



Reassessing the global anti-money laundering regime: FATF standards, cyber-enabled fraud, and the structural limits of territorial enforcement

Thai Lam Ngoc

Faculty of International Law, Hanoi Law University, Hanoi, Vietnam

Abstract

The global anti-money laundering regime has long been organised around the Financial Action Task Force (FATF) as the central source of international standards, evaluative pressure, and policy coordination. Yet the operating environment of illicit finance has changed profoundly. Cyber-enabled fraud, scam-centre economies, virtual assets, platform-mediated payment systems, and transnational laundering chains now allow criminal proceeds to move across jurisdictions with a speed and modularity that challenge conventional models of detection, investigation, confiscation, and recovery. This article reassesses whether the present regime remains institutionally fit for contemporary risk conditions. It argues that the regime remains normatively indispensable but operationally strained. FATF still provides the core architecture of global AML governance, and its recent reforms on beneficial ownership, payment transparency, digitalisation, and virtual assets demonstrate continuing adaptive capacity. However, the practical effectiveness of the regime is increasingly constrained by a structural mismatch between transnational digital criminality and territorially bounded enforcement. The article contends that the central weakness of the current AML order lies less in the absence of standards than in the limits of state-based enforcement in a digitally integrated criminal environment. It concludes that future reform must focus on operational interoperability, faster cross-border information-sharing, coordinated supervision, and more effective tracing, freezing, and recovery mechanisms.

Keywords: Anti-money laundering, FATF, cyber-enabled fraud, territorial enforcement, virtual assets, transnational crime, asset recovery

Introduction

The contemporary anti-money laundering debate can no longer be framed solely through conventional laundering models in which criminal proceeds are generated, layered, and integrated within relatively stable territorial and institutional settings. Illicit finance today is increasingly shaped by cyber-enabled fraud, online scam networks, underground banking, digitally mediated payment systems, and virtual asset ecosystems that move value across several jurisdictions in near real time. In this environment, the central problem is not merely whether states possess AML legislation. It is whether a system built on nationally implemented standards and territorially bounded enforcement remains capable of addressing criminal conduct that is transnational by design and digitally accelerated in practice.

The question is therefore one of institutional fit. The global AML regime has succeeded in diffusing norms across jurisdictions. Through the FATF Recommendations, mutual evaluations, follow-up processes, and blacklisting practices, it has generated a common grammar of compliance, effectiveness, risk-based supervision, and international cooperation. Yet digital fraud economies now operate through fragmented but highly coordinated infrastructures involving social media platforms, telecommunications networks, payment intermediaries, shell entities, money mules, informal transfer systems, and virtual asset service providers. The resulting laundering chains are fast, layered, and adaptive. They expose the extent to which global standards have moved ahead of globally effective enforcement.

This article does not argue that the present regime has become obsolete. Rather, it argues that the regime should be reassessed. FATF remains normatively central, but the

enforcement model on which the broader regime depends is under structural strain. The core difficulty lies in the mismatch between transnational digital criminality and territorially organised enforcement. As long as illicit proceeds can be displaced across jurisdictions faster than legal authority can move, the gap between formal compliance and operational effectiveness will remain a defining weakness of the global AML order.

FATF and the normative architecture of global AML governance

Any reassessment of the global AML regime must begin with the continuing centrality of FATF. FATF is not a treaty body and does not legislate in the formal sense, yet it remains the principal standard-setter in the field. Its authority derives from a combination of technical expertise, peer review, reputational pressure, market signalling, and the capacity to influence legislative and supervisory reform across jurisdictions. In this respect, FATF functions as the normative centre of global AML governance rather than as a conventional international organisation endowed with coercive jurisdiction.

That normative role has not diminished. FATF has continued to revise its standards and guidance in response to evolving risk. Recent updates concerning beneficial ownership, payment transparency, and virtual assets show that the regime remains capable of doctrinal adaptation. The FATF paper on cyber-enabled fraud, published in 2026, further confirms that the organisation understands digitalisation not as a peripheral issue but as a major driver of money laundering, terrorist financing, and proliferation financing risk. The regime is therefore not conceptually static. It remains responsive and increasingly conscious of technological transformation.

At the same time, normative responsiveness should not be confused with operational sufficiency. FATF can refine standards, sharpen methodology, and encourage convergence, but it cannot by itself overcome the institutional fragmentation that characterises domestic enforcement. The more that AML risk is produced through distributed digital infrastructures, the more visible the distinction becomes between the globalisation of standards and the incomplete globalisation of enforcement capacity.

Cyber-enabled fraud and the transformation of laundering chains

Cyber-enabled fraud has altered both the source of illicit proceeds and the manner in which those proceeds are concealed, moved, and converted. Unlike older laundering typologies that often presupposed a relatively linear process, contemporary fraud schemes may combine social engineering, impersonation, fraudulent investment interfaces, deepfakes, romance scams, online marketplaces, and transnational call-centre operations. The predicate offence itself is often geographically dispersed, technologically mediated, and capable of targeting large numbers of victims across borders within a short period.

Cyber-enabled fraud has altered both the source of illicit proceeds and the manner in which those proceeds are concealed, moved, and converted. Unlike older laundering typologies that often presupposed a relatively linear process, contemporary fraud schemes may combine social engineering, impersonation, fraudulent investment interfaces, deepfakes, romance scams, online marketplaces, and transnational call-centre operations. The predicate offence itself is often geographically dispersed, technologically mediated, and capable of targeting large numbers of victims across borders within a short period.

Reports issued by INTERPOL and UNODC underscore this transformation. They describe scam-centre economies, underground banking, and technologically enabled criminal services as deeply interconnected. In Southeast Asia in particular, cyber-enabled fraud has become embedded in broader organised-crime ecosystems involving digital platforms, migration routes, coercive labour practices, and cross-border financial infrastructures. In such settings, the laundering of proceeds is not an afterthought. It is built into the architecture of the criminal enterprise from the beginning.

