Observatoire ARGA

Report on Sanctions and Compliance for 2025

Use of AML/KYC Mechanisms Against Entrepreneurs and Investors from CIS Countries

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, 01 November 2025

Table of Contents

Executive Summary

The report documents a persistent and systemic pattern of AML/KYC mechanism misuse against entrepreneurs and investors from CIS countries, in which financial-control measures are applied for purposes unrelated to anti-money-laundering objectives or genuine financial-risk mitigation. In several states across the region, financial monitoring is shifting from a tool designed to protect the banking system into an instrument of administrative pressure, business control and restriction of cross-border economic activity.

Abuse is manifested across multiple practices: automatic account freezes are triggered without substantiated grounds; banks decline service without explanation or access to appeal channels; clients are labeled *high-risk* solely due to nationality or capital origin; foreign banks receive false or incomplete FIU requests; politically motivated financial cases are initiated; assets are frozen prior to verification, without established damages and without a predicate offense. These measures lead to reputational destruction, business shutdowns, involuntary loss of assets or forced return to the home jurisdiction under pressure.

Observatoire ARGA holds extensive empirical material from assisting entrepreneurs and investors from CIS states, including public cases, court documents, compliance correspondence, FIU requests and NDA-restricted files. This allows recurring patterns to be identified, institutional dynamics to be traced and transboundary effects to be documented.

The report includes:

– an expanded review of 11 jurisdictions showing state and corporate models of AML/KYC use beyond legitimate scope;

– a typology of violations, including fact-free automated freezes, politicized risk-scoring, blank FIU requests, and nationality-based denial of service;

– a risk map for banks, FIUs and compliance systems, illustrating systemic intensity and structural misuse;

– a case portfolio (public + NDA) showing application in corporate disputes, actions against investors, family offices, journalists and tech firms;

– recommendations for international banks, regulators, FATF, OFAC, EU DG FISMA and independent FIUs to reduce wrongful and politically motivated freezes;

– an infographic systematizing red flags, transborder coercion channels and automatic-trigger mechanisms.

Accordingly, the report shows that misuse of AML/KYC regimes targeting CIS entrepreneurs and investors is not an isolated irregularity but a growing transnational trend — requiring a coordinated international response and implementation of protective filters within banking systems and global regulatory frameworks.

Methodology

1. **Case-based analysis: 12 real anonymized business cases**

The study is grounded in twelve practical cases illustrating different scenarios of AML/KYC application to entrepreneurs and investors from CIS jurisdictions. The approach involved:

– tracing full event chronologies from initial bank contact to final outcome;

– analyzing documentation: compliance notices, correspondence, offboarding letters, FIU requests, legal opinions, audit materials;

– recording consequences: asset loss, service termination, reputational damage, forced business closure or relocation;

– identifying recurring triggers: corporate disputes, political exposure, capital origin, jurisdiction change;

– applying structured classification by measure type (freeze, offboarding, de-risking, enhanced scrutiny).

All data were anonymized to respect NDAs while preserving analytical transparency and reproducibility.

2. **OSINT: FATF, Moneyval, Basel AML Index, global media, FIU datasets**

The research utilized an expanded OSINT framework, including:

– FATF & Moneyval country assessments, with focus on Immediate Outcomes 3, 4, 6 (independence, cooperation, preventive measures);

– Basel AML Index 2023–2025 as a risk correlation and calibration reference;

– international media monitoring (FT, WSJ, OCCRP, Reuters, Bloomberg) for documented financial coercion cases;

– open-source FIU and regulatory data (SAR/STR dynamics, legislative amendments, supervisory guidance);

– human-rights reporting from HRW, Amnesty, Freedom House, CEPR as indirect indicators of financial politicization.

OSINT served not only as context but as triangulation material to validate internal findings.

