND EXCHANGED HERE" for information of general public. Banks should ensure that all their branches provide facility for exchange of notes and coins not only to their customers but also others. However, they should ensure that the note exchange facility is not cornered by money changers / dealers in defective notes.

**12. Disposal of Notes Adjudicated at Bank Branches**

Regarding audit of the notes adjudicated by bank branches, the full value paid notes have to be remitted by all branches to the chest branches with which they have been linked and therefrom to the RBI Issue Offices concerned together with the next soiled note remittance in the manner already laid down. The half value paid notes and rejected notes, which are held by the chest branches in their cash balance, may either be remitted separately packed together with the full value paid notes or sent by registered and insured post as and when required. The full value paid notes will be treated as chest remittance by the RBI Issue Office while the half value paid notes and rejected notes will be treated as notes tendered for adjudication and processed accordingly. All chest branches are required to submit to our RBI Issue Offices a monthly statement showing the number of notes adjudicated during the month.

**13. Uncurrent Coins**

The coins of 25 paise and below, issued from time to time, ceased to be legal tender for payments as well as account with effect from June 30, 2011 in terms of Gazette Notification No. 2529 dated December 20, 2010 issued by the Government of India.

**14. Monitoring and Control**

**(a)** The Regional Managers / Zonal Managers of the banks may pay surprise visits to the branches and report the position of compliance in this regard to the Head Office which will review such reports and take prompt remedial action, wherever necessary.

**(b)** Any non-compliance in this regard shall be viewed as violation of instructions issued by the Reserve Bank of India.

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12052&Mode=0>

**11. Framework for processing of e-mandates for recurring online transactions**

**RBI/2020-21/118 CO.DPSS.POLC.No.S34/02-14-003/2020-2021 March 31, 2021**

*The Chairman / Managing Director / Chief Executive Officer, All Scheduled Commercial Banks, including Regional Rural Banks /Urban Co-operative Banks / State Co-operative Banks /District Central Co-operative Banks / Payments Banks /Small Finance Banks / Local Area Banks / Card Payment Networks /Non-bank Prepaid Payment Instrument Issuers /National Payments Corporation of India*

A reference is invited to our [circulars DPSS.CO.PD.No.447/02.14.003/2019-20 dated August 21, 2019](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11668&Mode=0), [DPSS.CO.PD.No.1324/02.23.001/2019-20 dated January 10, 2020](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11784&Mode=0) and [DPSS.CO.PD.No.754/02.14.003/2020-21 dated December 4, 2020](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12002&Mode=0), wherein the framework for registering e-mandates for recurring online transactions using cards / wallets / Unified Payments Interface was put in place. The framework had ensured that changing payment needs of customers were accommodated by adequately balancing safety, security and convenience of such transactions. Stakeholders were given sufficient time to complete the process of migration to the framework by March 31, 2021.

2. It is, however, noted that the progress of onboarding existing as well as new mandates of customers as per the framework is not satisfactory. Keeping in view the requests of some stakeholders and to prevent any inconvenience to customers, it has been decided, as a one-time measure, to extend the timeline for ensuring full compliance to the framework till September 30, 2021. During the extended timeline, no new mandate for recurring online transactions shall be registered by stakeholders, unless such mandates are compliant with the framework.

3. Any further delay in ensuring complete adherence to the framework beyond the extended timeline will attract stringent supervisory action.

4. This directive is issued under Section 10(2) read with Section 18 of the Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

**12. Guidelines on Regulation of Payment Aggregators and Payment Gateways**

**RBI/2020-21/117 CO.DPSS.POLC.No.S33/02-14-008/2020-2021 March 31, 2021**

*All Payment System Providers and Payment System Participants*

We invite a reference to our [circular DPSS.CO.PD.No.1810/02.14.008/2019-20 dated March 17, 2020](https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0) (as updated from time to time) and the clarification dated September 17, 2020 issued on the subject ([Annex](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12050&Mode=0#ANN1)). Accordingly, neither the authorised Payment Aggregators (PAs) nor the merchants on-boarded by them can store customer card credentials within their database or server.

2. Based on the representations received from the industry seeking additional time for implementing the above instructions, it has been decided, as a one-time measure, to extend the timeline for non-bank PAs by six months, i.e., till December 31, 2021, to enable the payment system providers and participants to put in place workable solutions, such as tokenisation, within the framework set out in the [circular dated March 17, 2020](https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0) cited above and our [circular DPSS.CO.PD No.1463/02.14.003/2018-19 dated January 08, 2019](https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11449&Mode=0) on “Tokenisation – Card transactions”. All other provisions of the [circular dated March 17, 2020](https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0) referred to above, shall remain unchanged.

3. This directive is issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

**Annex**

**RBI circular CO.DPSS.POLC.No.S33/02-14-008/2020-2021 dated March 31, 2021**

**Clarification issued by RBI on**[**circular DPSS.CO.PD.No.1810/02.14.008/2019-20 dated March 17, 2020**](https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0)**(as updated from time to time) on “Guidelines on Regulation of Payment Aggregators (PAs) and Payment Gateways (PGs)”**

**1. Definition and applicability related**

1.1. The circular is applicable to online PAs and PGs. The guidelines seek to regulate the activities of online PAs while providing baseline technology-related recommendations to PGs.

1.2. In the case of bank PAs, there is no requirement of authorisation; they shall ensure compliance with the guidelines by September 30, 2020 (as extended vide [circular DPSS.CO.PD.No.1897/02.14.003/2019-20 dated June 04, 2020](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11910&Mode=0)). For non-bank PAs, the instructions will come into force from the date of their authorisation, subject to the submission of application for authorisation before the end date of June 30, 2021.

1.3. The circular is also applicable to e-commerce marketplaces that are undertaking direct payment aggregation; e-commerce marketplaces availing the services of a PA shall be considered as merchants.

1.4. The circular is not applicable on ‘Delivery vs. Payment’ transactions but addresses the transactions where the payment is made in advance while the goods are delivered in a deferred manner.

