FINANCIAL ACCESS OF HUMAN RIGHTS DEFENDERS IN EXILE

Policy paper

February 2026

European Center for
Not-for-Profit Law

Acknowledgements

Authors: Esther Meester and Ivana Rosenzweigova (European Center for Not-for-Profit Law, ECNL)

The authors would like to thank Sangeeta Goswami (Human Security Collective) and Nelleke Hoffs for their review of this policy paper. We are also grateful for the support of Francesco Zatelli (Pro Publico).

European Center for
Not-for-Profit Law

www.ecnl.org

February 2026

Introduction

Over the past decade, the European Center for Not-for-Profit Law (ECNL) has supported civil society organisations (CSOs) and associated activists working in the defence of human rights (collectively referred to as "human rights defenders" or "HRDs") who have been forced to relocate from their home countries due to serious threats to their safety, freedom, health, or lives. These threats often arise from repressive actions by authoritarian regimes targeting individuals and groups engaged in human rights work or are the consequences of war and conflict.

In the past years, HRDs in involuntary relocation (also referred to as "exile") have increasingly reported challenges in accessing financial services, including difficulties with opening bank accounts, blocked transfers, and account closures in several countries. As they operate in constraining conditions and are faced with costs associated with relocation, having access to financial services is essential for these groups to be able to continue their work. Such impediments therefore put them in an extremely vulnerable position.

With the rise of authoritarian tendencies across different regions pushing groups to find new operational models or relocate to other countries, this issue is becoming ever more important. To better understand the challenges faced by civil society organisations (CSOs) and activists in involuntary relocation or exile, ECNL conducted a global survey in 2024 among these groups on their experiences with financial service providers. The survey examined both the financial access of the organisations themselves and of individuals associated with them, such as staff members and activists. The results of the survey were published in two consecutive reports and are available here (financial access of organisations in exile) and here (financial access of activist and individuals associated with CSOs on the move) and summarised in the next section.

This paper aims to provide policy recommendations based on the results of the survey and numerous conversations ECNL has had with groups in exile, to address the issue of financial exclusion of these groups. The recommendations are targeted towards the European Union, competent national institutions or governments and financial institutions in the European Union as the EU Member States are typically the safe places that HRDs relocate to. While the survey also examined alternative ways groups use to transfer funds, this paper

focuses on the financial exclusion from traditional banking services and ways forward. In the subsequent sections, we will summarise the survey results, explore the drivers behind them and conclude with policy recommendations.

Data on financial access of CSOs and HRDs in exile

The European Union Member States are some of the main locations where CSOs and activists in exile look for safety. Of the 34 responses received regarding organisational financial access, 19 were from groups that had relocated to an EU Member State[1]; for the questions on individual financial access, 3 out of 14 respondents were in the same category.

The responses demonstrate that CSOs in involuntary relocation predominantly turn to traditional banking; 74% of the respondents attempted to open a bank account with a traditional bank in the new host country. However, more than half of them (52%) reported having issues with this process, with 23% being unable to open the bank account even after one year from their initial application. The most reported challenges can be traced back to the country of citizenship of their representatives and their visa status in the new country. For example, legal representatives of the organisations were required to show long-term residency or citizenship in the bank's country, which is often impossible for human rights defenders who stay on short-term visas or are in the process of obtaining a long-term residence permit. Additionally, banks terminated or restricted relationships when CSO representatives or their funding sources were linked to countries labelled as "high-risk" or their countries were associated with sanctions.

More than half of the respondents used alternative financial services, such as online payment systems or cryptocurrencies to access, transfer, and receive funds for their organisations. They reported significantly fewer challenges accessing these services than traditional banking services. Several respondents who were unable to open a bank

[1] Some groups reported multiple countries of relocation, for instance because staff members were spread across different countries.

account successfully resolved their financial access issues through these alternative solutions.

While individual CSO representatives and activists reported fewer difficulties opening personal bank accounts compared to opening accounts for their organisations (27% vs. 52%), challenges persist. As with organisations, the most common barriers relate to eligibility requirements, particularly the individual's legal status in the host country. For example, asylum seekers in European countries are often required to surrender their passports during the application process, and temporary residence permits are frequently not accepted by banks, hence making it difficult to open an account.

