Unintended consequences of AML/CTF regulation: the challenges of banking non-profit organisations

A review of onboarding and monitoring practices across financial institutions

European Center for
Not-for-Profit Law

European Center for
Not-for-Profit Law

A report prepared for the
European Center for Not-for-Profit
Law Stichting (ECNL)
by
Noémi També

December 2021

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

Sweden
Sverige

ICNL
INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW

This report was developed as part of the Technical Assistance Support in Kosovo and North Macedonia projects, managed by the European Center for Not-for-Profit Law Stichting (ECNL). The project is made possible by the International Center for Not-for-Profit Law (ICNL) through the Civic Space Initiative. This publication is partially financed by the Government of Sweden. The Government of Sweden does not necessarily share the opinions here within expressed. The author bears the sole responsibility for the content.

PREFACE

In the past 20 years, the policies of regulators and banks to address anti-money laundering and counter-terrorism financing (AML/CFT) risks have created an additional layer of challenges for the nonprofit sector. Nonprofits are still considered as a high(er) risk sector, even though there is scarce evidence to support that. Financial institutions' risk scoring and profiling mechanism track if organisations work on "risky" issues or with "risky" areas and countries, building a specific level of risk profile of nonprofits. Moreover, each financial institution does its own risk-based approach that might not be consistent or mutually coherent, leaving the sector scramble for guidance that is often lacking or difficult to understand, especially for the majority of (mostly small size) organisations.

The Financial Action Task Force (FATF), as a key global standard setter on AML/CFT issues, has identified the wholesale de-risking of nonprofits as a problem, and most recently highlighted as such through its unintended consequences work stream. The 2021 FATF Stocktake of the Unintended Consequences of the FATF Standards warns that, despite ongoing efforts, de-risking and financial exclusion remain challenges for many sectors and run contrary to the risk-based approach promoted by the FATF. Moreover, various research papers* indicate that the FATF Standards and/or their incorrect implementation have an impact on furthering and sustaining these phenomena. Therefore, the FATF plans to propose measures to address these issues during 2022.

De-risking is fueled by other considerations. For example, national level regulators interpret strictly and narrowly the AML/CFT standards and their guidance to the financial institutions. In addition, governments do not enhance financial inclusion efforts and take their share of the risk when financing organisations conducting essential and humanitarian services in "risky areas".

With this report, the European Center for Not-for-Profit Law (ECNL) aims to provide insight into the onboarding and monitoring practices for nonprofit sector across financial institutions. We also provide recommendations for further actions in tackling the root causes of financial exclusion for the nonprofit sector. The report does not assess in detail whether the presented practices of financial institutions are compatible with the international AML/CFT or international human rights law and humanitarian law standards. We hope that findings and recommendations from this report will contribute to an increased understanding of different sectoral positions, actions and drivers, and facilitate national level action to help bring the nonprofit sector closer to a full financial inclusion.

---

* See for example: https://fatfplatform.org/news/new-report-a-business-and-human-rights-perspective-on-bank-de-risking-of-non-profit-clients/https://ecnl.org/publications/understanding-drivers-de-risking-and-impact-civil-society-organizations or https://fatfplatform.org/news/new-report-a-business-and-human-rights-perspective-on-bank-de-risking-of-non-profit-clients/

GLOSSARY OF ABBREVIATIONS

AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Counter Finance Terrorism
CTR	Currency Transaction Reports
ECNL	European Center for Not-for-Profit Law
EDD	Enhanced Due Diligence
ESG	Environmental, Social and Governance
EU	European Union
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
KYC	Know Your Customers
LEA	Law Enforcement Agency
ML	Money Laundering
MLRO	Money Laundering Reporting Office
MSB	Money Service Business
NRA	National Risk Assessment
NPO	Non-Profit Organisation
OE	Obliged Entity
PEP	Politically Exposed Person
RBA	Risk-Based Approach
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorism Financing

EXECUTIVE SUMMARY

"Although de-risking is the empirical manifestation of financial institutions' appetite to risk"[1], de-risking is currently narrowly defined as "the phenomenon of financial institutions (FIs) terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk in line with the Financial Action Task Force's risk-based approach"[2].

This research aims to understand the extent to which FIs are responsible for de-risking through their internal processes and controls. However, interviews of financial crime practitioners and experts, analysis of responses to the European Center for Not-for-Profit Law (ECNL) designed questionnaires as well as desk-based reviews of open-source material, indicate that de-risking is complex and multi-factored. It is driven by a lack of regulatory support and guidance highlighting the absence of incentives to address de-risking in a meaningful way. In addition, it is the result of the failure to understand that banking NPOs, exposes FIs to financial, legal, reputational, and regulatory risks. Those risks may be low probability, but they are nonetheless high impact. Finally, de-risking is also the result of the low profits/high costs equation that FIs face.

To address those points, an incentivisation strategy needs to be devised to ensure that regulators provide adequate support and guidance to both, the banking and NPO sectors.

In addition, assessing the different risk categories that FIs face beyond TF and ML when banking NPOs, is essential. This would enable the implementation of a truly risk-based supervision and facilitate a risk-based approach to banking NPOs. Furthermore, the NPO sector being heterogeneous in terms of size, activities, profile, goals and modus operandi, an assessment of key risk characteristics needs to be performed to enable FIs to target their efforts and resources adequately.

Also, key stakeholders need to have a clear understanding of their respective responsibilities and accountabilities with regards to preserving the integrity of society through the support of the financial sector.

---

1 També Bearpark, N. and Demetis, D. (2021) 'Re-thinking De-risking: A systems theoretical Approach'. Journal of Money Laundering Control. Available online: https://www.emerald.com/insight/content/doi/10.1108/JMLC-04-2021-0030/full/html

2 FATF (2014) 'Guidance for a risk based approach: the banking sector', para. 1. .Available online: http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf . Paris: FATF.

Finally, to move away from what can often be described as anecdotal grievances, a cost benefit analysis of banking NPOs should be performed across a selection of FIs. This would facilitate multi-stakeholder dialogue on de-risking and enable both, the banking and NPO sectors to assess the proportionality of current banking fees.