**2. Authorisation, capital and net-worth related**

2.1. Banks maintaining the escrow account/s need not monitor the net-worth of the PA.

2.2. For existing non-bank PAs, the CA certificate of net-worth evidencing that the requirement of net-worth is ensured (as on March 31, 2021) will be required to be submitted to RBI at the time of application for authorisation (in case of an existing entity desirous of applying before March 31, 2021 a similar certificate shall be submitted as on the nearest half-year ending date). Newly incorporated non-bank entities which may not have an audited statement of financial accounts shall submit a certificate from their CA regarding the current net-worth along with provisional balance sheet.

**3. Governance related**

3.1. The Promoters / Promoter Groups, shall conform to the Reserve Bank’s ‘fit and proper’ criteria. Director of the PA company shall be deemed to be a “fit and proper” person if:

3.1.1. Such person has a record of fairness and integrity, including but not limited to:

1. financial integrity;
2. good reputation and character; and
3. honesty;

3.1.2. Such person has not incurred any of the following disqualifications:

1. Convicted by a court for any offence involving moral turpitude or any economic offence or any offence under the laws administered by the RBI;
2. Declared insolvent and not discharged;
3. An order, restraining, prohibiting or debarring the person from accessing / dealing in any financial system, passed by any regulatory authority, and the period specified in the order has not elapsed;
4. Found to be of unsound mind by a court of competent jurisdiction and the finding is in force; and
5. Is financially not sound.

3.1.3. If any question arises as to whether a person is a fit and proper person, the RBI’s decision on such question shall be final.

3.2. Para 5.4 related to disclosure of comprehensive information regarding merchant policies, customer grievances, privacy policy and other terms and conditions on the website and / or their mobile application, refers to policies of the PA and not of individual merchants on-boarded by it.

**4. KYC and merchant on-boarding related**

4.1. In case a PA is maintaining an account-based relationship with the merchant, the KYC guidelines of Department of Regulation (DoR), RBI is applicable. Thus, to this extent, para 6 on ‘Safeguards against Money Laundering (KYC / AML / CFT) Provisions’ shall also be applicable.

4.2. For merchant on-boarding, the PA can have a Board approved policy (Para 7.1). There would not be a requirement to carry-out entire process of KYC (in accordance with the KYC guidelines of DoR), in cases where the merchant already has a bank account which is being used for transaction settlement purpose.

**5. OPGSP related**

5.1. Entities functioning as OPGSP and undertaking cross-border transactions in terms of OPGSP guidelines shall ensure compliance with the instructions issued vide [A.P. (DIR Series) Circular No.16 dated September 24, 2015](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10037&Mode=0).

5.2. If OPGSP is also an entity which is functioning as PG or PA under the guidelines stipulated by DPSS, for undertaking any domestic leg of import / export transaction, it has to be ensured that the timelines and other guidelines, including those relating to authorised modes of collection, i.e. debit card, credit card and internet banking, indicated for the purpose of cross-border transactions in [A.P. (DIR Series) Circular No.16 dated September 24, 2015](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10037&Mode=0), are also adhered to.

**6. Security, fraud prevention and risk management framework related**

6.1. The PA needs to ensure compliance of the infrastructure of the merchants to security standards like PCI-DSS and PA-DSS, as applicable.

6.2. Merchants are not allowed to store payment data irrespective of their being PCI-DSS compliant or otherwise. They shall, however, be allowed to store limited data for the purpose of transaction tracking; for which, the required limited information may be stored in compliance with the applicable standards.

6.3. The PA cannot also store customer card credentials within its database or the server (irrespective of it being accessed by merchant or not) except for the limited purpose of transaction tracking; for which, required credentials may be stored in compliance with the applicable standards.

6.4. Para 10.5: A standard system audit, including cyber security audit, conducted by CERT-In empanelled auditors may be carried out.

**7. Settlement and escrow account related**

7.1. For the purpose of maintenance of the escrow account, the operations of PAs are deemed to be ‘designated payment systems’ under the Payment and Settlement Systems Act (PSS Act) after the entity obtains authorisation from RBI.

7.2. The applicability of [circular DPSS.CO.PD.No.1102/02.14.08/2009-10 dated November 24, 2009](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=5379&Mode=0) on “Directions for opening and operation of Accounts and settlement of payments for electronic payment transactions involving intermediaries” shall be as follows:

7.2.1. The circular shall be considered repealed for authorised PAs from the date of authorisation;

7.2.2. The circular shall be considered repealed with effect from June 30, 2021 except for such PAs who have applied for authorisation and a decision on it is pending with RBI.

7.3. The existing entities can continue to maintain nodal accounts till they have been authorised by RBI. Since the PA needs to move towards an escrow account, the bank and the PA may take a call about maintaining the same from an earlier date as well. However, this alone shall not make them eligible for a “designated payment system” status under Section 23A of the PSS Act.

7.4. If the bank can satisfactorily establish that the nodal account of an entity has been migrated to escrow account in compliance with the new instructions, it can allow the balances under existing nodal accounts of PAs to be considered for calculation of ‘Core portion’.

7.5. Those entities who have not attained the requisite net-worth as of March 31, 2021 shall wind up their PA business. Banks shall be required to close such nodal accounts after June 30, 2021 unless the PA produces evidence to the bank regarding application for authorisation being made to RBI.

7.6. The pre-funding has been allowed to tide over temporary mis-matches. Taking back of surplus pre-funding is not allowed.

7.7. There can be different “t” for different merchants as per the agreement between PA and merchants.

7.8. Para 8.6: The amount due to the merchant will be reckoned only after the settlement and credit to the escrow account. There is no need to prefund the account for this purpose. However, the proceeds shall be credited to escrow on the settlement day itself.

7.9. Where PAs have no control over incoming funds and its delay thereof, the PAs need to follow the instructions and transfer the funds to the merchant within T+0 / T+1 basis, post receiving of funds into its account.

7.10. The settlement accounts opened under Bharat Bill Payment System (BBPS) would be governed by BBPS instructions.

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12050&Mode=0>

**13. Extension of Cheque Truncation System (CTS) across all bank branches in the country**

**RBI/2020-21/107 DPSS.CO.RPPD.No.SUO 21102/04.07.005/2020-21 March 15, 2021**

*The Chairman and Managing Director / Chief Executive Officer, All Scheduled Commercial Banks including Regional Rural Banks / Urban Co-operative Banks / State Co-operative Banks /District Central Co-operative Banks / Local Area Banks / Payment Banks / Small Finance Banks / National Payments Corporation of India*

Please refer to the [Statement on Developmental and Regulatory Policies dated February 5, 2021](https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=51078) wherein Reserve Bank of India (RBI) had announced pan-India coverage of CTS by bringing all branches of banks in the country under image-based CTS clearing mechanism.