Analysis

Financial exclusion as a broader trend

The challenges faced by CSOs and activists in exile are not stand-alone issues, but part of a larger phenomenon of financial exclusion. An ESGB analysis of the Global Findex Database 2021 demonstrated that 13 million adults within the EU face financial exclusion. Specific communities are particularly impacted, including stateless people, refugees, asylees, homeless people, Roma and Sinti communities. The Economic Inclusion Group, in partnership with the European Endowment for Democracy, has collected over 47 cases of financial exclusion in the European Union, including of prominent foundations known for promoting democratic values within and beyond the EU, humanitarian organisations, well-known foreign universities establishing new campuses in Europe, and innovative technology firms. However, information about financial exclusion of organisations remains anecdotal as this is not systematically documented and many affected individuals and organisations are reluctant to speak up.

Impact of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regulations

The primary drivers of financial exclusion are regulatory frameworks that aim to prevent money laundering and counter the financing of terrorism (AML/CFT) and are not tailored to specific situations and groups. Within the European Union, the regulatory framework governing anti-money laundering and countering the financing of

terrorism is currently defined by a series of Directives[2] on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, which are transposed by Member States into national law. However, in May 2024, the European Parliament and the Council of the EU adopted a new AML/CFT package to address emerging risks and harmonise measures within the Union. This package includes a Regulation[3] which, effective July 2027, will be directly applicable in Member States.

Banks and other financial institutions are subject to multiple obligations under AML/CFT frameworks, including customer due diligence, transaction monitoring, and reporting of suspicious activities. The implementation of these obligations can result in disproportionate administrative burdens imposed on clients, as well as cases of de-risking; the restriction or termination of financial services to clients perceived as high risk. Banks and other financial institutions may tend to adopt a risk-averse approach, to mitigate potential legal, financial, and reputational liabilities. This can be exacerbated by a lack of clarity on how to implement open norms, which are designed to allow for flexibility and a risk-based approach, as highlighted in ECNL's research on unintended consequences of AML/CFT regulations. Potential differences of interpretation between a bank and the supervisory authority regarding what is adequate and proportionate in a specific situation may encourage a more cautious approach. In addition, commercial considerations are an important factor. The costs associated with implementing due diligence measures can increase banks' tendency to refuse clients perceived as 'high risk', particularly individuals or small organisations. Altogether, incentives to avoid risks are much stronger than incentives -if any- to enhance financial inclusion. At the same time, a bank may also be compelled to refuse a client because of the failure or inability of the client to provide required information or documentation. Risk assessment of clients and transaction monitoring is usually done through a combination of an automated system and human review. Client acceptance decisions usually combine automated risk scoring with deliberation by a multidisciplinary committee that decides on possible rejection. FATF Recommendation 8 states that AML/CFT measures should not unduly disrupt or discourage legitimate activities of not-for-profit

[2] The most recent one being Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

[3] Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, also referred to as "AML Regulation" or "AMLR".

organisations (NPOs).[4] Moreover, the UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises on Responsible Business Contact state that business enterprises are required to respect human rights by avoiding harm through their own activities, addressing any negative impacts they cause or contribute to, and preventing or mitigating harm linked to their business relationships, even if they do not contribute to those impacts.

Yet, civil society organisations have been significantly affected by de-risking, as acknowledged in the EU Supranational Risk Assessment, which negatively affects the freedom of association and indirectly the ability of civil society organisations to advance human rights. De-risking poses particular challenges for organisations in exile, as demonstrated by the results of our survey. Next to the visa status of their representatives, linkages of these organisations or their representatives to countries labelled as "high-risk" appears to be among the main drivers, even if there is no evidence or even indications of wrongdoing. This aligns with the findings of an analysis of the European Banking Authority (EBA) on de-risking, which indicate that customers with links to jurisdictions that are associated with higher ML/TF risks, including CSOs operating in or having business relationships with these jurisdictions and asylum seekers from these jurisdictions, are among the categories of customers who are disproportionately affected by de-risking.

