Observatoire ARGA

ALGORITHMIC AML, FALSE POSITIVES, AND INSTITUTIONAL PROPORTIONALITY:

A STRUCTURAL ASSESSMENT OF RISKS FOR ASIA'S FINANCIAL CENTERS

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA

Mailing address: 21 route de l'Aviation, 12 C, 64600 Anglet, FRANCE

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

Website: www.argaobservatory.org

Paris, 17 February 2026

Purpose of the Document:

To provide Asian regulators with an analytical framework for assessing the risks associated with automated AML systems, including false-positive alerts, algorithmic signal amplification, and their impact on financial stability and investment attractiveness.

CONTENTS

1. EXECUTIVE SUMMARY

Asia's financial centers are at the forefront of compliance digitalization. Singapore and Hong Kong actively deploy algorithmic AML/CTF models based on large-scale data processing, machine learning, and behavioral transaction analytics.

Automation has significantly increased the speed of detecting suspicious activity and the scalability of monitoring systems. At the same time, however, it has generated a set of systemic risks:

– a rise in the number of false-positive alerts;

– opacity in algorithmic decision-making logic;

– automatic amplification of secondary and low-quality data sources;

– the institutionalization of defensive compliance as a dominant behavioral strategy.

False positives are no longer merely a technical issue. In global financial centers, they acquire strategic significance and may:

– undermine client and investor trust;

– weaken jurisdictional competitiveness;

– increase reputational and legal risks;

– encourage capital outflows to alternative financial centers.

This report proposes a structural model of algorithmic risk, an analysis of the “signal amplification” mechanism, and a package of safeguards aimed at strengthening proportionality, transparency, and institutional resilience in AML systems without reducing their effectiveness.

2. THE ROLE OF AUTOMATION IN AML SYSTEMS IN ASIA

2.1. Drivers of Digitalization

The digital transformation of AML has become inevitable due to:

– exponential growth in transaction volumes;

– globalization of financial flows and increasingly complex ownership structures;

– stricter regulatory requirements and enhanced managerial liability;

– competition among financial centers in terms of speed and service quality.

Manual review processes no longer provide sufficient scalability or responsiveness.

2.2. Technological Instruments

Modern AML systems incorporate:

– machine learning algorithms for anomaly detection;

– behavioral analytics of transactional patterns;

– automated client risk-scoring models;

– integration of sanctions lists, adverse media sources, and external databases;

– network analytics to identify indirect associations.

While this architecture enhances system sensitivity, it also increases the risk of overestimating weak or context-dependent signals.

2.3. Specific Features of Asian Financial Centers

Singapore and Hong Kong are characterized by:

– high-speed transaction processing environments;

– internationally diversified client bases;

– significant exposure to private banking and high-net-worth (HNW) clients;

– complex cross-border corporate structures.

Under these conditions, algorithmic precision is strategically critical. Errors may generate not only operational disruptions but also macroeconomic and reputational consequences for the financial center as a whole.

3. ARCHITECTURE OF ALGORITHMIC RISK

Algorithmic risk is multi-layered and cumulative.

3.1. Data Layer

Input errors, outdated records, unreliable data sources, and duplication are scaled by automated systems and propagated across the entire client risk profile.

Poor data quality at the input stage can produce systemic distortions at the output stage.

3.2. Model Layer

Opaque "black-box" models may amplify secondary signals without sufficient contextual analysis. Through training processes, models may learn to overweight specific risk indicators, leading to structural bias or systematic overclassification of risk categories.

3.3. Threshold Layer

Lowering risk-score thresholds increases the volume of alerts, which:

– burdens compliance departments;

– elevates operational costs;

– increases the proportion of false positives;

– reduces focus on genuinely material threats.

Threshold calibration therefore becomes a core governance issue.

3.4. Interpretation Layer

Compliance teams often place significant reliance on automated outputs, particularly in environments characterized by regulatory pressure and potential liability.

This dynamic:

– reduces the scope of critical human judgment;

– reinforces conservative decision-making;

– contributes to the institutionalization of defensive compliance.

In combination, these layers may produce a structural tendency toward over-escalation of risk signals within automated AML ecosystems.

4. FALSE POSITIVES: SCALE AND NATURE

4.1. Primary Causes

False-positive alerts arise from multiple structural and technical factors, including:

– name matches and transliteration inconsistencies;

– outdated or revoked records remaining in databases;

– incorrect risk categorization;

– duplication of data across integrated systems;

– automatic inclusion of adverse media without qualitative source assessment.

Even a single inaccuracy at the data level may trigger a chain of escalation within automated systems, particularly when thresholds are set conservatively and human review is limited.

4.2. Consequences for Banks

For financial institutions, persistent false positives lead to:

– overload of compliance departments;

– diversion of analytical resources away from genuine high-risk cases;

– rising operational and staffing costs;

– delays in transaction processing and onboarding procedures;

– increased regulatory exposure if genuine risks are overlooked due to alert saturation.

Excessive alert volumes may ultimately weaken the effectiveness of AML controls by diluting analytical focus.