3. **Financial forensic: analysis of KYC/EDD flows & FIU trigger logic**

A forensic methodology was applied to reconstruct decision pathways:

– review of internal KYC/EDD frameworks (risk scoring, source-of-funds, SOW verification);

– analysis of automated monitoring triggers (PEP-matching, nationality-risk scoring, sanctions-shadow linking);

– identification of decision points—based on evidence, documents, or external signals alone;

– detection of algorithmic de-risking (client removal without fact-based review);

– assessment of whether manual review was conducted or freeze occurred automatically.

This approach separates technical errors from politically influenced decisions and reveals systemic compliance breakdowns.

4. **Cross-jurisdictional comparison: EU, UK, CH, UAE, Hong Kong**

The report compares five jurisdictions based on:

– evidentiary thresholds for freeze measures (court-order vs administrative instruction);

– FIU-request requirements (predicate detail, evidence, amounts, documentation);

– de-freeze mechanisms & response timeframes;

– appeal rights and ombudsman access;

– automation level of AML systems (HFT-automated vs analyst-screened);

– prevalence of de-risking over individualized risk assessment.

Findings show that high-automation systems without mandatory second-layer review are most vulnerable to false cross-border signals.

5. **Double-source verification of all analytical conclusions**

Conclusions are based on two-factor validation using:

– combined documentary and interview evidence;

– cross-checks with independent experts, lawyers, ex-bank AML/EDD officers;

– reconfirmation via alternative channels (OSINT, court records, registries, media);

– incorporation only of claims verified by at least two independent sources.

This minimizes analytical error in low-transparency and politically sensitive environments.

6. **Expert validation**

Selected chapters were reviewed by:

– former international banking compliance officers;

– sanctions regulation specialists;

– cross-border litigation & extradition lawyers;

– OSINT analytics professionals.

Expert validation refined interpretation, strengthened typology accuracy and confirmed the operational realism of findings.

7. **Ethical & confidentiality safeguards**

The methodology ensured:

– full anonymization of individuals and corporate identifiers;

– exclusion of data enabling reverse identification of banks or jurisdictions;

– reliance only on verifiable structural elements;

– exclusion of leak-based or non-validated datasets.

These measures maintain legal neutrality and protect involved parties.

Key Concepts

AML/KYC Overblocking — excessive freezes without evidentiary basis.

Occurs when banks impose account freezes or deny service absent verified risk, relying on automated triggers and over-cautious policy frameworks. As a result, legitimate clients are caught in restrictions, leading to financial loss and reputational damage.

Jurisdictional Bias — elevated risk scoring based solely on nationality.

A client is classified as *high-risk* solely due to citizenship or jurisdiction of incorporation, with no assessment of transaction patterns or source of funds. This results in refusals, offboarding and silent discrimination, undermining individualized risk evaluation.

FIU Shadow Influence — informal regulatory pressure.

Banks make decisions based on undocumented FIU signals, which cannot be appealed. Such cues are perceived as mandatory, resulting in opaque freezes without accountability from the initiating authority.

Constructed Risk File — artificially engineered risk profile.

A client's record becomes "toxic" through accumulated unverified suspicions and fragmented data. Even in absence of wrongdoing, recovery takes years and access to financial infrastructure remains restricted.

Corporate AML Weaponization — AML as a corporate conflict tool.

Compliance measures are used to pressure or displace business counterparts: accounts are frozen, operations halted, and ownership redirected under the appearance of regulatory procedure.

Political AML Targeting — financial pressure with political motive.

AML tools are deployed against journalists, NGOs and entrepreneurs linked to opposition networks. Formally framed as unlawful-funding prevention, measures function as instruments of coercion and isolation.

Crypto Mislabeling — risk contamination of legitimate assets.

Blockchain transactions are flagged as suspicious without chain-analysis, due to flawed scoring or outdated tagging. Consequences include asset freezes, wallet restrictions and loss of access to stablecoins.

Regional Overview

1. **AML/KYC as a business-pressure mechanism.**

   In multiple CIS states, financial monitoring no longer performs a preventive function but operates as a lever of administrative influence: in corporate disputes, asset redistribution, capital blockage and pressure on business migrants. AML/KYC shifts from system protection to control infrastructure, prompting capital outflow and weakening institutional trust.