Territorial enforcement and the structural limits of implementation

The most important weakness of the present AML regime lies in the continued territorial organisation of enforcement. Investigation, prosecution, freezing, confiscation, and asset recovery remain anchored in domestic legal systems. Even where international standards require broad criminalisation and effective cooperation, the use of coercive authority still depends on national legislation, national institutions, evidentiary rules, procedural thresholds, and political priorities. Global norms can travel quickly; enforcement powers cannot.

This distinction becomes critical in digital cases. Illicit funds can be transferred, layered, and dissipated across several jurisdictions almost instantly, whereas legal authority usually moves through slower channels such as mutual legal assistance, supervisory requests, domestic court orders, and inter-agency coordination. The result is a

structural asymmetry. Criminal actors exploit speed, fragmentation, and jurisdictional diversity, while public authorities remain constrained by sovereignty, admissibility, due process, and institutional compartmentalisation.

This distinction becomes critical in digital cases. Illicit funds can be transferred, layered, and dissipated across several jurisdictions almost instantly, whereas legal authority usually moves through slower channels such as mutual legal assistance, supervisory requests, domestic court orders, and inter-agency coordination. The result is a structural asymmetry. Criminal actors exploit speed, fragmentation, and jurisdictional diversity, while public authorities remain constrained by sovereignty, admissibility, due process, and institutional compartmentalisation.

The same is true of beneficial ownership and asset recovery. Requirements for adequate, accurate, and up-to-date information are central to the FATF framework, but the ability to obtain, verify, and use such information in time-sensitive cross-border cases remains inconsistent. Asset recovery faces similar obstacles. It often depends on exceptional operational coordination rather than on an ordinary baseline of seamless international execution. This is why headline enforcement successes, while important, do not negate the underlying structural problem. They illustrate what is possible when coordination is intensive, not what is routinely available to all competent authorities in everyday cases.

From rule proliferation to operational interoperability

If the weakness of the current regime is structural, the solution cannot lie merely in multiplying formal rules. The next phase of AML development should focus on operational interoperability. This means creating systems in which lawful information-sharing, supervisory coordination, beneficial ownership access, tracing, freezing, and recovery can function across borders with greater speed and reliability. The issue is no longer only what obligations states should adopt. It is how public and private actors can act on those obligations in real time.

An interoperability-based approach would require closer coordination between financial intelligence units, law enforcement agencies, supervisors, payment intermediaries, telecommunications operators, and virtual asset service providers. It would also require more robust mechanisms for cross-border preservation of evidence and assets, clearer expectations concerning data access and privacy safeguards, and more meaningful effectiveness metrics tied to disruption and recovery rather than formal legislative compliance alone.

Such a shift would remain faithful to the core logic of FATF while correcting a persistent imbalance within the present regime. The objective is not to displace state sovereignty, but to ensure that territorially bounded legal authority can still function effectively in a criminal environment structured by digital speed and transnational integration.

Conclusion

The global AML regime remains indispensable, but it should no longer be assessed solely by the breadth of its standards. FATF continues to provide the normative architecture of AML governance, and recent reforms demonstrate substantial adaptive capacity. In that sense, the regime remains fit as a framework of standard-setting, coordination, and evaluative discipline.

However, the article has argued that the regime is operationally constrained by a structural mismatch between transnational digital criminality and territorially organised enforcement. Cyber-enabled fraud, scam-centre economies, virtual assets, and layered digital payment infrastructures have exposed the limits of a system in which norms are global but coercive legal authority remains fragmented by jurisdiction. Reassessment is therefore necessary not because the regime has failed, but because normative centrality alone is no longer sufficient.

The future effectiveness of global AML law depends on a shift from rule proliferation to operational interoperability. Faster lawful information-sharing, more coordinated supervision, stronger tracing and freezing mechanisms, and more credible asset recovery pathways are now essential. Without such reforms, the gap between compliance and effectiveness will continue to define the limits of the global AML regime in the digital age.

Reference

1. Financial Action Task Force. The FATF Recommendations. FATF, 2025.
2. Financial Action Task Force. Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems. FATF, 2025.
3. Financial Action Task Force. Guidance on Beneficial Ownership for Legal Persons. FATF, 2023.
4. Financial Action Task Force. Illicit Financial Flows from Cyber-Enabled Fraud. FATF, Egmont Group of Financial Intelligence Units and INTERPOL, 2023.
5. Financial Action Task Force. Explanatory Note to Recommendation 16 on Payment Transparency. FATF, 2025.
6. Financial Action Task Force. Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. FATF, 2025.
7. Financial Action Task Force. Cyber-Enabled Fraud: Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks. FATF, 2026.
8. Case-Ruchala D, Nance M. The Limits of Enforcement in Global Financial Governance: Blacklisting in FATF as Rational Myth. *International Studies Quarterly*, Volume 68, Issue 3, 2024, Article sqae115.
9. Pavlidis G. International Regulation of Virtual Assets under FATF's New Standards. *Journal of Investment Compliance*, Volume 21, Issue 1, 2020, Pages 1-8.
10. Karasek-Wojciechowicz I. Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces. *Journal of Cybersecurity*, Volume 7, Issue 1, 2021, Article tyab004.
11. Interpol. Interpol Global Financial Fraud Assessment. INTERPOL, 2024.
12. Interpol. Interpol Global Financial Fraud Threat Assessment. INTERPOL, 2026.
13. United Nations Office on Drugs and Crime. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. UNODC, 2024.
14. United Nations Office on Drugs and Crime. Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia. UNODC, 2025.