This is illustrated by the case of a respondent to ECNL's survey, an organisation working on civil society development whose legal representatives are of Syrian origin. After initial registration of their organisation in Turkey, they experienced challenges because of the legislative restrictions prohibiting organisations with Syrian board members to make international transfers. To overcome this challenge, they decided to relocate and set up a nonprofit in Belgium. According to the respondent, who serves as the organisation's legal representative, they were rejected by most banks despite having submitted extensive documentation to meet Know Your Customer requirements, including proof of a license under U.S. sanctions regulations and support letters from several reputable donor organisations. Even when temporarily successful with a couple of banks, their bank accounts were eventually closed after a few months, often without any official explanation.

[4] In the context of AML/CFT frameworks, the term Non-Profit Organisations is commonly used. This encompasses Human Rights Defenders in exile.

The right of individuals to a basic payment account

Access to banking services is a prerequisite for participation in society. Therefore, EU Directive 2014/92 (Payments Account Directive or "PAD") provides a right of access to a payment account with basic features (art. 16), which is transposed into domestic laws by Member States. This right applies to consumers legally resident in the Union, including consumers with no fixed address and asylum seekers, and consumers who are not granted a residence permit, but whose expulsion is impossible for legal or factual reasons. However, the Directive explicitly states that Member States must ensure that credit institutions refuse an application for a payment account with basic features where opening such an account "would result in an infringement of the provisions on the prevention of money laundering and the countering of terrorist financing laid down in Directive 2005/60/EC" (art. 16 (4)). Hence, this Directive does not provide adequate protection against de-risking in the context of the application of AML/CFT measures. Credit institutions are required to inform consumers of the reasons for refusing a payment account with basic features, unless such disclosure would be contrary to national security interests or AML/CFT requirements (art. 16 (7)). In practice, the application of the "tipping-off" prohibition (which prevents them from informing customers or third parties that a suspicious transaction report has been filed or that an AML/CFT investigation is underway) often results in banks providing little or no explanation for refusals, which negatively affects redress opportunities. In this context it should also be noted that EU Directive 2015/2366 (Payment Services Directive or "PSD2"), which establishes the legal framework for the provision of payment services in the EU, does not provide a requirement for payment services providers to motivate any decision on termination or refusal of a service agreement. This gap is relevant because payment services agreements determine whether a payment account can be used in practice, so their refusal or termination may effectively undermine access to banking services even where an account formally exists.

In its 2022 Opinion on de-risking, the EBA noted that no clarification is provided on the interaction between AML/CFT requirements and the right of individuals to open and use a payment account with basic features. After this publication, the European Commission asked the EBA to issue new guidelines on the steps institutions should take to facilitate access to financial services by those categories of customers that the EBA's analysis had highlighted as particularly vulnerable to unwarranted derisking, including those within the scope of the PAD.

These new guidelines were published in March 2023 and include guidance on applying customer due diligence measures vis-à-vis individuals that may have credible and legitimate reasons to be unable to provide traditional forms of identity documentation, as can be the case for human rights defenders in exile. The EBA guidelines state that credit and financial institutions should have policies and procedures in place which specify which alternative, independent documentation they can rely on to meet their customer due diligence requirements. They also provide recommendations on enhancing access to basic payment accounts, e.g. by adjusting customer due diligence measures to account for the fact that the limited functionalities of a basic payment account help mitigate the risk that the customer could abuse these products and services for financial crime purposes. This is in line with the recently updated FATF Guidance on Financial Inclusion which acknowledges that verification of the customer identify does not need to rely on official identity documentation. More specifically, the guidance states "In a lower risk context, fulfilling the customer identification, verification and monitoring requirements of R.10 could entail less intensive and formal means of information gathering and monitoring and a reliance on appropriate assumptions regarding the intended usage of basic products, or less detailed and frequent information." The publication highlights, among others, the example of Sweden, where the Swedish Bankers Association, in collaboration with the Swedish Migration Agency, designed a process to enable identification of asylum seekers for the purpose of opening a bank account, through the Swedish Migration Agency.

