European Center for
Not-for-Profit Law

Navigating access to financial services for CSOs

A practical guidance

Introduction

Civil society organizations (CSOs) often face difficulty in accessing financial services in banks or other financial institutions. Based on previous research we know that such financial difficulties are complex and multi-factored. They can be driven by **a lack of regulatory support and guidance for financial institutions and CSOs**, highlighting the **absence of incentives** to address the issue in a meaningful way. It is also the result of **lack of knowledge** by financial institutions on how CSOs operate in practice and how this logic differs from private business operations.

With this Practical Guidance, ECNL aims to provide **experience-based insight** into the customer risk profiling and monitoring practices for CSOs across financial institutions – namely, banks. We also provide **recommendations** for navigating the often opaque and complex system, based on current and concrete practices of financial institutions without analyzing if these are fully compatible with the international anti money laundering and counter-terrorism financing (AML/CFT) measures or international human rights law and humanitarian law standards. From the CSO perspective, it is crucial to understand, unpack and know in advance what is expected or required in their context, with aim to foster more understanding and dialogue between the CSO sector and the financial institutions. It is also relevant for donors and funders to acknowledge difficulties in accomplishing some actions (such as opening a separate bank account by a CSO) and to provide support to civil society as they navigate through burdensome financial requirements.

Glossary

Customer Due Diligence: the act of collecting identifying information in order to verify a customer's identity and more accurately assess the level of risk they present.[1]

Financial institution: any natural or legal person who conducts as a business one or more activities or operations for or on behalf of a customer, such as acceptance of deposits and other repayable funds from the public, lending money or value transfer services, issuing and managing means of payment, etc[2].

Onboarding: the process through which a customer establishes a relationship with the bank and provides all of the necessary information for the bank to open an account.[3]

[1] https://complyadvantage.com/insights/cdd-customer-due-diligence/

[2] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[3] https://www.elixirr.com/2016/11/customer-onboarding-banking/

Politically Exposed Person: individuals who are or have been entrusted with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.[4]

1. What is a financial institution's process of including a new customer?

Check ECNL's video on financial access issues here: https://youtu.be/p3xcoGX3Pc0

- CSOs are subject to Customer Due Diligence (CDD) based on FATF standards.
- CDD is performed to all persons and legal entities opening an account or having a business relationship with a financial institution (bank), not only CSOs.
- Financial institutions research, discuss with the customer and establish expected transactions and activities of their customers prior to account opening. This is part of the onboarding - a process of including a new customer.
- During the onboarding of a CSO, financial institutions collect information to ensure that the potential CSO customer has the right internal governance, systems and financial controls in place.
- The following are among the documents that are typically asked to verify the customer governance and control structure:
  - Legal entity registration
  - Legal and governance structure
  - Statutes
  - CRS / FATCA form (FATCA - Foreign Account Tax Compliance Act is legislation to prevent tax evasion by US persons. CRS - Common Reporting Standard is the global non-US equivalent of FATCA)
  - Authenticated copy of identification (legal representative)
  - If possible, annual report
  - Evidence of review and/or sign-off by relevant charity commission or regulator (if applicable)
  - Annually (not in the beginning but afterwards) audited accounts
  - Certificate from registration authority, confirming the names of the members of the Board and/or the Founders of the CSO
  - Clean criminal record for founders/board members and/or declaration confirming that no record

[4] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

- Financial institutions create an activity and risk profile of their customers. To do this, they typically ask the following questions:
    - Why are you opening an account in this jurisdiction? Is it logical, rational, and plausible for you to open it here?
    - What are the expected incoming and outgoing money flows?
    - What kind of transactions and other activities are expected on the account you seek to open?
    - What are your activities, which sector are you operating in and what countries do you have dealings with?
    - Are you a Politically Exposed Person (PEP) or are you affiliated to a PEP?
    - Are transactions being carried out in connection with a high-risk country as defined by our jurisdiction, our organisation and/or the FATF?
    - What is the expected turnover on the account (currencies, products, and services, donations)?