2. The CTS is in use since 2010 and presently covers around 1,50,000 branches. All the erstwhile 1219 non-CTS clearing houses (ECCS centres) have been migrated to CTS effective September 2020. It is, however, seen that there are branches of banks that are outside any formal clearing arrangement and their customers face hardships due to longer time taken and cost involved in collection of cheques presented by them.

3. To leverage the availability of CTS and provide uniform customer experience irrespective of location of her/his bank branch, it has been decided to extend CTS across all bank branches in the country. To facilitate this, banks shall have to ensure that all their branches participate in image-based CTS under respective grids by September 30, 2021. They are free to adopt a model of their choice, like deploying suitable infrastructure in every branch or following a hub & spoke model, etc. and concerned banks shall coordinate with the respective Regional Offices of RBI to operationalise this.

4. Banks are advised to inform us (helpdpss@rbi.org.in) the roadmap to achieve pan-India coverage of CTS and submit a status report before April 30, 2021.

5. This directive is issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

**14. Master Direction on Digital Payment Security Controls**

**RBI/2020-21/74 DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21 February 18, 2021**

*The Chairman/ Managing Director/ Chief Executive Officer, All Scheduled Commercial Banks excluding RRBs/Small Finance Banks/Payments Banks/ Credit Card issuing NBFCs.*

Please refer to para II (7) of the Statement on Developmental and Regulatory Policies of the Bi-monthly Monetary Policy Statement for 2020-21 dated December 4, 2020 ([extract given below](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0#S1)). The [Master Direction](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0#MD) provides necessary guidelines for the regulated entities to set up a robust governance structure and implement common minimum standards of security controls for digital payment products and services.

Going by the pre-eminent role being played by digital payment systems in India, RBI gives highest importance to the security controls around it. Now it is proposed to issue Reserve Bank of India (Digital Payment Security Controls) Directions 2020, for regulated entities to set up a robust governance structure for such systems and implement common minimum standards of security controls for channels like internet, mobile banking, card payments, among others. While the guidelines will be technology and platform agnostic, it will create an enhanced and enabling environment for customers to use digital payment products in more safe and secure manner. Necessary guidelines will be issued separately.

**INTRODUCTION**

In exercise of the powers conferred by the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934 and Payment and Settlement Systems Act, 2007, the Reserve Bank, being satisfied that it is necessary and expedient in the public interest so to do, hereby, issues the directions hereinafter specified.

**CHAPTER – I**

**PRELIMINARY**

**1. Short Title and Commencement**

1. These directions shall be called the Reserve Bank of India (Digital Payment Security Controls) directions, 2021.
2. These directions shall come into effect six months from the day they are placed on the official website of the Reserve Bank of India (RBI). However, in respect of instructions already issued either by Department of Payment and Settlement Systems (DPSS), Department of Regulation (DoR) or Department of Supervision (DoS) of RBI including those to select Regulated Entities (REs), by way of circular or advisory, the timeline would be with immediate effect or as per the timelines already prescribed.

**2. Applicability**

The provisions of these directions shall apply to the following Regulated Entities (REs):

1. Scheduled Commercial Banks (excluding Regional Rural Banks);
2. Small Finance Banks;
3. Payments Banks; and
4. Credit card issuing NBFCs.

**3. Definitions**

All expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, Reserve Bank of India Act, 1934, Payment and Settlement Systems Act, 2007 or Information Technology Act, 2000/ Information Technology (Amendment) Act, 2008 and Rules made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

**CHAPTER – II**

**GENERAL CONTROLS**

**Governance and Management of Security Risks**

4. REs shall formulate a policy for digital payment products and services with the approval of their 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, customer experience, etc., should explicitly discuss about 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 e.g. human resources, technology, etc. with necessary back up;
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.

The Board and Senior Management shall be responsible for implementation of this policy. The policy shall be reviewed periodically, at least on a yearly basis. REs may formulate this policy separately for its different digital products or include the same as part of their overall product policy. Further, the policy document should require that every digital payment product/ services 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 and exception handling. In addition, 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 UAT) and data archival requirements shall also be taken in to account. 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 should be clearly articulated.

5. REs shall incorporate appropriate processes into their 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. The Board/ Senior Management of REs shall have appropriate performance monitoring systems/ key performance indicators for assessing whether the product or service offered through digital payment channels meet operational and security norms.

6. As part of this process, the REs shall define product-level limits on the level of acceptable security risk, document specific security objectives and performance criteria including quantitative benchmarks for evaluating the success of the security built into the digital payment product or service, periodically compare actual results with projections and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner and modify the business plan/ strategy involving the product, when appropriate, based on the security performance of the product or service.

7. REs shall have trained resources with necessary expertise to manage the digital payment infrastructure. Wherever the REs are dependent on third party service providers, adequate oversight and controls for monitoring the activities of the third party personnel, in line with RBI guidelines on outsourcing, shall be put in place.

8. REs shall conduct risk assessments with regard to the safety and security of digital payment products and associated processes and services as well as suitability and appropriateness of the same vis-a-vis the target users, both prior to establishing the service(s) and regularly thereafter. The risk assessment should take into account –

1. The technology stack and solutions used;
2. Known vulnerabilities at each of the touchpoints of the digital product and the remedial action taken by the entity;
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 RE, including core systems and systems of payment systems operators, etc.;
5. The customer experience, convenience and technology adoption required to use such products;
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 cyber security requirements; and
12. Compatibility aspects.

Such assessment shall cover the surrounding ecosystem as well. The assessment of risks shall address the need to protect and secure payment data[1](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0#F1) and evaluate the resilience of systems. The internal Risk and Control Self-Assessment (RCSA) exercise shall cover the risks (inherent) & controls vis-à-vis the probability and impact of threats to arrive at residual risk. In such an exercise, it is imperative for REs to maintain database of all systems and applications storing customer data in the payment ecosystem and compliance with applicable PCI standards in each of the systems (notwithstanding mandatory requirements of certification/ standard accreditation).