The four key issues can be summarised as follows:

- Lack of incentives for regulators in the provision of regulatory support and guidance to both FIs and NPOs.
- Multiple, layered, and complex risks faced by FIs when banking NPOs which are not accounted for.
- Lack of accountability with regards to the responsibility of preventing de-risking.
- High banking fees.

Based on the issues listed above, it is recommended to:

- Identify tools to effectively incentivise regulators to provide guidance and support to NPOs as well as FIs.
- Perform National Risk assessments[3] covering ML, TF, Fraud, Corruption, sanctions, liability, and regulatory risk to ensure that jurisdictions have a holistic understanding of the risks faced by FIs when providing products and services.
- Identify at-risk NPO subsets to understand the types of NPOs that are most vulnerable to financial crime thus facilitating a risk-based approach to banking NPOs.
- Discuss and agree at national level the roles and responsibilities of key stakeholders with regards to enabling and facilitating the prevention of de-risking. As part of this multistakeholder[4] discussion, the following should be explored:
    - The role of the regulators.
    - The use of technology such as Artificial Intelligence or Digital Identification tools to facilitate CDD and make it more affordable.
    - The appointment of a recognised NPO body (aligned to the Wolfsberg Group for instance) to agree on standards, principles, and best practice.
    - Education material to support the NPO sector.

3 This NRA could also be performed at regional level as illustrated by the Commonwealth of Australia (refer to footnote no. 15).

4 The following entities and bodies should be part of this multistakeholder dialogue: High-risk NPOs, the FATF, the regulator, Banking Association, Central Bank, FIU, Ministry of Finance, Civil Society Organisations that support the issue of de-risking, Think Tanks.

- Assess the cost faced by FIs when onboarding and monitoring NPOs.
- Perform a survey to assess banking fees faced by NPOs.
- Explore feasibility of having fees and/or costs of NPO onboarding and monitoring being subsidised at government and/or donor level.

BACKGROUND AND INTRODUCTION

In March 2021, the Financial Action Task Force (FATF) which sets binding and mandatory international standards for Anti-Money Laundering (AML) and Counter Finance Terrorism (CFT), announced it would launch a new initiative to review and address the "unintended consequences of poorly implemented AML/CFT measures – from financial exclusion to the abuse of counter terrorism measures to suppress civil society"[5]. The FATF identified four main affected areas: de-risking; financial exclusion; suppression of non-profit organisations or the non-profit sector as a whole; and threats to fundamental human rights. It has committed to consider on an ongoing basis how these risks can be better identified and mitigated.

The research project initiated by ECNL in October 2021 is particularly apt as it aims to map across a selection of jurisdictions the way Financial Institutions (FIs) determine suspicious transactions for Non-Profit Organisations (NPOs) and how this manifests into the de-risking of the latter (1) which has wider repercussions on financial exclusion and the NPO sector's ability to continue accessing the formal financial system. In essence, it directly explores three of the FATF's identified areas. Furthermore, the research looks at collecting criteria and principles used for NPOs' transaction monitoring (2). Finally, it aspires to deliver a set of recommendations based on the field work and findings. The research aims to better understand the root causes of de-risking.

This report documents practices in relation to onboarding and monitoring of NPOs as observed within a selection of FIs based across multiple jurisdictions. This report does not aim to document onboarding and monitoring best practice nor assess whether these practices are in line with FATF and human rights standards.

5 Lewis, D. (2021) 'Speech at the Chatham House Illicit Financial Flows Conference, 1-2 March 2021'. Available online: https://www.fatf-gafi.org/publications/fatfgeneral/documents/chatham-house-march-2021.html.

METHODOLOGY

A total of 12 financial crime risk practitioners and experts were interviewed between 12th October and 18th November. Interviewees operate within the banking industry (private, retail and corporate banking), Payment Services Businesses, Money Services Businesses, Think Tanks, NPOs and financial services consultancy. The sample was selected to ensure that relevant stakeholders impacted by the phenomenon of de-risking were represented and interviewed. Furthermore, interviews with Think Tanks and consultancies triangulated and validated the information obtained by stakeholders, enabling the researcher to minimise any potential bias. Practitioners that were interviewed, have experience and knowledge that spans across Australia, the Middle East, Latin America, Luxembourg, the Netherlands, Switzerland, Turkey, Great Britain, and the United States. Three of those risk practitioners work, or have worked, for international financial institutions that operate a network of business entities across the globe.

Interviews were semi-structured and conducted via videoconferencing phone conversations. Although no Non-Disclosure Agreements were signed, the consultant agreed to maintain the anonymity of the interviewees and institutions they work for or have worked for. Table 1 lists interviewees, job profile, institution type, and jurisdiction.

Inter-viewee	Role, Sector, Jurisdiction
1	Executive Director of policy advocacy NPO, Netherlands
2	Global Transaction Monitoring Controls, Banking, Global reach (includes the U.S.)
3	AML Risk Practitioner and consultant, Private Banking, Australia and the U.S.
4	Expert on de-risking, public sector, Latin America
5	Chief Executive Officer, Payment Services Provider, Middle East
6	Executive Director, Money Services Businesses, UK, Scandinavia and Russia
7	Research Fellow, Think Tank and Charity, International reach
8	Chief AML Officer, Retail, Corporate and Private Banking, Turkey
9	Risk Practitioner and Consultant, UK
10	Relationship Manager, Corporate Banking, Netherlands
11	Head of AML, Correspondent Bank, UK and Luxembourg
12	Chief AML Officer, Private Banking; Switzerland, UK, and the U.S.

Table 1: List of interviewees

In addition, ECNL sent the consultant questionnaires filled by FIs operating in France, Germany, Luxembourg, Poland and the United Kingdom. The questionnaire was designed by ECNL prior to the consultant being contracted. The questionnaire collates information relating to due diligence requirements, transaction monitoring criteria, restrictions relating to providing banking activities within specific jurisdictions and reporting requirements. The consultant was not involved in the design and dissemination of the questionnaire and does not know the identity of the respondents nor the type of institution they work for. The consultant has reviewed the responses collected by ECNL. Review of those responses validates the data collected during field work.

Finally, the consultant performed a desk-based review of open-source material, media reports, grey literature as well as governmental policies and reports.