Certain national regulators have also issued guidance on de-risking. For example, on 1 February 2022 the Belgian National Bank of Belgium (NBB) published a circular regarding prudential expectations on de-risking. According to the NBB, de-risking entire categories of customers without due regard to individual customers' risk profiles is a sign of ineffective management of money laundering and terrorist financing risks. The NBB considers that it is not appropriate, and not consistent with AML/CFT legal and regulatory requirements, for a financial institution's customer acceptance policy to exclude all business relationships with potential or existing customers on the basis of general criteria such as, inter alia, their belonging to a particular economic sector or a link to a high-risk country.

The NBB further clarifies that a financial institution must only in a limited number of cases refuse to enter into a business relationship. Such obligation to refuse a business relationship does not apply merely because the financial institution's individual risk assessment has determined that high ML/FT risks are associated with the business

relationship, in which case enhanced due diligence measures are required by law.

In October 2025, the EBA published its advice on a draft Regulatory Technical Standard on Customer Due Diligence under the new EU AML/CFT package (effective from July 2027), at the request of the European Commission. In its advice, the EBA acknowledges the risk of financial exclusion for groups such as asylum seekers, refugees, individuals unable to be repatriated, homeless persons, and other vulnerable groups. While the new AMLR does not exempt obliged entities from collecting required customer information, even when traditional identity documents cannot be provided for legitimate reasons, the draft RTS allows key data, such as nationality or place of birth, to be obtained through other credible means in such cases, as the EBA also set out in its earlier guidelines.

Despite positive steps taken, a mystery shopping exercise conducted by Finance Watch at the end of 2023 in three Member States to assess the effectiveness of the PAD demonstrated that refugees, asylum seekers and homeless people are often prevented from opening a basic payment account because they do not have the proper identification and residency documents requested from them to open the account. This is in line with our survey results. Other challenges identified in the Finance Watch report are cost associated with the bank (in some Member States a basic payment account can be more expensive than a standard account) and lack of awareness of the right to a basic payment account among target groups while banks often do not proactively offer this option.

CSOs and access to banking services

As stated above, civil society organisations are significantly affected by de-risking. The EU Directive does not extend the right to a basic payment account to legal entities, leaving CSOs, including those in exile, with even less options to access banking services. Respondents to a call for input on de-risking issued by the EBA in 2020 stated that a lack of understanding within financial institutions of specific customers' business models, including non-profit organisations, can lead to refusal of such customers. To address this, recognising also that not-for-profit organisations are disproportionately affected by bank de-risking, the EBA concluded in its 2022 Opinion on derisking that a more detailed guidance on customer due diligence vis-à-vis NPOs is necessary. Therefore, following a request from the European Commission, the EBA issued specific guidelines for risk assessment of

not-for-profit organisations in March 2023. The EBA added an annex to existing guidelines on risk assessment, which clarifies the steps that financial institutions should undertake to get a good understanding of how an individual NPO is set up and operates, and the ML/TF risks it is exposed to. Although this has been a positive development, it does not appear to have resulted in adequate protection against unwarranted de-risking of NPOs to date.

Around the same time as the publication of the EBA guidelines, in the Netherlands a Sector Industry Baseline for NPOs was developed by the Dutch Banking Association with the same objective: reduce de-risking of not-for-profit organisations and enhance a risk-based approach. Through a multi-stakeholder dialogue, involving the legislator, supervisor, banks and sector representatives, detailed guidance was developed for banks on risk assessment of non-profit clients, including a list of risk enhancing and risk reducing factors. The participatory approach and involvement of all stakeholders have enhanced Dutch CSOs' access to banking services, although research shows that challenges remain, particularly related to administrative requests that CSOs have difficulty with responding to and banking cost.

As a good practice, EU Member States can also decide to expand the right to a basic payment account to legal entities. In Belgium, this was done in 2020 to include legal entities and unregistered organisations, thereby ensuring their access to a payment account and essential banking services. When an entity is denied a basic payment account by three banks, the Federal Public Service for Economy (FOD Economie) can designate a bank to provide the service against a maximum annual fee of 420 EUR (2025 amount). The designated bank can refuse to provide the basic bank account only on limited grounds. One of these grounds, similar to right to a basic bank account for individuals, is violation of any provision of the Belgium AML/CFT law. In such case, the bank is not required to provide a justification for rejecting to open a bank account. There are known cases, like the case of the before-mentioned organisation with Syrian legal representatives, where designated banks have delayed the decision or have refused to comply, and legal mechanisms to enforce this obligation are limited.