2. **Incomplete FIU requests to foreign banks.**

   Cross-border alerts are frequently issued without predicate offense, loss estimates or judicial basis. Despite lack of evidence, banks in the EU, UK, Switzerland and UAE react with preventive freezes because verification channels are absent and underlying case files remain inaccessible.

3. **Automatic high-risk classification of CIS clients.**

   In many jurisdictions, nationality or CIS affiliation is treated as a standalone risk factor. Clients face account refusals, abrupt offboarding and intrusive KYC despite transparent activity — forming latent origin-based discrimination.

4. **Freeze-before-verification and without proven harm.**

   Asset freezing is increasingly implemented before case initiation and expert review. In practice, funds are blocked first, and fact-finding begins later — often without resulting evidence. Losses fall on entrepreneurs: halted operations, broken contracts, liquidity collapse.

5. **Political triggers masked as economic offenses.**

   Financial restrictions substitute open political prosecution and are framed as “money laundering,” “foreign financing,” or “tax evasion.” Real triggers often involve criticism of authorities, investigative reporting, elite conflict or refusal to surrender assets. Banks become enforcement vectors, allowing governments to apply coercion while avoiding political labelling.

Country Analysis

Kazakhstan

In Kazakhstan, AML mechanisms are highly institutionalized and actively used in corporate conflicts and ownership redistribution. Freezes are applied even before forensic examination or case initiation, turning asset restriction into a pressure instrument: payments halt, contracts collapse, and leverage emerges to force negotiation. The FIU systematically sends blanket requests to banks in the EU, Switzerland and the UAE with no predicate description or evidence. Foreign banks interpret these alerts as high-risk and introduce freezes automatically, amplifying cross-border consequences.

The largest concentration of cases is observed in strategic sectors: large enterprises and holding groups, agricultural exports, oil & gas and logistics, development and commercial real estate.

Typical patterns include:

1. initiation of an inspection,
2. freezing of operating capital,
3. suspension of contracts,
4. “resolution” through forced share transfer or control change.

Thus, Kazakhstan demonstrates a stable model of improper AML use, where freezing functions not to protect the financial system but as a mechanism of administrative and economic coercion.

Uzbekistan

In Uzbekistan, AML mechanisms are used as a tool of political-economic leverage and elite competition. Freezes are imposed not for investigating financial crime, but for controlling assets of entrepreneurs linked to previous power clusters or large corporate groups.

A key feature is pressure on diaspora investors. Asset freezes are frequently executed outside national borders (UAE, Turkey, EU), where family offices and holding structures are registered—making freeze measures a de-facto alternative to extradition and an instrument for forced “settlement.” The FIU regularly issues blanket requests lacking predicate detail or proof, using vague terminology (“possible enrichment,” “foreign financing”). International banks interpret such alerts as high-risk and apply freezes automatically, resulting in prolonged lockouts without judicial authorization.

Affected segments include industry, wholesale and export trading, family business groups, logistics and transport.

Typical patterns include:

1. launch of investigation or media attack,
2. cross-border freeze,
3. prolonged status without charges,
4. proposal to transfer shares or exit operations.

Despite reform claims, FIU opacity and absence of judicial oversight entrench these practices. As a result, AML tools operate not as safeguards of financial integrity but as instruments of pressure and forced redistribution of assets.

Russia

In Russia, AML/KYC has taken the most politicized form in the region. Financial controls are used not to prevent crime, but as a tool of pressure on businesses, media and civil society. A key feature is the AML + Interpol linkage: freezes are frequently imposed in parallel with search requests, even when no Red Notice exists, when the alert is flagged as politically motivated, or when legal grounds are absent.

The mere fact of Interpol contact is treated by banks in the EU/UK/UAE as a high-risk trigger, activating automatic freezes.

