

ASIAPAC BANKING GUIDE FOR NONPROFITS


*HOW TO OPEN AND MANAGE AN ORGANIZATIONAL
BANK ACCOUNT*



INDIA



Law firms participating in this research are not liable towards third parties for the accuracy of the information contained in this guide. The research cannot be considered as legal advice. It was carried out in 2022 and 2023 and responds to the regulatory framework on organizational banking in this time period. If you have further queries please reach out to our clearinghouse for legal help.

 PILnet is a global non-governmental organization that creates opportunities for social change by unlocking law's full potential. With programs in Europe & Eurasia, Asia, and at the global level, PILnet aims to reclaim and reimagine the role of law so that it works for the benefit of all. PILnet builds networks and collaborations of public interest and private lawyers who understand how law works when it serves the interests of the privileged and then it uses that knowledge to strengthen civil society and the communities they serve. PILnet not only obtains high-quality, free legal assistance for civil society organizations when they urgently need it but also helps organizations to capitalize on the full range of specialized legal expertise that can be provided by corporate lawyers, including against ongoing, or even yet-to-be-determined, challenges.

1. OPENING AN ORGANIZATIONAL BANK ACCOUNT

a. What are the requirements to open an organizational bank account?

i. Do organizations have to be physically present in the country to open a bank account? I.e., can they operate in country X but have a bank account in country Y? Is the presence of a statutory representative required or can the presence be fulfilled through an authorization?

Organizations do not have to be physically present in India to open a bank account. It must be noted that a foreign CSO can only open account with a bank which is an authorised bank under the applicable laws to maintain an account of a person resident outside India.

Under the applicable laws and the rules and regulations issued by the Reserve Bank of India (“RBI”), which is the Indian regulator for banks, overseas CSOs (being persons resident outside India) can only open certain types of accounts as prescribed by RBI which currently are (i) a non-resident (ordinary) rupee account (“NRO Account”) or (ii) a special non-resident rupee account (“SNRR Account”) with an authorised bank. The procedure, restrictions, and applicable guidelines with respect to NRO Accounts and SNRR Accounts are specifically covered under the *(India) Foreign Exchange Management (Deposit) Regulations, 2016*.¹

NRO Account and SNRR Account: Comparison

Notably, SNRR Accounts can only be opened by CSOs having a business interest in India, while NRO Accounts can be opened and maintained by individuals for the purpose of putting through bona fide transactions denominated in Indian rupees. Further, an SNRR Account can be held only as a non-interest earning account, while an NRO Account can earn interest. However, a significant advantage of SNRR Accounts over NRO Accounts is that the former is a repatriable account (conversion of offshore capital back to the currency of the origin country of a person),

¹ [https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTINO5\(R\)DE2833D3DFA8415BA5B586CFA3D4A946.PDF](https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTINO5(R)DE2833D3DFA8415BA5B586CFA3D4A946.PDF)

while the latter is non-repatriable. Further, NRO Accounts are primarily used for managing income and can be maintained in the form of current, savings, recurring, or fixed deposit accounts. The same is not permitted in the case of SNRR Accounts and all transactions made through an SNRR Account shall be specific or ancillary to the business of the account holder alone.

While the RBI does not require presence of a statutory representative for opening a SNRR Account or NRO Account, the requirement of having a statutory representative in India may vary upon the internal processes of each of the authorised banks. India is an exchange-controlled jurisdiction, and the RBI prescribes instructions and procedures in relation to opening of accounts, and the relevant permissible credits and debits in such accounts; therefore, before the opening of any bank account in India by a CSO, specific regulations and rules should be evaluated at the relevant point, depending on the need of the CSO. Authorised banks in India can assist CSOs in determining the nature of the account to be opened and the process/steps for opening such account.