9. REs shall evaluate the risks associated with the chosen technology platforms, application architecture, both on the server and client side. Further, REs should undertake a review of the risk scenarios and existing security measures based on incidents affecting their services, before any major change to the infrastructure or procedures is made or, when, any new threats are identified through risk monitoring activities. Further, unused or unwanted features of the platform should be closely controlled to minimise risk.

10. REs shall develop sound internal control systems and take into account the operational risk before offering digital payment products and related services. This would include ensuring that adequate safeguards are in place to protect integrity of data, customer confidentiality and security of data.

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

12. REs shall have necessary capacity, systems and procedures in place to periodically test the backed-up data, application pertaining to digital products to ensure recovery without loss of transactions or audit-trails. These facilities should be tested at least on a half-yearly basis for digital payment products and services.

**Other Generic Security Controls**

13. 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.

14. Web applications providing the digital payment products and services should not store sensitive information in HTML hidden fields, cookies, or any other client-side storage to avoid any compromise in the integrity of the data.

15. REs shall implement Web Application Firewall (WAF) solution and DDoS mitigation techniques to secure the digital payment products and services offered over Internet.

16. 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, authentication purpose, shall be strong, adopting internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable and the configurations involved in implementing such controls are in general, compliant with extant instructions and the law of the land.

17. REs shall renew their digital certificates used in digital payment ecosystem well in time.

18. The mobile application[2](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0#F2) and internet banking application should have effective logging and monitoring capabilities to track user activity, security changes and identify anomalous behaviour and transactions.

**Application Security Life Cycle (ASLC)**

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

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

21. REs shall explicitly define security objectives (including protection of customer information/ data) during (a) requirements gathering, (b) designing, (c) development, (d) testing including source code review, (e) implementation, maintenance & monitoring and (f) decommissioning phases of the digital payment applications.

22. REs (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 their policies, processes, guidelines and procedures.

23. For digital payment applications that are licensed by a third party vendor, REs shall have an escrow arrangement for the source code for ensuring continuity of services in case the vendor defaults or is unable to provide services.

24. REs shall conduct security testing including review of source code, Vulnerability Assessment (VA) and Penetration Testing (PT) of their 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 should invariably cover compliance with various standards like OWASP. If the source code is not owned by the RE, then, in such cases, the RE shall obtain a certificate from the application developer stating that the application is free of known vulnerabilities, malwares and any covert channels in the code.

In this context,

1. The VA shall be conducted at least on a half-yearly basis; PT shall be conducted at least on a yearly basis. 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 application or infrastructure;
2. Testing related to review of source code/ certification shall be conducted/ obtained. This shall continue on a yearly basis, if changes/ upgrades have been made to the application during the year;
3. Testing/ Certification should broadly address the objective that the product/ version/module(s) functions only in a manner that it is intended to do, is developed as per the best secure design/ coding practices and standards, addressing known flaws/threats due to insecure coding; and
4. Penal provisions shall be included by the RE into third-party contractual arrangements for any non-compliance by the application provider.

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

26. REs 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 should be fixed in a time-bound manner.

27. REs shall ensure that all 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.[3](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0#F3)

28. REs 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 its launch/ moving to the production environment.

29. REs shall institute a mechanism to actively monitor for the non-genuine/ unauthorised/ malicious applications (with similar name/ features) on popular app-stores and the Web and respond accordingly to bring them down.

30. The server at the RE’s end should 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.

31. The security controls for digital payment applications must focus on how these applications handle, store and protect payment data. The APIs for secure data storage and communication have to be implemented and used correctly in order to be effective. REs shall refer to standards such as OWASP-MASVS, OWASP-ASVS and other relevant OWASP standards, security and data protection guidelines in ISO 12812, threat catalogues and guides developed by NIST (including for Bluetooth and LTE security), for application security and other protection measures. Such testing has to necessarily verify for vulnerabilities including, but not limited to OWASP/ OWASP Mobile Top 10, application security guidelines/ requirements developed/ shared by operating system providers/ OEMs.

32. REs shall redact/ mask customer information such as account numbers/ card numbers/ other sensitive information when transmitted via SMS/ e-mails.

**Authentication Framework**

33. In view of the proliferation of cyber-attacks and their potential consequences, REs should 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 should be generally dynamic or non-replicable. [e.g., Use of One Time Password, mobile devices (device binding and SIM), biometric/ PKI/ hardware tokens, EMV chip card (for Card Present Transactions) with server-side verification could be termed either in dynamic or non-replicable methodologies.].

34. REs may also adopt adaptive authentication to select the right authentication factors depending on risk assessment, user risk profile and behaviour. Properly designed and implemented multi-factor authentication methods are more reliable and stronger fraud deterrents and are more difficult to compromise. The key objectives of multi-factor authentication are to protect the confidentiality of payment data as well as enhance confidence in digital payment by combating various cyber-attack mechanisms like phishing, keylogging, spyware/ malware and other internet-based frauds targeted at REs and their customers. In this regard,

1. The implementation of appropriate authentication methodologies should be based on an assessment of the risk posed by the RE’s digital payment products and services. The risk should 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.
2. Beyond the technology factor, the success of a particular authentication method depends on appropriate policies, procedures, and controls. An effective authentication method should take into consideration customer acceptance, ease of use, reliable performance, scalability to accommodate growth, customer profile, location, transaction, etc., and interoperability with other systems.
3. To enhance online processing security, multi factor authentication and alerts (like SMS, e-mail, etc.) should be applied in respect of all payment transactions (including debits and credits), creation of new account linkages (addition/ modification/ deletion of beneficiaries), changing account details or revision to fund transfer limits. In devising these security features, REs should take into account their efficacy and differing customer preferences for additional online protection.
4. 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.
5. As an integral part of the multi factor authentication architecture, REs should also implement appropriate measures to minimise exposure to a 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. This is to ensure, among other things, that the data in transit is secured and the transactions are authenticated only by genuine/ authorised source/ process.
6. An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. Else, in the event of interference or in case the customer closes the application, the session should be terminated, and the affected transactions resolved or reversed out. The customer should be promptly notified about the status of the transaction by email, SMS or through other means.