A separate mechanism is the use of “foreign agent” designation in KYC risk-scoring. After placement in the registry:

– banks initiate enhanced EDD,

– offboarding and service denial become common,

– freezes are introduced even without criminal charges or predicate offense — resulting in financial isolation of NGOs, media outlets and associated persons.

Additional patterns observed:

1. Freeze without charges — at pre-investigation stage, without forensic review, including offshore accounts;
2. KYC refusal for emigrants — Russian capital origin becomes a standalone risk trigger;
3. Forced AML application — freezes used to pressure individuals to return to Russia, halt investigations or relinquish assets.

Typical sequence:

1. initiation of case or media campaign,
2. freeze without evidentiary basis,
3. parallel Interpol signal,
4. waiting for response/negotiation leverage,
5. partial unfreeze once desired outcome is achieved.

Result: the Russian model reflects a persistent merger of political and financial control, where AML/KYC functions as an extension of state coercion and a channel for extraterritorial pressure.

Kyrgyzstan

In Kyrgyzstan, AML/KYC enforcement remains selective but is expanding — shifting from isolated episodes toward a developing pattern of pressure against media, NGOs and certain business groups. Unlike Kazakhstan or Russia, mechanisms are not yet fully institutionalized, but systemic characteristics are emerging.

Freezes are imposed pre-charge, particularly against investigative journalists, NGOs with foreign funding, and investors in infrastructure/energy. FIU and law-enforcement agencies rely on vague triggers (“suspicion,” “risk of interference”), prompting automatic blocks lasting from weeks to months — without transaction evidence or loss assessments.

Political context increasingly influences KYC:

– anti-corruption reporting,

– public criticism of authorities,

– links to international foundations

act as informal risk multipliers triggering extra scrutiny.

For infrastructure and construction sectors, freezes function as a negotiation lever: operating capital is blocked, then a “settlement” or ownership concession is proposed.

While scale remains limited, the trend is accelerating: freezes last longer, FIU authority expands, and appeal transparency decreases. If trajectory continues, Kyrgyzstan may evolve into a stable model of AML-based control without formal legal reform.

Azerbaijan

Azerbaijan presents the most systematized and institutionally embedded AML model in the region, operating not as a financial-crime prevention framework but as an instrument of control over the civic sphere and economic assets. Freezes are applied to media and investigative outlets, human-rights NGOs, opposition-linked networks, and individual investors.

Grounds are typically framed under “smuggling,” “money laundering,” and “illegal entrepreneurship,” enabling avoidance of direct political qualification and reducing external reputational exposure. Outcomes include operational shutdown, funding collapse, forced liquidation of organizations and emigration of staff.

Notably extensive is the cross-border dimension of freezes — executed via offshore corridors and accounts in Turkey, UAE, Cyprus and the EU. Appeal is extremely difficult because:

– FIU does not disclose underlying grounds,

– banks cite external risk signals,

– foreign courts cannot act without access to case files.

Azerbaijan thus demonstrates a stable model of AML deployment for suppression of independent actors and redistribution of influence, with long-term, often irreversible consequences and a pronounced transnational reach.

Tajikistan

In Tajikistan, AML/KYC mechanisms are centrally controlled by security agencies — the FIU lacks operational independence, creating a high probability of politically motivated freezes. Asset restrictions are used against entrepreneurs and diaspora members, especially those conducting business abroad, connected to opposition or exile networks, or controlling significant assets.

Freezes are frequently imposed pre-charge, without predicate offense, using ambiguous national-security narratives. Unfreezing depends not on judicial review but on security-agency approval.

Highest-risk sectors include construction and infrastructure, import and wholesale trade, international logistics, and remittance-linked business. Typical scenarios:

1. investigation without evidentiary basis,
2. domestic freezes + informal warnings issued to foreign banks,
3. pressure on relatives and business partners,
4. “settlement” proposals involving asset transfer or return to Tajikistan.

