# THE FATF'S LONG SHADOW OVER CIVIC SPACE

European Center for
Not-for-Profit Law

# The FATF's Long Shadow Over Civic Space

## Misuse of anti-money laundering/counter-terrorism financing (AML/CFT) frameworks to embolden foreign agents/interference laws and transnational repression

**Author:**
Stephen Reimer
Associate Fellow, Centre for Finance & Security (RUSI)
Adjunct Professor, SciencesPo

European Center for
Not-for-Profit Law

www.ecnl.org

The report is available under the Creative Commons license:
CC-BY SA 4.0 Attribution ShareAlike 4.0 International

OAK FOUNDATION

Co-funded by the European Union

This publication was co-funded by the European Union within the framework of the project CSO Meter – Empowered for Action, and by the OAK foundation. The findings and conclusions presented in this publication are the sole responsibility of the author and do not necessarily reflect the views or opinions of the European Union or the Oak Foundation.

June 2026

# Contents

# THE NEXT GENERATION OF REPRESSION

Democratic backsliding and rising authoritarianism globally have been driven by diverse tactics that seek to limit civic space. Chief among these are so-called foreign agents/foreign interference laws,[1] as well as tactics of transnational repression (TNR).[2] Both are reinforced by appealing to notions popularised in the Global North of state sovereignty, non-interference, and combatting corruption and economic crime, making them challenging to call-out.

Against that backdrop and given the diminishing returns on traditional "name-and-shame" tactics, civil society needs new avenues for advocacy and resistance. In seeking out strategies to counteract compounding threats, a unique entry point for challenging autocratic trends may be found in the Financial Action Task Force (FATF) – the global stand-setter and watchdog for anti-money laundering/countering the financing of terrorism (AML/CFT). This also involves harnessing the influence and capacity of the banking sector to push-back against being implicated in authoritarian tactics that abuse AML/CFT standards.

This study seeks to elucidate examples of authoritarian tactics involving foreign interference/agents laws or transnational repression that draw on AML/CFT and FATF for legitimisation and orchestrating attacks on civil society. In doing so, it identifies novel advocacy pathways for civil society actors to consider and adapt to their own contexts.

Global civil society already has existing connections with the FATF and a track-record of achieving tangible reforms (to both its standards and its processes) to mitigate abuses of FATF standards. It is therefore useful to examine the FATF's influence over its members, its capacity to achieve behaviour change (including the enacting and retracting of laws and measures) and its goodwill connections with civil society organisations to raise awareness of and seek redress for a new generation of repression and "unintended consequences".

---

[1] See International Center for Not-for-Profit Law, "Foreign Influence Registration Laws and Civil Society: An Analysis and Responses", updated January 2025, <https://www.icnl.org/wp-content/uploads/foreign-influence-report_Jan_2025_update.pdf>, accessed 16 March 2026; and Office of the High Commissioner for Human Rights, "Joint Declaration on Protecting the Right to Freedom of Association in Light of 'Foreign Agents'/'Foreign Influence' Laws", 13 September 2024, <https://www.ohchr.org/sites/default/files/documents/issues/association/statements/2024-09-13-statement-sr-foaa.pdf>, accessed 16 March 2026.

[2] See Saipira Furstenberg, Marcus Michaelsen and Siena Anstis, "Transnational Repression of Human Rights Defenders: The Impacts on Civic Space and The Responsibility of Host States", European Parliament, 12 June 2025, <https://www.europarl.europa.eu/RegData/etudes/STUD/2025/754475/EXPO_STU(2025)754475_EN.pdf>, accessed 16 March 2026; "G7 Leaders' Statement on Transnational Repression", 17 June 2025, <https://www.consilium.europa.eu/media/wynouur4/transnational-en.pdf>, accessed 16 March 2026.

## Methodology

This research draws on several data-collection methods. First, a survey among civil society partners in the Western Balkans, Central Europe, Central Asia and the Eastern Partnership countries yielded case studies and experiences with foreign agents/interference laws or transnational repression involving AML/CFT measures or objectives. Second, a series of interviews with 17 experts from civil society and the legal sector provided additional context and case details. Third, early analyses from the findings were shared at online civil society roundtables for validation, and their feedback and further examples or case studies were incorporated into subsequent report drafts.

# FOREIGN AGENTS LAWS / INTERFERENCE MEASURES

Recent proliferation in so-called "Russia-styled Foreign Agents Laws" among countries typically enforce a "self-labelling" regime, whereby entities in receipt of funding from abroad must sign-up to a register of "foreign agents" and brand their outputs as such. Such laws supposedly seek to manage threats to national sovereignty that stem from extra-national funding of civil society organisations and journalists. This includes instances where the security, transparency, and accountability narratives underpinning such laws are conflated with the aims of AML/CFT, thereby leeching legitimacy from the FATF system to justify curtailing international financial support for civil society. For the purposes of this study, "foreign agents laws" are considered broadly as laws or other measures that seek to restrict funding and other support for civil society organisations, and which are generally justified as a means of limiting unwanted foreign interference in domestic affairs.

For example, a proposed law[3] in **Slovakia** cited among its justifications protection against the laundering of the proceeds of criminal activity and the financing of terrorism. The government framed the proposed legislation as fulfilling the recommendations of the FATF in relation to

[3] Slovakia, Act No. 109/2025, An Act Amending Act No. 213/1997 on Nonprofit Organizations Providing Services of General Interest, as amended, <https://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=9699>, accessed 11 June 2026.

"systemic deficiencies in the regulation of financial resources in relation to the non-governmental sector".[4]

A law[5] adopted in February 2025 in **Republika Srpska** (an autonomous governing entity within Bosnia & Herzegovina) was suspended by the country's constitutional court owing to incompatibility with the constitution and European human rights conventions.[6] Civil society organisations highlighted that AML/CFT measures and requirements were being used as justification for the law at the time of its proposal, writing to MONEYVAL (the FATF-style regional body to which Bosnia & Herzegovina is a member) in October 2023 that "the measures proposed go beyond international standards on AML/CFT and hinder the NPOs' [non-profit organisations] free operation".[7]

Multiple laws modelled on the United States' Foreign Agents Registration Act (FARA) proposed in the parliament of **Bulgaria** have briefly mentioned efforts to counter money-laundering and terrorism financing as justification.[8] Following five unsuccessful attempts to pass such legislation, Russia-aligned parliamentarians changed tact and succeeded in proposing an ad-hoc commission mandated to investigate financial support to Bulgarian civil society from George and Alexander Soros specifically.[9] The commission was established in late 2025 but is no longer active following the April 2026 elections and resultant change in parliament.[10] The practice however illustrates a tactic whereby political actors unable to secure adequate parliamentary support for a foreign agents law may settle for an alternative measure to achieve similar aims, such as an ad hoc commission.

