



Observatoire ARGA

**Misuse of AML/CFT Tools as a Mechanism of Economic Pressure: A
Structural Risk Assessment for Latin America**

Author:

Sergey Khrabrykh — President of ARGA, PhD
Ekaterina Khomutinnikova

Organization: Observatoire ARGA – Sanctions and Compliance Unit

Mailing address: 14 rue Jacques Laffitte, Bayonne, 64100

Contacts: info@argaobservatory.org, +33 7 58 49 62 27

Website: www.argaobservatory.org

Table of Contents

1	Executive Summary
2	Problem Statement and Analytical Framework
3	AML/CFT Architecture in Latin America: Roles and Responsibilities
4	Typology of Misuse: Misuse Patterns
5	Escalation Mechanics: From Risk Signal to Economic Damage
6	Secondary Effects: Investment Climate, Banking Access, De-banking, Reputational Trace
7	Early Warning Indicators and Institutional Stress Testing
8	Safeguards: Measures for FIUs, Banks, Regulators, and Data Providers
9	Recommendations for GAFILAT: Typology Agenda and Stakeholder Engagement
10	Conclusion
	Appendix A Terminology
	Appendix B Structural Risk Source Verification Checklist

EXECUTIVE SUMMARY

The AML/CFT system is designed to protect financial infrastructure from money laundering and terrorist financing. However, in the context of expanding compliance automation, increasing data sources (sanctions lists, adverse media, international notices, PEP databases, third-party screening), and uneven procedural standards across jurisdictions, a structural risk emerges: AML/CFT tools may be used as mechanisms of economic pressure.

Within this report, “misuse” refers not to good-faith compliance errors but to recurring structural scenarios in which AML signals, law enforcement notifications, or reputational flags become instruments of competitive pressure, corporate conflict, political leverage, or asset redistribution.

Financial institutions, seeking to minimize regulatory exposure, often adopt defensive compliance strategies that extend beyond formal requirements. These may include de facto de-banking and financial isolation of entities not formally subject to sanctions or judicial findings.

This report provides:

- a typology of misuse patterns;
- an escalation-chain model from initial signal to economic consequences;
- a vulnerability map for FIUs, banks, regulators, and data providers;
- early warning indicators;
- a package of safeguards designed to strengthen AML/CFT resilience without weakening crime prevention.

Core thesis: AML/CFT effectiveness increases when systems are able to distinguish between high criminal risk and politically or economically driven misuse signals, minimizing false positives and secondary effects.

PROBLEM STATEMENT AND ANALYTICAL FRAMEWORK

2.1 Defining the problem

The problem does not lie in the existence of AML/CFT mechanisms or legitimate enhanced scrutiny. It lies in structural asymmetry:

- AML systems prioritize speed, prevention, and risk-based action;
- procedural safeguards and verification of initial signals often lag behind;
- automated systems scale reputational or informational signals faster than correction mechanisms can respond.

As a result, economic restrictions may arise:

- before a verified evidentiary picture exists;
- without clear legal grounding;
- based on external signals of uneven reliability.

2.2 Why this matters for Latin America

Regional characteristics include:

- strong reliance on banking access for capital and cross-border payments;
- high sensitivity of the investment climate to legal predictability;
- uneven institutional strength across jurisdictions;
- frequent corporate conflicts in which legal or regulatory channels may be strategically leveraged.

When AML/CFT systems intersect with such conflicts, they can influence business outcomes more strongly than intended, potentially undermining trust in financial institutions and regulatory frameworks.

2.3 Methodology

This report applies:

- an institutional approach (roles and responsibilities);
- typological analysis (patterns rather than individual cases);
- risk mapping (probability × impact);
- analysis of secondary effects (banking access, capital flows, reputational impact).

AML/CFT ARCHITECTURE IN LATIN AMERICA: ROLES AND RESPONSIBILITIES

3.1 GAFILAT as a regional standard-setting hub

GAFILAT functions as a key regional node influencing:

- evaluation methodologies;
- typology development;
- regulatory improvement recommendations;
- coordination of national approaches.

