CENTEF | Center for Research of Terror Financing

Operation Economic Outcast: The Emerging Architecture of Network-Based Financial Integrity Ecosystems

Using the A7 Network as a test case for applying the integrated financial integrity framework as structured in "Rethinking Correspondent Banking and Financial Integrity Risks: A Financial Integrity Ecosystem for Strengthening Correspondent Banking and Combating Illicit Finance,"[1]

By: Avi Vishnevich[2]
Senior Research Fellow
CENTEF[3]

Executive Summary

This analysis identifies and examines the October 1, 2026, U.S. Treasury measures against the A7 Network as an important evolution in the methodology of economic pressure and financial-integrity regulation.

On October 1, 2026, the U.S. Department of the Treasury announced, as part of Operation Economic Outcast, a coordinated package of measures targeting the A7 Network, a transnational shadow-banking infrastructure associated with Russian sanctions evasion and reportedly exploited also by Iranian actors, including the Islamic Revolutionary Guard Corps. The operation combined a FinCEN notice of proposed rulemaking, a dedicated financial-intelligence alert, and an OFAC designation of the A7 Network as a significant transnational criminal organization.

The coordinated use of designations and sanctions, transaction-based restrictions, and financial-intelligence tools reflects a shift from targeting specific actors toward identifying and disrupting the wider networks through which illicit finance operates.

The significance of this initiative extends beyond the specific entities targeted. It reflects a recognition that contemporary sanctions-evasion infrastructures cannot be understood solely through individual banks, designated persons, or isolated transactions. They increasingly operate through interconnected networks of commercial intermediaries, payment facilitators, controlled companies, alternative settlement mechanisms, and correspondent-banking relationships.

[1] Please see the original publication here.
[2] Avi Vishnevich, Senior Research Fellow at CENTEF, is a former deputy supervisor of the banks in Israel, a former senior official at the Israeli Prime Minister's Office. He spent his entire career analyzing, researching and implementing economic measures.
[3] CENTEF is a global research institute dedicated to advancing the understanding of terror financing and its impact worldwide. www.centef.org

This approach demonstrates significant methodological convergence with the Financial Integrity Ecosystem proposed by us lately for correspondent banking, particularly regarding **network-based risk identification**, indirect exposure, ownership and control, risk-based network illumination, and systematic use of regulatory information (*Rethinking Correspondent Banking and Financial Integrity Risks* – "the correspondent Banking Research"). There, we argue that the effectiveness of financial restrictions depends not only on the legal prohibitions imposed on illicit actors, but also on the ability of the wider financial system and additional players to identify, transmit, evaluate, and respond to risks embedded in complex cross-border networks.

However, the Treasury measures remain principally instruments of targeted governmental intervention on the A7 Network. As detailed in Chapter 4 of this article, the proposed Financial Integrity Ecosystem goes further by integrating also public disclosure and financial reporting, governance, independent assurance, calibrated liability, ownership transparency, and prudential incentives to create continuous preventive discipline across the international financial system.

Operation Economic Outcast provides a particularly relevant case study. It demonstrates how several existing regulatory instruments can be coordinated to address different components of a common illicit-finance infrastructure. At the same time, it raises a broad policy question: could the effectiveness and durability of such campaigns be strengthened by activating additional mechanisms of market discipline, institutional governance, independent assurance, and prudential supervision.

The Operational Innovation: Targeting the Financial Network Alongside Its Individual Components

The A7 Network illustrates the structural vulnerability identified in the Correspondent-Banking Research. According to FinCEN's October 2026 proposed rule, A7 employed companies operating in third-country jurisdictions - described as sub-agents - to receive and transmit payments on behalf of clients whose identities or connections to sanctioned activities could be obscured.

Treasury reported that A7 sub-agents served not only Russian and Iranian sanctions-evasion activity but also other illicit actors, including cybercriminals. It also described connections to Iranian oil sales, weapons procurement and alternative payment instruments.

