Observatoire ARGA

Report on Sanctions and Compliance for 2025

Transnational pressure through financial channels: analytical case review

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA – Sanctions and Compliance Division

Correspondence Address: 14 rue Jacques Laffitte, Bayonne, 64100

Contact: info@argaobservatory.org

Paris, 02 November 2025

Table of Contents

Executive Summary

Report identifies the emergence of a new type of transnational pressure in which state actors employ financial mechanisms — AML/CTF procedures, FIU requests, sanctions framing, banking KYC/EDD controls and asset freezing — not to prevent money laundering, but as unconventional instruments of influence beyond domestic jurisdiction.

In several CIS and neighbouring states, there is a sustained practice of exerting pressure on entrepreneurs, journalists, activists, NGOs and investors residing in the EU, the UK, the UAE, Turkey, Switzerland and other jurisdictions via financial infrastructure. Unlike classical prosecution, such pressure is silent, without warrants or public charges, making it difficult to track yet highly effective.

Mechanisms of transnational influence include:

- falsified, incomplete or misleading FIU requests sent to foreign banks with generic phrasing;
- international Freeze Actions where asset blocking is triggered by a risk signal without court approval;
- sanctions shadowing — simulating sanctions exposure to create an impression of sanction linkage where none exists;
- automated banking de-risking triggers acting without human review;
- political motivation masked as economic predicates ("money laundering", "tax evasion", "foreign financing");
- parallel use of Interpol, extradition channels and AML signals, producing cumulative coercive pressure.

The defining feature is cross-border asymmetry: the requesting state bears no responsibility for consequences, while international banks and AML supervisors face escalating risks of wrongful freezes.

The report is based on dozens of Observatoire ARGA cases (public and NDA) collected 2021–2025. These materials allow us to:

- map financial pressure across 11 jurisdictions;
- identify typologies and recurring triggers;
- form a transnational risk map for banks, FIUs and regulators;
- present analytical findings on automation growth, declining transparency and convergence of economic and political instruments;
- develop recommendations for FATF, OFAC, EU DG FISMA, Interpol, global banks and crypto-platforms.

Thus, the report documents an emerging phenomenon in which financial infrastructure becomes a tool of cross-border coercion without overt prosecution, yet resulting in severe consequences — asset freezes, business collapse and forced migration.

METHODOLOGY

1. **Case-based research: 12 anonymised ARGA transnational cases**

Analysis is based on twelve real cases of cross-border financial pressure involving AML/KYC controls, FIU requests, freeze actions and parallel international procedures. For each case we reconstructed:

— decision sequence from initial signal to final outcome,

— jurisdictions involved in the request chain,

— impact on assets, business continuity and individual status,

— transition point from financial measure to political-administrative coercion.

All data is fully anonymised to maintain legal safety without compromising analytical value.

2. **OSINT: Egmont Group, OECD, FATF, World Bank INT, global media, public complaints**

   Sources include:

   — Egmont Group guidance on FIU information exchange,

   — OECD materials on anti-corruption instrument misuse,

   — FATF country/thematic reports (especially Immediate Outcomes 3 & 6),

   — World Bank INT analytical briefs,

   — FT, Reuters, Bloomberg, OCCRP,

   — open filings, court submissions, public complaints on unjust freezes.

   OSINT served not as illustration but as validation.

3. **Forensic financial analysis: Freeze Actions, request chains, bank algorithms**

   We applied a forensic decision-trace reconstruction examining:

   — freeze structure (initiator → transmission → execution),

   — FIU request routing across jurisdictions,

   — internal bank logic (risk scoring, sanctions-shadowing triggers, nationality flags),

   — presence/absence of manual review,

   — time lag between signal and freeze.

   This differentiation isolates system error from deliberate transnational leverage.