4.3. Consequences for Clients

For clients, false positives may result in:

– temporary or prolonged account freezes;

– termination or refusal of services;

– deterioration of reputational profiles;

– restricted access to credit and financial products;

– disruption of legitimate business activity.

In international financial centers, such consequences may have cross-border implications, affecting counterparties and associated entities.

5. ALGORITHMIC AMPLIFICATION AND THE “RISK AMPLIFICATION EFFECT”

Algorithms are capable of:

– incorporating indirect and network-based associations;

– amplifying weak or context-neutral indicators;

– generating cascading risk escalation dynamics.

The amplification mechanism typically unfolds as follows:

initial signal → increase in risk score → enhanced monitoring → generation of additional alerts → further escalation of risk classification.

Absent meaningful human intervention, the system may reinforce its own outputs, producing a self-sustaining escalation of perceived risk. Over time, this dynamic may institutionalize structural bias and reduce proportionality in compliance responses.

6. DEFENSIVE COMPLIANCE AND INSTITUTIONAL DISPROPORTIONALITY

6.1. Drivers of Defensive Compliance

Defensive compliance is driven by:

– fear of regulatory penalties and enforcement actions;

– legal and supervisory uncertainty;

– pressure from correspondent banks and international partners;

– heightened global regulatory expectations.

Under such conditions, institutions may prioritize risk avoidance over calibrated risk management.

6.2. Disproportionality

Measures adopted in response to algorithmic alerts may significantly exceed the objective level of threat. Compliance decisions may shift from risk-based evaluation to liability minimization strategies.

This transformation undermines proportionality and may weaken trust in institutional fairness.

6.3. Risk for Financial Centers

If clients perceive compliance systems as excessively rigid or unpredictable, they may reallocate assets to alternative jurisdictions. Over time, such capital migration can affect competitiveness, liquidity, and the strategic positioning of financial centers.

7. IMPACT ON PRIVATE BANKING, WEALTH MANAGEMENT, AND FINTECH

Private banking is grounded in trust, discretion, and long-term relationship management. False positives and automated risk escalation may:

– undermine durable client relationships;

– complicate strategic asset allocation decisions;

– create uncertainty for family offices and investment structures.

Fintech firms, which rely heavily on seamless banking infrastructure and rapid transaction processing, are particularly vulnerable to algorithmic errors. Given their business models, even short-term service interruptions may materially affect operations and investor confidence.

8. REGULATORY CHALLENGES FOR MAS AND HKMA

Regulators face a structural balancing task. They must:

– maintain robust AML enforcement standards;

– safeguard the competitiveness of their financial centers;

– prevent disproportionate restrictions arising from automated systems.

The equilibrium between technological efficiency and institutional fairness is central to long-term resilience. Regulatory guidance must therefore address both enforcement rigor and proportionality safeguards.

9. PROPORTIONALITY MODEL AND EXPLAINABLE AI

9.1. Explainable AI

Algorithmic systems should provide:

– transparent reasoning for alerts;

– mechanisms for human review and override;

– documented decision logic (audit trail);

– alignment between risk classification and verifiable factual data.

Explainability enhances accountability and strengthens institutional legitimacy.

9.2. Secondary Verification

Signals originating from politically or commercially sensitive contexts require mandatory secondary verification before restrictive measures are imposed. Qualitative assessment should complement automated outputs.

9.3. Regular Recalibration

Models must undergo periodic stress testing, including:

– evaluation of false positive rates;

– bias detection;

– threshold recalibration;

– performance benchmarking against supervisory expectations.

Continuous recalibration is essential to preserve proportionality.

10. SAFEGUARDS AND PRACTICAL RECOMMENDATIONS

1. Develop formal guidance on managing false-positive alerts and proportional responses.
2. Promote the adoption of explainable AI frameworks within AML systems.
3. Mandate comprehensive audit trails for material compliance decisions.
4. Establish minimum review standards for restrictive measures, including timelines and appeal mechanisms.
5. Create a regional expert dialogue within APG to address algorithmic risk governance and best practices.

11. CONCLUSION

Algorithmic AML is an integral component of Asia's contemporary financial architecture. However, the resilience of financial centers depends on proportionality, transparency, and the capacity to correct systemic errors.

A balanced approach to algorithmic risk strengthens trust among clients, investors, and international partners while preserving technological efficiency and institutional legitimacy.

ARGA Observatory views this report as a contribution to institutional resilience and the responsible deployment of financial technologies in Asia.

APPENDIX A. TERMINOLOGY

False positives — alerts incorrectly identifying legitimate activity as suspicious.

Explainable AI — machine learning models capable of providing transparent and interpretable decision logic.

Audit trail — documented traceability of decision-making processes.

Risk amplification — the systemic escalation of perceived risk through automated signal reinforcement.

APPENDIX B. ALGORITHMIC STRESS TEST

1. Source and quality of the signal.
2. Level of verification and evidentiary support.

3. Availability of human review mechanisms.
4. Model update frequency and recalibration cycle.
5. Error correction procedures.
6. Documentation and transparency of decision logic.