Within this context, GAFILAT can serve as a platform for identifying misuse patterns as a distinct typology of risk, strengthening AML/CFT effectiveness through improved signal quality rather than weakening enforcement.

3.2 Financial Intelligence Units (FIUs)

FIUs represent critical analytical nodes:

- receiving and analyzing STR/SAR reports;
- interacting with law enforcement;
- producing analytical outputs for the financial system.

Misuse risks increase when FIUs:

- receive high volumes of low-quality signals;
- must process excessive informational “noise”;
- become indirectly involved in corporate or political conflicts via information flows.

3.3 Banks and fintech institutions

Financial institutions constitute the primary interface with the real economy:

- they implement transaction restrictions;
- they manage KYC/EDD procedures;
- they rely on third-party screening tools.

Defensive compliance is rational at the institutional level but becomes systemically problematic when triggers are poorly calibrated and remediation pathways are weak or absent.

3.4 Data providers and compliance platforms

Third-party data sources (adverse media aggregators, watchlists, risk-scoring platforms) can:

- accelerate detection of genuine risks;
- simultaneously propagate outdated or inaccurate signals.

Limited transparency regarding data sources and correction mechanisms increases the likelihood of persistent reputational traces.

TYPOLOGY OF MISUSE: MISUSE PATTERNS

4.1 General logic

Misuse patterns are recurring structural scenarios in which AML/CFT instruments are applied in a formally compliant manner but generate disproportionate economic pressure on specific actors.

Identifying such patterns is intended not to weaken AML enforcement but to strengthen it by improving signal quality and proportionality.

4.2 Pattern 1: Corporate-conflict escalation

In shareholder or corporate conflicts, AML signals may be used as pressure multipliers.

Typical sequence:

- corporate conflict or control dispute;
- emergence of legal or media signals;
- appearance of adverse media;
- intensified banking monitoring;
- transaction or account restrictions;
- weakening of negotiation position.

Each stage may formally comply with regulatory standards, yet the cumulative effect creates economic pressure outside judicial procedure.

4.3 Pattern 2: Reputational amplification through international databases

A localized signal may be scaled through:

- global compliance platforms;
- adverse media aggregators;
- cross-border KYC exchange.

Once entered into international databases, signals may persist independently of the underlying case status.

4.4 Pattern 3: De-banking without formal designation

Financial institutions may terminate relationships:

- without official prohibition;
- without sanctions designation;
- without judicial determination.

Decisions are often based on cumulative risk perception rather than confirmed legal exposure.

4.5 Pattern 4: Information asymmetry

Affected subjects frequently:

- do not know the source of the signal;
- lack clarity regarding risk criteria;
- have no rapid correction mechanism.

This produces long-term reputational traces that remain even in the absence of formal legal findings.

ESCALATION MECHANICS: FROM RISK SIGNAL TO ECONOMIC DAMAGE

5.1 Escalation chain

Initial signal → internal risk assessment → enhanced monitoring → operational restrictions → relationship termination → secondary market effects.

Each stage amplifies the next. Even a weak or ambiguous signal may generate significant consequences when processed through automated systems lacking sufficient calibration.

5.2 Role of automation

Algorithmic models tend to:

- amplify correlations;
- operate without full contextual differentiation;
- incorporate media exposure as a risk factor.

As a result, reputational signals may acquire weight comparable to verified legal findings.

5.3 Economic consequences

Consequences may include:

- loss of access to banking services;
- inability to conduct international transactions;
- termination of commercial contracts;
- decline in investment attractiveness.

Even short-term restrictions can produce long-term structural effects.

SECONDARY EFFECTS: INVESTMENT CLIMATE, BANKING ACCESS, DE-BANKING, REPUTATIONAL TRACE

6.1 Investment climate

If market participants perceive AML/CFT frameworks as unpredictable, this may:

- reduce investment inflows;
- increase cost of capital;
- encourage capital relocation to alternative jurisdictions.

