ASIAPAC BANKING GUIDE FOR NONPROFITS

HOW TO OPEN AND MANAGE AN ORGANIZATIONAL BANK ACCOUNT

PILnet

HONG KONG

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.

Cover illustration by the European Center for Not-for-Profit Law Stichting (ECNL).

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 Hong Kong to open a bank account? I.e., can they operate in Hong Kong but have a bank account in another jurisdiction? Is the presence of a statutory representative required or can the presence be fulfilled through an authorization?

It is possible for organizations which are not physically present in Hong Kong to open a bank account. The Hong Kong Monetary Authority[1] has issued guidance to the effect that Hong Kong banks should not expect to receive a Hong Kong business registration certificate for all applicants or evidence of a Hong Kong office for all overseas corporates, irrespective of business model or mode of operation as part of the account opening for such overseas corporates.

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 jurisdiction)

While the requirements for account opening may vary from bank to bank and on a case-by-case basis, generally banks may require the following information/documents from a civil society organization ("**CSO**") for account opening and to complete relevant "know your customer" checks:

- corporate identification documents (e.g., certificate of incorporation, record of registration, constitutional

1 https://www.hkma.gov.hk/eng/smart-consumers/account-opening/banks-should-not/

document, etc., including to satisfy the bank of the legitimate purpose of the CSO);
- information of the address of the registered office and other address proof of the CSO (if different from the registered office);
- information of the beneficial owner(s) (e.g., identification document and address proof of the beneficial owner(s) or details of the ownership and control structure of the CSO);
- purpose and intended nature of the account; and
- information of the person acting on behalf of the CSO (e.g., identification documents of the person acting on behalf of the CSO, and authorisation documents authorising that person to act on behalf of the CSO).

Where the CSO is set up as a trust or other legal arrangement, there may be additional information and documents that the bank will need to be satisfied with. There may also be requirements relating to annual turnover and years of operations, depending on the type of account that is being opened, such as a current/overdraft account.

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

In general, a person appointed to act on behalf of the CSO to establish banking relationships, or authorised to give instructions to a bank to conduct various activities through the account or the business relationship established, can open a bank account in the name of the CSO.[2] The banks are required to identify and verify the identity of that person, as well as obtain the written authority (such as minutes of meetings or powers of attorney) to verify that such person has the authorisation of the CSO to open the bank account and establish a business relationship with the bank.

iv. Can this person complete the requirements online, or must they to be physically present in Hong Kong?

While it may be possible for banks to open accounts and verify the identity of the customer through non-face-to-face channels (e.g., internet), banks are required to comply with relevant anti-money laundering and counter-financing of terrorism

2 See Guideline 4.5.1 (Microsoft Word - AML Guideline (AI)_ENG_final draft_clean (after formatting & page no.).docx (hkma.gov.hk))

requirements, which means that they will need to take additional measures to mitigate the risk associated with customers not physically present for identification purposes.

As such, in practice, remote account opening service is very limited in Hong Kong, and while certain parts of the account opening process may be completed online (such as through submission of application forms and supporting documents for account opening online), a physical meeting with an authorised person(s) of the CSO is usually required to complete the account opening process. Once opened, the account can usually be managed online.

v. If physical presence is normally required, is it acceptable to instead sign the paperwork at an embassy or before a notary?

As part of the account opening and customer due diligence ("**CDD**") process, banks may accept verification of identification documents certified by an officer of an embassy or other professional persons such as certified public accountant, lawyer, or notary public. However, as mentioned above, banks are required to take additional measures to mitigate the risk associated with customers not physically present for identification purposes, and therefore, account openings must normally be done, in part, by the authorised person physically present at the bank.

vi. 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 typical account opening process is as follows:

(a) gather all the required documents and submit applications to the bank (online/in person);

(b) internal approval by the bank;

(c) submit additional documents/information (if required); and

(d) notification of application result by the bank.

Depending on whether sufficient information has been provided to the bank for the CDD process, the account opening process may take several days for simple cases or several weeks.

As mentioned above, a physical meeting with all the authorised person(s) of the CSO is usually required to finalise 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?

Banks must undertake CDD measures and on-going monitoring for existing and new customers in accordance with the *Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)* (the "**AMLO**").[3] The *Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions)* (the "**AML Guide**")[4] provides general guidance on this. Generally speaking, and as mentioned above, banks are required to carry out CDD to verify the identity of new customers, to verify that funds deposited are from a legitimate source, and to carry out on-going monitoring to identify suspicious transactions. In the case of a company or a CSO, due diligence will also be conducted on directors and beneficiary owners (as the case may be).

Where the money laundering and terrorist financing risks associated with a business relationship are high, banks will need to conduct enhanced due diligence, such as obtaining additional information on the customer, the intended nature of the business relationship, the source of wealth or funds of the customer, etc. If the CSO is itself, or its directors are identified as, "politically exposed person(s)," banks will conduct enhanced due diligence prior to account opening and throughout the banking relationship.