---

[4] The legislative proposal was ultimately struck down by the Slovak Constitutional Court. See Slovak Constitutional Court decision PL US 11/2025.

[5] Republika Srpska, Draft Law on the Special Registry and Transparency of the Work of Nonprofit Organizations <https://vladars.rs/sr-SP-Cyrl/Vlada/Ministarstva/mpr/PublishingImages/Pages/default/%D0%9F%D1%80%D0%B8%D1%98%D0%B5%D0%B4%D0%BB%D0%BE%D0%B3%20%D0%97%D0%B0%D0%BA%D0%BE%D0%BD%D0%B0%20%D0%BE%20%D0%BF%D0%BE%D1%81%D0%B5%D0%B1%D0%BD%D0%BE%D0%BC%20%D1%80%D0%B5%D0%B3%D0%B8%D1%81%D1%82%D1%80%D1%83%20%D0%B8%20%D1%98%D0%B0%D0%B2%D0%BD%D0%BE%D1%81%D1%82%D0%B8%20%D1%80%D0%B0%D0%B4%D0%B0%20%D0%BD%D0%B5%D0%BF%D1%80%D0%BE%D1%84%D0%B8%D1%82%D0%BD%D0%B8%D1%85%20%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%98%D0%B0.pdf>, accessed 11 June 2026.

[6] Constitutional Court of Bosnia and Herzegovina, "158th Plenary Session", 29 May 2025, <https://www.ustavnisud.ba/en/158th-plenary-session-the-course-of-the-session-so-far>, accessed 30 March 2026.

[7] Balkan Civil Society Development Network, "Urgent Appeal for MONEYVAL's Response to the Draft Law on 'Foreign Agents' in Republika Srpska", 5 October 2023, <https://balkancsd.net/novo/wp-content/uploads/2023/12/BCSDN-Letter-to-Moneyval-051023_-RS-foreign-agents-law.pdf>, accessed 30 March 2026.

[8] Interview with the Bulgarian Centre for Not-for-Profit Law (BCNL), 27 November 2025, online.

[9] *Civil Space Watch*, "Bulgaria: Parliament Establishes Commission Targeting 'Soros-Funded' CSOs", 7 November 2025, <https://civicspacewatch.eu/alert/bulgaria-parliament-establishes-commission-targeting-soros-funded-csos/>, accessed 30 March 2026; National Assembly of Bulgaria, 7 November 2025, <https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=238710>, accessed 30 March 2026.

[10] Nikolay Zabov, "Parliament Debates Ending Ad-Hoc Committee Investigating Soros-Linked Activities in Bulgaria", *BTA*,15 January 2026, <https://www.bta.bg/en/news/bulgaria/1044295-parliament-debates-ending-ad-hoc-committee-investigating-soros-linked-activities>, accessed 30 March 2026.

Other foreign agent laws propose utilising their country's AML/CFT regime, including national financial intelligence units (FIUs), to operationalise repressive provisions, representing an abuse of FIUs' intended function of investigating financial crime. For example, draft legislation[11] introduced in **Hungary** in May 2025 included provisions that would task financial institutions with policing the fundraising sources of civil society organisations, requiring them to be on the lookout for suspected "foreign funding".[12] The draft law would also effectively subject all senior executives of non-profits and other civil society organisations to enhanced due-diligence processes by banks in a personal capacity, to account for the supposed extra financial crime risk they pose. Under this law, senior civil society leaders would be made into Politically Exposed Persons (PEPs) for the purposes of AML/CFT compliance. This is a clear case of overreach and mutation of the intended purpose of classifying certain clients (such a politicians and executives of state-owned companies, who in virtue of their position and unique access to state resources represent a heightened risk of corruption or financial crime) as higher-risk PEPs.

The legislative proposal from Hungary received strong push-back from the private sector, including from the Hungarian Banker's Association who highlighted, among other aspects, the depth of the divide between the ambitions of lawmakers and the practical realities of the private sector:

> *"It is impossible to comply with this draft law, the person who drafted it knows nothing about the operation of banks, and due to the political goal, even the minimum sense of reality has been lost."*[13]

The association highlighted the high costs their members would bear to overhaul their compliance systems to meet the new obligations. Further, they illustrated a possible further consequence of the law whereby diminished confidentiality of clients' personal data would accelerate an undesirable trend of Hungarians holding their wealth in

[11] Hungary, Bill on "Transparency of Public Life" <https://www.parlament.hu/irom42/11923/11923.pdf>, accessed 12 June 2026.
[12] European Center for Not-for-Profit Law, "Alert: The Hungarian Draft Law on Transparency of Public Life", 15 May 2025, <https://ecnl.org/news/alert-hungarian-draft-law-transparency-public-life>, accessed 27 March 2026.
[13] Unofficial translation of a quote from the Hungarian Banker's Association in response to questions from the Telex news outlet in Hungary, see *24.HU*, "Capital Flight Started from Hungary Due to the Violation of the Transparency law" ["Tőkemenekítés indult Magyarországról az átláthatósági törvény belengetése miatt"], 26 May 2025, <https://24.hu/fn/gazdasag/2025/05/26/tokemenekites-indult-magyarorszagrol-az-atlathatosagi-torveny-belengetese-miatt/>, accessed 30 March 2026.

foreign currencies and financial institutions.[14] Overall, the stance of the Hungarian Bankers Association was premised on technical and economic arguments and were also motivated by concern for reputational risks they would face, rather than concern for civic space directly.

A foreign agents law[15] was adopted in **Kyrgyzstan** in 2024, according to an expert on civil society organisation (CSO) law, largely in response to political pressure from Russia, though the majority of its most potentially damaging provisions were successfully watered down after intensive involvement from the UN and Organization for Security and Cooperation in Europe (OSCE).[16] At this time the Bankwatch Network sent letters to three development banks active in Kyrgyzstan – including the World Bank, the European Bank for Reconstruction and Development, and the Asian Development Bank – requesting these bodies to apply pressure on the Kyrgyz government and highlight the risk the law would pose to long-term economic development.[17] Such strategies have seen success elsewhere, such as in Zimbabwe where appeals to the World Bank contributed to a controversial bill curtailing the work of "private voluntary organisations" (allegedly to comply with FATF requirements) being indefinitely postponed before expiring at the end of the parliament.[18] Subsequent implementation in Kyrgyzstan has been lacklustre, with only a small handful of CSOs voluntarily signing up to the register of "foreign agents", and none having been inspected by the Ministry of Justice.[19] This could reflect the government's own ambivalence towards passing the law, but nonetheless keeps the door open for potential future, targeted implementation against particular entities.