Conclusions and recommendations

Exiled CSOs and activists often face significant obstacles when trying to access traditional banking services. These ongoing financial barriers threaten their operational survival and their capacity to defend human rights. Without inclusive access to financial services, their essential contributions to democracy and human rights are diminished.

These challenges are part of a broader trend of financial exclusion, caused by the misalignment between AML/CFT frameworks and the specific characteristics of certain groups of clients, as well as a risk-averse implementation of frameworks by banks and regulators. De-risking practices disproportionately affect legitimate civil society actors, especially those with links to sanctioned or "high-risk" jurisdictions, resulting in unnecessary service restrictions and account closures regardless of actual risk and therefore negative impact on the communities they support.

Current EU measures do not adequately protect exiled individuals and organisations from financial exclusion. While the Payment Accounts Directive establishes a right to a basic payment account for individuals, AML/CFT obligations often override the Directive's intention, and implementation varies significantly among Member States. The non-binding EBA Guidelines on customer due diligence are to date insufficient to protect certain groups of individuals and civil society organisations from financial exclusion. Some Member States, such as Belgium and the Netherlands, have adopted progressive policy innovations like extending basic banking rights to legal entities and developing sector-specific guidance to limit de-risking of NPOs. However, these initiatives are inconsistently enforced and lack EU-wide harmonization, leaving many CSOs and activists in exile still unable to benefit from increased access or practical protections.

To strengthen financial access of CSOs and activists in exile within the European Union, we recommend the following:

For the EU:

- Assess the effectiveness of the Payment Account Directive and strengthen its implementation through effective enforcement mechanisms, including legal remedies in cases where financial institutions refuse to provide a basic payment account. The scope of the tipping-off prohibition should also be clarified.

- Expand the right to a basic payment account as laid down in the Payment Accounts Directive to legal entities.
- Include a provision in PSD2 or the Payment Services Regulation proposal (PSR) that, in case of a the refusal of a payment account or the termination of an existing payment account, the payment services provider must inform the (candidate) payment services user (both natural persons and legal entities) of the grounds and the justification for the refusal or termination, without prejudice to the tipping-off prohibition, similar to what already exists for payment accounts with basic features under article 19.4 PAD and the Belgian basic banking service for undertakings.
- Clarify in PSD2/PSR proposal and PAD that a refusal or termination of a (basic) payment account on the basis of AML/CFT reasons can only take place if opening or maintaining the (basic) payment account would be in violation of the payment service provider's AML/CFT obligations (i.e. enhanced customer due diligence or monitoring would not suffice; cfr. EBA and NBB guidance).
- Follow the advice of the EBA on the RTS on customer due diligence under the new EU AML/CFT package and allow for a more flexible approach in collection of information in cases where customers have credible and legitimate reasons for being unable to provide traditional forms of identity documentation.
- Issue under the new EU AML/CFT package further guidelines to financial institutions on customer due diligence vis-à-vis certain groups of customers, including NPOs and the before mentioned groups, to prevent unwarranted de-risking. These guidelines should build on those issued by the EBA in 2023 on these topics and the FATF Guidance on financial inclusion issued in June 2025 and take the reality of HRDs in exile into account. These guidelines should also clarify that financial institutions cannot refuse or terminate a business relationship merely because of a high ML/FT-risk. AMLA should play an active role in ensuring their effective implementation.
- Stimulate Member States to develop an industry baseline for the non-profit sector, following the Dutch example and tailored to the national context.
- Explore the establishment of a viable mechanism to ensure the financial inclusion of customers who are considered "high-risk" clients due to certain characteristics and are currently excluded from mainstream banking because they do not fall within the risk appetite of financial institutions and/or because of

compliance cost.[5] This mechanism should be accessible to civil society organisations and activists who have relocated to a Member State. It could involve a vetting process, for example through a letter of referral from a trusted third party and should include binding provisions requiring financial institutions to provide such entities or individuals with access to basic banking services.