1. How do FIs determine suspicious transactions for the NPO sector? How does this translate into NPO de-risking?

All risk practitioners interviewed have confirmed that NPOs are subject to Customer Due Diligence (CDD) and where applicable, to Enhanced Due Diligence as per FATF standards. Those requirements apply to all persons and/or legal entities opening an account or having a business relationship with an FI. The exception was interviewee 8 who explained that as per Turkish regulatory requirement (Law. No. 7262 on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction), FIs are required to automatically identify NPOs as high risk and perform Enhanced Due Diligence (EDD) regardless of the NPOs actual risk profile. This regulatory requirement is not aligned to the FATF's Recommendation to apply a risk-based approach to risk management and supervision. The EDD process is documented in Box 2.

FIs do not determine suspicious transactions prior to conducting customers' Due Diligence (CDD) during onboarding. FIs research, discuss and establish expected transactions and activities of their customers prior to account opening. If the FI identifies through transaction monitoring and ongoing due diligence that actual transactions and/or behaviour is not aligned to expected transactions and/or behaviour (mapped during onboarding), the said activity will be flagged as suspicious. If neither the alert analyst, the investigator assigned to the case nor the relationship manager identify a rationale to explain the out of character transactions and/or behaviour, a suspicious activity report (SAR) is logged with the Financial Intelligence Unit (FIU). The FIU is then in charge of reviewing the SAR to determine whether

it will be archived or analysed. Each FIU has its own method and criteria for determining whether a SAR is archived or analysed. This is not discussed in this report as it is not in the scope of the mandated research.

Transaction Monitoring of NPOs does not drive NPO de-risking. The fieldwork indicates that de-risking of NPOs is driven by other factors. This is documented in Section 3.

a. Onboarding:

At onboarding of a new client, whether a company/business, an NPO or a private individual, Financial Institutions (FIs) are required, as per FATF Recommendation 10, to undertake Customer Due Diligence (CDD). This principle is set out in law as prescribed by the European Union's AML 4th Directive (Article 10-14) for EU Member States. Jurisdictions outside of the EU are also subject to such legal and regulatory requirements (driven by the FATF 40 Recommendations). In addition, as per FATF Recommendation 8, FIs need to ensure that the NPO it is banking is not misused for the purpose of financial crime.

As part of the CDD documented in Box 1, at onboarding of an NPO, the FI collects further information to ensure that the potential customer has the right internal governance, systems and controls in place. This aims to give the FI assurance that the NPO has a thorough understanding of its legal and/or regulatory responsibilities and is less likely to be vulnerable to threats of fraud, bribery, terrorism financing, sanctions violations, or the laundering or proceeds of crime such as corruption for example. This in turn protects the banking institution from exposure to regulatory, reputational, ML, TF, sanctions, bribery/Corruption and regulatory risk.

Box 1: Standard Customer Due Diligence measures

a. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

b. Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the

transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to undertake customer due diligence (CDD) measures when:

i. establishing business relations;

ii. carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

iii. there is a suspicion of money laundering or terrorist financing; or

iv. the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

Source: FATF Recommendations, 2012-2021

To obtain such assurance, the following documentation is typically required during onboarding (note that this may vary across jurisdictions):

- Chamber of Commerce registration
- Legal and governance structure
- Statutes
- CRS / FATCA form
- Authenticated copy of identification
- Private address data Ultimate Beneficial Ownership control
- If possible, annual report
- Evidence of review and/or sign-off by relevant charity commission or regulator (if applicable)

b. Transaction Monitoring:

As per the FATF Recommendation 10 and the European Union's AML 4th Directive (Article 13) CDD measures require FIs to scrutinise transactions undertaken throughout the course of the relationship with their customers. This is called transaction monitoring. To perform transaction monitoring, FIs need to understand the activities undertaken by their client. This includes mapping transactions and activity profile. More specifically, the FI will collect information relating to the kind of transactions that will be performed, frequency of transactions, activities, counterparts, and jurisdictions within which NPOs' activities are performed. Boldly: 'what are

you doing, why are you doing it, where are you doing it, who are you doing it with and how often are you doing it'.

The FIs will therefore seek to establish a profile of activity and behaviour by asking a set of questions as follows:

- Why are you opening an account in this jurisdiction? Is it logical, rational, and plausible?
- What are the 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) you seek to open?

Box 2: Enhanced Due Diligence (EDD)

The fourth AML Directive (EU) 2015/849 lists specific cases that firms must always treat as high risk:

- Where the customer, or the customer's beneficial owner, is a PEP. A PEP is a natural person who is or who has been entrusted with prominent public functions (Article 3).
- Where a firm enters a correspondent relationship with a respondent institution from a non-EEA state.
- Where a firm deals with natural persons or legal entities established in high-risk third countries.
- All complex and unusually large transactions, or unusual patterns of transactions, that have no obvious economic or lawful purpose

Source: EU 4th AML Directive, Article 18.

Once the above information is obtained and the FI has established the expected transaction and activity profile of the NPO, the NPO will be monitored against the information provided at onboarding. The transaction monitoring rules are calibrated for the customer in line with the information that is provided during the CDD process. In addition, the NPO along with any other customers are screened on an ongoing basis, for adverse media as well as targeted financial sanctions as per United Nations Security Council

Resolutions and other sanctions list should the FI be operating within jurisdictions that have their own sanctions lists in place (for example, Japan, Australia, the U.S., the E.U.). Clients are generally screened against U.S. sanctions because FIs typically rely on U.S. based FIs to provide correspondent banking. A correspondent banking relationship enables a bank (in this case a respondent bank) to provide its own customers with cross-border products and services in a jurisdiction that it does not have a presence in. Preserving a correspondent banking relationship is essential.

Transaction monitoring scenarios and thresholds are not discussed without a Non-Disclosure Agreement and are not publicly available. FIs and financial Crime risk practitioners do not advertise their internal scenarios and/or thresholds to potential money launderers and terrorist financiers. The latter may use such information to circumvent controls by operating just below advertised thresholds for instance.

It is important to note that banks may have varying thresholds when determining which transaction will be subject to individual review prior to processing them. This is determined by the CDD process and is also in line with Article 11 of the 4th AML Directive and the FATF Recommendation 16.