Diaspora entrepreneurs are especially vulnerable — EU/UK/UAE banks report KYC refusals and freezes driven by elevated nationality-risk. Lack of appeal and opaque procedures form a model in which AML functions as capital-control architecture rather than a safeguard against crime, generating substantial cross-border exposure for both clients and institutions.

Turkmenistan

In Turkmenistan, AML/KYC enforcement operates under full opacity and security-service dominance — the FIU publishes no data and is not subject to external oversight. Freezes are enacted without predicate reasoning, forensic review or notification, and no timelines for appeal exist, making restrictions indefinite by default.

Highest-risk groups include importers and construction operators, overseas workers, and diaspora-linked capital holders. Freezes accompany politically aligned economic cases, especially involving loss of loyalty, capital export attempts, or contact with foreign organizations.

Turkmen citizens face the highest nationality-risk in EU/UK/UAE:

– automatic account-opening refusals,

– offboarding without explanation,

– prolonged KYC procedures,

– remittance blocks.

Underlying causes include unverifiable documentation, a closed banking system and high political-economic opacity. The result is structural financial isolation and severe cross-border risk exposure both for entrepreneurs and for banks that service Turkmenistan-linked clients.

Belarus

In Belarus, AML frameworks are deployed primarily in politically driven cases, where financial measures substitute direct repression. Asset freezes target entrepreneurs, IT specialists and business owners involved in protest activity, civil initiatives, independent media support, or NGO funding.

Freezes are introduced pre-charge, justified by references to “possible laundering” or “financing of extremist activity” without forensic evidence or proven financial harm.

Externally, sanctions shadowing amplifies impact — banks in the EU and UK classify Belarus-linked clients as high-risk by default due to political and sanctions overlap. This results in:

– service refusals and account closures,

– interruption of cross-border payments,

– heightened EDD even with transparent funds.

Thus, AML operates as a mechanism of financial isolation and deterrence, while international banks reinforce the effect due to elevated sanctions sensitivity and lack of independent verification channels.

Armenia

Armenia maintains a comparatively stable and institutionally coherent AML system, yet external perception drives an increase in KYC restrictions. International banks increasingly categorize Armenian clients as elevated-risk due to regional context (CIS exposure, liquidity migration, capital flows), leading to:

– more frequent account-opening refusals,

– intensified EDD on cross-border transactions,

– delays and sporadic payment freezes.

Domestic freeze measures arise mainly in tax disputes and corporate conflicts, especially in construction, IT, and import sectors. Grounds are economic, and freeze duration is generally limited.

Political influence remains moderate:

– isolated cases of NGO/media pressure do exist,

– FIU retains relative autonomy,

– judicial appeal mechanisms function, albeit imperfectly.

Risks for international banks stem less from systemic abuse and more from perception-driven risk assignment, where regional origin prompts precautionary overreaction.

Georgia

In Georgia, freezes occur selectively but are noticeable in cases involving foreign funding, investigative journalism and public criticism of authorities. Assets may be frozen pre-indictment, creating a form of preventive pressure without overt repressive acts.

Political context increasingly shapes KYC procedures:

– enhanced review of organizations with foreign grants,

– journalists and rights groups face payment delays and temporary freezes,

– banks request extended source-of-funds verification even when documentation is clean.

FIU requests occasionally lack substantiated predicate detail, using general “risk factor” arguments that trigger excess compliance responses and short-term freezes.

Although no systemic model exists, there is a clear trend toward growing politicization of financial oversight, particularly amid intensified scrutiny of foreign funding and media-linked entities.

Moldova

In Moldova, AML instruments are widely used within anti-corruption policy and financial-crime investigations, yet alongside legitimate enforcement there are documented politically influenced cases and selective freezes in corporate disputes.

Asset restrictions may be imposed:

– in early-stage investigations,

– in conflicts over corporate control,

– during power shifts between influential groups.

Political influence is moderate, but specific cases show AML measures applied as leverage against businesses linked to opposition networks or media. International banks (EU/UK) treat Moldovan clients with heightened caution due to:

– governance volatility,

– frequent regulatory changes,

– risk of abrupt political swings.

