Observatoire ARGA

How criminals use KYC/AML against regulators:

paradoxes of compliance, institutional vulnerabilities, and consequences for law enforcement

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, 16 January 2026

Table of Contents

Abstract

This report analyzes the paradoxical phenomenon in which KYC/AML tools, designed to combat financial crime, are themselves used by criminal and quasi-criminal structures to conceal beneficiaries, redistribute liability, and create a formal appearance of legitimacy for operations. It examines architectural and institutional vulnerabilities of compliance models, international practice of abuse, and the consequences for investigations, victims, and bona fide participants in financial markets.

Introduction

KYC/AML systems have become a cornerstone of global financial regulation. Their purpose is client identification and the prevention of money laundering and illicit financing. However, as financial and cryptocurrency infrastructures have grown more complex, these tools increasingly demonstrate the opposite effect: formal compliance is used as a protective shield for illegal operations.

In cryptocurrency and transnational schemes, KYC/AML ceases to function as a risk-detection mechanism and instead becomes a tool for redistributing risk — from the real beneficiaries to intermediaries, nominees, and bona fide users.

Evolution of KYC/AML: from control to formality

Historically, KYC/AML developed within the banking sector, where there were:

- centralized operators;
- a stable client base;
- clear chains of responsibility.

With the transfer of these models into the crypto and fintech environment, a gap emerged between:

- formal compliance with procedures;
- actual control over economic flows.

As a result, compliance has come to be perceived as a box-ticking exercise rather than a risk analysis tool.

Compliance as a protective shield

International practice reveals a consistent pattern: the existence of formally correct KYC/AML procedures is used to:

- deflect claims from platforms and intermediaries;

- shift responsibility onto end users;
- justify the “good faith” of infrastructure operators.

Meanwhile, real control over assets and managerial decisions remains outside the compliance perimeter.

Nominees and straw KYC profiles

One of the key methods of abusing KYC procedures is the use of:

- straw persons;
- purchased or coerced identity documents;
- nominee directors and employees.

Formally, such accounts pass identification procedures, but in reality do not reflect the true beneficiary. As a result, KYC does not detect risk, but legitimizes it.

Separation of roles and fragmentation of responsibility

Modern schemes are built on functional separation:

- one subject passes KYC;
- another controls the wallets;
- a third makes economic decisions;
- a fourth conducts OTC conversion.

Such fragmentation makes it impossible to identify a single responsible person within the framework of a standard compliance approach.

Exchanges and compliance asymmetry

Centralized crypto exchanges formally comply with AML/KYC requirements, but:

- they do not control off-platform operations;
- they do not track the subsequent use of funds;
- they are limited by the scope of their own monitoring systems.

This creates an asymmetry in which formal compliance exists in parallel with real grey flows.

KYC as a tool of pressure and selective enforcement

In some cases, KYC/AML is used not to prevent crime but as a tool for:

- selective blocking of accounts;
- exerting pressure on users;
- freezing funds without judicial decisions.

At the same time, the individuals who actually control the schemes remain outside the scope of enforcement.

International practice: recurring scenarios

Analysis of international cases reveals typical patterns:

- investigations begin with formally identified users;
- attention is focused on nominees;
- infrastructure operators refer to KYC compliance;
- beneficiaries retain control over assets.

This reduces the effectiveness of investigations and undermines trust in regulatory mechanisms.

Consequences for victims and bona fide participants

For victims of financial crimes, a formalized KYC/AML approach often leads to a paradoxical situation:

— funds are frozen at the level of the victims rather than the organizers of the schemes;

— the status of having “passed KYC” is used against the victim as an argument of alleged conscious participation;

— access to legal protection is complicated by references to the internal compliance policies of private platforms.

Thus, compliance procedures intended to protect the market become a source of secondary victimization and undermine trust in financial institutions.

The role of private compliance providers and private normativity

A significant portion of KYC/AML functions in the modern financial ecosystem is delegated to private providers. These entities:

— establish their own risk criteria;

— use closed scoring algorithms;

— make decisions with direct legal and economic consequences for users.

At the same time, their activities:

— are not fully subject to judicial review;

— are not accompanied by procedural safeguards;

— effectively create a regime of "private normativity" outside public oversight.

As a result, key decisions regarding the fate of assets and access to the market are made outside the framework of public law.

Mismatch between FATF standards and practical implementation

International FATF standards declare a risk-based approach and the need to identify beneficial ownership. In practice, however, substance is replaced by form:

— identity verification replaces analysis of economic substance;

— complex multi-layered schemes pass formal compliance;

— attention is focused on technical adherence to procedures.

This leads to KYC/AML losing its preventive function and becoming a tool of ex post sanctions.

Compliance in cross-border and political-economic conflicts

In the context of international and corporate conflicts, KYC/AML acquires an additional dimension. It can be used as a tool for:

— economic pressure;

— restricting access to financial infrastructure;

— redistribution of assets in favor of the stronger party.

At the same time, formal reference to AML/KYC compliance allows the political-economic nature of the conflict to be masked as neutral regulatory practice.

Institutional limits of compliance reform

Despite the continuous tightening of requirements, systemic vulnerabilities of KYC/AML persist. The main reasons are:

— technological asymmetry between regulators and illicit schemes;

— the cross-border nature of operations;

— fragmentation of responsibility;

— absence of a global supervisory body.

Without revising the underlying logic of compliance, current reforms will increase formalization rather than real control.

Conclusions

Modern KYC/AML systems are increasingly used not as tools for detecting and preventing financial crime, but as mechanisms for the formal legitimization of operations and redistribution of responsibility. This creates a paradox: the stricter the compliance requirements, the greater the risk of their instrumentalization by criminal and quasi-criminal structures.

In the cryptocurrency and fintech environment, this effect is particularly pronounced, undermining trust in regulatory models and reducing the effectiveness of international law enforcement.

Recommendations

- Shifting the focus of compliance from formal identification to analysis of beneficial and economic control.
- Integrating KYC/AML with financial intelligence, corporate investigations, and off-chain investigations.
- Increasing the accountability of infrastructure operators and compliance providers for the consequences of their decisions.
- Establishing procedural mechanisms to protect bona fide users and victims.
- Taking into account the political and economic context when applying AML/KYC in cross-border cases.

List of sources and materials used

1. https://www.fatf-gafi.org/en/topics/virtual-assets.html
2. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html
3. https://www.fatf-gafi.org/en/topics/mutual-evaluations.html
4. https://www.imf.org/en/publications/fandd/issues/2022/09/regulating-crypto-narain-moretti
5. https://www.imf.org/en/Publications/Staff-Discussion-Notes
6. https://www.bis.org/publ/qtrpdf/r_qt2103.htm
7. https://www.unodc.org/unodc/en/money-laundering/
8. https://www.europol.europa.eu/crime-areas/economic-crime
9. https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances
10. https://www.interpol.int/What-you-can-do/Crimes/Financial-crime
11. https://www.interpol.int/How-we-work/Notices
12. https://www.interpol.int/How-we-work/Data-protection
13. https://argaobservatory.org