Framework

Internet Banking

Current Effective Date: May 2025

TABLE OF CONTENTS

1. Summary or Rationale

JPMorgan Chase Bank, N.A., a scheduled commercial bank under the Reserve Bank of India Act, 1934 acting through its branches in India (hereinafter referred to as "JPMCB India" offers various internet products to enhance our client access interface to our clients. This is viewed as an extension of existing access mechanisms to allow our clients to send payment instructions and trade related instructions to JPMCB India for processing as well as retrieving their account balance and transaction information.

2. Scope

Lines of Business	**Subject To**	**Role To Play**
	• Commercial and Investment Banking	• Payments
Function(s)	**Subject To**	**Role To Play**
	• NA	• NA
Locations	• APAC - India	
Legal Entities	• JPMorgan Chase Bank, N.A.	

3. Changes from Previous Version

- Annual Review

4. Framework Statements

- KYC - Internet Banking services will only be provided to Customers of the JPMCB India after verifying the identity of customers and completion of KYC formalities in accordance with the KYC & AML Framework& Procedures of the Bank. The Bank may receive a request for opening an account over the internet; however, accounts should only be opened after proper verification of the identity of the customer.
- Client coverage - JPMCB India shall offer Internet banking products only to its Customers.
- Internet Banking Services – This section outlines the internet banking services offered by the Bank. JPMCB India may offer its customers internet-based platform for foreign exchange services, for permitted underlying transactions, subject to compliance with certain terms and conditions
- Risk Management - The JPMCB India shall ensure that it maintains secrecy and confidentiality of customers' accounts. The Bank's IT Risk Management Framework (available on the JPMCB Intranet) addresses various aspects pertaining to security measures and policies of the Bank as well as secrecy of customer data.

- The JPMCB India shall clearly notify its customers of the timeframe and the circumstances in which any stop-payment instructions would be accepted by it.
- Documentation - The JPMCB India shall enter into such documentation and agreements with the Customer as determined appropriate by Legal and Compliance.
- Reporting to RBI - JPMCB India will report to RBI every breach or failure of security systems and procedure.
- RBI Guidelines – This section covers the guidelines laid down by RBI on Internet Banking
- Payment Gateway instructions - All instructions of RBI relating to 'Inter-bank Payment Gateways' for settlement of e-commerce and other transactions shall be complied with.
- Disclosures - JPMCB India shall make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through Internet through Electronic Channel Service Terms..
- Customer Protection for Unauthorized Electronic Banking Transactions – This section includes details on Customer compensation guidelines in case of unauthorized transactions
- Awareness around Electronic banking and Payments related frauds - This section includes details on the procedures in place to create awareness among JPMCB India's customers on electronic banking and payments related frauds
- Hyperlinks - Hyperlinks from the Bank's website shall be confined to only those portals with which JPMCB India has a payment arrangement or sites of their subsidiaries or principals. Hyperlinks to the JPMCB India's website from other portals will be normally meant for passing on information relating to purchases made by JPMCB India's customers in the portal. JPMCB India shall follow the minimum recommended security precautions while dealing with request received from other websites, relating to customers' purchases.
- Security - The technology and security standards prescribed by RBI and recommended by the 'Working Group on Internet Banking' including the security framework will be meticulously followed by the JPMCB India.
- Notifying Management Committee - Prior to offering of any banking services over the internet, JPMCB India shall put up a note to its Management Committee stating details such as the business plan, analysis of cost and benefit, operational arrangements like technology adopted, business partners as relevant, third party service providers, systems and control procedures we propose to adopt for managing risks, and any other pertinent information.
- Approvals - JPMCB India (i.e., the unit offering the service over the internet) shall obtain an approval from its ITRM (Information Technology Risk Management) Department and ORM (Operational Risk Management) Department prior to offering of any new or further banking services over the internet.
- Framework Renewal - This framework is subject to review annually. The gap between two reviews should not be more than 12 months. It may also be reviewed as and when felt necessary by the Management Committee.