35. REs should set down the maximum number of failed log-in or authentication attempts after which access to the digital payment product/ service is blocked. They should have a secure procedure in place to re-activate the access to blocked product/ service. The customer shall be notified for failed log-in or authentication attempts.

**Fraud Risk Management**

36. The REs shall document and implement the configuration aspects for identifying suspicious transactional behaviour in respect of rules, preventive, detective types of controls, mechanism to alert the customers in case of failed authentication, time frame for the same, etc.

37. System alerts shall be parameterised and monitored in terms of various applicable parameters. Such parameters, as applicable could be: transaction velocity (e.g., fund transfers, cash withdrawals, payments through electronic modes, adding new beneficiaries, etc.) in a short period, more so in the accounts of customers who’ve never used mobile app/ internet banking/ card ever (depending upon the type of payment channel), high risk merchant category codes (MCC) parameters, counterfeit card parameters (String of Invalid 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/ VPAs on whom vishing fraud or other types of fraud is/are registered/ recorded, declined transactions, transactions with no approval code, etc.

38. Fraud analysis shall be conducted to identify the reason for fraud occurrence and determine mechanism to prevent such frauds.

39. The staff, especially in the fraud control function, shall be educated about frauds and trained 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 and 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.

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

**Reconciliation Mechanism**

41. 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 RE 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, other participants, etc., shall be put in place for better detection and prevention of suspicious transactions. A mechanism shall be introduced to monitor the implementation and effectiveness of such framework.

**Customer Protection, Awareness and Grievance Redressal Mechanism**

42. REs shall incorporate secure, safe and responsible usage guidelines and training materials for end users within the digital payment applications. They shall also make it mandatory (i.e. not providing any option to circumvent/ avoid the material) for the consumer to go through secure usage guidelines (even in the consumer’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.

43. REs shall mention/ incorporate a section on the digital payment application clearly specifying the process and procedure (with forms/ contact information, etc.) to lodge consumer grievances. A mechanism to keep this information periodically updated shall also be put in place. 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 RE's response should be clearly defined.

44. REs shall adhere to extant instructions[4](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0#F4), updated from time to time, to put in place system/s for online dispute resolution for resolving disputes and grievances of customers pertaining to digital payments.

45. REs shall educate customers about the need to maintain the physical and logical security of their devices accessing digital payment products and services including recommending secure/ regular installation of operating system and application updates, downloading applications only from authorised sources, having anti-malware/ anti-virus applications on devices, etc.

46. REs shall ensure that its customers are provided information about the risks, benefits and liabilities of using digital payment products and its related services before they subscribe to them. Customers shall also be informed 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 are to be offered on express willingness of customers and shall not be bundled without their knowledge.

47. Whenever new operating features or functions, particularly those relating to security, integrity and authentication, are introduced to online delivery channels, clear and effective communication followed by sufficient instructions to properly utilise such new features should be provided to the customers.

48. REs may continuously create public awareness on the types of threats and attacks used against the consumers while using digital payment products and precautionary measures to safeguard against the same. Customers shall be cautioned against commonly known threats in recent times like phishing, vishing, reverse-phishing, remote access of mobile devices and educated to secure and safeguard their account details, credentials, PIN, card details, devices, etc.

49. REs shall provide digital payment products and services, to a customer only at her/ his option based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions.

50. REs should provide a mechanism on their mobile and internet banking application for their customers to, with necessary authentication, identify/ mark a transaction as fraudulent for seamless and immediate notification to his RE. On such notification by the customer, the REs may endeavour to build the capability for seamless/ instant reporting of fraudulent transactions to the corresponding beneficiary/ counterparty’s RE; vice-versa have mechanism to receive such fraudulent transactions reported from other REs. The objective of this mechanism is to accelerate early detection and enable the banking/ payment system to trace the transaction trail and mitigate the loss to the defrauded customer at the earliest possible time.

**Chapter III**

**INTERNET BANKING SECURITY CONTROLS**

In addition to the controls prescribed in [Chapter II](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0#6), the following instructions are applicable to REs offering/ intending to offer internet banking facility to their customers:

51. Internet banking websites are vulnerable to authentication related brute force attacks/ application layer Denial of Service (DoS) attacks. Based on the RE’s individual risk/ vulnerability assessment on authentication-related attacks such as brute force/ DoS attacks, REs shall implement additional levels of authentication to internet banking website such as adaptive authentication, strong CAPTCHA (preferably with anti-bot features) with server-side validation, etc., in order to plug this vulnerability and prevent its exploitation. Appropriate measures shall be taken to prevent DNS cache poisoning attacks and for secure handling of cookies. Virtual keyboard option should be made available.

52. An online session shall be automatically terminated after a fixed period of inactivity.

53. Secure delivery of password for login purpose shall be ensured. The password generated and dispatched by the RE should be valid for a limited period from the date of its creation. If the password is generated and dispatched by the RE, then, the user shall be compulsorily required to change the password, on the first login.

54. When the internet banking application is accessed through external websites (eg: in case of payment of taxes, e-commerce transactions, etc.), the procedure for authentication and the appearance/ look and feel of the RE’s internet banking site should be made uniform as far as possible.

**Chapter IV**

**MOBILE PAYMENTS APPLICATION SECURITY CONTROLS**

In addition to the controls prescribed in [Chapter II](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0#6), the following instructions are applicable to the REs offering/ intending to offer mobile banking/ mobile payments facility to their customers through mobile application:

55. 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. REs shall be able to verify the version of the mobile application before the transactions are enabled.

56. Specific Controls for mobile applications include:

1. Device policy enforcement (allowing app installation/ execution after baseline requirements are met);
2. Application secure download/ install;
3. 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;
4. Storage of customer data;
5. Device or application encryption;
6. Ensuring minimal data collection/ app permissions;
7. Application sandbox/ containerisation;
8. Ability to identify remote access applications (to the extent possible) and prohibit login access to the mobile application, as a matter of precaution; and
9. Code obfuscation.

57. REs may consider to 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.

58. REs 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.

59. Checksum of current active version of application shall be hosted on public platform so that users can verify the same.