- Require Member States to set up an appeal mechanism (for example, in the frame of the ombudsperson offices) for addressing unjustified account closures or refusals, ensuring affected organisations and individuals can access remedies.
- Create an EU-wide database for tracking cases of financial exclusion affecting CSOs and activists in exile. This would support evidence-based policymaking and increase transparency around the scale of the issue.

For competent authorities at the national level:

- Expand the right to a basic payment account as laid down in Directive 2014/92/EU to legal entities, even if this is not mandatory based on EU legislation.
- Investigate methods for absorbing or sharing some of the risk carried by financial institutions when facilitating the work of CSOs who provide vital assistance in higher risk environments.
- (for supervisors) Assess to what extent obliged entities adopt a risk-based approach and encourage adoption of proportionate measures (not a "zero failure" approach) and simplified measures in cases of low risk, taking also into account the inherent risk of the financial product offered, e.g. the basic payment account with limited features, in line with the updated FATF Guidance on Financial Inclusion.
- Engage with national contact points for responsible business conduct and relevant authorities to assess the overlap with mechanisms like the OECD Guidelines and UN Guiding Principles on Business and Human Rights to ensure that banks respect human rights.
- Launch a dialogue between key stakeholders, including decision-makers, bank associations, individual banks and CSO representatives to enhance a shared understanding of the realities of CSOs and human rights defenders with a migration

[5] See also similar recommendations made in: "Financial Exclusion, a Hidden Crisis: How EU Banking Regulations are Leaving People Behind", Economic Inclusion Group and European Endowment for Democracy, 2025, and "Undesirable consequences of de-risking for customers and banks", Dutch Banking Association, 2022

background, as well as ML/CT risks and proportionate mitigation measures, with the aim to find long-term structural solutions to issues these groups are facing with accessing financial services, including with transfers to conflict areas or countries considered to be "high risk".

- Develop guidance for banks regarding the application of customer due diligence measures vis-à-vis CSOs and individuals who have relocated from abroad, based on EBA Guidelines and country-specific challenges identified through multistakeholder dialogues. This should include a list of key documents that they need to provide during the onboarding process. It should reflect the realities of human rights defenders in exile, which (can) include inability to provide a passport, travel or produce documents that do not exist in their country of origin, and allow for more flexibility in applying customer due diligence measures in such cases. Such guidance can also provide a list of risk reducing factors (e.g. receiving government funding or a letter or referral from a trusted third party) to avoid unnecessary derisking. The Dutch NPO Sector Industry Baseline, developed through a multistakeholder dialogue led by the Dutch Banking Association, could serve as inspiration for this.
- Introduce a legal review mechanism (for example, in the frame of the ombudsperson offices) for addressing unjustified account closures or refusals, ensuring affected organisations and individuals can access remedies.