6.2 Banking access

An expansive risk-based approach may result in:

- contraction of client coverage;
- reluctance to serve complex or cross-border clients;
- increased financial exclusion.

6.3 De-banking

Widespread de-banking may:

- undermine financial inclusion;
- stimulate use of informal channels;
- reduce transparency of economic activity.

6.4 Reputational trace

Even after the initial signal is resolved:

- data may persist in private compliance databases;
- algorithms may continue to factor in outdated flags;
- restoration of reputation may require extended periods.

EARLY WARNING INDICATORS AND INSTITUTIONAL RESILIENCE STRESS TESTING

7.1 Purpose of early warning indicators

Early identification of misuse patterns allows:

- reduction of escalation probability;
- protection of financial systems from signal overload;
- preservation of trust in AML/CFT frameworks.

7.2 Possible indicators

Regulators and FIUs may monitor:

- sharp increases in SAR/STR volumes without corresponding criminal cases;
- repeated alerts concerning the same subject without procedural progression;
- clusters of account closures within specific sectors;
- reliance on adverse media as the sole risk basis;
- correlation between corporate disputes and AML escalation.

7.3 Institutional stress testing

Regulatory systems may periodically assess:

- speed of correction for inaccurate signals;
- availability of remediation procedures;

- transparency of communication between banks and clients;
- resilience to political or corporate pressure.

SAFEGUARDS: MEASURES FOR FIUs, BANKS, REGULATORS, AND DATA PROVIDERS

8.1 For FIUs

- strengthen signal-quality filtering;
- prioritize substantiated risks;
- coordinate with banks to reduce informational noise;
- develop guidance for evaluating indirect signals.

8.2 For banks

- implement proportionality frameworks;
- document de-banking decisions;
- apply multi-source verification;
- establish client feedback and remediation channels.

8.3 For regulators

- issue guidance on managing secondary effects;
- maintain regular dialogue with financial institutions;
- monitor market impact of AML measures;
- encourage explainable risk models.

8.4 For data providers

- increase transparency of sources;
- provide correction mechanisms;
- periodically purge outdated data;
- conduct algorithmic audits.

RECOMMENDATIONS FOR GAFILAT: TYPOLOGY AGENDA AND STAKEHOLDER ENGAGEMENT

9.1 Misuse typologies as a distinct analytical track

GAFILAT may consider:

- inclusion of misuse patterns within typology workstreams;
- development of proportionality guidance;
- dissemination of best practices.

9.2 Stakeholder engagement

- structured dialogue with banking sector;
- engagement with fintech providers;
- FIU-to-FIU knowledge exchange;
- participation of academic and policy institutions.

9.3 Transparency enhancement

- publication of aggregated analytical data;
- periodic reviews of secondary effects;
- strengthening regional analytical capacity.

CONCLUSION

AML/CFT systems remain central to protecting financial infrastructure. Their effectiveness, however, depends on the ability to distinguish between genuine criminal threats and situations in which risk signals are used as instruments of economic pressure.

A balanced framework combining technological efficiency with procedural safeguards can:

- increase trust in financial institutions;
- improve investment climate predictability;
- reduce disproportionate restrictions;
- strengthen regional financial stability.

This report is intended to support professional dialogue on enhancing resilience of AML/CFT architecture in Latin America without weakening its core mission of combating financial crime.

APPENDIX A. TERMINOLOGY

AML/CFT — anti-money laundering and counter-terrorist financing measures.

Defensive compliance — expanded precautionary measures aimed at minimizing regulatory exposure.

De-banking — termination of banking services.

Adverse media — negative media references used in compliance screening.

Reputational risk — risk to business reputation and relationships.

APPENDIX B. STRUCTURAL RISK SOURCE VERIFICATION CHECKLIST

Before applying restrictive measures, it is recommended to assess:

- source of the signal;
- level of verification;
- presence of judicial determinations;

- data relevance and timeliness;
- potential secondary systemic effects.