These arrangements reportedly allowed transactions to appear as ordinary commercial payments, notwithstanding the involvement of sanctioned or otherwise high-risk parties. The network combined corporate intermediaries, trade documentation, foreign-currency accounts, correspondent-banking access, and alternative settlement instruments.

The Treasury response incorporated three complementary regulatory mechanisms:

First, FinCEN proposed a transaction-class restriction. Acting under Section 9714 of the Combating Russian Money Laundering Act, FinCEN identified transactions involving A7-controlled foreign sub-agents as a class of transactions of primary money-

laundering concern in connection with Russian illicit finance. Its proposed special measure would prohibit specified transmittals of funds involving that class of transactions by covered financial institutions.

This approach is especially significant because it addresses the operational function performed by the sub-agent network, alongside and rather than depending exclusively on identifying each individual participant through conventional designation mechanisms.

Second, FinCEN issued Alert FIN-2026-Alert007. The alert provided financial institutions with red flag indicators intended to improve their ability to identify and report suspicious activity associated with A7.

As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider all of the available facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices and whether the customer exhibits multiple red flags before determining that a behavior or transaction is suspicious.

This component extends the operation beyond legal prohibition by mobilizing the monitoring capabilities of financial institutions themselves.

Third, OFAC designated the A7 Network as a significant transnational criminal organization. This measure applied blocking consequences to the designated network and its property interests within the scope of U.S. sanctions jurisdiction, complementing the proposed transaction-based restriction and FinCEN's detection-oriented alert.

The measures are not identical in their legal nature. The OFAC designation applies and is already enforceable, while FinCEN's proposed prohibition remained subject to final rulemaking. The FinCEN alert, meanwhile, provided detection and reporting guidance rather than establishing a new general prohibition.

Nevertheless, their coordination represents an important departure from an exclusively entity-by-entity enforcement model.

Methodological Convergence with the Financial Integrity Ecosystem

The central argument of the earlier Correspondent-Banking Research is that illicit-finance risk is transmitted through fragmented networks, while responsibility and information are frequently distributed among institutions that see only fragments of the relevant activity.

The A7 case provides substantial support for this analysis.

The network reportedly exploited the distance between the original economic beneficiary, the nominal commercial counterparty, the financial institution executing a payment, and the correspondent bank facilitating settlement. This separation reduced the visibility of the underlying risk.

The October 2026 Treasury package responds to that problem through several mechanisms that correspond closely to the proposed Financial Integrity Ecosystem in my previous article:

The first is **network-based risk identification**. Rather than concentrating namely on individual sanctioned persons and entities, FinCEN's proposed rule addresses transactions involving companies controlled by a common illicit-finance infrastructure. This reflects the same methodological principle underlying the proposed adaptation of supply-chain due-diligence techniques to correspondent banking: risk may originate beyond the immediate counterparty, requiring proportionate inquiry into the wider network.

The second is **the systematic mobilization of existing regulatory authorities**. Section 9714 provides Treasury with an instrument for targeting classes of transactions associated with specified money-laundering concerns. The operation illustrates the value of deploying such authorities alongside sanctions designations and financial-intelligence mechanisms. This is consistent with the research's argument that important improvements can be achieved by coordinating existing authorities rather than relying exclusively on new legislation and regulations.

The third is **ownership-and-control analysis**. FinCEN's attention to companies controlled by A7 is significant because the formal identity or nominal ownership of a commercial entity may not accurately represent the persons directing its activities or benefiting from its transactions. The A7 case therefore reinforces examining effective control, indirect relationships, and the economic reality underlying apparently independent corporate structures.

The fourth is **earlier institutional detection**. By publishing red flags indicators of A7-related activity, FinCEN seeks to convert governmental knowledge into information that financial institutions can incorporate into their monitoring and risk-assessment processes. This is consistent with the proposed ecosystem's emphasis on moving regulatory information into the institutions best positioned to identify and mitigate exposure.