## Key connections between foreign agent laws and AML/CFT

Across these cases, we see two modes of abusing AML/CFT for emboldening foreign agents laws:

1. **Compliance with the FATF or its AML/CFT objectives being used as a pretence or justification for enacting foreign agents laws, either**

[14] *24.HU*, "Hungarians Hold a Record Amount of Foreign Currency" ["Rekordösszegben tartanak devizát a magyarok"], 20 May 2025, <https://24.hu/fn/gazdasag/2025/05/20/rekordosszegben-tart-devizat-magyar-lakossag/>, accessed 30 March 2026.
[15] Kyrgyzstan, Law No. 72 of 2 April 2024 Amending the Law "On Non-Profit Organisations", <https://kenesh.kg/bills/634426>, accessed 12 June 2026.
[16] Nokatbek Idrisov, CSO law expert, interview on 20 November 2025.
[17] Polina Veretelnikova, "Kyrgyzstan's Crackdown on Civil Society: Are International Development Banks Doing Enough?", Bankwatch Network, 20 February 2024, <https://bankwatch.org/blog/kyrgyzstan-s-crackdown-on-civil-society-are-international-development-banks-doing-enough>, accessed 31 March 2026.
[18] See Reimer "Weaponisation of the FATF Standards", p. 35.
[19] Nokatbek Idrisov, CSO law expert, interview on 20 November 2025.

explicitly through reference to the FATF directly, or implicitly through reference to, among other things, preventing money-laundering or terrorism financing or countering illicit financial flows.

2. Less common, though potentially more concerning, are legislative proposals where AML/CFT architecture, including the function of the FIU, are co-opted to operationalise the provisions of foreign agents laws.

In devising push-back strategies against foreign agents/interference laws, regardless of the degree to which they evoke the FATF's principles or overall mission of the AML/CFT regime, civil society actors should contend with the fact that the stated policy goals and aims of such laws are mostly legitimate. Seeking to fully repeal or block these laws runs the risk of backlash. CSOs may be perceived as being against transparency or otherwise have "something to hide", not unthinkable outcomes particularly in contexts where trust in civil society is already low. Addressing overreach must therefore employ nuance and specificity, especially considering that a key feature of such laws enabling abuse is their strategic vagueness. Allying with unlikely partners, such as bankers' associations or international development banks, to pursue push-back strategies premised on technical and economic arguments may see more success.

# FINANCIAL TRANSNATIONAL REPRESSION

Recently, there is growing interest among European policymakers in how legal assistance cooperation related to AML/CFT, including international financial information sharing, has/can be used as an accelerant of transnational repression (TNR).[20] According to the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe (2023):

> *"The misuse on politically motivated grounds of interstate legal co-operation mechanisms such as anti-money laundering and anti-terror financing measures may result in violations of the right to a fair trial [...] The misuse on politically motivated grounds of interstate legal assistance mechanisms such as anti-money laundering and anti-terror financing measures is also a form of transnational repression, which may have far-reaching consequences for the individuals targeted including asset freezing, financial exclusion and violation of property rights."*[21]

A January 2026 report commissioned by the European Parliament's Committee on Foreign Affairs sees financial TNR as an area of growing concern. The report documents how home states abuse AML/CFT tools "to restrict individuals' international access to financial services such as bank accounts", requiring authorities in host states to "recognise that financial institutions' compliance with AML/CFT regulations can be weaponised to target civil society".[22]

Based on the present evidence collection and review of available literature, three modes of financial TNR emerge: (i) Transnational Financial Intelligence Fishing; (ii) Transnational Red-Tagging; and (iii) De-Banking from Abroad.

[20] Parliamentary Assembly of the Council of Europe (PACE), "Misuse of the anti-money laundering measures and countering the financing of terrorism regulations as a tool of transnational repression", Motion for a resolution, Doc. 15697, 30 January 2023, <https://pace.coe.int/en/files/31622/html>, accessed 17 March 2026.
[21] PACE, "Transnational Repression as a growing threat to the rule of law and human rights", Report, Doc. 15787, 5 June 2023, <https://rm.coe.int/transnational-repression-as-a-growing-threat-to-the-rule-of-law-and-hu/1680ab5b07>, accessed 17 March 2026.
[22] Nate Schenkkan et al., "Perpetrators and Methods of Transnational Repression and Possible Counter Strategies", European Parliament, January 2026, <https://www.europarl.europa.eu/RegData/etudes/STUD/2026/775286/EXAS_STU(2026)775286_EN.pdf>, accessed 17 March 2026.

## Transnational Financial Intelligence Fishing: Abuse of Information Sharing Mechanisms

Beyond limiting access to banking, there is potential for information exchange between national FIUs, a core AML/CFT institution, to be weaponised to target dissidents either living abroad or who have expatriated financial services or other operational arrangements as a necessity for carrying out their work. Sensitive information held by financial institutions in a host country can be used in the context of TNR by home countries to launch or sustain a smear campaign, or be used as evidence to open criminal proceedings of financial crime such as money laundering or terrorism financing. This is possible under the FATF system, which gives FIUs the authority to receive and store spontaneous data transmissions from the banking sector, as well as the power to "obtain additional information from reporting entities".[23] Intended as a means of investigating financial crime, the FIU provides a pathway for ill-intentioned states to scrape sensitive information held by the private sector when principles of FIU operational autonomy are ignored or overruled.[24] Once harvested, that financial information may be relayed from a state hosting a dissident back to the FIU of their home country in response to an international information request.

This was the case with Nobel Peace Prize Laureate Ales Bialiatski of Belarus, who following the "de-recognition" of his human rights organisation by Belarus, used personal bank accounts hosted in Poland and Lithuania to continue operations. Financial information pertaining to those accounts was requested by and granted to the Belarussian FIU by Polish and Lithuanian authorities. This was used as a basis for tax-related charges made against Bialiatski in 2011. Both countries later apologised for this information exchange and suspended bilateral legal assistance treaties with Belarus.[25]

The exchange of financial data between FIUs is a routine AML/CFT practice typically conducted through the Egmont Secure Web: an information sharing platform available to all members of the Egmont

[23] Stephen Reimer, "Weaponisation of the FATF Standards: A Guide for Global Civil Society", RUSI Special Resources, June 2025, <https://static.rusi.org/weaponisation-of-fatf-standards-a-guide.pdf>, accessed 17 March 2026, p. 19.
[24] Jorge Jraissati, "Combatting Transnational Financial Repression: Evidence for Reforming AML/CFT Laws", Economic Inclusion Group and International Republican Institute, working draft, January 2025, <https://econinclusion.com/wp-content/uploads/2025/02/IRI.pdf>, accessed 17 March 2026, pp. 20-23.
[25] See, Viasna, "Judgement in the Case of Ales Bialiatski by the Court of Pershamaiski District of the City of Minsk", 27 December 2011, <https://spring96.org/en/news/48631>, accessed 30 April 2026.