Overall, the AML system is developing but remains vulnerable to selective application, particularly in periods of domestic instability.

Typology of Abuses

1. KYC Rejection Without Grounds — refusal of service without clear basis

Banks decline onboarding or terminate service without citing reasons or identifying violations.

Typical indicators:

– generic wording (“not compliant with internal policy”),

– no appeal mechanism,

– automatic offboarding after minimal review.

Outcome: loss of financial access and forced jurisdiction relocation.

2. Nationality-Based High-Risk Scoring — citizenship as a standalone risk trigger

Clients from certain countries are labeled high-risk regardless of behavior or fund origin.

Markers include:

– enhanced EDD solely due to passport,

– onboarding refusal without transactional assessment,

– account closure absent suspicious activity.

This undermines individual risk assessment and results in latent discrimination.

3. Freeze Before Verification — asset freezing prior to evidence

Accounts are blocked:

– pre-investigation,

– pre-forensics,

– without proven financial harm.

Model: freeze first → verify later → evidence never materializes but damage persists.

Used as leverage in disputes and investigative actions.

4. FIU Shadow Requests — informal intelligence-based pressure

FIU influences banks through non-official channels:

– verbal warnings,

– “risk signals,”

– incomplete notices with no predicate offense.

Banks treat them as mandatory, leading to opaque freezes with no appeal pathway.

5. Corporate AML Weaponization — compliance as a business conflict tool

AML procedures are used to pressure commercial rivals.

Patterns include:

– inspections aimed at halting operations,

– freezing working capital before negotiations,

– coercive ownership transfer or control change.

Formally an AML check — functionally a takeover mechanism.

6. Crypto Mislabeling — risk contamination of legitimate blockchain transactions

Freezes occur without chain-analysis due to:

– automated scoring,

– contaminated address deep in transaction history,

– outdated or erroneous risk-trace datasets.

Result: lawful USDT/ETH funds are blocked, especially in P2P and exchange-linked flows.

7. Political AML Targeting — financial measures as political coercion

Used against:

– journalists and investigative outlets,

– NGOs and human-rights groups,

– opposition-linked entrepreneurs,

– diaspora investors.

Economic framing is used to mask political repression, producing a narrative of "lawful" isolation.

Case Examples

Kazakhstan

KZ-1 — agriculture sector; freeze before expert review; motive: redistribution of control.

A freeze was applied at the stage of a tax review without financial-economic examination. Working capital of a grain-export company was blocked. Consequences included:

– halted supply chains and logistics,

– cancelled contracts with foreign buyers,

– bank refused to lift the freeze without FIU clearance.

After nine months the owner was offered a "settlement" — partial transfer of corporate control. The case was later closed for lack of offense, but the business was lost.

KZ-2 — real estate; KYC rejection in EU following FIU request; motive: corporate dispute.

The owner of a development group was denied continuation of service by a European bank after a blanket FIU request from Kazakhstan with no predicate offense. The bank cited “inability to maintain relationship.”

Consequences:

– collateral reserves frozen,

– project financing terminated,

– forced share transfer to partners.

Uzbekistan

UZ-1 — diaspora family; freeze in UAE; FIU request without predicate.

Assets of a family office in the UAE were frozen following an FIU Uzbekistan request containing only the wording “possible illicit enrichment.”

Key elements:

– no stated loss amount or transaction detail,

– no access to the request text,

– freeze lasted 11 months.

The restriction was lifted after UAE regulators declined to validate the request.

UZ-2 — industrial investor; freeze in EU; motive: elite conflict.

The EU account of an industrial-sector owner was frozen after public confrontation between Uzbek power groups. The FIU provided no evidence, yet the bank maintained the freeze pending “official clarification,” which never arrived.

Result — investor divested assets under pressure.

Russia

RU-1 — entrepreneur; freeze + Interpol; motive: asset repatriation.