4. **Legal comparative method: FIU–FIU exchange, AML regimes, international requests & Interpol**

Comparative study across the EU, UK, Switzerland, UAE and CIS states covered:

— minimum requirements for FIU request validity,

— evidentiary thresholds for administrative vs court-based freezing,

— FIU-to-FIU forwarding protocols,

— boundaries of legitimate Interpol/extradition usage,

— availability of appeal mechanisms.

Findings show that lack of filtering converts external risk signals into automatic repressive outcomes.

5. **Double-source verification: each scheme confirmed by ≥2 independent sources**

   Every analytical claim underwent dual verification via:

   — document–interview correlation,

   — OSINT + expert confirmation,

   — exclusion of single-source assertions.

   This reduces interpretive risk and ensures reproducibility despite opacity.

KEY CONCEPTS

Transnational Financial Pressure (TFP) — cross-border financial coercion in which a state influences individuals located outside its jurisdiction through AML/CTF procedures, asset freezing, KYC controls and international information-exchange channels, without the need for formal prosecution.

FIU Message Propagation (FMP) — transmission of false or partially false intelligence through FIU channels internationally. Even without evidentiary basis, such signals trigger foreign bank freezes, causing chain-reaction effects and eliminating opportunities for reverse verification.

Sanctions Shadow Pressure (SSP) — artificial linkage of an individual or entity to a sanctions environment. The initiating state creates the appearance of sanctions exposure despite the absence of actual restrictions, leading to automatic refusals and freezes.

Freeze Action Cascade (FAC) — cascading multi-jurisdictional freezes triggered by a single risk signal. One FIU message or alert results in asset blocking across several countries without independent validation, making outcomes transnational and difficult to reverse.

Interpol–FIU Coupled Pressure (IFCP) — combined use of Interpol mechanisms and financial requests. Freeze actions are applied in parallel with notices or extradition signals, amplifying perceived risk — even when the request is later deemed politically motivated.

Cross-Border Constructed Risk (CBCR) — creation of an artificial international risk profile, where an individual becomes high-risk due not to activity but to accumulated unverified signals across jurisdictions. This profile persists automatically even after claims are withdrawn.

REGIONAL OVERVIEW

Observatoire ARGA records persistent forms of transnational financial pressure originating from eleven countries: Russia, Kazakhstan, Uzbekistan, Azerbaijan, Kyrgyzstan, Belarus, Tajikistan, Turkmenistan, Georgia, Moldova and Armenia. Despite differences in political systems and institutional independence, these jurisdictions demonstrate similar mechanisms of cross-border financial signal transmission.

Core patterns:

1. CIS FIUs transmit incomplete or distorted intelligence to foreign banks.

   Requests frequently contain vague language, lack predicate-offence description, quantified damage or supporting evidence. Despite this, foreign banks classify such alerts as high-risk due to the absence of verification mechanisms or access to source material.

2. Banks in the EU/UK/CH/UAE apply automated freeze algorithms.

   Asset freezes are initiated by automated de-risking and KYC-screening systems without human review or contextual analysis. Combined with national signals, this produces immediate blocking even in the absence of suspicious transactions.

3. Freezes are initiated with no damage, no predicate, no forensic review.

   Asset restrictions are often applied prior to case initiation or financial-economic assessment, functioning as pre-emptive punishment where losses fall on entrepreneurs and investors rather than authorities.

4. Interpol and AML are deployed in parallel to intensify pressure.

   Even unconfirmed Red Notice attempts are interpreted by banks as high-risk indicators. The “freeze + Interpol” combination amplifies coercive effect and simulates legitimacy, though such notices are later frequently deemed political.

5. Investors, journalists and beneficial owners face international isolation via financial tools.

   Consequences include offboarding, denial of banking access, cross-border asset freezes and transactional paralysis — all without judicial decisions or appeal mechanisms, forming a new model of transnational coercion.

TYPOLOGY OF ABUSES

1. **FIU Shadow Export** — export of false or unverified FIU signals.

