



Observatoire ARGA

**Compliance Failures by Intermediaries and Secondary Liability:
How Infrastructure Breakdowns Turn into Criminal and Sanctions
Risks**

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA – Sanctions and Compliance Unit

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, 24 January 2026

Table of Contents

Abstract	3
1. Introduction.....	3
2. The Concept of Secondary Liability in Digital Finance	3
3. Typology of Compliance Failures by Intermediaries	3
4. Algorithmic Risk Scoring and Its Limits.....	3
5. Selective Compliance and Conflict of Interests	4
6. From Compliance Failure to Criminal Risk.....	4
7. The Sanctions Dimension and Extraterritorial Consequences	4
8. Procedural Deficits of Protection	5
9. Impact on Bona Fide Users and Businesses.....	5
10. International Practice and Recurring Scenarios	5
11. Political and Economic Context of Secondary Liability	5
12. Property Rights and the Presumption of Good Faith.....	6
13. Institutional Limits of the Current Model.....	6
14. Conclusions.....	6
15. Recommendations	6
List of sources and materials used	7

Abstract

This report examines the phenomenon of secondary liability arising from compliance failures by intermediaries within the cryptocurrency and fintech ecosystem. It analyses typical KYC/AML breakdowns, risk-scoring errors, improper account freezes, and selective enforcement measures that evolve into criminal, administrative, and sanctions-related risks for third parties — users, partners, and counterparties. Particular attention is paid to the institutional incentives of private providers, information asymmetry, procedural deficits in protection, and the consequences for property rights and human rights.

1. Introduction

As regulation of the crypto market intensifies, the primary burden of AML/KYC and sanctions compliance is increasingly shifted onto private intermediaries. These entities make decisions with public-law consequences while lacking full procedural obligations and judicial oversight. Errors and simplifications in their compliance procedures become a source of secondary liability for persons who are not initiators of any wrongdoing.

2. The Concept of Secondary Liability in Digital Finance

Secondary liability arises when negative legal consequences are imposed on a person not for committing an unlawful act, but for being part of an infrastructure chain: using a service, conducting a transaction, or holding assets. In the crypto sphere, such liability is formed through the decisions of intermediaries rather than courts.

3. Typology of Compliance Failures by Intermediaries

The most common failures include:

- formal KYC without analysis of beneficial ownership;
- automated freezes based on heuristics;
- incorrect attribution of addresses and links;
- disregard for the context of transactions;
- delayed or excessive response measures.

These failures are amplified by automation and affect a wide range of individuals.

4. Algorithmic Risk Scoring and Its Limits

Risk scoring relies on probabilistic models and closed algorithms. In the absence of transparency and audit:

- the number of false positives increases;
- reproducibility of decisions decreases;
- defence is deprived of the ability to challenge outcomes.

The algorithm effectively becomes a quasi-judge without procedural safeguards.

5. Selective Compliance and Conflict of Interests

Intermediaries tend to apply selective measures guided by:

- regulatory pressure;
- reputational risks;
- commercial priorities.

This leads to asymmetry: small users and counterparties bear the consequences, while systemic actors adapt.

6. From Compliance Failure to Criminal Risk

Compliance decisions by intermediaries are often used by law enforcement as:

- grounds for initiating checks;
- indicators of “suspicious” activity;
- justification for freezing and seizure.

Thus a chain is formed: error → freeze → suspicion → prosecution.

7. The Sanctions Dimension and Extraterritorial Consequences

In the sanctions context, a compliance error may result in:

- secondary sanctions;
- denial of services across the market;
- long-term financial isolation.

A decision by one provider is propagated throughout the entire ecosystem.

8. Procedural Deficits of Protection

Those affected by compliance failures face:

- absence of reasoned decisions;
- inability to appeal;
- closed review procedures;
- undefined timeframes.

Private policies effectively replace public law.

9. Impact on Bona Fide Users and Businesses

Secondary liability:

- disrupts business relationships;
- blocks working capital;
- reduces investment attractiveness;
- incentivizes movement into grey zones.

The market penalizes good faith.

10. International Practice and Recurring Scenarios

Recurring patterns include:

- automatic freezes without court orders;
- cascading refusals of service;
- subsequent regulatory pressure;
- absence of compensation for errors.

These scenarios are reproduced across different jurisdictions.

11. Political and Economic Context of Secondary Liability

Secondary liability reflects:

- the desire of states to delegate control;

- the shifting of risks onto the private sector;
- optimization of enforcement costs.

Economic efficiency replaces legal safeguards.

12. Property Rights and the Presumption of Good Faith

Compliance failures undermine:

- the presumption of good faith;
- the stability of property rights;
- equality of parties.

Assets become conditional upon an algorithmic decision.

13. Institutional Limits of the Current Model

Without reform, the following persist:

- scaling of errors;
- fragmentation of protection;
- growth of shadow practices.

Control increases, fairness does not.

14. Conclusions

Compliance failures by intermediaries are a systemic source of secondary liability and legal risks. Delegating public functions to private actors without procedural safeguards undermines trust in markets and institutions.

15. Recommendations

1. Introduction of procedural standards for compliance decisions.
2. Mandatory transparency and auditability of risk-scoring algorithms.
3. Effective appeal and compensation mechanisms.
4. Clear distinction between compliance indicators and criminal grounds.
5. Development of international standards for protection against secondary liability.

List of sources and materials used

1. <https://www.fatf-gafi.org/en/topics/virtual-assets.html>
2. <https://www.imf.org/en/publications/fandd/issues/2022/09/regulating-crypto-narain-moretti>
3. https://www.bis.org/publ/qtrpdf/r_qt2103.htm
4. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html>
5. <https://www.europol.europa.eu/crime-areas/economic-crime>
6. <https://www.unodc.org/unodc/en/cybercrime/home.html>
7. <https://www.interpol.int/What-you-can-do/Crimes/Financial-crime>
8. <https://argaobservatory.org>