- Applicability - This framework is intended to address requirements under Indian regulations only and should be read in conjunction with applicable Firm wide policies

5. Internet Banking Services

The services include local currency products and foreign exchange products. JPMCB India may offer its customers internet-based platform for foreign exchange services, for permitted underlying transactions, subject to compliance with the following additional terms and conditions:

- The data relating to JPMCB India will be kept segregated.
- The data will be made available to RBI inspection / audit as and when called for.
- The services offered through Internet, for banks' customers on an Internet based platform for dealing in foreign exchange, shall allow only reporting and initiation of foreign exchange related transactions, with the actual trade transactions being permitted only after verification of physical documents.
- Banks will comply with FEMA regulations in respect of instructions involving cross-border transactions.

6. RBI Guidelines

JPMCB India shall comply with various guidelines issued by Reserve Bank of India as amended from time to time (including but not limited to)

- Internet Banking in India - Guidelines dated 14 Jun 2001
- Internet Banking in India – Guidelines dated 20 Jul 2005
- Internet Banking – Internet based platforms for dealing in Foreign Exchange dated 22 Aug 2006
- 'Risks and Controls in Computers and Telecommunications' vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 04 Feb 1998
- The recommendations of the 'Working Group on Internet Banking' referred to in the RBI circular on Internet Banking in India - Guidelines dated June 14, 2001
- Internet Banking - Internet Based Platforms for Dealing in Rupee Vostro Accounts dated 15 Nov 2007

7. Customer Protection for Unauthorized Electronic Banking Transactions

This framework refers to RBI Circular reference: DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017.

JPMCB India provides Electronic Banking to its Customers. Customers can report unauthorized transactions through the Electronic Banking platform or other channels. In the

event of any unauthorized transaction, Customer will be compensated for any consequential financial loss as per the below guidelines:

- Limited Liability of a Customer
  - Zero Liability of a Customer
    - A customer's entitlement to zero liability shall arise where the unauthorized transaction occurs in the following events:
    - Contributory fraud/ negligence/ deficiency on the part of the Bank (irrespective of whether the transaction is reported by the customer).
    - Third party breach where the deficiency lies neither with the Bank nor with the customer but lies elsewhere in the system, and the customer notifies the Bank within three working days of receiving the communication from the Bank regarding the unauthorized transaction.
  - Limited Liability of a Customer
    - A customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:
    - In cases where the loss is due to negligence by a customer, such as where he has shared the user credentials, the customer will bear the entire loss until he reports the unauthorized transaction to the Bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the Bank.
    - In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the Bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the Bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in below Table , whichever is lower.

7.1. Summary of Customer's Liability

Time taken to report the fraudulent transaction from the date of receiving the communication from the Bank	Customer's liability (Rs)
Within 3 working days	Zero liability
Within 4 to 7 working days (Current Accounts/ Cash Credit/ Overdraft Accounts/ Trade Transactions with annual average balance / limit up to Rs.25 lakh)	The transaction value or 10,000, whichever is lower

Time taken to report the fraudulent transaction from the date of receiving the communication from the Bank	Customer's liability (Rs)
Within 4 to 7 working days (All Other current/ Cash credit/ Overdraft Accounts/ Trade Transactions)	The transaction value or 25,000, whichever is lower
Beyond 7 working days	Liability shall be determined and approved on a case by case basis by head of the concerned Line of Business

Note: The number of working days shall be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

On being notified by the customer, the bank shall credit (shadow reversal) the amount involved in the unauthorized electronic transaction to the customer's account within 10 working days from the date of such notification by the customer (without waiting for settlement of insurance claim, if any). Also, the Customer service committee shall periodically review the unauthorized electronic transactions reported by customer. The credit shall be value dated to be as of the value date of the unauthorized transaction.

The bank shall report the customer liability cases to Management committee. These cases will be made available to audit for review.

Further, Bank shall ensure that:

- A complaint is resolved and liability of the customer, if any, established within such time, as may be specified in the bank's Board approved framework, but not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions of table above;
- Where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in table above is paid to the customer; and
- In case of bank account, The customer does not suffer loss of interest or does nor bear any additional burden of interest.
- The burden of proving customer liability in case of unauthorized electronic banking transactions shall lie on the bank.