A financial intelligence unit sends incomplete, distorted or intentionally inaccurate data abroad without framing it as a formal international request. Such messages typically contain vague wording ("possible money laundering", "risk of illicit transactions") without evidence, quantified damage or a predicate offence. Because FIU channels are considered highly reliable, even an unofficial signal can trigger automated response mechanisms. The initiating state avoids responsibility, while consequences — freezes, offboarding, blocked transfers — materialise in jurisdictions where the affected party cannot defend itself.

2. **Cross-Border Freeze Propagation** — cascading freezes across jurisdictions.

   After a single risk signal, blocking spreads step-by-step: one bank freezes funds, correspondent banks mirror it, then payment platforms and crypto services follow. As a result, the client can lose access to accounts simultaneously in the EU, UK, Switzerland or UAE. No jurisdiction makes an independent decision — each relies on the previous one, creating a snowball effect. Even if the original signal is later dismissed, the cascade may persist for months due to the lack of coordinated unfreezing procedures.

3. **Sanction-Mimicking** — simulated sanctions profile.

   Banks are led to believe that a person is linked to sanctioned structures despite the absence of any listing. The illusion may be created through suggestive FIU wording, references to "proximity to sanctioned actors", or confusion with similarly named entities. Fearing secondary sanctions, banks impose immediate offboarding or freezes. A de-facto sanction emerges without legal sanctions, placing the individual in financial isolation with no legal basis.

4. **Interpol Reinforcement** — R/Blue/Diffusion Notice + FIU pressure.

   The state initiates an Interpol notice simultaneously with FIU alerts. Even if the notice is unconfirmed or appears political, its mere presence in Interpol systems is interpreted as critical risk by banks. Combined mechanisms accelerate initiation of freezes, prolong their duration and make reversal almost unattainable. This coupling generates quasi-sanction effects without legal sanctions or court rulings.

5. **Constructed High-Risk Profile** — artificial assignment of "high-risk" status.

   Risk scoring reflects accumulated fragments of unverified alerts rather than transaction history or legitimate source of funds. Internal banking systems store such flags permanently, so even after rebuttal, the risk score remains elevated. The individual becomes "structurally high-risk", faces service denials across countries and often loses access to basic financial infrastructure.

6. **Regulatory Ambiguity Exploitation** — leveraging differences between EU/UK/UAE/CH regimes.

   Abuse exploits gaps between national standards for FIU requests, freezing thresholds and appeal procedures. The initiator targets the weakest link — e.g., absence of mandatory second-layer review — allowing an unverified signal to pass. It then propagates to stricter jurisdictions where it appears "validated". Transnational impact is achieved without meeting minimum evidentiary standards.

7. **Crypto-Chain Distortion** — manipulating transaction chains to create suspicion.

A false impression of illicit origin is formed by referencing an address linked to illegal flows deep in the chain or by artificially intersecting transaction paths. Platforms relying on automated AML flags freeze assets without proper chain analysis. Legitimate funds become "contaminated", shutting the investor out of stablecoins, exchange wallets and P2P services. Unfreezing requires months and independent forensic reporting.

8. **Corporate TFP** — transnational pressure in corporate conflicts.

   Financial channels are used to seize control or redistribute ownership between business groups. Initial administrative checks or media framing are followed by a FIU-triggered freeze on foreign accounts, paralysing operational liquidity. The company loses solvency and is pushed into concessions — ownership transfer, management change, withdrawal of claims. Formally an AML procedure, in practice a tool of corporate coercion with cross-border reach.

COUNTRY ANALYSIS

Russia

– **Parallel Interpol + FIU requests.**

Russian authorities simultaneously trigger Interpol notices (including Diffusion and Blue Notice) while transmitting signals via FIU channels even at early or politically sensitive stages of a case. Banks interpret such combined inputs as critical risk and freeze accounts automatically, creating cross-border pressure without formal sanctions.