Table 2 documents the specific monitoring processes and controls reported by interviewees when discussing CDD performed and transaction monitoring

Inter-viewee	Monitoring process/controls
2	It really is a question of mapping expected behaviour against actual behaviour. If there are discrepancies, it will generate an alert. When unexpected behaviour is picked by the transaction monitoring tool, we also perform additional checks on charities' websites as well as on other websites likely to document relevant information to see if any unexpected behaviour is documented. For example, there could be a new project that the NPO has omitted to discuss with the relationship manager. We also welcome NPOs coming in advance to warn us about out of character activities. Transparency from NPOs is welcome. When there is no advance warning of out of character transactions (for example dealings with Afghanistan without prior history of such dealings), an alert will be generated and will require AML/CTF analysts and investigators to undertake research and liaise with Relationship Managers who will in turn have to contact their clients to understand the transaction, the source of wealth, the source of funds[6]. This is a costly exercise for the FI. We also aim to understand the nature of the business that the NPO conducts. This will determine the NPO's risk profile. Does it support an orphanage in Chad or a cats' charity in the Northwest of England? This will help us determine what transaction is out of character and which one is not. Also, if the nature of your business has changed, we want to know and we want to know why.
3	We map the customer's expected activity and behaviour. The client is not identified as an NPO on the system. The only element that generates a 'red flag' is when the activity and behaviour picked by the transaction monitoring tool does not match expected activity and behaviour of customer, regardless of whether it is an NPO, a private customer of a corporate. The usual red flags are the following: • funds from 3rd parties • receiving odd amounts • wire transfers • cross country transfers • cash deposits and withdrawals (as could be sign that money is being physically carried across borders) • cash transactions • adverse media

6 The source of wealth is the origin of the customer's entire wealth. The source of funds is the origin of funds for the specific transaction and/or business relationship at hand.

8	Because of the Turkish regulatory requirement (Law No. 7262), NPOs are always categorized as High-Risk which of course means that Enhanced Due Diligence is required. Once a customer is High-Risk there is a yearly periodic review performed on the customer. It can happen more frequently if/when there is a trigger event such as adverse media for example. The transaction monitoring tool will screen money transfers, wire transfers, jurisdictions, volumes of flows. This is exactly what we screen for with other clients that will be categorized as High-Risk. NPOs are not targeted because of their NPO status. We truly want to support NPOs, but the issue is that NPOs are high risk especially when it comes to working with NPOs that support Syria's population and Syrian refugees in Turkey. Those NPOs are not able to provide any information as to who the Ultimate Beneficial Owner is. Our other concern is dealing with PEPs which of course may be indicative of corruption. When we refuse to onboard NPOs (our KYC data does not indicate a high rejection rate of NPOs), it will be because the NPO cannot provide sufficient background information, Source of Funds (SoF), connections, history, areas of interest, international reputation, military assistance to refugees. As per FATF standards, this is the information we need to get assurance that the NPO has the right governance and control framework in place: • General information about the donor • Purpose and nature of the donation • Monetary value of the donation • Source of funds for the donation • Geographic locations of the donor, particularly any higher-risk areas where terrorist groups are most active • Organizational structure of any entity donating, including key principals, management and internal controls of an entity making the donation • Beneficial ownership of an entity, if applicable • State incorporation, registration, and tax status of the donor • Donor entity financial statements, audits, and any self-assessment evaluations • Negative news screening

10	Our institution does not automatically apply a high-risk status to NPOs. Each NPO is assessed based on its profile. In the Netherlands there is an independent certification called the ANBI status[7]. To obtain ANBI status the NPO needs to provide supporting documentation such as tax declaration, chamber of commerce registration, original statutes/Articles of Incorporation including any notarized changes, human resource policy manual (or similar), Financial Statement, names and addresses of all Board members, identification for the applicant. In addition, the Netherlands Central Bureau for fundraising (CBF) regulates the charity sector which commits to meeting a set of standards established by an independent body, the Standards Committee. The CBF ensures that the NPO has a robust code of practice in place. The NPO, through ANBI status and CBF recognition, demonstrates that it meets strict quality requirements. Accordingly, at onboarding the FI will assign the NPO a "neutral risk" unless there a high-risk criterion associated to the NPO such as activity in a high-risk jurisdiction for instance which would warrant a high-risk categorisation. A customer regardless of whether it is an NPO or not, that has been rated neutral or medium risk will have its profile reviewed once every four years. This includes due diligence (as per Box 1). A customer regardless of whether it is an NPO or not, that has been rated high-risk will have its profile reviewed on a yearly basis. Internal governance, countries within which activities are conducted, counterparts, Source of Funds and Source of Wealth, transaction velocity and volume, destination of funds are reviewed. In addition, annual reports are also consulted to identify any potential discrepancies in the information that the NPO provides. Our transaction monitoring tools will issue alerts when: • The transaction doesn't match the client's profile • The origin or destination of the money is unclear or unknown • The transaction was executed with a (foreign) counterparty who is insufficiently verifiable by the FI through third party or open-source verification tools. • The transaction was executed with a counterparty over whom there has been adverse media reports • The client's statement about the transaction is unclear and cannot be sufficiently substantiated by documentation • There are buzzwords that match pre-defined terms that are identified as indicative of suspicious activity

7 In Dutch Algemeen Nut Beogende Instelling translated as Public Benefit Organisation. For more information refer to the ANBI website available online at https://anbi.nl. Additional information relating to

11	As a payment services institution we expect our clients to perform CDD on their clients. We have prohibited businesses and restricted businesses. This is based on our appetite to risk or based on our Business Ethics internal policy. Restricted Businesses are crypto businesses, gambling, the CBD industry, the adult industry and NPOs. We are a correspondent bank and therefore need to meet our regulatory requirements as per the FATF's Recommendation 13 and the UK's Money Laundering Regulation, performing onsite reviews of all our customers which are banks or payment service providers. Our transaction monitoring tools will issue alerts when there are: • Unusual transaction frequency and/or volume • Transactions with high-risk countries • Cross border payments that are out of character • Transactions with sanctioned customers and/or countries • Transactions with politically exposed persons (PEPs) • Adverse media stories involving customers • Buzz words such as Islam, jihad, NCC code (National Clearing Code: required for any payments that are made to bank accounts that don't have an International Bank Account Number (IBAN).