Immediately after a case was opened, Russian authorities issued an Interpol request and initiated a freeze in the EU.

Key facts:

– Red Notice was never confirmed,

– bank froze assets citing “high risk,”

– case closed one year later.

Access restored only partially — remaining funds stayed locked due to absence of confirmation from Russia.

RU-2 — IT investor; KYC rejection in UK due to links with "foreign agent" partners.

A UK bank terminated service after identifying public connections between the investor and partners designated as "foreign agents" in Russia.

Consequences:

– closure of corporate account,

– payroll freeze,

– forced jurisdiction relocation.

Kyrgyzstan

KG-1 — journalists; freeze pre-charge.

Personal accounts of investigative reporters were frozen on grounds of "risk of illegal activity financing."

Details:

– no charges filed,

– freeze lasted over 6 months,

– newsroom lost funding and closed two projects.

KG-2 — entrepreneur; working-capital freeze; motive: project control.

Restrictions introduced during a dispute over an infrastructure contract. Payments to contractors were frozen, halting operations.

After the owner transferred a stake to local partners, the freeze was lifted within two weeks.

Azerbaijan

AZ-1 — export investor; freeze after corruption investigation.

Corporate accounts were frozen 10 days after publication of procurement-investigation materials. Formally justified as "money laundering suspicion."

Outcome:

– export halted,

– interrogation summons issued,

– partial unfreeze with no explanation.

AZ-2 — rights-focused foundation; grant-block freeze; motive: suppression of civil sector.

Foreign accounts of a political-prisoner support foundation were frozen.

Consequences:

– program shutdown,

– staff layoffs,

– no legal avenue to challenge freeze without access to FIU request.

International Cases

INT-1 — CIS entrepreneur; FIU signal → freeze in EU/CH; no evidence provided.

A European bank froze assets after receiving a CIS FIU request referencing “possible evasion.”

Following verification and lack of proof, freeze was lifted.

Losses — reputational damage and failed transaction.

INT-2 — crypto investor; erroneous USDT trigger; unfreeze after chain-analysis.

A platform blocked funds due to a contaminated address deep in chain history — without technical analysis.

Independent tracing confirmed legal origin; freeze removed.

Impact — 3-month delay and lost profit.

Risk Map

Country	**Bank Risk**	**FIU Risk**	**Scheme Types**	**System Level**
Russia	CRITICAL	CRITICAL	1–7	**Strongly Systemic**
Kazakhstan	**VERY HIGH**	High	**1,3,4,5**	Systemic
Azerbaijan	**VERY HIGH**	**VERY HIGH**	**1,2,3,5,7**	Systemic
Uzbekistan	High	**VERY HIGH**	**1,2,3,5,7**	Systemic
Belarus	High	**Very High**	**1–5**	Systemic
Tajikistan	High	**Very High**	**1–4,7**	Systemic
Turkmenistan	**VERY HIGH**	**VERY HIGH**	**1–3**	**Opaque Systemic**
Kyrgyzstan	Medium	Medium	**1,3,5**	Partially Systemic
Georgia	Medium	Medium	**1,4,5**	Mixed
Moldova	Medium	Medium	**1,3,4**	Reforming
Armenia	Medium	Low	**3,4**	Stable with External Risks

TABLE OF "RED FLAGS"

№	Red Flag	Essence
1	KYC Rejection Without Grounds	denial without explanation
2	Nationality-Based Risk	risk due to passport origin
3	Freeze Before Verification	freeze before verification
4	FIU Shadow Requests	requests without predicate basis
5	Corporate AML Weaponization	AML used in corporate seizure
6	Crypto Mislabeling	erroneous crypto risk flags
7	Political AML Targeting	politically motivated targeting

RECOMMENDATIONS

OFAC (USA)

Objective: prevent the use of sanctions and AML mechanisms for political pressure.