– **Freezes in EU/UK/CH under Articles 159/160/199/210.**

Standard economic charges—fraud, embezzlement, tax evasion, criminal association—serve as a universal pretext. Foreign jurisdictions treat these as serious financial crimes, leading to immediate freezes regardless of evidentiary stage or forensic review.

– **Exported Risk Files to EU and Middle Eastern banks.**

Russian materials are transmitted as "information signals" rather than formal requests, bypassing political-motivation checks. Banks record these tags internally and propagate them across correspondent networks, forming a persistent international risk profile.

– **Pressure on emigrants, investors, journalists.**

Freezes and offboarding function as leverage to force return, halt investigative activity or compel asset divestment. Even when cases are dropped, access is restored only partially and with delays, reinforcing isolation.

Kazakhstan

– **Active FIU use of Egmont channels.**

Requests are sent to EU/Swiss/UAE/Turkish banks rapidly and often at inquiry stage before a predicate is established. Egmont-level routing raises perceived reliability, triggering automatic offshore freezes.

– **Freezing corporate assets abroad.**

Subsidiary, holding and export-linked accounts are blocked, interrupting supply chains and payments. Measures precede court decisions and frequently lack proven damage, functioning as economic leverage.

– **Pressure on major enterprise owners.**

High-risk zones include construction, logistics, extractives and agribusiness. Freezes operate as negotiation tools to shift control or force shareholders' return.

– **Instrument of corporate conflicts.**

Affiliated groups may initiate checks that prompt transnational freezes as part of asset disputes. Even after unfreezing, damage remains irreversible—from liquidity loss to full market exit.

Uzbekistan

– **Freezes in UAE/Turkey/EU.**

Asset lockups frequently occur outside Uzbekistan, affecting family offices, holdings and real estate. Freezes operate as a surrogate for extradition: return of an entrepreneur to Uzbekistan becomes the implicit condition for "settlement."

– **FIU requests without predicate description.**

Signals include generic wording such as *foreign financing* or *possible illicit enrichment* with no facts, damage amount or expert review. International banks interpret such requests as high-risk and initiate automatic freezes.

– **Cross-border asset redistribution mechanisms.**

Financial pressure is used in elite disputes and corporate conflicts: an investigation is opened, overseas assets are frozen, and "negotiations" follow. Lack of access to case files makes contesting the measures nearly impossible.

Azerbaijan

– **Freezes targeting journalists, NGOs, opposition-linked figures.**

Asset freezes are applied as a primary instrument of pressure, without financial charges and prior to forensic review. Accounts of media groups, rights organisations and independent analysts are blocked, stopping operations before formal proceedings begin — a fast neutralisation tool without public process.

– **Cross-border blocking in Georgia, Turkey, EU.**

Restrictions extend to foreign accounts and grant flows, especially in neighbouring jurisdictions with operational structures and personal holdings. Offshore routing frustrates appeals and creates long-term financial isolation.

– **Tax/currency offences used as predicate.**

Instead of explicit political grounds, authorities rely on *illegal entrepreneurship*, *currency violations* or *money laundering* articles. This enables freezes without high risk of the case being classified internationally as political.

Kyrgyzstan

– **Freezes against journalists and entrepreneurs.**

Blocks are imposed pre-charge and used to halt activity — particularly where corruption investigations or infrastructure-linked disputes occur. Measures remain selective but increasingly recurrent.

– **Pressure via offshore banking channels.**

FIU signals trigger freezes in UAE, Turkey and EU accounts holding operational and personal capital. Even without evidence, banks maintain restrictions for months, turning freezes into negotiation leverage.

– **AML politicisation.**

Civic engagement, links to international funds or public criticism raise KYC-risk despite lawful financial conduct. AML shifts toward a regulatory control tool without legislative change.

Belarus

– **Freezes based on "extremist" and sanctions-linked framing.**

Financial blocks are imposed on entrepreneurs, media and NGOs labelled as *extremist* or *destructive*, even without financial violations. The designation acts as an automatic trigger for restrictions, including freezing of personal accounts.