Group of FIUs.[26] The Egmont Group encourages its member FIUs to "exchange information freely, spontaneously and upon request on the basis of reciprocity and mutual assistance", though maintains that

> *"FIUs receiving requests may, as appropriate, refuse to provide information if the requesting FIU cannot protect the information effectively"* and that *"exchanged information should be used only for the purpose for which the information was sought out or provided."*

Members have been suspended from the Egmont Secure Web for breach of these principles above, as was the case with Colombia who was suspended in 2024 for the public disclosure of information provided by a member FIU, namely information related to the purchase of Pegasus spyware by the country's police intelligence department under a previous administration.[27]

However, such suspensions are a rarity. Afterall, the Colombian case only came to light after the country's president revealed the confidential information procured via Egmont in a public speech. According to Egmont's own "Principles of Information Exchange Between FIUs" noted above, FIUs should ensure that information they have privileged access to (and are asked to share with a partner FIU) will be used for legitimate investigations and not to support a smear campaign or judicial reprisal against a dissident. An EU expert in international legal cooperation interviewed for this study underscores a difficult reality: cooperation mechanisms and treaties are trust-based and governments with strong rule of law systems therefore typically assume legitimate intentions from their counterparts.[28] Possibly reinforcing this position is the reality that substantial time and effort would be required on the part of states receiving requests to inject caution into the process and verify that requests are based on genuine, not politically motivated grounds. Typically, this results in all partners being given the benefit of the doubt.

[26] Egmont Group, "Principles for Information Exchange Between FIUs", July 2025, <https://egmontgroup.org/wp-content/uploads/2022/07/EG-Principles-for-Information-Exchange-Revised-July-2025.pdf>, accessed 17 March 2026.
[27] Egmont Group "Statement by the Chair of the Egmont Group on FIU Colombia", 23 September 2024, <https://egmontgroup.org/news/statement-by-the-chair-of-the-egmont-group-on-fiu-colombia/>, accessed 17 March 2026; Santiago Olivares Torres, "Colombia Suspended from Egmont Group Following Gustavo Petro's Speech Over Pegasus Spyware", *Finance Colombia*, 23 October 2024, <https://www.financecolombia.com/colombia-suspended-from-egmont-group-following-gustavo-petros-speech-over-pegasus-spyware/>, accessed 17 March 2026.
[28] Interview with an EU-based expert in international legal cooperation, 15 December 2025, online.

## EMERGING RISK: Georgian CSOs and Activists in Exile and with Hybrid Operations[29]

Speaking with Georgian civil society leaders currently facing ever-growing legal restrictions on their operations in the country, many express concern that they will soon be victims of Transnational Financial Intelligence Fishing themselves. Amendments to the country's Law on Grants and its Criminal Code passed on 4 March 2026[30] expand the scope of grants requiring prior government approval. This includes the provision of any funds by a foreign (non-Georgian) entity to a Georgian organisation, citizen or resident where the funds are used or may be used with the intent to influence the Georgian government, its institutions or any part of society, or for dealing with the country's domestic or foreign policy. The law has extraterritorial reach by also designating citizens and legal entities in another country that "substantively" work on Georgia-related issues as "grant recipients" also requiring government approval. These provisions serve to close the few remaining opportunities for international financial support to Georgian CSOs, including those working on Georgian political issues from outside the country.

Further, amendments to the money-laundering offence in the criminal code (article 194) add a new aggravating circumstance in "money-laundering carried out for the purpose of engaging in political activities related to Georgia", serving to link violations of the newly amended Law on Grants to money-laundering charges.

In circumstances where an exiled CSO working in another country on "Georgian issues" is in receipt of an unauthorised grant, the opening of a money-laundering case against them in Georgia gives an opportunity for the government to initiate AML/CFT information requests. This may occur through FIU channels, like in the case of Belarus mentioned above, where the third country is compelled to share financial information with Georgia about the CSO's financial dealing in their territory. This represents an abuse of not only FATF standards related to the ML offense, but also the associated principles of information sharing.

Despite the growing trends of abuse of these channels, cases often go unaddressed. At the same time, leading institutions within the AML/CFT world, such as the Egmont Group of FIUs, the FATF and the UN Office on Drugs and Crime encourage more and faster international cooperation and information sharing to tackle transnational illicit

[29] Civil Georgia, "GD Adopts Package Restricting Grants, Political Activity, Lobbying, Government Non-Recognition", 4 March 2026, <https://civil.ge/archives/723348 >, accessed 18 March 2026; Interview with Georgian civil society legal expert, 4 February 2026.
[30] Parliament of Georgia, "Parliament Approved Amendments to the Law on 'Grants'", 4 March 2026, <https://www.parliament.ge/en/media/news/parlamentma-grantebis-shesakheb-sakartvelos-kanonshi-tsvlilebebs-mkhari-dauchira>, accessed 18 March 2026

finance,[31] including through cross-border asset freezing orders, mutual legal assistance requests, and cooperation and extradition treaties used for financial crime cases. New UN guidance states that greater international cooperation, including the exchange of financial intelligence, increases the risk of abuse, owing to factors including disparities in human rights safeguards between states; that FIUs may access financial data directly and independently of judicial oversight; and that in many jurisdictions agencies holding financial intelligence are excluded from data privacy legislation.[32]

It is vital that financial information sharing channels such as the lawful exchange of information between national FIUs are not misused for politicised fishing expeditions. That misuse erodes delicate bonds of trust between national authorities needed for cooperation on genuine financial crime investigations, while allowing for TNR to be executed under the guise of combatting transnational illicit finance.

## Transnational Red-Tagging: Abuse of International Law Enforcement Cooperation

Abuse of international law enforcement mechanisms such as INTERPOL Red Notices are already well understood as a TNR tactic, being described as "the sniper rifle of autocrats – long-distance, targeted, and highly effective".[33] Red Notices are not international arrest warrants, but are communications issued by INTERPOL to alert member states that a person is wanted for criminal prosecution or to serve a sentence. Despite carrying no legal obligation on their own, Red Notices serve to "red-tag" individuals as suspected criminals and typically lead to tangible consequences such as arrest, restrictions on travel, triggering of extradition proceedings, and loss of access to banking services.[34]

[31] In September 2025, the FATF published a new handbook aimed at speeding up money-laundering investigations to bring more criminals to justice, in partnership with INTERPOL, the UN Office on Drugs and Crime, and the Egmont Group of FIUs. The handbook prescribes further informal co-operation as a response to slower and more procedurally complex mechanisms such as those in mutual legal assistance treaties to pursue money-laundering. See FATF, Interpol, UNODC and Egmont Group, "International Co-Operation on Money-Laundering Detection, Investigation, and Prosecution Handbook", September 2025, <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/International-Cooperation-ML-Detection-Investigation-Prosecution.pdf.coredownload.pdf>, accessed 17 March 2026.