The fifth is **risk-based network illumination.** The A7 case offers a particularly compelling argument for adapting supply-chain due-diligence methodologies to correspondent banking. As detailed by the FinCEN Alert, where relevant risk red flags indicators arise, financial institutions should conduct proportionate inquiries beyond the immediate respondent, including relevant nested relationships, intermediary entities, payment routes, and ownership or control structures. This should not become an indiscriminate obligation to identify every customer of every respondent bank. Instead, inquiry should be escalated according to clearly defined indicators of material risk.

The sixth is **systematic information gathering using existing regulatory and information gathering authorities.** The findings underlying FinCEN's A7 alert support targeted supervisory inquiries concerning correspondent-banking relationships, payment flows, and controls associated with identified risk indicators. This is a functional parallel to the full deployment of section 104(e) of CISADA that is suggested by us under the eight pillars framework for correspondent banking.

Despite these substantial similarities and methodological convergence, Operation Economic Outcast does not formally implement the full eight-pillar framework of the Correspondent Banking Research, and several elements of the research extend considerably beyond the measures announced by Treasury.

What Additional Elements of the Financial Integrity Ecosystem Could Strengthen the US Campaign Against A7 Network?

FinCEN's October 2026 measures provide a strong foundation for restricting A7's access to the international financial system. However, the proposed Financial Integrity Ecosystem suggests additional measures that could reinforce effectiveness, particularly by creating continuous incentives and market discipline mechanisms for financial institutions to identify and reduce exposure before enforcement action becomes necessary:

Enhanced financial-integrity disclosure and market discipline. Financial institutions with material exposure to correspondent relationships presenting elevated A7-related risks could be required, within an appropriately designed disclosure framework, to report relevant concentrations, governance arrangements, and risk-management deficiencies. Public reporting would enable investors, creditors, counterparties, and other market participants to assess the financial consequences of elevated integrity exposure.

Strengthened board and senior-management accountability. Supervisors could require institutions with material exposure to relevant payment corridors, correspondent relationships, or trade-finance channels to declare and certify under special reporting framework that the risks identified in the FinCEN package have been considered within their risk appetite, internal-control systems, and senior-management oversight. Such measures would convert a government warning into a matter of institutional governance and strategic risk management.

Independent assurance and external-auditor responsibilities. Material exposure to sanctions-evasion networks may generate financial, internal control, legal contingencies, or disclosure implications. Within the applicable auditing standards, auditors should evaluate information suggesting potential illegal acts and assess whether the institution's accounting, disclosure, or control representations are materially affected. A broader assurance framework specifically addressing correspondent-banking financial-integrity controls could also be considered as a prospective reform, without incorrectly treating existing audit standards as a general obligation to conduct sanctions investigations.

Calibrated liability and deterrence. Operation Economic Outcast also raises consideration of whether particularly severe and clearly identified financial-integrity risks warrant stricter consequences for institutions that continue facilitating prohibited activity.

Treasury's October 2026 measures towards the A7 Network do not explicitly establish a general strict-liability regime for foreign financial institutions. Under these

circumstances we suggest again the adoption of our proposal under Pillar 6 to the Correspondent Banking research- shifting to a consequence-based liability standard applying a strict standard for narrowly defined, exceptionally severe risks, which the A7 network surely demonstrates.

Targeted prudential incentives by regulatory capital charges as suggested under pillar 7 of the full 8 pillars framework. Where material A7-related exposure reveals exceptional weaknesses in risk management, governance, or controls, prudential supervisors could assess whether the resulting legal, operational, reputational, or funding risks are adequately captured by existing supervisory frameworks. In appropriate cases, institution-specific Basell Pillar 2-type supervisory measures could be considered. This would be a supervisory response to demonstrable risk, not an automatic capital penalty for maintaining a correspondent relationship in a particular jurisdiction.

Summary and Conclusions:

From Coordinated Network Disruption to Continuous Financial-Integrity Architecture

Operation Economic Outcast illustrates the increasing sophistication of U.S. financial-pressure operations, particularly the coordinated use of sanctions and designations, transaction-based restrictions, and financial-intelligence mechanisms against interconnected illicit-finance infrastructures.