– **Cross-border asset lockups in EU/UK.**

Requests are accompanied by references to sanctions exposure, making banks highly sensitive. As a result, assets are frozen even when individuals are not under sanctions but associated with protest activity or independent projects.

– **Pressure on protest-linked entrepreneurs.**

Freezes function as informal punishment and coercion: payments halt, contracts collapse, foreign transfers stop. Access is restored selectively, often only after behavioural change or relocation.

Tajikistan

– **Freezes targeting diaspora-linked entrepreneurs.**

Blocks apply to business figures abroad or supporting diaspora projects. Freezes are imposed pre-charge and serve as leverage for financial control and return to jurisdiction.

– **Criminal/religious predicates used instead of financial ones.**

Grounds include *extremism*, *illegal religious associations* or *national security threats*. Such framing avoids political scrutiny and triggers foreign freezes automatically.

– **FIU signals transmitted to RU/TR/EU banks.**

Requests circulate through cross-border channels without supporting evidence, leading to multi-jurisdiction freezes. Access to documentation is absent, and 解除 depends on informal decisions rather than court review.

Turkmenistan

– **Opaque FIU requests.**

Financial intelligence discloses no methodology, grounds or statistics, preventing verification. Requests lack predicate detail and enable preventive freezes for indefinite periods.

– **High nationality-based blocking risk.**

Turkmen citizenship itself triggers risk in EU/UK/UAE, causing onboarding refusals, offboarding and prolonged KYC holds. Inability to verify documents amplifies automated restrictions.

– **Freeze as an economic-control tool.**

Blocks regulate access to currency, imports and major contracts—especially construction and trade—functioning as administrative leverage to maintain state monopoly over financial flows.

Georgia

– **Freezes linked to foreign-influence investigations.**

Financial measures are applied in cases involving foreign funding and NGO activity in politically sensitive areas. Freezes are imposed at early stages, before charges are filed, paralysing organisational operations.

– **Pressure on journalists and activists.**

Media outlets and civic initiatives face account suspensions and halted transfers due to “interference-risk” flags. Restrictions serve as indirect pressure without criminal prosecution.

– **AML used in politico-economic disputes.**

In some cases AML tools appear in corporate and property conflicts, including control struggles over assets. Freezes operate as temporary leverage, particularly in projects tied to foreign investors and strategic sectors.

Moldova

– **Freezes in corruption and corporate confrontation cases.**

Asset blocks occur in anti-corruption investigations and disputes around large enterprises, including banking and energy. In select cases freezes are applied pre-damage assessment, functioning as leverage over beneficiaries and management.

– **Political overlay in select investigations.**

While formally enforcement-oriented, certain cases coincide with political turbulence and institutional rivalry, creating risk of AML being perceived or used as selective pressure.

– **Heightened risk due to institutional instability.**

Judicial weakness and regulatory volatility prompt international banks to treat Moldovan clients cautiously. This manifests in intensified KYC, delayed transactions and potential offboarding in EU/UK.

Armenia

– **AML usage largely compliant and institutional.**

Armenia maintains one of the more stable monitoring frameworks in the region, aligned with FATF/Moneyval norms. FIU demonstrates autonomy, with limited reported misuse.

– **Freezes mainly in tax and corporate disputes.**

Blocks typically relate to tax evasion, governance issues or registration conflicts and generally involve court-linked procedures supported by documentation.

– **Risks stem from external perception rather than internal misuse.**

Despite domestic compliance, clients face elevated scrutiny abroad due to regional proximity to higher-risk jurisdictions and CIS-linked capital flows. This results in selective transaction delays and enhanced due-diligence in EU/UK/CH.

CASE EXAMPLES

1. Russian business migrant — IFCP scheme

FIU RU → EU bank → Freeze → Interpol → offboarding.