Table 2: Monitoring and CDD as reported by interviewees

2. Criteria and principles used regarding monitoring transactions on NPOs.

ML and TF typologies are reviewed and documented by the FATF as well as the Egmont Group which represents Financial Intelligence Units (FIUs) across the Globe[8]. FIUs are national intelligence organisations in charge of receiving, analysing and disseminating transactions and activities that have been flagged by FIs as being suspicious in terms of ML, TF or the financing of weapons of mass destruction (also called proliferation finance). Section 1.b and Table 2 document the criteria and principles used within the institutions that were interviewed to monitor customers and identify when their activities and behaviours trigger an alert that requires investigation.

In addition to the information collated through interviews and documented in Table 2, Table 3 below lists indicators of NPO misuse also called red flags.

reporting requirements is available online at: https://www.dcnanature.org/wp-content/uploads/2013/09/ANBI-explanation-and-application-process.pdf.

8 Egmont Group (2019) 'About'. Available online: https://egmontgroup.org/en/content/about

Such red flags can be used to monitor NPOs' transactions, activities and/or behaviours. Table 3 compiles information collated during research, and review of relevant grey literature and opensource AML material[9].

Out of character behaviour:

- NPO staff withdraws cash from the NPO account and then deposits it into a personal account, before diverting the funds to a suspected terrorist's account.
- Vague justifications and a lack of documentation when the financial institution questions NPO requests to transfer funds to high-risk locations or entities.
- Unusual or atypical large cash withdrawals, particularly after the financial institution refuses to wire NPO funds overseas (thus raising cross-border cash smuggling suspicions).
- NPO transactions for which there does not appear to be a logical economic purpose or link between the NPO's stated activities and the other parties in the transaction.
- NPO uses crowd funding and social media to solicit donations, then its online presence vanishes or shuts down.
- Unusual feature NPO's account shows signs of unexplained increases in deposits and transaction activity.
- NPO is unable to account for the final use of all its funds/resources.
- NPO uses unnecessarily complex banking arrangements or financial networks for its operations, particularly overseas.
- NPO, or NPO representatives, use falsified or conflicting documentation.
- Inconsistencies between the pattern or size of financial transactions and the stated purpose and activity of the organisation.
- Unexpected absence of contributions from donors located in the country.
- NPO 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.
- NPO funds commingled with personal/private or business funds.

9 The Commonwealth of Australia (2017) 'Non-Profit Organisations and Terrorism Financing: Regional Risk Assessment'. Available online at: https://www.austrac.gov.au/sites/default/files/2019-06/regional-NPO-risk-assessment-WEB-READY_ss.pdf

The Commonwealth of Australia (2018) 'Non-Profit Organisations and terrorism Financing: Red flag indicators, p. 6-8. Available online at: https://www.austrac.gov.au/sites/default/files/2019-06/npo-red-flag-indicators.pdf

Country risk: • Parties to the transaction (for example: account owner, sender, beneficiary or recipient) are from countries known to support terrorist activities and organisations. • Funds sent from large international NPOs based in high-risk countries, to their branches in regional countries, are channelled to local NPOs based or operating in domestic conflict areas. • An NPO sending funds to multiple entities (individuals and companies) in a high-risk country. • NPO raises funds from a major public event and then authorises a third party to be a signatory to the NPO account, who uses it to send funds to high-risk countries. • Large outgoing transactions to the country of origin of NPO directors who are foreign nationals, particularly if the country is high risk.
Hit with Adverse media reports, sanctions screening, anti-terrorist screening, watchlist screening, buzzwords: • The NPO is linked to known terrorist organisations or entities that are engaged, or suspected to be involved, in terrorist activities. • Transactions, including international and domestic transfers, with NPOs that contain terms associated with violent extremism and other terrorist ideologies; for example, ghanimah or fai/fay (justified stolen funds) and mujahid/mujaheed/mujahideen (the term for one engaged in Jihad). • Use of NPO accounts to accept funds from suspected terrorists and their associates • Transactions (cash and transfers) involving key personnel of foreign NPOs associated with United Nations Security Council designated terrorist entities.

Table 3: Indicators and red flags for NPO misuse[10]

AUSTRAC (Australian Transaction Reports and Analysis Centre), the Australian regulator and FIU, published in 2018 a report on NPO TF indicator. While the report discusses typologies observed across Australia, Brunei, Indonesia, Malaysia, New Zealand, Philippines and Thailand, ML and TF typologies are homogeneous and not jurisdiction specific. The AML/CTF framework offers a global context that provides homogenous conditions across a considerable number of jurisdictions, all aiming to deliver AML and CTF. Indeed, to abide by the FATF standards, each country must have an FIU that processes SARs, a regulator that oversees obliged entities and, of course, regulated entities that balance their commercial objectives with that of the AML/CTF framework. While the researcher acknowledges the inevitability

10 The Commonwealth of Australia (2018) 'Non-Profit Organisations and terrorism Financing: Red flag indicators, p. 6-8. Available online at: https://www.austrac.gov.au/sites/default/files/2019-06/npo-red-flag-indicators.pdf

of variations within jurisdictions, the international standards and principles set out by the FATF nevertheless ensure a non-negligible degree of generalisation that can be applied to the European region.

The report lists the following as characteristics of high-risk NPOs:

- "More likely to be a service-style NPO[11]
- high cash intensity
- public donations are the main source of funds—membership fees can also be important
- support a particular ethnicity or religion
- based in provincial or capital cities rather than rural or border areas
- operate in a high-risk country or have links to NPOs operating in a high-risk country
- funds flow to and from a high-risk country"[12].