60. REs shall ensure device binding of mobile application[5](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0#F5).

61. Considering that the additional factor of authentication and mobile application may reside on the same mobile device in the case of mobile banking, mobile payments, REs may consider implementing alternatives to SMS-based OTP authentication mechanisms.

62. The mobile application should require re-authentication whenever the device or application remains unused for a designated period and each time the user launches the application. Applications must be able to identify new network connections or connections from unsecured networks like unsecured Wi-Fi connections and must implement appropriate authentication/ checks/ measures to perform transactions under those circumstances.

63. The mobile application should not store/ retain sensitive personal/ consumer authentication information such as user IDs, passwords, keys, hashes, hard coded references on the device and the application should securely wipe any sensitive customer information from memory when the customer/ user exits the application.

64. REs shall ensure that their mobile application limit the writing of sensitive information into ‘temp’ files. The sensitive information written in such files must be suitably encrypted/ masked/ hashed and stored securely.

65. REs may consider designing anti-malware capabilities into their mobile applications.

66. REs shall ensure that the usage of raw (visible) SQL queries in mobile applications to fetch or update data from databases is avoided. Mobile applications should be secured from SQL injection type of vulnerabilities. Sensitive information should be written to the database in an encrypted form. Web content, as part of the mobile application’s layout, should not be loaded if errors are detected during SSL/ TLS negotiation. Certificate errors on account of the certificate not being signed by a recognised certificate authority; expiry/ revocation of the certificate must be displayed to the user.

**Chapter V**

**CARD PAYMENTS SECURITY**

In addition to the controls prescribed in [Chapter II](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0#6), the following instructions are applicable to the REs offering/ intending to issue cards (credit/ debit/ prepaid) (physical or virtual) to their customers:

67. REs shall follow various payment card standards (over and above PCI-DSS and PA-DSS[6](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0#F6)) as per Payment Card Industry (PCI) prescriptions for comprehensive payment card security as per applicability/ readiness of updated versions of the standards such as –

1. PCI-PIN (secure management, processing, and transmission of personal identification number (PIN) data);
2. PCI-PTS (security approval framework addresses the logical and/ or physical protection of cardholder and other sensitive data at point of interaction (POI) devices and hardware security modules (HSMs);
3. PCI-HSM (securing cardholder-authentication applications and processes including key generation, key injection, PIN verification, secure encryption algorithm, etc.); and
4. 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).

68. REs should ensure that 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; 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.

69. Acquirers shall secure their card payment infrastructure (Unique Key Per Terminal – UKPT or Derived Unique Key Per Transaction – DUKPT/ Terminal Line Encryption – TLE).

70. The security controls to be implemented at HSM are:

1. The HSMs should have logging enabled, the logs must themselves be tamper proof;
2. HSM can become a single point of failure. This needs to be mitigated by ‘clustering’ for high availability and ensure secure backups;
3. Access to the HSM should be controlled through Access Control Lists (ACLs);
4. Separate ACLs should be maintained for each individual application to ensure application level isolation;
5. All access to HSM should be managed and monitored using a robust Privileged Identity and Access Management solution;
6. Decryption and validation of keys, PIN should be done at HSM;
7. Card PIN generation and printing should be directly at system connected HSM;
8. CVV generation and validation should be done at HSM;
9. Ensure HSM is implemented with secure PIN block format with controls to disable outputting PIN block in weaker format;
10. Secure key management for HSMs (such as LMKs, etc.); and
11. Security of the physical keys of the HSM device should be properly maintained.

71. REs shall implement the following for improving the security posture of the ATM:

1. Implement security measures such as BIOS password, disabling USB ports, disabling auto-run facility, applying the latest patches of operating system and other softwares, terminal security solution, time-based admin access, etc;
2. Implement anti-skimming and whitelisting solution; and
3. Upgrade all the ATMs with supported versions of operating system. Use of ATMs that have unsupported operating systems shall be prohibited.

72. REs shall ensure robust surveillance/ monitoring of card transactions (especially overseas cash withdrawals) and setting up of rules and limits commensurate with their risk appetites. REs shall take up with the card network and/ or ATM network as the case may be, to put in place transaction limits at Card, BIN as well as at the RE level. Such limits shall be mandatorily set at the card network switch itself. Limits could be mandated both for domestic as well as international transactions separately. REs shall 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 RE shall be put in place as per the Board-approved policy. REs shall institute a mechanism to monitor breaches, if any, on a 24x7 basis, including weekends, long holidays and put in place a robust incident response mechanism to mitigate the fraud loss, on account of suspicious transactions, if any. REs shall ensure that card details of the customers are not stored in plain text at the RE and its vendor(s) locations, systems and applications. REs shall also 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.

73. REs that use card data scanning tools to identify unencrypted (clear text) payments card data in their ecosystem especially during audits shall adhere to the following safety measures:

1. Any tool (procured by/ from a third-party) for the purpose of scanning of unencrypted card data should first be tested in a test environment to understand the scope and impact of the tool’s capabilities;
2. The scanning tool should be installed only in the RE's premises on their devices;
3. Card data scanning should not be done remotely;
4. The discovered data, if any, must preferably reside in the scanning tool. Exportable card data must be appropriately masked. (No data, even masked, must be taken out of the RE’s premises/ infrastructure); and
5. Limited access to service providers to conduct the scan or analyse the data, if at all, must be provided only on the RE’s devices.

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0>

**15. Introduction of Legal Entity Identifier for Large Value Transactions in Centralised Payment Systems**

**RBI/2020-21/82 DPSS.CO.OD No.901/06.24.001/2020-21 January 05, 2021**

*The Chairman / Managing Director / Chief Executive Officer of member banks participating in RTGS / NEFT*

The Legal Entity Identifier (LEI) is a 20-digit number used to uniquely identify parties to financial transactions worldwide. It was conceived as a key measure to improve the quality and accuracy of financial data systems for better risk management post the Global Financial Crisis.

2. LEI has been introduced by the Reserve Bank in a phased manner for participants in the over the counter (OTC) derivative and non-derivative markets as also for large corporate borrowers.

3. It has now been decided to introduce the LEI system for all payment transactions of value ₹50 crore and above undertaken by entities (non-individuals) using Reserve Bank-run Centralised Payment Systems viz. Real Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT).