Following the launch of a domestic investigation, the Russian FIU transmitted a signal to an EU bank without specifying loss amount or procedural stage. The bank imposed an automatic freeze, and several weeks later a Diffusion Notice amplified perceived risk. Despite no Red Notice and the eventual closure of the case, the client was offboarded and was unable to open new EU accounts due to an internal "high-risk" flag. Partial access to assets was restored after 14 months.

2. Kazakhstan company — Corporate TFP

Corporate dispute → FIU KZ → Freeze in CH/UAE → forced control transfer.

An internal shareholder conflict was followed by a Kazakh FIU request sent to banks in Switzerland and the UAE referencing "possible financial violations." Without a court ruling, corporate operating accounts were frozen, halting exports and triggering defaults. Months later, control was transferred to another group; the freeze was lifted with no explanation, indicating use of financial pressure as leverage.

3. Uzbekistan — Cross-Border Freeze

FIU UZ → UAE banks → family assets blocked; no evidence provided.

The FIU request alleged "possible illicit enrichment" without transaction detail. UAE banks froze family accounts and trust structures, including assets unrelated to Uzbekistan. No charges followed and no evidence was shared for over a year. The freeze functioned as coercive leverage, pushing negotiations despite the absence of criminal proceedings.

4. Azerbaijan — Journalistic TFP

Investigative reporter → "money-laundering" allegation → Freeze → equipment seizure.

Days after publishing findings on procurement corruption, the journalist's banking cards were frozen under a laundering suspicion. Funds, equipment and project financing were blocked pre-investigation, with no suspicious transactions identified. Freeze acted as the primary suppression tool rather than law-based prosecution.

5. Kyrgyzstan — Media Pressure

Journalists → operational freeze → newsroom collapse.

A newsroom investigating state procurement faced freezing of organisational accounts and personal cards of staff. The stated basis was "review of foreign inflows." No charges were filed, yet the freeze lasted over six months, halting publication, terminating leases and dissolving staff. Post-unfreeze, operations could not be restored.

6. Belarus — Sanctions Shadowing

Opposition figure → Freeze in EU/UK → FIU pressure.

Despite no sanctions listing, FIU narratives referencing "links to extremist structures" were treated by EU/UK banks as high-sanctions-risk signals. Personal and corporate accounts were frozen and transfers blocked. No charges followed; restrictions were only partially lifted, illustrating sanction-mimicking as an indirect pressure tactic.

7. Tajikistan — Diaspora Targeting

Business owner abroad → FIU TJ → Freeze in Turkey and EU.

A logistics and construction entrepreneur living outside Tajikistan received informal repatriation demands. After refusal, FIU sent risk signals to Turkey/EU banks alleging "possible financing of prohibited groups." No case existed, yet personal and corporate assets were frozen. Material access was denied, and unfreezing depended on informal negotiation. Restrictions lasted ~1 year, causing contract losses and forced asset sale.

8. Turkmenistan — Nationality-Based Blocking

Client → automatic KYC rejection → Freeze without FIU request.

A Turkmen national attempted to open an account in an EU bank after relocating a business. Automated scoring assigned a *high-risk nationality* flag, triggering service refusal without any source-of-funds review. Weeks later, existing accounts in another jurisdiction were frozen "for enhanced checks," despite no FIU request from Turkmenistan. The freeze persisted for 9 months; no violations were identified, but the client was unable to restore access to international payment channels.

9. Georgia — Foreign Influence AML

Activist → FIU GE → Freeze after critical publications.

After opposing a draft Foreign Influence law, the activist received an FIU inquiry into foreign funding. The account was frozen *prior* to document submission and without loss amount or predicate. The freeze suspended projects, rent payments and travel. No criminal case was opened; restrictions were lifted only after 5 months, demonstrating AML deployment in politically sensitive contexts.

10. Moldova — Corporate AML Weaponization

Corporate dispute → "corruption" predicate → freeze of external accounts.