Separately, if a foreign CSO wants to operate a bank account in India for its India operations (except to the extent that it operates out of a place of business in India such as a liaison office, branch office, or project office), it would need to open a foreign contribution account as regulated under *Foreign Contribution (Regulation) Act, 2010* (“FCRA”). Any subsidiary or grantee of a foreign CSO that receives foreign funding will require FCRA registration prior to receiving foreign contribution. An FCRA registered entity can only receive foreign contribution in the designated bank account of State Bank of India (“SBI”), Parliament Street branch, New Delhi. This SBI account is monitored by the bank, the RBI, and also the Ministry of Home Affairs (“MHA”) for any non-compliance under the FCRA.

ii. Are there specific requirements for CSOs to open accounts by law or asked in practice by the banks (e.g, years of operations, annual turnover, to have director or member of governing body to be national of the country)

The application to open a bank account can be made by one or more persons, who are authorized by a power of attorney²

² Under the Powers of Attorney Act, 1882, a PoA includes any instrument empowering a specified person to act for and in the name of the person executing such instruments under Indian laws.

(“PoA”) to act on behalf of the CSO, to the authorised bank, along with the requested documentation. The CSO, if required by the bank, can issue a PoA in favour of their representative to complete the process for opening a bank account on behalf of the CSO. Specifically, for NRO Accounts, at the time of opening the account, the CSO should furnish an undertaking to the respective authorised bank that in cases of debits to the account for the purpose of investment in India and credits representing sale proceeds of investments, the CSO will ensure that such investments/disinvestments will be in accordance with the regulations made by the RBI in this regard. With respect to NRO Accounts and SNRR Accounts, the following documents need to be submitted to the bank to open a bank account:

(a) certified copies of the documents showing the name of the person authorised to act on behalf of the CSO or the equivalent e-documents thereof;

(b) certified copies of the documents showing the person holding a PoA to transact on the CSO’s behalf, which, among other things, include the identity documents (such as permanent account number (“PAN”) and Aadhaar details) of the authorised person or the equivalent e-documents thereof; and

(c) such other documents as may be required by the bank under Indian laws to establish the legal existence of the CSO. Typically, these include incorporation documents of the CSO.

Additionally, every bank in India prescribes its own set of conditions and documentation and information requirements in terms of opening of bank accounts, which should be factored.

iii. Who is authorized/required to open a bank account? Can this be done online, or that person needs to be present in the country?

In most cases, banks would provide an option to open an NRO Account / SNRR Account online or by physically visiting the relevant branch. However, in the absence of such online facility for some banks, the authorised representative will be required to be physically present and to visit the authorised bank in person to open an NRO Account or SNRR Account. Once opened, most accounts can be managed through online banking.

There are no specific requirements with respect to signing the paperwork of the account opening forms at the bank premises and signing the same at the embassy or before a notary, and should generally be acceptable to the bank representatives. However, every bank has its own requirements that will need to be checked with the relevant bank.

iv. What is the process of setting up a bank account? E.g., how long it takes, is there a practice to have an interview in the bank?

The process involves submitting an account opening form and compliance with the know-your-customer (“KYC”) norms (which includes a customer identification process for obtaining consent of the CSO, customer due diligence, etc.). Subject to the bank’s internal checks and verification, it generally takes approximately 2 to 4 weeks for the whole process to be concluded and the NRO Account / SNRR Account to be opened. However, the process and how long it takes will vary from bank to bank. From the time of completion of the KYC process, it generally takes around 24 to 48 hours for an NRO Account / SNRR Account to be opened. Delays or failure to complete or provide documentation as requested by the relevant bank may slow down the process.

2. BANKING ACTIVITIES

a. What customer due diligence requirements are in place and what is their impact on civil society organizations’ banking activities?

Authorised banks need to comply with the Indian anti-money laundering regime and KYC requirements in respect of all customers, and CSOs will be treated in the same way as any other customer. Banks in India need to comply with various requirements, including regimes under the *Prevention of Money Laundering Act, 2002* (“PMLA”).

Banks are required to carry out due diligence to verify the identity of new clients, to verify that funds deposited are from a legitimate source, to understand the nature of their clients’ business, and to carry out on-going monitoring to identify suspicious transactions. CSOs will be required to provide all

documentation (such as incorporation documents, tax records, etc.) and evidence to allow the bank to satisfy its KYC, anti-money laundering, and other due diligence requirements, and will be unable to open a bank account or process certain transactions until these requirements have been satisfied.