Bank shall also periodically update the customer on

- The risks and responsibilities involved in cases of electronic banking transactions and the customer liability in cases of unauthorized electronic banking transactions focusing on the below

- The systems and procedures to ensure safety and security of electronic banking transactions carried out by customers.
- appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom

Note: JPMCB only serves corporate customers in India and therefore notifications are sent through email where necessary since SMS is not the most appropriate mode of communication for corporates.

7.2. Resolution of Grievances

The customers can highlight their complaints / issues vide the procedure outlined in this framework. For redressal of issues customers can email their complaint to: customerservice.india@jpmorgan.com.

Customers will receive a response within ten business days, and we shall do our best to resolve the complaint to the customer's satisfaction within this period. Complex complaints which would require time for examination of issues involved, may take a longer time to resolve. However, in such cases, customers will be informed about the status of their complaint within this period. Our focus would remain on the quality and completeness of the response, with speed of delivery being an important but not overriding factor

In case of unsatisfactory response from the above channel customers can escalate the complaint to the Principal Nodal Officer of the Bank (as approved by the MANCOM) whose details are available on the JPMCB India website under the section "Grievance handling mechanism".

7.3. Banking Ombudsman Scheme

If customers do not receive a response from us within one month after we have received the complaint, or if they are not satisfied with the reply given by us, they may approach the Banking Ombudsman. The details of the Banking Ombudsman Scheme as well as the contact details of the Ombudsman for respective City or State are available on www.bankingombudsman.rbi.org.in. This link is displayed on our website as well. A copy of this Scheme is available on request.

For the convenience of the customers, following have been displayed on our website:

- Appropriate arrangement for receiving complaints and suggestions.
- The name, address and contact number of the Principal Nodal Officer Contact
- Details of Banking Ombudsman of the area
- Code of bank's commitments to customers/Fair Practice code

The nodal officer of the JPMCB India is kept informed on the complaints which are not redressed within one month. The details of the Banking Ombudsman where the complainant can approach are included in the final closure letters/ emails for such cases.

8. Awareness around Electronic banking and Payments related frauds

To create awareness around Cyber security and help protect Customers from electronic banking & payments related frauds, JPMCB India has put in place the following procedures:

- JPMCB India's banking website includes information on the Electronic banking usage guidelines, training materials, along with the list of Do's and Don'ts, to help protect the users from cyber fraud and social engineering attacks.
- JPMCB India's banking website includes JPM framework on Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions JPMCB India shall provide access to training videos on secure online banking in JPMCB India's banking portal.
- JPMCB India shall circulate an email on cyber security awareness to all the client users enabled on the JP Morgan Internet Banking on a half-yearly basis

9. Legal and Other References

Statutes, Laws, Rules, Regulations or External Guidance	• Internet Banking in India - Guidelines dated 14 Jun 2001 • Internet Banking in India – Guidelines dated 20 Jul 2005 • Internet Banking – Internet based platforms for dealing in Foreign Exchange dated 22 Aug 2006 • 'Risks and Controls in Computers and Telecommunications' vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 04 Feb 1998 • Internet Banking - Internet Based Platforms for Dealing in Rupee Vostro Accounts dated 15 Nov 2007 • Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions - DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017 • Master Circular on Customer Service in Banks - DBOD No.Leg.BC.21/09.07.006/2014-15
Enterprise Library Application (ELA) Link	• ELA home page

10. Firm References

Other Firm Policies or Standards	• This framework will have to be read together with all applicable policies of the Firm
Framework Supplements, Procedures, and Other Documents	• N/A

Forms/Systems	• N/A

11. Document Information

Primary Risk Category	Operational Risk > Information Exposure, Misuse and Improper Records Management > Exposure of Information		
Framework Level	Level 3		
Framework Type	Country		
Framework Owner / Primary Contact / Secondary Contact/Framework Manager	Nikita Tambday Executive Director V729051	Nilay Ritwik Executive Director E914945	Varun Darji Executive Director O401548
Framework Owner's Line of Business	Corporate & Investment Banking – Treasury Services		
Framework Owner's Country	India		
Framework Approver	India Management Committee		
Approval Date / Annual Review Date	May 31, 2025	May 31, 2026	
Last Off-Cycle Update Date	February 2025		
Contact Group Email or Hotline Number	TS Products India		