3. Issues identified during the research:

This section presents the empirical findings of the research performed as documented in the methodology section followed by the researcher's conclusions based on the analysis of the qualitative data collected. Review and analysis of responses and intelligence collected during interviews has identified that there are four key themes that emerge. Each of those themes are discussed below:

a. Lack of support from regulators:

Interviewees unanimously denounce the lack of support and guidance from their respective regulators. FATF Recommendation 8 signaled to the market that NPOs were high-risk. Although the revised Recommendation 8 removes the identification of NPOs as being 'particularly vulnerable' to terrorist abuse and asks countries to apply a risk-based approach, "the damage has been done" (interviewee 7) and to make matters worse, the FATF has failed to provide FIs "clear indications of NPOs' risk characteristics" (interviewee 12). In Turkey for instance, despite having issued a specific regulation regarding the riskiness of NPOs (Law. No. 7262 on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction), interviewee 8 explains that the regulator failed to provide practical guidance in relation

11 A Service NPOs is involved in service activities which "include programmes focused on housing, social services, education, and health care. In some countries, it also includes religious education and affiliated social services" (The Commonwealth of Australia (2017) 'Non-Profit Organisations and Terrorism Financing: Regional Risk Assessment' p. 43. Available online at: https://www.austrac.gov.au/sites/default/files/2019-06/regional-NPO-risk-assessment-WEB-READY_ss.pdf

12 Austrac, 2018, 'Non-Profit Organisations and Terrorism Financing: red flag indicators', p. 5. Available online at: https://www.austrac.gov.au/sites/default/files/2019-06/npo-red-flag-indicators.pdf

to performing KYC and CDD on that very sector. The lack of guidance is even more surprising when considering that the FATF urged "Turkey to apply the risk-based approach to supervision of NPOs in line with the FATF standards"[13].

This issue is not exclusive to Turkey, however. Interviewees based in other jurisdictions describe similar scenarios. For instance, interviewee 10 based in the Netherlands explains that the banking sector needs non-interpretable guidance. Likewise, interviewees 3 and 7 with experience across Europe and particularly the UK, echo this comment lamenting the fact that there is no practical, detailed manual on how to risk assess NPOs. Essentially "despite the FATF issuing guidance on risk-based supervision[14], FIs operate in a non-failure regime" (interviewee 7). Unsurprisingly, interviewee 1 from the NPO sector, explains that "there is a gap in the support we get from the regulator. It is the hardest stakeholder to get onboard. It does not want to be part of the conversation".

This raises a key issue. While existing AML literature and interviewees (4, 5 and 9) discuss incentivising FIs to onboard NPOs, perhaps the conversation should instead shift on incentivising regulators. How can this be achieved? Interviewee 7 explains that FATF Mutual Evaluation Reports, Ministerial bodies such as the Ministry of Foreign Affairs and key initiatives such as the FATF's Unintended Consequences programme are all factors that should be leveraged to incentivise the regulator. Essentially, to tackle de-risking factors, there needs to be the political will to drive regulators' agendas.

The lack of guidance and support from regulators is an issue observed across jurisdictions, and experienced by both sectors, NPOs and FIs. Regulators need to be incentivised to tackle and address de-risking by providing adequate guidance and support to the banking industry as well as NPOs. Multistakeholder engagement is fundamental to ensure this is adequately tackled.

b. The risk(s) of banking NPOs:

Interviewees state that behaviours and transactions typically observed on NPOs' accounts (wire transfers, cross country transfers, payments to high-risk jurisdictions, odd amounts, cash deposits and withdrawals) are higher risk. In addition, NPOs fail to demonstrate robust governance and/or knowledge of wider financial crime risks. Finally, NPOs typically operate in high threat environments (high risk countries, disaster zones etc.).

13 FATF (2021) 'Jurisdictions under increased monitoring – October 2021'. Available online: https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-october-2021.html.

14 FATF (2021) 'Risk-based supervision'. Available online: https://www.fatf-gafi.org/media/fatf/documents/Guidance-Risk-Based-Supervision.pdf

Accordingly, NPOs are generally recognised as being vulnerable to financial crime.

More specifically, NPOs are more vulnerable to bribery, corruption, fraud and misuse of funds (interviewees 3, 9 and 12) than they are to TF risk. Further research and interviews indicate that there are additional risks associated to banking NPOs: regulatory risk. "Banks fear regulators: They do not want to onboard NPOs" (interviewee 5). Interviewee 9 explains that "we need to give credit to FIs for managing such high-risk customers from a regulatory risk perspective as well as TF and fraud risk! Despite what the regulator claims, this is a non-failure regime, there is no risk-tolerance, and to make matters worse, the regulator sends unexperienced junior staff that do not understand the NPO sector. So, what is the upside to taking the risk of banking NPOs?"

In addition, although there is a low probability of UN sanctions violation, a TF or corruption event from materialising, the impact of such an event is extremely high. This can result into the loss of a banking license as explained by interviewee 2 or into a civil liability case should victims of terrorism decide to sue a FI involved in TF (interviewee 12) as was the case for UBS in 2013, for instance[15].

Finally, NPOs claim that "there is a lack of information and evidence as to the NPO sector's vulnerability to TF misuse" (interviewee 1). However, the NPO sector "cannot be lumped into one risk profile" (interviewee 4). While some may be low risk, others may be particularly vulnerable to financial crime. Some NPOs have the right level of governance, processes, and controls in place to provide assurance to FIs. Others lack the knowledge and awareness of sanctions, TF, regulatory, ML, corruption and fraud risks that FIs need to manage. Accordingly, interviewee 9 questions whether the right indicators to truly assess and measure the NPO sector's risk profile have been identified. This would enable both NPOs and FIs to better assess the hot spots across the NPO sector and deliver a true Risk-Based approach to tackling financial crime.

> *The NPO sector is wide in terms of profile, donors, objectives, programmes, and operations. Current National Risk Assessments do not classify which types of NPOs represent the greatest threat to financial integrity. Similarly, the risks faced by FIs when banking NPOs are multiple, layered and complex. National Risk Assessments do not typically include sanctions, regulatory, corruption, liability and fraud risks. They focus on ML and TF and therefore fail to represent a holistic view of the risks FIs face when banking NPOs.*

15 https://www.reuters.com/article/us-ubs-hamas-idUSBRE91D17J20130214

C. Opaque accountability:

The majority of Interviews indicate that the banking industry faces an NPO sector unwilling or unable to educate itself in relation to sanctions risk (interviewee 2) and unable to naturally support FIs when the latter perform CDD and EDD as per regulatory requirements (interviewee 9). This arises despite the availability of high-quality guidance and educational material (interviewee 2). Furthermore, the NPO sector should support FIs who are not obligated to bank NPOs when it is neither profitable nor aligned to FIs' risk appetite (interviewee 7).