Customer due diligence over CSOs includes the requirement to submit the documents set out under the response to Question 1(a)(ii) above and the relevant account opening formalities. Further, periodic KYC updating for NRO Accounts / SNRR Accounts is undertaken by the authorised banks, and CSOs must specifically participate and cooperate with the authorised bank in this regard. Only permissible credit / debit and specified transactions are allowed for NRO Accounts / SNRR Accounts under the applicable laws, which must be noted by CSOs for their banking activities.

Additionally, banks in India are obligated to mandatorily report to the MHA within 48 hours of any transaction concerning receipt or utilization of foreign contribution by any Indian person. Usually, MHA investigates non-compliances under the FCRA by Indian entities that receive foreign contribution. Such investigation may be undertaken by the MHA as and when it receives information that an Indian entity is receiving and utilizing foreign contribution without due compliance (such as obtaining prior permission or registration for receipt of the foreign contribution).

During such inspection, if and when information is received by the MHA that a particular foreign CSO is transferring money to an ineligible Indian entity, such CSOs may be put on the Prior Reference Category list (“**PRC List**”) by the MHA for oversight by relevant regulators. Once a foreign donor is included in the watchlist, SBI is required to take prior clearance of the MHA before allowing the transfer of foreign contribution from the foreign CSO to any Indian entity.

On-going customer due diligence of bank accounts opened by CSOs in India helps banks ensure compliance with regulatory standards. It involves periodic reviews of account activity, source of funds, and adherence to anti-money laundering and counter-terrorist financing measures. This safeguards the financial system by preventing illicit activities and maintaining transparency. The impact of such on-going due diligence by banks may lead to increased scrutiny and periodic reviews by the bank. This may also lead to additional documentation requests, monitoring of funds sources, and reporting of suspicious transactions. While these measures aim to enhance financial

integrity, they may also result in administrative challenges for CSOs, requiring them to provide detailed information and documentation to ensure compliance with regulatory standards.

b. Which internal principles or official (central bank) “suspicious transaction” monitoring criteria are in place affecting the civil society organizations? Is it publicly available?

The *RBI KYC Directions, 2016*, which are also applicable to CSOs, provide that “suspicious transaction” means a transaction, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

- a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence, regardless of the value involved; or
- b. appears to be made in circumstances of unusual or unjustified complexity; or
- c. appears to not have economic rationale or bona-fide purpose; or
- d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

There are specific reporting requirements under applicable laws for suspicious transactions, which are standard and also applicable to CSOs. For instance, under the PMLA, banks are required to furnish details of suspicious transactions, whether made in cash or otherwise, under the specified format³ for suspicious transactions reports (“STRs”) to Financial Intelligence Unit India.

c. Do the banks in the country of operations have any restrictions/limitations to bank transactions and transfers to certain jurisdictions (such as high-risk ones).

i. If yes, is the list of jurisdictions publicly available?

The jurisdictions which do not apply or insufficiently apply the Financial Action Task Force (“FATF”) recommendations and

³ <https://fuindia.gov.in/pdfs/downloads/SBA.pdf>

guidelines include The Bahamas, Botswana, Ethiopia, Ghana, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen. While there are no restrictions/limitations to transactions relating to these jurisdictions, special attention shall be given by banks to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF recommendations and jurisdictions included in FATF statements.

ii. What would be the procedures the bank would follow in this case for their CSO clients?

Standard policies and procedures would be followed, and the relevant bank would apply sanctions and necessary restrictions to comply with Indian anti-money laundering regime requirements and any other relevant regulations. The procedures are specific to CSOs. However, the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF statements and countries that do not or insufficiently apply the FATF recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to the RBI / other relevant authorities, if so requested.

3. OBLIGATIONS AND REPORTING REQUIREMENTS

a. Are banks required to provide CSO clients' financial information to CSO regulatory authorities or public officials? If yes, under what circumstances must banks do so, and what types of information must they provide?

Yes, reporting requirements to the RBI are applicable to authorised banks maintaining both NRO Accounts and SNRR Accounts.

For NRO Accounts: The transactions in the NRO Account, which may appear to represent reimbursement in rupees against foreign exchange made available to a person resident in India other than an authorised dealer, as well as any other transaction of a suspicious nature, should be reported to the RBI along with

other transactions as specified by the RBI.