[32] UN Counter-Terrorism Global Coordination Compact, "Ensuring Respect for Human Rights While Taking Measures to Counter the Financing of Terrorism", November 2025, <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/respect-measures-financing-terrorism-1-en.pdf>, accessed 18 March 2026.

[33] See Rhys Davies, "Interpol Red Notices and Transnational Repression", *Solicitors Journal*, 14 January 2026, <https://www.solicitorsjournal.com/sjarticle/interpol-red-notices-and-transnational-repression?pass=g13r6gc1f9>, accessed 18 March 2026.

[34] Davies, "Interpol Red Notices and Transnational Repression".

This was the case for Igor Pestrikov, a Russian businessman who left Russia for France in 2022 after resisting the nationalisation of a mineral processing firm he was the majority shareholder for. He was accused by Russia of financial crime, namely "abetting the misappropriation of funds", and a notice was issued instructing France to arrest him.[35] In a similar instance involving Russian abuse of Red Notices, Ukrainian opera director Yevhen Lavrenchuk was arrested and imprisoned in Italy in December 2021. Russia sought his extradition for alleged financial crime and fraud dating back to his time working in Russia before leaving in 2014.[36] The Red Notice was eventually overturned by INTERPOL in both cases following a review, which in Pestrikov's case revealed that the information Russia provided was "generic and formulaic" and that his alleged financial crime was not adequately explained.[37] For Andrey Gnyot, a Belarussian filmmaker and activist detained in Serbia in response to a Red Notice for alleged tax evasion, his release was only secured after his extradition to Belarus was thwarted owing to Serbian law limiting extradition-related detention to one-year.[38]

In these cases, Red Notices were misused to amplify politicised financial crime charges, a tactic combining abuse of both INTERPOL and FATF. The Royal United Services Institute (RUSI) identifies "Lawfare for Transnational Repression", as one of five authoritarian tactics that make use of the FATF's standards:

> *"The FATF's standards for facilitating international cooperation, including Recommendation 37 on mutual legal assistance, Recommendation 38 on cross border asset freezing and confiscation, and Recommendation 39 on extradition, create opportunities for transnational repression of dissidents when used in combination with other international mechanisms for law enforcement cooperation, which may lack their own adequate safeguards to prevent politicised misuse."*[39]

[35] *Disclose*, "How Moscow Tracks Down its Opponents Thanks to INTERPOL", 26 January 2026, <https://disclose.ngo/en/article/how-moscow-tracks-down-its-opponents-thanks-to-interpol>, accessed 18 March 2026.
[36] Angela Giuffrida, "Ukrainian Opera Director Freed in Italy Hits Out at Russia's Misuse of Interpol", 9 March 2022, <https://www.theguardian.com/world/2022/mar/09/ukrainian-opera-director-yevhen-lavrenchuk-freed-italy-russia-interpol>, accessed 18 March 2026.
[37] Cate Brown, Max Hudson, Julia Luft, "Russia Using Interpol's Wanted List to Target Critics Abroad, Leak Reveals", *BBC News*, 26 January 2026, <https://www.bbc.co.uk/news/articles/c20gg729y1yo>, accessed 26 March 2026.
[38] Katarina Baletic, "Belarus Activist Freed From Detention in Serbia Leaves for EU", *Balkan Insight*, 1 November 2024, <https://balkaninsight.com/2024/11/01/belarus-activist-freed-from-detention-in-serbia-leaves-for-eu/bi/>, accessed 25 March 2026.
[39] Reimer, "Weaponisation of the FATF Standards, p. 25.

Nonetheless, INTERPOL does have a process for weeding out politicised requests. The agency's Commission for the Control of INTERPOL's Files (CCF) is an independent oversight body responsible for reviewing requests to remove a Red Notice if, say, the request is politically motivated or intended merely for suppression of a dissident.[40] Leaked INTERPOL data made available to the BBC and French investigative outlet Disclose in January 2026 revealed that over ten years, 700 subjects of Russian-issued Red Notices appealed to the CCF, and at least 400 had these notices overturned, more than any other country for which data is available.[41]

The leak also reveals how INTERPOL's internal messaging system between national police forces has been used as an informal route to request information about dissidents abroad, occasionally when a Red Notice request has been denied. A lawyer working with international coalitions on TNR that was interviewed for this study also explained how working through the messaging system in lieu of requesting a Red Notice can help ill-intentioned states in circumventing CCF safeguards or can act as an alternative where a request is denied by INTERPOL or expected to be denied.[42]

## EMERGING RISK: INTERPOL Silver Notices

Launched as a pilot programme in January 2025, INTERPOL's new Silver Notice system allows states to alert each other of suspected criminal assets (as opposed to individuals subjected to investigation or prosecution) in order to expedite financial intelligence sharing and, ideally, recover illicit assets.

Charlie Magri, a former INTERPOL lawyer who spent six years working with the CCF, now runs Other Side Law, a firm that specialises in rogue use of Red Notices. He says that "the very nature of the Silver Notice, designed to trace and recover funds, makes it a powerful tool that could be turned against political enemies",[43] noting a precedence for politicised abuse set by Red Notices. Here, risk of abuse is enhanced by the onus placed on rapid information sharing and cooperation, deemed necessary by law enforcement to keep abreast of criminals, but which necessarily comes at the cost of "rigorous safeguards of traditional legal channels and could, if misused, become a tool for transnational repression".[44]

[40] Red Notice Monitor, "Interpol Explained: What is the CCF?", <https://rednoticemonitor.com/interpol-explained/>, accessed 18 March 2026.
[41] Brown, Hudson, Luft, "Russia Using Interpol's Wanted List to Target Critics Abroad, Leak Reveals.
[42] Interview with TNR legal expert, 9 February 2026, online.
[43] Other Side Law, "New INTERPOL Silver Notices: What Could go Wrong?", 30 July 2024, <https://otherside.law/interpol-silver-notice-what-could-go-wrong/>, accessed 25 March 2026.
[44] Red Notice Monitor, "Examining Interpol's New Silver Notices: Tracking Criminal Assets or Targeting Dissidents?", 17 January 2025, <https://rednoticemonitor.com/examining-interpol-s-new-silver-notices-tracking-criminal-assets-or-targeting-dissidents/>, accessed 18 March 2026.

INTERPOL is of course clear that none of its notices or diffusions constitute binding legal obligations on states. Silver Notices must comply with all the same non-politicisation conditions contained in the INTERPOL constitution, and the CCF has oversight to ensure compliance. Yet these and other safeguards may not be sufficient for curtailing unintended impacts. States hosting suspected criminal assets subject to a Silver Notice are likely to enact administrative powers such as asset or account freezes,[45] which require no evidence of criminal wrongdoing, but has significant negative impact on the targets of politicised notices. Indeed, the Federal Bureau of Investigations in the United States has categorised "abusive legal practices" including asset freezes as a form of transnational repression.[46]

In this way, there is a notable risk of abuse for Silver Notices targeting supposed criminal assets, and which prompt asset freezing as a means of rapid cooperation to tackle transnational financial crime. In reality, the case may be that a dissident overseas finds their assets or bank accounts frozen by their host authorities as a response to a Silver Notices issued by their home country.