4. In preparation for the wider introduction of LEI across all payment transactions, member banks should:

* advise entities who undertake large value transactions (₹50 crore and above) to obtain LEI in time, if they do not already have one;
* include remitter and beneficiary LEI information in RTGS and NEFT payment messages (details of the identified fields in the messaging structures of RTGS and NEFT for inclusion of LEI information are at Annex);
* maintain records of all transactions of ₹50 crore and above through RTGS and / or NEFT.

5. Entities can obtain LEI from any of the Local Operating Units (LOUs) accredited by the Global Legal Entity Identifier Foundation (GLEIF), the body tasked to support the implementation and use of LEI. In India, LEI can be obtained from Legal Entity Identifier India Ltd. (LEIL) (https://www.ccilindia-lei.co.in), which is also recognised as an issuer of LEI by the Reserve Bank under the Payment and Settlement Systems Act, 2007.

6. These directions are issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007) and shall be effective from April 1, 2021.

**Annex**

**Bank Customers who must obtain LEI**

1. All non-individual customers initiating or receiving transactions of ₹50 crore and above through RTGS and / or NEFT.

Fields in NEFT and RTGS payment messages to be used for recording Remitter and Beneficiary LEI

1. For RTGS customer payment transactions, LEI information shall be provided in ‘Remittance information’ field.
2. For NEFT outward debit messages, LEI information shall be provided in ‘Sender to Receiver Information’ field.
3. Technical guidelines for populating LEI in identified fields in RTGS and NEFT messages shall be communicated separately.

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12010&Mode=0>

**16. Operationalisation of Payments Infrastructure Development Fund (PIDF) Scheme**

**RBI/2020-21/81 DPSS.CO.AD No.900/02.29.005/2020-21 January 05, 2021**

*The Chairman / Managing Director / Chief Executive Officer, Card Issuing and Acquiring Banks and Non-banks / Authorised Card Networks*

Please refer to the Statement on Developmental and Regulatory Policies dated October 4, 2019 and the Press Release dated June 05, 2020 announcing creation of Payments Infrastructure Development Fund (PIDF). PIDF is intended to subsidise deployment of payment acceptance infrastructure in Tier-3 to Tier-6 centres with special focus on North-Eastern States of the country. It envisages creating 30 lakh new touch points every year for digital payments.

2. The framework of PIDF is enclosed (Annex – I). An Advisory Council (AC), under the Chairmanship of the Deputy Governor, RBI, has been constituted for managing the PIDF. PIDF will be operational for a period of three years from January 01, 2021 and may be extended for two more years depending upon the progress. PIDF presently has a corpus of ₹ 345 crore (₹ 250 crore contributed by RBI and ₹ 95 crore by the major authorised card networks in the country).

3. All stakeholders are requested to co-operate in this endeavour by – (a) making their contributions to PIDF within the timelines, and (b) deploying acceptance infrastructure and seeking reimbursement from PIDF.

4. These directions are issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

**Annex - I**

**Payments Infrastructure Development Fund (PIDF) Scheme**

The objective of PIDF is to increase the number of acceptance devices multi-fold in the country. The Scheme is expected to benefit the acquiring banks / non-banks and merchants by lowering overall acceptance infrastructure cost.

**1. Validity Period and PIDF Target**

1.1 Three years from January 01, 2021, extendable by two further years, if necessary.

1.2 Increasing payments acceptance infrastructure by adding 30 lakh touch points – 10 lakh physical and 20 lakh digital payment acceptance devices every year.

**2. Governance Structure of PIDF**

2.1 PIDF shall be governed by an ex-officio Advisory Council (AC).

2.2 Composition of the AC :–

Shri B P Kanungo, Deputy Governor, Reserve Bank of India;

Shri Sunil Mehta, Chief Executive, Indian Banks’ Association;

Shri D Nageswara Rao, Chief General Manager, DFIBT, NABARD;

Shri Dilip Asbe, Chief Executive Officer, National Payments Corporation of India;

Shri Vishwas Patel, Chairman, Payments Council of India;

Shri Shailesh Paul, Vice President and Head Merchant Sales and Solutions, Visa;

Shri Rajeev Kumar, Senior Vice President, Market Development, Mastercard;

Shri R Vittal Raj, Chartered Accountant, Kumar & Raj Chartered Accountants; and

Shri Ajay Michyari, Regional Director, Reserve Bank of India, Mumbai Regional Office (Administrator of PIDF).

The Chief General Manager, Department of Payment & Settlement Systems, Reserve Bank of India shall function as the Secretariat to the AC.

2.3 The AC may constitute sub-committees to look into different aspects of the PIDF, as required.

2.4 The AC may co-opt members at its discretion.

2.5 AC shall devise suitable rules for operating the PIDF.

**3. Target Geographies**

3.1 The primary focus shall be to create payment acceptance infrastructure in Tier-3 to Tier-6 centres.

3.2 North Eastern states of the country shall be given special focus.

3.3 While setting parameters for utilisation of funds, the focus shall be to target those merchants who are yet to be terminalised (merchants who do not have any payment acceptance device).

3.4 The AC shall devise a transparent mechanism for allocation of targets to acquiring banks / non-banks in different segments / locations.

3.5 The tentative distribution of targets across centers will be as follows:

|  |  |
| --- | --- |
| **Distribution of Acceptance Devices** | **% Share of Total** |
| Tier-3 and Tier-4 centres | 30 |
| Tier-5 and Tier-6 centres | 60 |
| North Eastern States | 10 |

**4. Market Segments and Merchant Categories**

4.1 Merchants providing essential services (transport, hospitality, etc.), government payments, fuel pumps, PDS shops, healthcare, kirana shops may be targeted, especially in the targeted geographies.

**5. Types of Acceptance Devices Covered**

5.1 Multiple payment acceptance devices / infrastructure supporting underlying card payments, such as physical PoS, mPoS (mobile PoS), GPRS (General Packet Radio Service), PSTN (Public Switched Telephone Network), QR code-based payments, etc.

5.2 As the cost structure of acceptance devices vary, subsidy amounts shall accordingly differ by the type of payment acceptance device deployed. A subsidy of 30% to 50% of cost of physical PoS and 50% to 75% subsidy for Digital PoS shall be offered.