- In addition, the CSOs along with any other customers are screened on an ongoing basis, for adverse media as well as targeted financial sanctions (including commercially compiled sanctions lists, lists of high-risk individuals, etc.). These commercial databases might include flawed or unverified information that may end up guiding decisions about (un) acceptable customer risk profiles.
- Different risk criteria related to the customer risk will be considered, such as the type of customer (human or legal person), economic activity, origin of funds, real and/or estimated transactional volume of operations, nationality and residence.
- Final step is assigning the customer a risk profile that will form the basis of ongoing monitoring. Financial institutions use international guidelines in assigning each of customer groups a different risk level for money laundering or terrorist financing, balanced with their own 'risk appetite'.

2. What is considered suspicious activities or transactions from the financial institution perspective?

- Financial institutions are required to scrutinise the transactions undertaken throughout the course of the relationship with their customers. This process is called transaction monitoring.
- During the transactions monitoring of CSOs, financial institutions compare actual transactions versus expected/mapped/profiled of the customer during the onboarding process, based on the information gathered by asking the above questions. *The activities need to match the profile of the customer, otherwise red flags are raised.*
- Anything out of character that does not match the profile raises red flags. The financial institutions are then required to investigate why there are

discrepancies between the expected and actual transactions, which is time and resource consuming for the financial institutions and also for CSOs.

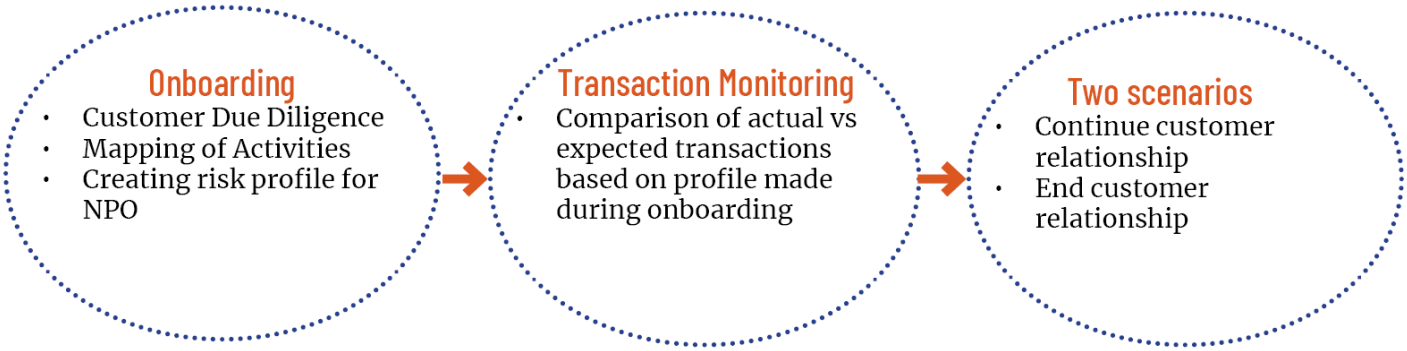
- **Examples of typical red flags for any customer:**
  - sending money to regions/countries CSOs have not listed as place of their activities;
  - receiving strange amounts of money from strange or unknown sources;
  - withdrawing and deposing cash;
  - receiving odd amounts;
  - origin or destination of the money is unclear or unknown;
  - transaction was executed with a (foreign) counterparty who is insufficiently verifiable through third party or open-source verification tools;
  - transaction was executed with a counterparty over whom there has been adverse media reports;
  - customer's statement about the transaction is unclear and cannot be sufficiently substantiated by documentation;
  - unusual transaction frequency and/or volume;
  - transactions with high-risk countries;
  - transactions with sanctioned customers and/or countries;
  - transactions with politically exposed persons (PEPs);
  - cross border payments that are out of character;
  - buzz words that match pre-defined terms that are identified as indicative of suspicious activity such as Islam, jihad, etc.
  - The goal of the donation is not in line with the NPOs scope of work.