On the other hand, the NPO sector explains that banks refuse to be part of roundtable exercises and to support NPOs by delivering for instance, best practice or guidance relating to minimum standards (interviewee 1). This point is not consistent across Europe, however. Interviewee 10 states that the Dutch Banking Associations is funding an NPO portal to provide all the information necessary to NPOs as well as to financial crime practitioners. This initiative, which will be piloted in Q2 2022, aims to educate all key stakeholders on matters ranging from key regulation, good NPO governance, Ultimate Beneficial Ownership registry, etc.

This, however, raises the issue of liability. Can a sector create guidance and standards for another sector? While there is unquestionable value in banks creating guidance aligned to what the Wolfsberg Group[16] did with regards to correspondent banking activities or sanctions screening, the banking sector is neither an elected body nor a law-making one. It does not have the legitimacy to guide NPOs or MSBs for instance (as raised by interviewee 12). However, FIs' infrastructures are consistently targeted by launderers, terrorists, proliferation financiers. Accordingly, the financial sector is the first line of defence when it comes to ML and TF prevention within the financial sector. Essentially FIs have collective knowledge and understanding of financial crime risk that NPOs simply lack. It would be apt to leverage that breadth of expertise.

This conflicting narrative is indicative of a lack of clarity in terms of responsibility and accountability across key stakeholders. If banking is a basic right that FIs are obligated to provide NPOs with, should the NPO sector be expected to support the banking industry in meeting its regulatory requirements and preserving the integrity of the financial sector by providing all the necessary information to facilitate onboarding and ongoing CDD? Alternatively, should the responsibility be solely that of the banking industry?

16 The Wolfsberg Group is an association of global banks which provide standards and principles for the management of financial crime risks. More information is available at: https://www.wolfsberg-principles.com.

Interviewee 12 believes that NPOs should do their part and that a consortium of NPOs should be set up to drive and implement a code of practice, defining good NPO governance. Furthermore, high-risk NPOs (as defined in section 2) should be pushing the agenda. In addition, interviewee 12 claims that NPOs and MSBs which also face de-risking[17], should leverage one another's initiatives and existing dialogue to generate further momentum in addressing de-risking. Interviewees 3 and 7 go further explaining that de-risking should become part of Environmental, Social and Governance (ESG) banking initiatives, thus incentivising FIs to subsidise such initiatives.

The NPO sector is criticised for not supporting FIs in meeting their AML/CTF responsibilities. Likewise, the banking sector is criticised for not providing NPOs adequate guidance on how to manage their financial crime risk. This may be indicative of a lack of accountability with regards to the responsibility of supporting and preserving NPOs from the dangers of de-risking.

d. The cost of banking NPOs:

Interviewees confirm that NPOs do not typically generate profits and do not require profit generating services and/or products such as asset management and/or loan and liquidity products for example. In addition, on average, NPOs do not traditionally keep large reserves while having large cash positions which generates low returns compared to other financial assets.

In contrast, compliance costs are high. While the cost of onboarding an NPO may vary across FIs and depend on NPO profile, performing due diligence on a client that has an opaque structure for instance and analysis on transactions that have been flagged as high risk (as documented in Table 2) is pricey. Interviewee 5 explains that digital identification for NPOs, would remove the cost of performing CDD. More specifically, interviewee 5 states "we are working with our government to push for digital identification because FIs are scared to onboard NPOs, they do not trust the regulator. With this tool all verification would be done and would also enable remote onboarding with a digital signature. The digital identification of the NPO would deliver verification of the Ultimate Beneficial Owner, proof that the NPO is formally registered and CDD of the founder. This enables the authorities to enhance the integrity of the financial sector and enables the FI to know straight away whether the NPO is bogus or not. Finally, it removes the need and hence the cost of performing CDD".

17 Dahabshiil & others v Barclays Bank Plc (2013) EWHC 3379 (CH) [Online]. Available at: http://www.brickcourt.co.uk/news-attachments/LWT_2013_11_31877320.pdf.

Such costs are reflected in the FI's banking fees. Banking and transaction fees are consistently criticised by NPOs (as well as Money Services Businesses customers) for being too high. However, discussions with interviewees from the banking industry confirm that banking and transaction fees are aligned to fees charged to other customers with similar risk profiles. Fees reflect costs of CDD, EDD and investigations of transactions.

When challenged further on costs, interviewees confirmed that Risk Practitioners are not involved in those decisions because "risk should not be driving pricing decisions" (Interviewee 11). Furthermore, no FI wants to signal to the market that it is generating profits by banking a high-risk account.

NPOs denounce high banking fees while FIs claim such fees reflect banking costs. There is a lack of data relating to banking fees and costs of performing CDD/EDD. The intelligence, relating to banking fees and costs, available through open-source literature or through interviews conducted is anecdotal and sparse. This gap in NPO de-risking literature needs to be addressed to facilitate communication between stakeholders.

RECOMMENDATIONS

The four key issues that were raised by interviewees and explored in Section 3 can be summarised as follows:

- Lack of incentives for regulators in the provision of regulatory support and guidance to both FIs and NPOs.
- Multiple, layered, and complex risks faced by FIs when banking NPOs which are not accounted for.
- Lack of accountability with regards to the responsibility of preserving society through support of the financial sector's integrity.
- High banking fees.

Based on the issues listed above, it is recommended to:

- Identify tools to effectively incentivise regulators to provide guidance and support to NPOs as well as FIs.
- Perform National Risk assessments[18] covering ML, TF, Fraud, Corruption, sanctions, liability, and regulatory risk to ensure that jurisdictions have a holistic understanding of the risks faced by FIs when providing products and services.
- Identify at-risk NPO subsets to understand the types of NPOs that are most vulnerable to financial crime thus facilitating a risk-based approach to banking NPOs.
- Discuss and agree at national level the roles and responsibilities of key stakeholders with regards to enabling and facilitating the prevention of de-risking. As part of this multistakeholder[19] discussion, the following should be explored:
    - The role of the regulators.
    - The use of technology such as Artificial Intelligence or Digital Identification tools to facilitate CDD and make it more affordable.
    - The appointment of a recognised NPO body (aligned to the Wolfsberg Group for instance) to agree on standards, principles, and best practice.
    - Education material to support the NPO sector.
- Assess the cost faced by FIs when onboarding and monitoring NPOs.
- Perform a survey to assess banking fees faced by NPOs.
- Explore feasibility of having fees and/or costs of NPO onboarding and monitoring being subsidised at government and/or donor level.