Like with international sharing of financial intelligence, the abuse of international law enforcement cooperation mechanisms for (financial) TNR serves to disguise politically motivated investigations or prosecutions. The consequence: trust is shattered as partner agencies are forced to weed-out politicised requests from genuine ones, a waste of time and resources that could otherwise be allocated to combatting actual crime.

[45] For more on the consequences of asset freezing where targets are the victims of instrumentalised AML/CFT measures, see Reimer "Weaponisation of the FATF Standards", pp. 28-29.
[46] FBI, "Transnational Repression", <https://www.fbi.gov/investigate/counterintelligence/transnational-repression>, accessed 25 March 2026.

## De-Banking From Abroad: Contaminating Tools for AML/CFT Compliance

> *"This is precisely why I want to address the specific link in the chain that facilitates the export of repression from post-Soviet dictatorships into the free world: Compliance Data Provisioning companies."*[47]

Politically motivated terrorism designations of individuals by home countries have emerged as useful means of transnationally repressing dissidents in host countries, as FATF-mandated financial crime compliance expectations on the private sector result in bank de-risking and financial exclusion of dissidents. This is achieved where home countries list dissidents on their own domestic list of terrorists, which is then picked-up by third-party compliance data providers such as Dow Jones Risk & Compliance, Lexis Nexus, and LSEG (formerly Refinitiv),[48] alongside "adverse media" content that associates individuals with terrorist movements. Data trawling techniques[49] turbocharged by artificial intelligence may pick-up, for example, unverified local media reports from an authoritarian state linking a person to a nationally designated terrorist group,[50] resulting in their name being tagged as "terrorism-related" in the database product. These database tools are a go-to resource for bank compliance staff to conduct due diligence/know your customer checks for new and existing clients.

Being flagged up as a terrorist on those databases has given impetus for many banks to promptly close accounts. When queried by their clients about such actions, banks typically do not justify those closures in accordance with FATF obligations to not "tip-off" suspected criminals or otherwise reveal their compliance tradecraft; knowledge of which could then be used to devise workarounds.

[47] Quote from Dmitry Navosha, who brought a case before the UK's Information Commissioner's Office concerning his terrorism designation by Belarus being replicated in a database maintained by Down Jones Risk & Compliance.
[48] Koos Couvee, "Global AML Standards, Third-Party Databases Inadvertently Aiding Authoritarianism", *MoneyLaundering.com*, 13 August 2024, <https://www.acams.org/en/news/global-aml-standards-third-party-databases-inadvertently-aiding-authoritarianism>, accessed 25 March 2026.
[49] Data trawling refers to the automated, wide-scale scanning and aggregation of information from numerous digital sources to identify matches against specific criteria or patterns, regardless of source verification or contextual accuracy.
[50] For detailed examples from Turkiye, see Solidarity with Others, "Misuse of FATF Standards as a Tool of Transnational Repression", February 2025, <https://solidaritywithothers.com/misuse-of-fatf-financial-action-task-force-standards-as-a-tool-of-transnational-repression/>, accessed 27 March 2026.

Rosfinmonitoring, the FIU of the **Russian Federation**, maintains a list of "terrorists" and "extremists" for purposes of implementing AML/CFT obligations, like FATF Recommendation 6 which calls on states to apply counter-terrorism sanctions in line with UNSCR 1267, and to make domestic terrorism designations in line with UNSCR 1373. For Russia, these designations include countless human rights defenders, but also everyday offenders of political crimes like offending the Russian military.

Regardless of the legitimacy of their supposed "terrorism", individuals subjected to those listings, once absorbed by the above-mentioned database providers in a largely automated process, generate alerts within overseas financial institutions that a client has been associated with terrorism and is therefore – again, automatically - regarded as high-risk for terrorism financing. A perverse financial incentive drives the problem: data providers compete with one another to sell a superior product - which in the world of AML/CFT equates to the largest database possible containing the most risks possible,[51] even if many of these are unverified and the product of politicisation.

**Turkiye** is another prolific abuser of this method of financial transnational repression. Lawyers Michael Polak and Ali Yildiz surveyed 34 overseas Turks who were targeted by terrorism-affiliated asset freezing orders issued by Turkiye in April and December 2021. Respondents suffered several consequences, including account closures and declined account openings. Lines of credit and accounts with online payment platforms were also cancelled following designations. Survey participants claim that their financial institutions became aware of the Turkish listings through alerts issued by the compliance databases tools they use, with some participants even claiming that "the Turkish embassy in his/her country visited the banks and informed them" about the listings.[52]

Some individual cases of this form of financial TNR are rectified on the back of persistent self-advocacy, resulting in supposed terrorist affiliations being removed from the database or additional contextualising information being added to one's entry. For example, Ismail Sezgin's supposed affiliation with the Turkish-designated

[51] Alexandra Prokopenko, "The Kremlin Has Weaponized Western Financial Checks to Punish Russian Dissidents", *Carnegie Politika*, 13 November 2025, <https://carnegieendowment.org/russia-eurasia/politika/2025/11/russia-eu-banking-exploits>, accessed 25 March 2026.
[52] Michael Polak and Ali Yildiz, "Weaponization of Anti-Terror Financing Measures: The Turkish Government's New Transnational Repression Tool to Silence Its Critics", International Journalists Association, July 2022, <https://aliyildizlegal.com/wp-content/uploads/2022/09/barcode_ija-report-weaponization-of-anti-terror-financing-measures.pdf>, accessed 25 March 2026, pp. 9-10.

Fethullah Terrorist Organisation (FETÖ) was eventually updated in LSEG's World Check database to reflect the politicisation of FETÖ sanctions in Turkiye and that his designation carries no legal obligations outside Turkiye.[53] Another target of the same association with FETÖ, Mehmet Baltaci, brought libel charges against the provider of World Check and was awarded £10,000 in damages in a settlement.[54]

Piecemeal remedies, however, fail to address the systematic pollution and corruption of these database tools by ill-intentioned regimes, who succeed in perpetrating financial transnational repression by using these essential AML/CFT compliance tools used by financial institutions every day to amplify and extend the reach of their national terrorism designations.

Across all three sub-types of financial transnational repression, we see a common competition between priorities: speed of cooperation and action against transnational financial crime; and robustness of human rights safeguards. Financial transnational repression becomes possible where tools for quicker AML/CFT cooperation and compliance, needed to stay abreast of criminal innovations, are hijacked and rerouted to meet ulterior motives under the guise of meeting FATF expectations.