Furthermore, banks are required to continuously monitor their business relationship with the customer, including but not limited to review from time-to-time documents, data, and information relating to the customer and to scrutinize the transactions of the customer to ensure that they are consistent with banks' knowledge of the customer and the customer's business, risk profile, and source of funds.

CSOs will need to provide the CDD information required from the banks, including as mentioned above, the documents required to open the bank accounts in the name of the CSOs, in order for the banks to be able to comply with their CDD requirements, failing

3 https://www.elegislation.gov.hk/hk/cap615?xpid=ID_1438403530197_001

4 https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/Guideline_on_AML-CFT_(for_AIs)_eng_May%202023.pdf

which CSOs will not be able to open or continue operating an account with the banks.

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

While the specific internal principles and systems for monitoring "suspicious transactions" are proprietary to the banks and not publicly available, in general, paragraph 7.7 of the AML Guide requires banks to implement appropriate anti-money laundering and counter-financing of terrorism policies, procedures, and controls (the "**AML/CFT Systems**") in order to fulfil their statutory reporting obligations for suspicious transactions, and properly manage and mitigate the risks associated with any customer or transaction involved in a suspicious transaction report.

The AML/CFT Systems should include:

(a) appointment of a Money Laundering Reporting Officer;

(b) implementing clear policies and procedures over internal reporting, reporting to the Joint Financial Intelligence Unit of the Hong Kong Government, post-reporting risk mitigation, and prevention of tipping off; and

(c) keeping proper records of internal reports and suspicious transaction reports.

Meanwhile, banks have the obligation to conduct ongoing check to ensure that their AML/CFT Systems in relation to suspicious transaction reporting comply with relevant legal and regulatory requirements and operate effectively.

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

Hong Kong fully implements targeted financial sanctions in compliance with United Nations Security Council Resolutions, which are implemented in Hong Kong via the *United Nations Sanctions Ordinance (Cap. 537)* ("**UNSO**")[5] and *United Nations*

5 https://www.elegislation.gov.hk/hk/cap537

(Anti-Terrorism Measures) Ordinance (Cap. 575) ("**UNATMO**").[6] The Hong Kong Monetary Authority mandates the banks to maintain a database of individuals and entities designated under UNSO and UNATMO for customer and transaction screening purposes.

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

Paragraph 4.15.1 of the AML Guide requires banks to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons from jurisdictions for which this is called for by the Financial Action Task Force.

The statement[7] issued by the Financial Action Task Force in February 2023 identified three high-risk jurisdictions and called for members to apply enhanced due diligence measures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing risks emanating from these countries:

(a) Democratic People's Republic of Korea;

(b) Iran; and

(c) Myanmar.

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

The Hong Kong Monetary Authority ("HKMA") expects banks to adopt a risk-based approach with their customers, which means that banks should differentiate the risk levels of individual customers in accordance with their backgrounds and circumstances, and apply proportionate risk-mitigating and CDD measures, rather than simply adopting a "one-size-fits-all" approach to all customers in the approval process.

Generally speaking, banks should establish and maintain effective policies, procedures, and controls to comply with the terrorist financing, financial sanctions, and proliferation financing-related legislations and regulations. There is no special procedure or policy targeting CSO clients in this case.

When there are high-risk jurisdictions involved, banks should conduct enhanced due diligence measures set out in paragraph 4.9 of the AML Guide, such as obtaining approval from their senior management to establish a business relationship that presents a high money laundering and terrorist financing risk

6 https://www.elegislation.gov.hk/hk/cap575

7 https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-February-2023.html

or requesting for additional information from the customer in relation to the customer's identity, intended nature of the business relationship, source of funds, and reasons for intended or performed transactions.

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?

Banks would normally be required to comply with their own regulatory reporting requirements and the requirements under the AMLO, including to the financial regulators such as HKMA. However, in general, banks are not required to provide CSO clients' financial information to regulatory authorities or public officials, unless under a specific Hong Kong court order/ warrant or there are requests from law enforcement agencies, which legally compel the banks to disclose information and in accordance with applicable laws and regulations. In this case, banks should handle such requests for disclosure of CSO clients' financial information with caution and in accordance with the *Personal Data (Privacy) Ordinance (Cap. 486)* (the "**PDPO**").[8] In the event that there are grounds of knowledge or suspicion of suspicious transactions after internal review, banks should report to the Joint Financial Intelligence Unit by observing the relevant procedures on reporting suspicious transactions set out in the AML Guide. The types of information that would be in a suspicious transaction report include:

1. Triggering factors (e.g., crime involved, warrant/court orders received, news/list of regulatory agencies, pattern of suspicious transaction);
2. Background of the subject (e.g., date of establishment, business nature, expected transaction amount);
3. Transactions (e.g., review period, fund movement pattern, total amount deposited/withdrawn, suspicious transaction patterns); and

8 https://www.elegislation.gov.hk/hk/cap486

4. Reporting entities' enquiries & open-source information (e.g., suspicious indicators, KYC queries, world check, links to news reports).