Its methodological significance lies in the recognition that financial-integrity risks may originate and remain concealed across networks of commercial intermediaries, payment facilitators, controlled entities, and financial institutions. Effective regulatory intervention therefore requires attention not only to individually designated persons and entities, but also to the structures and relationships through which illicit financial activity is conducted.

Yet October 1, 2026 measures do not establish the full comprehensive incentive architecture advanced in the Financial Integrity Ecosystem which offers a general regime of enhanced institutional disclosure, expands independent auditor assurance responsibilities, and introduces targeted prudential capital requirements for exceptional financial-integrity exposure.

These distinctions do not diminish the importance of Treasury's initiative. Rather, they clarify the complementary nature of two regulatory approaches: targeted governmental intervention against identified illicit-finance networks, and continuous preventive discipline generated through the interaction of financial institutions, markets, boards, auditors, and supervisors.

The proposed Financial Integrity Ecosystem seeks to integrate these approaches. Its objective is not merely to improve the capacity of public authorities to disrupt identified networks, but to strengthen the incentives and capabilities of the international financial system to detect, evaluate, price, and mitigate comparable risks before they mature into serious violations.

Enforcement establishes the regulatory floor. An integrated incentive architecture can create continuous discipline above that floor.

APPENDIX

Comparison with the Financial Integrity Ecosystem

The Financial Integrity Ecosystem is based on the proposition that effective financial-integrity regulation requires more than prohibitions and enforcement actions.

It requires coordinated architecture through which information, governance, supervision, independent assurance, legal liability, market discipline and prudential incentives continuously influence financial institutions' behavior.

The October 1 Treasury package illustrates important elements of that architecture, although it does not implement the ecosystem in its entirety.

Treasury's October 1 package is primarily a specific - targeted exercise of governmental enforcement and preventive financial restrictions. My proposed Financial Integrity Ecosystem goes further, seeking to make financial institutions, markets, auditors, boards and supervisors continuous participants in detecting, pricing and mitigating such risks in general.

The following comparison uses the substantive eight-pillar structure of the earlier article.

Pillar of the Financial Integrity Ecosystem	Relationship with the October 1 Treasury measures
Pillar 1 — Enhanced financial-integrity disclosure	Partial convergence. Treasury's public identification of the A7 Network increases transparency and alerts counterparties to financial-integrity exposure. However, this is government-generated transparency, not the systematic institution-level public disclosure proposed in the article.
Pillar 2 — Expansion of Section 219 ITRA disclosure methodology	Indirect convergence. The measures increase awareness of indirect exposure to sanctions evasion, but do not create expanded SEC reporting duties or the investor-facing disclosure mechanism advocated in the article.
Pillar 3 — Supply-chain-style due diligence for correspondent banking	Strong methodological convergence. Treasury traces indirect relationships, sub-agents, control structures and transaction channels. This resembles the network-mapping and risk-based inquiry methodology proposed under Pillar Three.
Pillar 4 — External auditor responsibilities	No direct implementation. The announcement does not establish new PCAOB or IAASB duties. Nevertheless, the risks identified could be relevant to existing auditor

	responsibilities where they materially affect financial statements, disclosures or internal controls.
Pillar 5 — Systematic use of supervisory information and existing authorities	Strong convergence. FinCEN combines intelligence gathering, red-flag dissemination, suspicious-activity reporting and proposed payment restrictions. This illustrates the operational value of existing regulatory information and authorities.
Pillar 6 — Reassessment of knowledge standards in secondary sanctions	Partial convergence. The package emphasizes sanctions exposure arising from indirect financial relationships. It does not, however, establish the article's proposed recalibration of knowledge requirements for narrowly defined exceptional risks.
Pillar 7 — Prudential capital incentives	Not implemented. Treasury measures may affect institutions' risk assessments and correspondent relationships, but they do not establish a financial-integrity capital add-on or a Pillar 2 supervisory capital mechanism.
Pillar 8 — Ownership and control transparency	Strong convergence. Treasury identifies control of sub-agents, accounts and associated entities and highlights the application of OFAC's 50 Percent Rule. This supports the article's emphasis on effective control rather than formal corporate separation alone.