# OPPORTUNITIES FOR CIVIL SOCIETY PUSH-BACK

## Reframe the Debate: Speed v. Safeguards

Systems must benefit from both prompt action against genuine threats and safeguards against abuse. Advocacy approaches to counteracting authoritarian tactics need not contend with the equally important aim of rapid and effective law enforcement cooperation and private sector compliance with AML/CFT objectives. Effective partnerships that thwart illicit finance must be genuinely trusted partnerships. When authoritarian or ill-intentioned states systematically abuse these tools, doubt is injected into the system, having pernicious effects. Democratic or well-intentioned states are

[53] Couvee, "Global AML Standards, Third-Party Databases Inadvertently Aiding Authoritarianism".
[54] Neil Johnston, Flora Bowen, "Database Giant Used by Banks Wrongly Flagged up Businessman as a Terrorism Risk", *The Telegraph*, 20 July 2023, <https://www.telegraph.co.uk/news/2023/07/20/data-giant-refinitiv-wrongly-labelled-businessman-terrorist/>, accessed 30 April 2026.

faced with a choice: to blindly trust counterparts and private data-providers; or to scrutinise these inputs, thus wasting precious time and resources that could be spent on genuine investigations and prevention. Robust, principled safeguards that promptly and consistently filter-out politicised information requests, INTERPOL notices, and database red-flags would serve to speed-up legitimate cooperation: delivering on both improved AML/CFT outcomes alongside respect for human rights. This core principle underpins each of the proposed advocacy pathways offered below.

## Advocacy Pathways

### Challenging foreign agent laws which abuse the mechanisms or justifications of AML/CFT

1. *Showcase how proposed laws would contravene FATF standards, drawing on the FATF Recommendations and FATF's Unintended Consequences workstream.*

In Slovakia, for example, attempts at passing a Foreign Agents Law took the form of proposed amendments to the country's main law on non-profit organisations, which is examined under the FATF assessment of compliance with Recommendation 8 on non-profit organisations and terrorism financing. If this law had not been struck down by the constitutional court, it might have otherwise been challenged at the FATF level by demonstrating how the law would be highly disruptive to "legitimate non-profit activity", a core aspect of the revised Recommendation 8.

Similarly, a provision in Kyrgyzstan's foreign agents law, authorising the Ministry of Justice to request and obtain banking information on listed entities from their financial institutions, violates the country's law on banks and banking activity. Should this transmission of banking information occur via the country's FIU (ie. a request coming from the ministry to the FIU to, in turn, solicit banking information from a private financial institution), an argument could be constructed that this violates the principles of FIU operational independence enshrined in FATF Recommendation 29.

Further, foreign agents legislation proposed by the parliamentary opposition in Moldova (and thus unlikely to be passed into law at this time) would permit asset and bank account freezing as a sanction against organisations that meet the criteria of a "foreign funded

organisation" but fail to declare this. This could be argued to be an improper use of asset freezing powers outlined under Recommendation 4 of the FATF standards, particularly if exemptions for allowable expense or rights to judicial review to freezing are not made available.

In all instances, engagement with MONEYVAL assessors or with MONEYVAL outside the mutual evaluation process could help in dragging foreign agents laws and restrictive measures into the scope of FATF evaluations. This could be achieved in various ways including, for example, through outreach to assessment teams in the months before a scheduled assessment visit to inform the scoping notes that will guide what issues the on-site assessment will delve into. In the case of grey-listed countries, such issues could be eligible for review under the Unintended Consequences mechanism,[55] provided that adequate alignment with FATF or FATF-Style Regional Body (FSRB) members, the World Bank or the IMF is present to trigger the mechanism.

### *2. Ally with technical implementers, leveraging their influence to push back against laws which would task them with further (unwanted) duties.*

Identify and ally with the agencies or private sector entities who would be the "implementers" of such laws and who may be disincentivised from taking on further responsibilities. More generally, building coalitions with domestic banks about shared compliance burdens and costs between the financial and civil society sectors would be a strong basis from which to initiate push-back against further restrictive regulation and measures. While in the case of Hungary it seems the Hungarian Bankers Association spoke out against the proposed law without coordinated action involving civil society actors, other cases may require civil society engagement to spark interest in pushing back and to help craft advocacy strategies. These ought to be based on technical, possibly financial (profit) rationale and be implementer-facing.

[55] See ECNL, "FATF Unintended Consequences Process", 22 August 2025, <https://ecnl.org/publications/fatf-unintended-consequences-process>, accessed 30 April 2026.

3. *Appeal to international financial institutions and other technical bodies to consider the impacts of proposed foreign agents laws on, among other things, long term economic development or investment climate.*

Stronger linkages between civil society and international financial institutions, such as development banks and credit rating agencies,[56] could assist with framing restrictions on civil society as a threat to investment climate and overall economic development, prompting further economic actors to join in push-back.

## Challenging financial transnational repression

4. *Direct engagement with the Egmont Group's working groups via observer members and/or likeminded FIUs to:*
    a. *Propose a project in the Policy and Procedures Working Group (PPWG) to devise a technical protocol for member FIUs to follow to help filter out politicised FIU requests (based on objective, technical criteria);*
    b. *Trigger Support and Compliance processes on problematic FIUs through the Membership, Support and Compliance Working Group (MSCWG).*

Where civil society advocates can identify instances of misuse of FIU information sharing powers – or cases where legislative or other policy changes enable or raise risk of such abuse – direct engagement with the Egmont Group of FIUs may help in awareness raising and push-back. Egmont observers include like-minded organisations such as the OSCE, World Bank and MONEYVAL,[57] who could raise concerns on behalf of CSOs and use information collected by them. It may be necessary to identify other like-minded, reliable organisations that are eligible for observer status at Egmont, and to support their application. Egmont observers have a standing invitation to attend plenary and working group meetings and may submit "proposals/projects of mutual interest and benefit to the Egmont Group".[58] Supportive observer organisations and/or current FIU members may propose a concept to the PPWG for a project that devises

[56] See, for example, a case from Paraguay where a proposed foreign agents law was taken into consideration by Fitch Ratings in their assessment of the country's rule of law. This contributed, in part, to the country receiving a below investment grade rating from the agency. *ABC*, "Anti-NGO Law Affects Paraguay's Rating, According to Fitch Ratings", 22 October 2024, <https://www.abc.com.py/economia/2024/10/22/ley-anti-ong-afecta-calificacion-de-paraguay-segun-fitch-ratings/>, accessed 30 April 2026.
[57] Egmont Group, "Affiliates", <https://egmontgroup.org/affiliates/>, accessed 23 March 2026.
[58] Egmont Group, "Egmont Group of Financial Intelligence Unites Charter", revised November 2025, <https://egmontgroup.org/wp-content/uploads/2022/07/1.-Egmont-Group-Charter-Revised-Nov-2025-English.pdf>, accessed 23 March 2026, pp. 10-11.

a protocol for member FIUs to help identify and filter out information requests that have a high likelihood of being politically motivated. Such a protocol would be evidence-based and draw on objective, technical criteria to be devised by the project team. Establishing such a protocol would support member FIUs to be compliant with Egmont's principles for information exchange and the FATF's standards related to confidentiality and protection of financial information shared in the name of AML/CFT.