Furthermore, there are reporting obligations under the National Security Law in respect of offence-related property. *The Hong Kong Association of Banks*[9] advised that banks should disclose property held by any client who is arrested or charged for an offence endangering national security or when they have knowledge or suspicion that a property is "offence related property" after receiving information from law enforcement agencies.

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

Banks should ensure that their data privacy policies and practices comply with the requirements under the PDPO[10] and any relevant codes of practice, rules, or guidance issued or approved by the Office of the Privacy Commissioner for Personal Data in protecting their clients' personal data.

Banks need to manage clients' personal data properly throughout the entire life cycle, from collection to disposal, and with due regard to data integrity, use, security, and access. Examples of clients' personal data include their names, addresses, telephone numbers, identity card numbers, dates of birth, occupations, account information, financial information, etc. When handling clients' personal data, banks as data users must observe the following six data protection principles set out in Schedule 1 to the PDPO:

(a) personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user; all practical steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred; data collected should be necessary but not excessive;

(b) practical steps shall be taken to ensure that personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used;

(c) personal data is used for the purpose for which the data is collected or for a directly-related purpose, unless voluntary and

9 https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/AML_FAQ_20221005.pdf

10 https://www.elegislation.gov.hk/hk/cap486

explicit consent is obtained from the data subject;

(d) a data user needs to take practical steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss, or use;

(e) a data user must take practical steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used; and

(f) a data subject must be given access to his personal data and to make corrections where the data is inaccurate.

In addition, banks should refer to various codes of practice for practical guidance in respect of any requirements under the PDPO imposed on data users. For example, the collection of Hong Kong identity card numbers or other identification document numbers should follow the Code of Practice on the Identity Card Number and other Personal Identifiers.[11] The Code of Practice on Consumer Credit Data[12] sets out guidance for banks as credit providers on the handling of consumer credit data through credit reference agencies. Further, comprehensive protection regimes mandated to the banking industry are set out in the Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry.[13]

From a practical perspective, banks are advised to adopt good practices to comply with the requirements of the PDPO. For example, an adequate Personal Information Collection Statement that includes information such as the purpose of data collection, third parties to whom the personal data may be transferred, whether it is obligatory or voluntary for the individuals to supply their personal data, consequences of failing to supply the obligatory information, individuals' right of access and correction of their personal data, etc. shall be sent to the clients on or before collecting clients' personal data. Banks should also devise and implement clear privacy policies and practices in relation to the retention of clients' personal data, as well as inform clients of the security measures in place to protect the data during the data-sharing process and the safe disposal of the data after use.

Banks are generally liable for the acts of their staff, agents, and contractors and should therefore ensure that all staff members are alert in protecting personal data and implement security

11 https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/picode_en.pdf

12 https://www.pcpd.org.hk/english/publications/files/CCDCode_2011_e.pdf

13 https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_banking_e.pdf

control to prevent data loss or leakage.

Please refer to the Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry for more details.

The Hong Kong Monetary Authority also issued a circular on Customer Data Protection[14] and its update[15] setting out the importance in protecting confidentiality of customer data (in particular clients' personal data) and control measures for protecting customer data.

CSOs are also reminded that under the PDPO, there is a general right for data subjects to issue a data access request to banks that hold personal data belonging to the CSO, and can be made via a prescribed form[16] as issued by the Privacy Commissioner for Personal Data.

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

Banks have no specific reporting obligations to inform governments about CSO banking in normal circumstances. Standard requirements shall apply. Please refer to section 3(a) above.

Going forward, however, it will be prudent to continually monitor any new legislation on online fundraising. The Hong Kong government has sought consultations from December 2022 to March 2023 on regulating online fundraising and crowdfunding, and are currently considering the responses from the industry (see the press release issued by the Hong Kong government on 26 April 2023 online[17]). Based on past practices, the Hong Kong government may roll out legislation on the same in due course. If the suggested scope in the consultation papers stands, soliciting online donations will likely be a regulated activity. Should any such legislation be passed, CSOs which illicitly conduct crowdfunding may be reported by banks to the relevant authorities.

---

14 https://www.hkma.gov.hk/eng/regulatory-resources/regulatory-guides/circulars/2008/07/circu_20080710-1/

15 https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf

16 https://www.pcpd.org.hk/english/publications/files/Dforme.pdf

17 https://www.info.gov.hk/gia/general/202304/26/P2023042500449.htm

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

As mentioned above, the UNSO[18] and the UNATMO[19] are generally applied in Hong Kong. The Hong Kong Monetary Authority,[20] though stating that banks are not obliged to implement unilateral sanctions imposed by foreign governments, reminds banks to carefully assess the risks and properly manage all relevant risks and strive to treat customers fairly. In fact, certain banks in Hong Kong are affected by the sanctions enacted by the US, the UK, and the EU when handling their Russian clients.

18 https://www.elegislation.gov.hk/hk/cap537
19 https://www.elegislation.gov.hk/hk/cap575?p0=1&p1=1
20 https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200808e1.pdf

PILnet

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