- **Further red flags that are considered for the CSO sector:**
  - CSO uses crowdfunding and social media to solicit donations, then its online presence vanishes or shuts down;
  - Unusual feature CSO account shows signs of unexplained increases in deposits and transaction activity;
  - CSO is unable to account for the final use of all its funds/resources;
  - CSO uses unnecessarily complex banking arrangements or financial networks for its operations, particularly overseas;
  - CSO, or CSO representatives, use falsified or conflicting documentation;
  - Unexpected absence of contributions from donors located in the country;
  - CSO appears to have few or no staff and limited or no physical presence, which is at odds with its stated purpose and scale of financial activity;
  - CSO funds commingled with personal/private or business funds.

- Investigation launched by the red flag includes consulting internal records to learn about any previous risk assessments and transactions of CSO which might have been internally reported in the past.
- After conducting the initial research, the analyst might decide that a customer outreach procedure should be initiated: a relationship manager or the person or

unit responsible for the customer needs to approach CSO and request clarification.

- The production of an (un)acceptable customer risk report is highly dependent on the expertise and subjectivity of the particular analyst.
- In addition, ongoing monitoring includes screening customers for inclusion on sanctions and PEP lists, media sources for bad press on individuals or CSOs.
- External providers offer major financial institutions 'adverse media screening' (also called 'bad press screening') that is defined as "any kind of unfavourable information found across a wide variety of news sources – both 'traditional' news outlets and those from unstructured sources".
- There is also social media monitoring software that enables social media activity to be included in the monitoring process.
- Based on customer reviews, financial institutions can make several security decisions.
    - They can come to an agreement with a customer after customer queries are posed and answered by the customer. In many cases, no action can, or need be taken, or the institution may amend the customers risk profile and initiate increased monitoring.
    - However, the financial institution may decide that the risk profile of a customer is unacceptable, and the customer should be 'offboarded', and account closed.



3. How to address issues on a practical level to make the process less harmful

A number of typical "red flags" for the financial institution present usual, typical activity or situation from the non profit practice and CSO operations. Receiving odd amounts from various donors, transactions with new countries due to newly approved projects (not listed in initial conversation during onboarding process), less physical staff then expected (because of e.g. large number of volunteers on the

Learn more at
ECNL's Learning Center:
https://learningcenter.ecnl.org/

ground), transactions with high risk countries (where aid and services are needed), online crowdfunding, absence of donors in resident country – all of these are common situations in civil society domain yet appear risky from financial and business perspective.

In countries where it is possible, it is necessary to promote strategic dialogues between CSOs, banking associations, authorities to jointly address these bank practices and find a common denominator of requirements that satisfy compliance with the supervision activities of banking entities, but that do not hinder the legitimate work of CSOs.

In addition to enhanced education and advocacy towards regulators and financial institutions, **here is what CSOs can do in practice to alleviate some of these issues**:

a) Initially, investigate the financial institution requirements and arrive knowing that you have all (or most) required information.
b) Provide ample information during *onboarding* process, be as open and transparent as possible about sources of funding and projects, activities and places of work, or possible future difficulties.
c) Ask the financial institution about the risks they consider in particular for CSO customers, what they use as reference for sanctions regime (e.g. what are high risk countries for sending or receiving funding) and other guidance for customers. Ask for written guidance if available.
d) Update the financial institution with the most recent information about your activities, work, donors, countries you operate in – at least once a year. Send them an email with this information and ask for a contact person.
e) If the nature of work or activities change (new significant projects are undertaken, new donors, new risk countries) or CSOs start transactions with countries potentially in crisis or high-risk areas (ask financial institution which are high risk areas for them), notify the financial institution immediately.
f) Always notify the financial institution before undertaking transactions to/from high-risk countries.
g) If you need to deposit or withdraw cash in large amounts or frequently, notify the financial institution in advance.
h) If there are adverse media reports (bad press) about your organisation, work, staff, donors or partners, communicate with the financial institution about those and explain the situation, showing why it is false or misunderstood.
i) Make sure to have proper documentation that can support and justify every transaction. Try to agree in advance with the financial institution representative what supporting information they will accept to justify the transaction.
j) Ask the banks for "interpretation" or interpretative notes of suspicious indicators or expected customer behaviour based on NPO risk profile.

European Center for
Not-for-Profit Law

European Center for Not-for-Profit Law Stichting
5 Riviervismarkt, 2513 AM
The Hague, Netherlands
www.ecnl.org
twitter.com/enablingNGOlaw