Recommended measures:

– second-layer AML analysis — mandatory secondary review of all requests from CIS states before any restrictive action is taken;

– no reaction without predicate offence — freeze and blocking measures must not be applied if there is no description of the offence, no loss amount, and no verified evidence;

– introduction of PMAF-risk (Politically Motivated Asset Freezing) as a category in analytical models;

– notification to banks prohibiting automatic freezes based solely on unverified external signals.

EU DG FISMA — Sanctions & AML Unit (European Commission)

Objective: reduce the exposure of European banks to cross-border misuse.

Recommended measures:

– classification of FIUs in certain CIS states as high-risk sources if their requests lack evidence and predicate facts;

– mandatory description of the predicate offence and financial loss in FIU submissions;

– implementation of an expert screening mechanism prior to forwarding signals to banks;

– issuance of guidance clarifying that banks have no obligation to react to blanket-requests.

FATF

Objective: reflect politically motivated misuse within global standards.

Recommended measures:

– integration of the “AML/KYC misuse” indicator into country assessments, especially Immediate Outcomes 3 and 6;

– mandatory consideration of political context when evaluating predicate offences;

– requirement of chain-analysis in crypto-related cases before applying freeze measures;

– preparation of a separate typology report on political misuse of AML frameworks.

International Banks (EU/UK/US/UAE/CH)

Objective: reduce the risk of erroneous freezes and financial discrimination.

Recommended measures:

– implementation of a CIS Enhanced Due Diligence Protocol — a dedicated standard for onboarding and monitoring clients from CIS jurisdictions;

– inclusion of political context as a mandatory risk factor, not only transactional indicators;

– refusal to execute blanket-requests lacking predicates and documentation;

– mandatory manual review prior to any freeze action.

FIUs of EU/UK/UAE/CH

Objective: prevent automatic transmission of false or unverified signals.

Recommended measures:

– requirement of evidence of financial damage and factual description prior to forwarding requests to banks;

– rejection of incomplete or generic requests (“possible enrichment”, “risk signal”);

– introduction of an independent analysis chain to verify the credibility of third-country FIU submissions;

– publication of decline/return statistics as a transparency measure.

CONCLUSION

The analysis shows that the misuse of AML/KYC mechanisms in the region is no longer episodic — it has taken on a stable, cross-border form. False or incomplete signals issued by national FIUs trigger automatic freezes in the EU, the UK, the UAE and Switzerland — even in the absence of a predicate offence, confirmed losses or a court order. As a result, financial tools originally intended to combat money laundering are increasingly used as an instrument of pressure on entrepreneurs, investors, journalists and civil society.

The systemic vulnerability lies in the fact that international banks and regulators lack screening mechanisms for such signals, while compliance automation amplifies the effect: a single unsubstantiated notification can result in long-term and irreversible consequences — asset freezes, offboarding, business collapse and forced relocation.

Accordingly, there is a need to establish an international system for filtering and verifying false AML/KYC triggers, including:

– mandatory verification of the predicate offence before forwarding requests;

– rejection of blanket notifications;

– independent second-layer review in receiving jurisdictions;

– consideration of political context in risk assessment;

– publication of statistics on rejected requests.

Without such mechanisms, the financial architecture remains vulnerable to instrumentalization, and cross-border freeze measures continue to function as a concealed repressive tool under the guise of lawful compliance.

SOURCES

1. Basel AML Index, https://index.baselgovernance.org/.
2. EBA, EBA/Op/2022/01, Opinion of the European Banking Authority on 'de-risking', 5 January 2022, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Opinions/2022/Opinion%20on%20de-risking%20%28EBA-Op-2022-01%29/1025705/EBA%20Opinion%20and%20annexed%20report%20on%20de-risking.pdf.
3. EBA, Amending Guidelines on ML/TF risk factors, 22 August 2023, https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-guidelines-challenge-unwarranted-de-risking-and.
4. EBA, Guidelines on policies and controls for the effective management of ML/TF risks when providing access to financial services, 22 August 2023, https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-guidelines-challenge-unwarranted-de-risking-and.