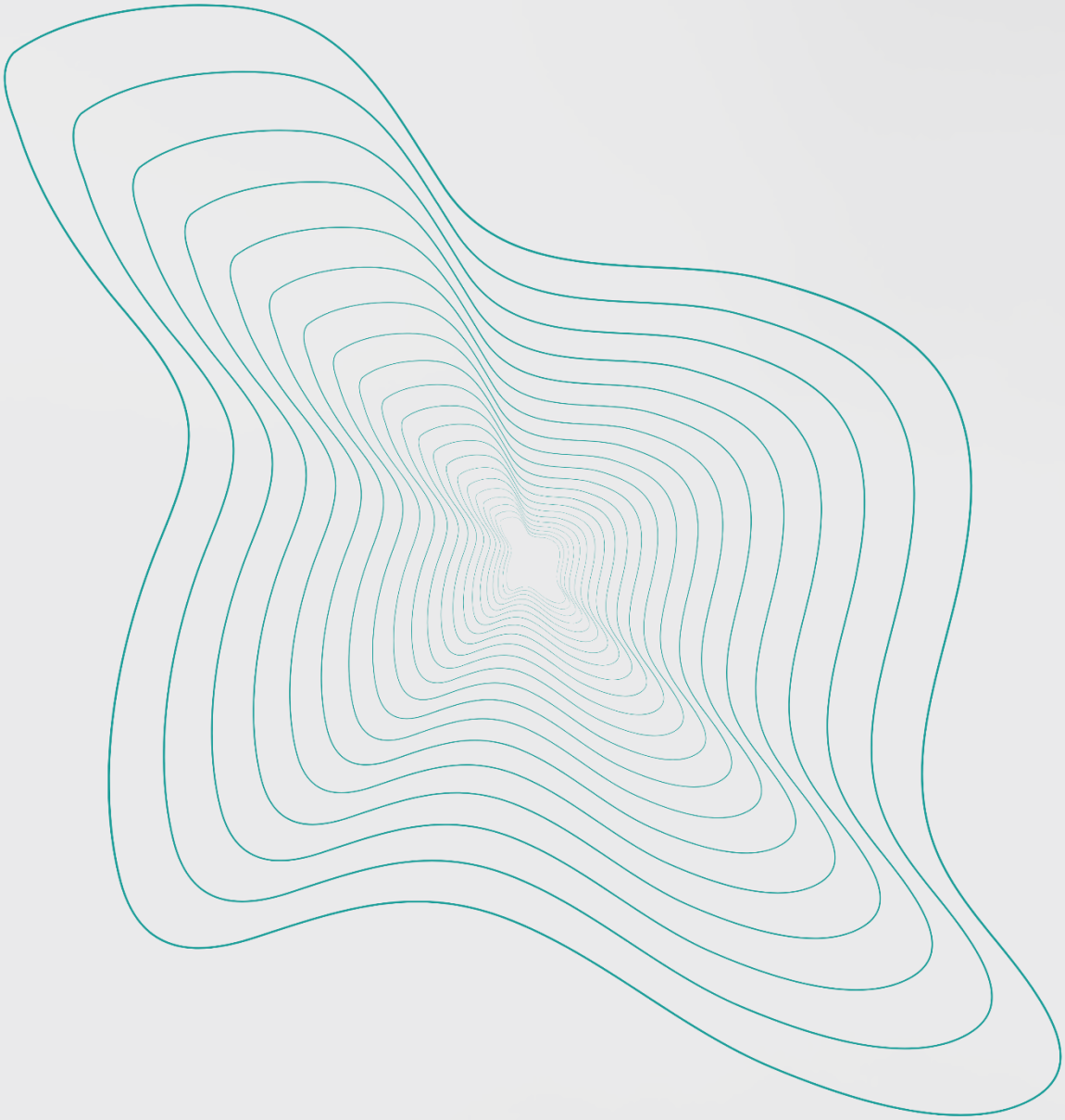
For banks and other financial institutions:

- Proactively offer the basic payment account to all customers.
- Adhere to the recommendations laid out in the Tbilisi principles, which provide guidance for an effective and human rights-compliant crisis response, in particular the following:
    - Simplify processes for accessing banking services by those affected by crises, including refugees and CSOs and individual human rights defenders in exile.
    - Provide clear and concise justification in writing for refusals of service to CSOs, such as refusals to open an account, refusals to make a payment or the withdrawal of banking services. Provide general guidance on the reasons why these actions occur.
    - Allow bank accounts to be opened online.
    - Establish and declare a time limit for opening a bank account.

    - Establish and publicise a simplified mechanism for complaints for refusal of financial services to CSOs to enable systemic problems to be identified and addressed.
- Enhance internal knowledge of the civil society sector and operations internally, including knowledge of HRDs in exile, and establish dedicated service desks or focal points. These teams should receive training on applying AML/CFT rules to nonprofit clients to reduce over-compliance.

For CSOs and human rights defenders in exile:

- Proactively investigate the financial institutions' requirements, prepare the required documents and provide ample information during the onboarding process. Be as open and transparent as possible. See also ECNL's publication "Navigating access to financial services for CSOs" for more practical guidance on this.
- Join forces and create coalitions to address any challenges experienced, and raise awareness on the Tbilisi principles among banks and other financial institutions.



European Center for
Not-for-Profit Law

FINANCIAL ACCESS OF HUMAN RIGHTS DEFENDERS IN EXILE

February 2026