5.3 Payment methods that are not inter-operable shall not be considered under PIDF.

5.4 The subsidy shall not be claimed by applicant from other sources like NABARD, etc. In case other mechanisms exist for providing subsidy or reimbursing cost of deployment of acceptance infrastructure,

no reimbursement shall be claimed from PIDF therefor.

**6. Initial Corpus**

6.1 Initial corpus of PIDF has to be substantial to initiate pan-India terminalisation and to cover the pay-outs in the first year. Contributions to the PIDF shall be mandatory for banks and card networks.

6.2 RBI shall contribute ₹ 250 crore to the corpus; the authorised card networks shall contribute in all ₹ 100 crore.

6.3 The card issuing banks shall also contribute to the corpus based on the card issuance volume (covering both debit cards and credit cards) at the rate of ₹ 1 and ₹ 3 per debit and credit card issued by them, respectively.

6.4 It shall be the endeavour to collect the contributions by January 31, 2021.

6.5 Any new entrant to the card payment eco-system (card issuer and card network) shall contribute an appropriate amount to the PIDF.

**7. Recurring Contribution**

7.1 Besides the initial corpus, the PIDF shall also receive annual contribution from card networks and card issuing banks as under:

a) Card networks – Turnover based – 1 basis point (bps) i.e., 0.01 paisa per Rupee of transaction;

b) Card issuing banks – Turnover based – 1 bps and 2 bps i.e., 0.01 paisa and 0.02 paisa per Rupee of transaction for debit and credit cards respectively; also at the rate of ₹ 1 and ₹ 3 for every new debit and credit card issued by them respectively during the year.

7.2 RBI shall contribute to yearly shortfalls, if any.

**8. Collection Mechanism**

8.1 By January 31st and July 31st based on card data of December 31st and June 30th respectively.

**9. Types of Expenses Covered**

9.1 The parameters / rules for claiming the amount of subsidy for the capital expenditure, taking into account the type of device, deployment location etc., shall be framed by the AC.

9.2 Subsidy shall be granted on half yearly basis, after ensuring that performance parameters are achieved, including conditions for ‘active’ status of the acceptance device and ‘minimum usage’ criteria, as defined by the AC.

9.3 The minimum usage shall be termed as 50 transactions over a period of 90 days and active status shall be minimum usage for 10 days over the 90-day period.

9.4 The subsidy claims shall be processed on half yearly basis and 75 percent of the subsidy amount shall be released. The balance 25 percent shall be released later subject to the status of the acceptance device being active in 3 out of the 4 quarters of the ensuing year.

**10. Deployment Targets for Acquirers**

10.1 Acquirers need to adopt a scientific process for identification of deployment areas, submit proposals to Regional Director, Mumbai Regional Office (MRO), RBI and effectively implement the project. The PIDF proposal format for submission in this regard is enclosed ([Format I](https://rbidocs.rbi.org.in/rdocs/content/pdfs/FORMAT_I.pdf)).

**11. Claims**

11.1 The scheme is on reimbursement basis; accordingly, the claim shall be submitted only after making payment to the vendor.

11.2 Maximum cost of physical acceptance device eligible for subsidy – ₹ 10,000 (including one-time operating cost up to a maximum of ₹ 500).

11.3 Maximum cost of digital acceptance device eligible for subsidy – ₹ 300 (including one-time operating cost up to a maximum of ₹ 200).

11.4 Subsidised amount of cost of physical and digital payment acceptance devices based on location of deployment shall be as under:

|  |  |  |
| --- | --- | --- |
| **Location** | **Physical payment acceptance device(% of total cost)** | **Digital payment acceptance device(% of total cost)** |
| Tier-3 and Tier-4 centres | 30 | 50 |
| Tier-5 and Tier-6 centres | 40 | 60 |
| North Eastern States | 50 | 75 |

11.5 Acquirers shall submit their claims through their bankers to RBI, MRO with self-declaration about fulfilment of ‘minimum usage’ and ‘active status’ criteria for deployed devices.

11.6 All initial claims shall be submitted for reimbursement of expenses (less the Input Tax Credit received / receivable by the bank / non-bank under GST) as per format ([Format II](https://rbidocs.rbi.org.in/rdocs/content/pdfs/FORMAT_II.pdf)). The second claim for 25% of eligible subsidy shall be submitted as per format ([Format III](https://rbidocs.rbi.org.in/rdocs/content/pdfs/FORMAT_III.pdf)).

**12. Monitoring of Implementation of Targets**

12.1 Implementation of targets under PIDF shall be monitored by RBI, MRO with assistance from Card networks, Indian Banks’ Association (IBA) and Payments Council of India (PCI).

12.2 Acquirers shall submit quarterly deployment reports on achievement of targets to RBI, MRO.

12.3 Acquirers meeting / exceeding their targets well in time and / or ensure greater utilisation of acceptance devices in terms of transactions shall be incentivised while those who do not achieve their targets shall be disincentivised, by scaling up or down the extent of reimbursement of subsidy as follows:

|  |  |
| --- | --- |
| **Target Achievement / Utilisation** | **% of Subsidy Eligible** |
| Less than 75 percent | 90 |
| 75 percent to 125 percent | 100 |
| Greater than 125 percent | 110 |

<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12009&Mode=0>

**17. Booklet on Payment Systems in India 25 Jan 2021**

The Reserve Bank today released the [Booklet on Payment Systems](https://www.rbi.org.in/Scripts/OccasionalPublications.aspx?head=Payment%20Systems%20in%20India%20-%20Booklet) covering the journey of Payment and Settlement Systems in India during the second decade of the millennium, viz., from the beginning of 2010 till the end of 2020.

This Booklet captures the transformation of India in the sphere of payment and settlement systems and describes, inter-alia, the legal and regulatory environment underpinning the digital payments systems, various enablers, payment options available to consumers, extent of adoption, etc. during 2010 to 2020.

Reserve Bank had earlier come out with Booklets on Payment Systems in the years 1998 and 2008. This third Booklet in the series is expected to serve as a reference document for those interested in knowing more about payment system developments in the country.

<https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/PSSBOOKLET93D3AEFDEAF14044BC1BB36662C41A8C.PDF>