A shareholder conflict in an energy company triggered a corruption-related allegation. Despite lack of expert review, the FIU sent requests to EU banks, freezing overseas subsidiary accounts. Operations stopped, contracts collapsed, and one shareholder exited management under pressure. Later review found no violations, but asset access was restored only after more than a year.

11. Armenia — Economic Freeze

Tax dispute → freeze before audit.

A company entered a review for alleged tax under-reporting. Prior to audit completion and without a court order, the corporate account was frozen. Payments to suppliers stalled, production paused. Although the audit found no breach, the bank retained an *elevated-risk* tag, resulting in refusal to open accounts in another jurisdiction.

12. ARGA International Case — Crypto Distortion

USDT transfers → faulty chain link → 90-day freeze → lifted after chain analysis.

Client transactions were auto-flagged due to legacy interaction with a historical high-risk address. The platform froze assets for 90 days, demanding proof of origin but withholding technical rationale. Independent blockchain forensics confirmed legitimacy; the freeze was lifted, yet liquidity loss and market volatility caused financial damage.

RISK MAP

Country	Risk to Banks	Risk to FIU	TFP Level
Russia	CRITICAL	CRITICAL	Strongly Systemic
Kazakhstan	VERY HIGH	HIGH	Systemic
Azerbaijan	VERY HIGH	VERY HIGH	Systemic
Uzbekistan	HIGH	VERY HIGH	Systemic
Belarus	HIGH	VERY HIGH	Systemic
Tajikistan	HIGH	VERY HIGH	Systemic
Turkmenistan	VERY HIGH	VERY HIGH	Opaque Systemic
Kyrgyzstan	MEDIUM	MEDIUM	Partially Systemic
Georgia	MEDIUM	MEDIUM	Mixed
Moldova	MEDIUM	MEDIUM	Reforming
Armenia	MEDIUM	LOW	Stable with External Risks

“RED FLAGS”

1. **FIU Exported Alert**

   A signal sent by a national FIU to a foreign bank contains vague wording, no predicate offence, no damage amount, and no supporting documents. These notifications trigger automatic freezing procedures even where no criminal case exists or the matter is still at the verification stage.

2. **No Predicative Offence**

   Asset freezing is applied without specifying a predicate offence — no article, no transactional evidence, no expert review, no identified victim. Freeze becomes a form of pre-punishment, where verification takes place only after restrictions are imposed.

3. **Freeze-before-investigation**

   Assets are frozen prior to case initiation, audit, or forensic financial analysis. The mechanism is used as leverage in corporate, politically sensitive, or administrative disputes rather than to prevent money laundering.

4. **Parallel Interpol Use**

   An FIU request is paired with an Interpol notice (Blue, Diffusion, or attempted Red), increasing perceived risk for banks. Even if the notice is rejected or withdrawn, consequences in the financial system persist for months.

5. **Sanctions-Mimicking**

   Artificial creation of an association with sanctions risk despite no actual sanctions in place. Terms such as “links to extremist structures” or “foreign influence” are used to trigger automatic restrictions in EU/UK/CH/UAE.

6. **Crypto Chain Distortion**

   Misinterpretation of blockchain transaction history: transferring a “dirty” status from deep-chain addresses, absence of proper chain analysis, reliance on inaccurate high-risk wallet lists. Legitimate assets become frozen for 60–120 days.

7. **Corporate TFP**

   Transnational financial pressure in corporate disputes: FIU requests trigger freezing of operational funds, followed by “negotiation offers” involving control transfer or share dilution. Judicial mechanisms are bypassed through financial leverage.

8. **High-Risk Labeling by Nationality**

A client is automatically classified as “high-risk” due to nationality or capital origin, without transactional analysis. Leads to onboarding refusals, abrupt offboarding, payment delays, and freezes even without FIU involvement.