Further, Egmont's Support and Compliance process is managed by the MSCWG,[59] the Egmont body responsible for maintaining high standards among members, including in relation to FIU operational independence and principled information sharing. It provides four pathways (or "triggers") for informing the group of member state non-compliance with Egmont principles. Under Trigger 2 member FIUs must inform the Secretariate of any significant changes[60] that could affect their or other members' compliance with Egmont rules. Failing to do this makes a Trigger 4 process applicable, whereby another member or any part of the Egmont operating structure, including working groups hosting observer members, can notify the secretariat to launch a Support and Compliance Process. Further, a Trigger 3 process is launched automatically following poor performance on FIU-related aspects of a mutual evaluation (namely non- and partially-compliant ratings on Recommendations 29 and 40, and low or moderate ratings on Immediate Outcomes 2 and 6). These include specified benchmarks such as "the FIU does not protect the security and confidentiality of information exchanged with counterparts" and "the FIU faces challenges related to its operational independence and autonomy, which affects the proper development of its expected functions".[61]

Dissuasive sanctions resulting from a failure to address the non-compliance highlighted by these processes include suspension from the Egmont Secure Web, and suspension or removal of membership. Advocacy efforts to launch such processes within Egmont on problematic FIUs – as well as the development of the above-mentioned protocol – would enhance Egmont's ability to scrutinise,

[59] Egmont Group, "Working Groups: Membership, Support, and Compliance Working Group (MSCWG)", <https://egmontgroup.org/working-groups/mscwg/>, accessed 23 March 2026.
[60] "Significant changes" are defined by Egmont as legislative, regulatory and/or administrative changes that impact organizational structure, mandate, operational status or activities of the FIU that may affect their compliance with the Egmont Group requirements or infringe on other members' functioning or mandate. See Egmont Group, "Egmont Group of Financial Intelligence Units Support and Compliance Process", updated November 2025, <https://egmontgroup.org/wp-content/uploads/2014/06/EG-New-Support-and-Compliance-Process-November-2025.pdf>, accessed 26 March 2026, p. 24.
[61] Egmont Group, "Egmont Group of Financial Intelligence Units Support and Compliance Process", p. 30.

call-out and appropriately sanction misuse of FIU-FIU information sharing and increase the costs of doing so.

### *5. Target banking regulators to establish rule-changes on account closures and denial of services, to enhance transparency of private sector decision making and possible connections with financial transnational repression.*

Cases of financial transnational repression that result in victims being shut-out of the banking system are exceedingly difficult to identify owing largely to FATF provisions on "tipping-off", where financial institutions are required not to notify (or imply or suggest through their actions) a customer that a suspicious transaction report has been filed related to them. Broadly, this extends to a "say as little as necessary" approach taken by banks,[62] to limit the risk of inadvertently signalling to customers that they may be of interest to law enforcement or, in the case of financial TNR, other governments. Despite these rules, recent amendments to financial sector regulations in the United Kingdom (UK) require banks to provide clear, written justification for account closures, in part to aid customers choosing to challenge decisions through channels like the country's Financial Ombudsman Service.[63] In theory, where an account has been closed off the back of a politicised FIU request or a terrorism red-flag raised by a compliance database, customers can be automatically informed of that rationale for their account closure.

Advocacy towards the banking sector and relevant regulatory bodies outside the UK should seek to carve out similar transparency enhancing measures, though the UK provision has its own drawback. Exceptions related to money-laundering omit financial institutions from the obligation to justify closures if they have "reasonable grounds to suspect that a payment service [has, is, or will be] used in connection with a serious crime".[64] Here, awareness raising to financial institutions and regulators on this issue is urgently needed to compel more compliance officers to go further than merely, for example, taking a World Check alert at face value when forming those reasonable grounds for suspicion.

---

[62] See Kalyeena Makortoff and Anna Isaac, "Bank Rule Changes After Nigel Farage Furore Could Tip Off Criminals, Say Experts", *The Guardian*, 22 July 2023, <https://www.theguardian.com/uk-news/2023/jul/22/bank-rule-changes-nigel-farage-closure-accounts-criminals-money-laundering>, accessed 26 March 2026.
[63] HM Treasury and The Rt Hon Emma Reynolds MP, "Millions of People and Businesses Protected Against Debanking", press release, 28 April 2025, <https://www.gov.uk/government/news/millions-of-people-and-businesses-protected-against-debanking>, accessed 26 March 2026.
[64] Draft Statutory Instruments, "The Payment Services and Payment Accounts (Contract Termination)(Amendment) Regulations 2025", <https://www.legislation.gov.uk/ukdsi/2025/9780348271485/pdfs/ukdsi_9780348271485_en.pdf>, accessed 26 March 2026.

Exposing cases of financial TNR and illustrating the scale of the problem could assist further advocacy to secure preventative measures. Furthermore, concretising financial TNR within the broader TNR playbook will serve to raise awareness among victims, recasting what might be perceived as atomised instances of financial exclusion, as implication in a systematic abuse of AML/CFT systems.

### *6. Explore strategic litigation pathways to confront financial TNR on data privacy grounds.*

Past litigation approaches related to the De-Banking from Abroad tactic offer insights for future strategic litigation efforts. Some data-protection authorities have ruled that they are in no position to challenge, for example, the legitimacy of a national terrorism designation from a foreign state or foreign court.[65] From a data-privacy perspective, AML compliance tools are not seen to violate subject's privacy, as they merely aggregate information available in the public domain, without passing judgement on its authenticity. Further, the case of Mehmet Balaci was settled out of court, a legal outcome that assigns no wrongdoing to the part of the defendant. Future strategies might further the position that information, such as a dissident's politically motivated terrorism designation by their home state, is re-shaped and legitimised by AML compliance tools, including inaccurate information.

[65] See the case of Dimitry Navosha in Anton Saifullayeu and Natasza Krawczky, "Abuse of the Counter-Terrorism and Financial Control Frameworks by the Lukashenka Regime Through the Inclusion of Targeted Exiled Individuals in the Government-Drawn List of 'Extremists' and 'Terrorists'", Institute of Central Europe and International Strategic Action for Network and Security, October 2025, <https://ies.lublin.pl/wp-content/uploads/2025/10/ies_policy_papers_no_2025-010.pdf>, accessed 30 April 2026.

# THE FATF'S LONG SHADOW OVER CIVIC SPACE

European Center for
Not-for-Profit Law