18 This NRA could also be performed at regional level as illustrated by the Commonwealth of Australia (refer to footnote no. 15).

19 The following entities and bodies should be part of this multistakeholder dialogue: High-risk NPOs, the FATF, the regulator, Banking Association, Central Bank, FIU, Ministry of Finance, Civil Society Organisations that support the issue of de-risking, Think Tanks.

CONCLUSION

This research aims to map across a selection of jurisdictions the way Financial Institutions (FIs) determine suspicious transactions for Non-Profit Organisations (NPOs) and how this manifest into the de-risking of the latter. Furthermore, the research looks at collecting criteria and principles used for NPOs' transaction monitoring. Finally, it aspires to deliver a set of recommendations based on the field work and findings.

Research consisted in the interview of 12 financial crime risk practitioners and experts operating across the banking industry, Payment Services, Money Services Businesses, Think Tanks, NPOs and financial services consultancy. Furthermore, the research involved the analysis of responses to ECNL designed questionnaires as well as the desk-based review of open-source material, media reports, grey literature and governmental policies and reports.

Fieldwork and analysis indicate that de-risking is complex and multi-factored. It is driven by a lack of regulatory support and guidance highlighting the absence of incentives to address de-risking in a meaningful way. In addition, it is the result of the failure to understand that banking NPOs exposes FIs to financial, legal, reputational, and regulatory risks. Those risks may be low probability, but they are nonetheless high impact. Finally, de-risking is also the result of the low profits/high costs equation that FIs face.

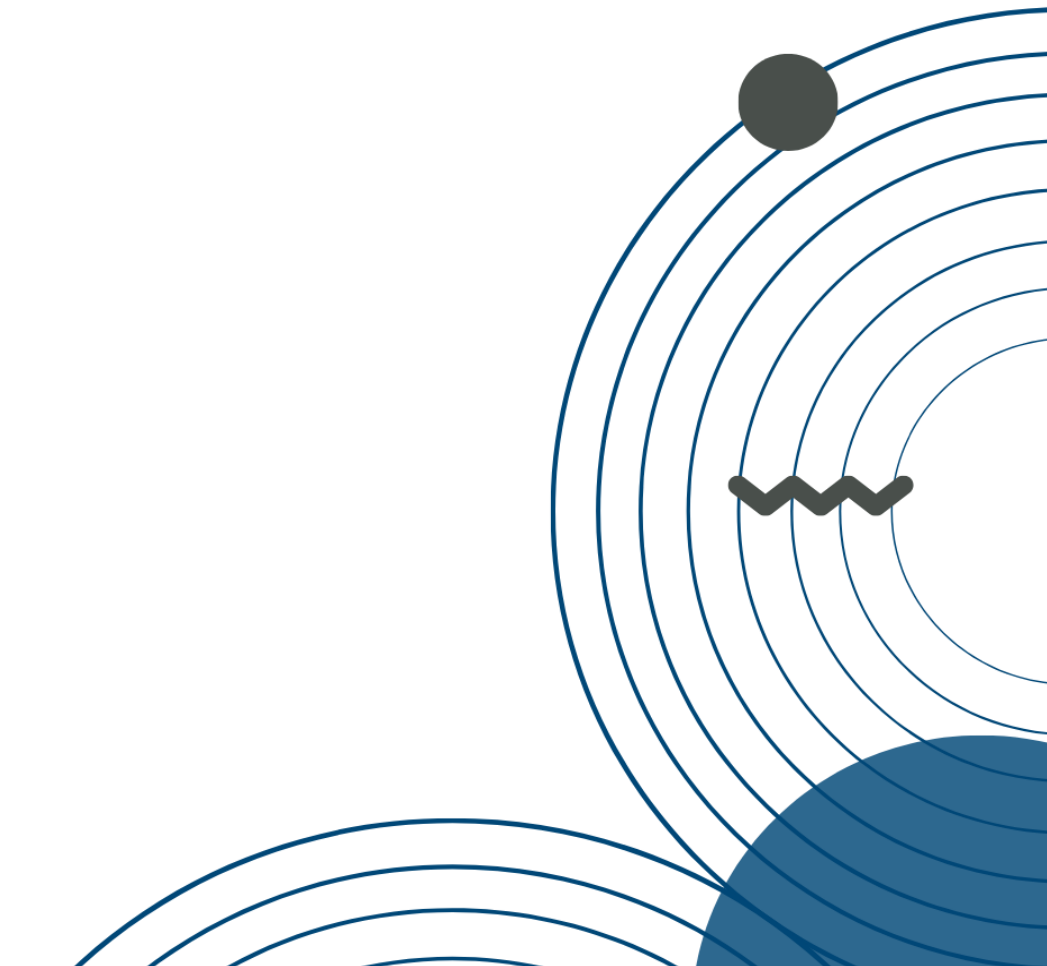
To address those points, an incentivisation strategy needs to be devised to ensure that regulators provide adequate support and guidance to both, the banking and NPO sectors.

In addition, assessing the different risk categories that FIs face beyond TF and ML when banking NPOs, is essential. This would enable the implementation of a truly risk-based supervision and facilitate a risk-based approach to banking NPOs.

Furthermore, the NPO sector being heterogeneous in terms of size, activities, profile, goals and modus operandi, an assessment of key risk characteristics needs to be performed to enable FIs to target their efforts and resources adequately. This assessment could be performed by FIUs and would have to be disseminated across all relevant stakeholders.

Key stakeholders need to have a clear understanding of their respective responsibilities and accountabilities with regards to preserving the integrity of society through support of the financial sector.

Finally, to move away from what can often be described as anecdotal grievances, a cost benefit analysis of banking NPOs should be performed across a selection of FIs. This would facilitate multi-stakeholder dialogue on de-risking and enable both, the banking and NPO sectors to assess the proportionality of current banking fees.



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