RECOMMENDATIONS

OFAC

– **Second-layer verification for TFP-pattern countries**

Introduce mandatory secondary review for alerts originating from jurisdictions with documented Transnational Financial Pressure patterns. Freeze actions must follow evidence verification rather than rely on initial signal recognition.

– **Refusal to act on FIU alerts without predicative offence**

Restrictive measures should not be applied to FIU notifications lacking predicate description, loss amount, case stage, or documentary evidence. Any freeze without a predicate offence should be treated as a due process breach.

EU DG FISMA

– **Classify selected FIU as high-risk sources**

Designate certain FIUs from CIS states as high-risk origins, requiring enhanced verification and prohibiting automatic processing of their alerts.

– **Mandatory explanation of predicative offence**

FIU requests from third countries should be accepted only where full predicate detail is provided: facts, amounts, transactions, investigation status, and references to supporting documents.

– **Enhanced screening of CIS-origin alerts**

Implement a specialised analytical filter for alerts from the region, incorporating political-context assessment, corporate-trigger analysis, and constructed-risk detection.

FATF

– **Introduce Transnational AML Abuse metric**

Add a separate indicator to country evaluations to capture cross-border AML misuse beyond legitimate scope — including FIU export signalling and freeze actions without demonstrable loss.

– **Evaluate politicization of FIU activity**

Mutual evaluations should consider FIU independence, law-enforcement pressure, and use of financial tools in politically motivated cases.

FIU (EU/UK/UAE/CH)

– **Reject blank requests**

Do not process alerts without predicate offence, transactional description, loss estimates, or documentary attachments.

– **Require independent evidence packages**

Only review notifications accompanied by verifiable evidence rather than preliminary assumptions or generalised statements.

Banks

– **Apply TFP EDD Protocol**

Implement an Enhanced Due Diligence framework for clients from TFP-linked jurisdictions, including context scrutiny, case-status verification, and independent risk substantiation.

– **Political context analysis**

Consider the likelihood of political motivation, particularly in cases involving journalists, NGOs, emigrants, or beneficiaries of corporate disputes.

– **Reject freeze actions without evidence**

Do not apply asset freezes on the basis of undocumented signals; freezing should be a last-resort outcome, not an automated response.

CONCLUSION

Transnational financial pressure constitutes an emerging form of extra-jurisdictional control in which states employ AML/CTF instruments, FIU signalling, KYC/EDD banking procedures and asset freezing not to protect the financial system, but to influence entrepreneurs, journalists, activists and investors outside their own territory.

The core risk lies in the fact that such measures are applied without a predicative offence, without evidence and without judicial oversight, while international banks become an involuntary tool of enforcement — through automatic freezes, offboarding, and the creation of artificially elevated risk profiles.

The report demonstrates that the absence of global filtering mechanisms, fragmented regulatory standards and banks' reliance on external alerts generate a structural vulnerability that enables the export of politically driven decisions into the financial systems of other states.

International coordination is necessary: verification mechanisms for FIU notifications, refusal of freeze actions without predicate basis, integration of political-context assessment, and the establishment of safeguards against misuse. Without such steps, transnational financial measures will continue to erode trust in the AML regime, increasing the risk of unlawful isolation and the destruction of economic activity beyond national borders.

SOURCES

1. OECD, Illicit Financial Flows from Developing Countries, 2014, https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/04/illicit-financial-flows-from-developing-countries_g1g331b9/9789264203501-en.pdf.
2. FATF, Trade-Based Money Laundering, March 2021, https://www.fiu-nederland.nl/wp-content/uploads/2022/03/202103_fatf_trade-based-money-laundering-risk-indicators-1.pdf/.
3. FATF Report, Global Money Laundering & Terrorist Financing Threat Assessment, July 2010, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Global%20Threat%20assessment.pdf.
4. IFC, Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks, 2019, https://www.ifc.org/content/dam/ifc/doc/mgrt/45464-ifc-aml-report.pdf.