For SNRR Accounts: Any underlying transaction by a domestic Indian party, which requires reporting under Form A2 to the RBI for remittance overseas, will require the same in case of a domestic remittance for credit to an SNRR Account. Further, the regulatory reporting under the FETERS (R Return) will be undertaken by the bank maintaining the SNRR Account, which includes:

- (i) Any credit/debit to/from an SNRR Account from/to an offshore account of the non-resident entity holding the SNRR Account will be reported under an authorised dealer bank transfer; and
- (ii) Any credit/debit to/from an SNRR Account from/to a domestic (Indian) party will be reported on the basis of the underlying transaction (import, export, trade credit, services, external commercial borrowing, etc.).

The RBI has also provided that the banks holding and maintaining SNRR Accounts shall follow the reporting procedure as applicable to other Indian rupee vostro accounts held by them. Additionally, RBI regularly prescribes rules and directions on the various types of transactions that can or cannot be undertaken through such accounts.

As mentioned in the response to question 2(a) above, banks in India are obligated to mandatorily report to the MHA within 48 hours of any transaction concerning receipt or utilization of foreign contribution by any Indian person. Further, the SBI has an obligation to report CSO details (such as the name, currency, etc.) on a daily basis to the MHA. If information is received by the MHA that a foreign CSO is transferring money to an ineligible Indian entity, then such CSO may be put on the PRC List by the MHA.

Additionally, the FCRA also imposes various obligations on recipients of foreign contribution. For instance, a recipient who has registered under the FCRA is required to intimate the specified authority about the amount of each foreign contribution received by it, its source, and manner of receiving it, along with the purpose for which and the manner in which the foreign contribution was utilised by the recipient.

b. What obligations do banks have to protect the privacy of clients' information?

All Indian banks have a duty to maintain the confidentiality of their customers. Specifically, under the *RBI KYC Directions, 2016*, banks are obligated to maintain information secrecy, which arises out of the contractual relationship between the banks and its customers. Further, the information collected by a bank from its customers for the purpose of opening of their accounts is to be treated as confidential, and details thereof cannot be divulged for the purpose of cross-selling, or for any other purpose, without the express permission of the customer.

Moreover, under the *Information Technology Act, 2000* (“IT Act”) and the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*,⁴ banks are required to protect personal data (such as residential details) and sensitive personal data or information (such as financial information) of the authorised representatives or key managerial personnel of CSOs by complying with data protection requirements, including but not limited to obtaining explicit consent and security certificates, among other things. However, banks may be required by law enforcement agencies to disclose certain information, provided they obtain the CSO’s express written consent.

Additionally, as per the RBI circular on [Storage of Payment System Data](#)⁵ and clarifications issued in that regard, banks are required to ensure data localisation, and store data related to payment systems operated by banks only in India. Such data will include end-to-end transaction details and information pertaining to the payment or settlement transaction that is collected, transmitted, or processed as part of a payment message or instruction, such as the customer and beneficiary account details.

4 The Indian Parliament has enacted the Digital Personal Data Protection Act 2023 (“DPDP Act”), which seeks to replace the existing data protection regime in India, i.e., Section 43A of the IT Act read with the rules issued thereunder. However, the DPDP Act is yet to be enforced. Once enforced, the DPDP Act may place incremental compliance obligations on banks for ensuring customer data protection.

5 <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244>

c. Are there specific reporting obligations for banks to inform governments on civil society banking in certain circumstances?

No specific reporting obligations, apart from standard reporting requirements, apply to CSO banking, which includes informing the RBI in case of fraud and suspicious transactions. Separately, please refer to the above responses regarding obligations of banks under the FCRA.

d. Are you aware of any change in regulation/practice due to the Russian sanctions?

There has not been any change in the banking regulation or practice in India owing to the ongoing sanctions against Russia. Given that India is an exchange control jurisdiction and the RBI is a fairly active regulator, it is advisable that specific advice is sought from the authorised bank depending on the product offering and prospective transaction.



PILnet
199 Water Street, 11th Floor
New York, NY 10038 U.S.A.
<https://www.pilnet.org>
twitter.com/PILnet