White Collar Defense & Investigations Update

March 2026

Treasury's 2026 National Risk Assessments Signal Expanding Exposure

Key Notes:

- Fifteen drug cartels designated as Foreign Terrorist Organizations expand criminal exposure under 18 U.S.C. § 2339B for companies with Latin American ties.
- Treasury's laundering typologies—AI tools, chain-hopping, and pig butchering schemes—signal a DOJ enforcement roadmap for digital asset and fintech companies.
- Sanctions evasion risks and shell company misuse remain central enforcement priorities, warranting proactive compliance audits.

The U.S. Department of the Treasury recently released its 2026 National Risk Assessments, including the money laundering, terrorist financing, and proliferation financing reports—offering a clear signal of where enforcement is headed. The headline development: fifteen drug cartels are now designated as Foreign Terrorist Organizations and Specially Designated Global Terrorists. For the first time, Treasury addresses transnational criminal organizations (TCOs) in its terrorist financing assessment alongside ISIS, Al-Qa'ida, and Hizballah.

The practical implications are significant. Material support charges under 18 U.S.C. § 2339B may now reach financial activity connected to these cartels. For clients with business operations, supply chains, or banking relationships touching Latin America, this substantially expands potential criminal exposure. Conduct that previously carried narcotics or money laundering risk may now trigger terrorism-related liability—with corresponding consequences for sentencing, asset forfeiture, and reputational harm.

- Companies with Latin American operations should work with counsel and compliance teams to conduct immediate risk assessments, mapping their counterparties, correspondent banking relationships, and supply chains against the fifteen designated TCOs and their known affiliates.
- Companies in industries historically adjacent to cartel activity, including logistics, money transmission, and cross-border trade—should implement enhanced due diligence protocols and assess whether existing compliance programs adequately address these new terrorism-related risks.
- For clients already under investigation for narcotics or money laundering offenses, counsel should anticipate that prosecutors may add or leverage material support charges to increase sentencing exposure and forfeiture remedies.

Example: *A U.S.-based freight logistics company discovers that one of its Mexican subcontractors has ties to a newly designated TCO. Under the prior framework, the company's primary concern was potential money laundering exposure. Now, if prosecutors can establish that the company knowingly provided services benefiting the designated organization, it could face material support charges carrying up to 15 years per count, plus civil forfeiture of any assets involved in or traceable to the offense. Defense counsel should advise the client to sever the relationship, preserve records, and evaluate whether voluntary disclosure is appropriate.*

What Else Should Be on Your Radar:

Digital assets and AI-related prosecutions are likely to increase. Treasury quantifies $5.8 billion in "pig butchering" losses and $6.5 billion in total investment fraud losses in 2024. AI tools, encrypted communications, and blockchain “chain-hopping” are now documented laundering methodologies—effectively providing DOJ with a detailed evidentiary roadmap for building cases in these areas. Companies in fintech, digital assets, and financial services should treat these risk assessments as forward-looking enforcement signals.

- Clients operating digital asset platforms or payment services should conduct gap analyses of their AML/CFT programs against Treasury's identified typologies, particularly stablecoin misuse and chain-hopping before regulators do it for them.
- Clients who have received or processed funds linked to investment fraud schemes should consider proactive voluntary self-disclosure to mitigate criminal exposure.
- Defense counsel should expect prosecutors to cite these assessments to support the foreseeability of AI-enabled and digital asset-related laundering risks.

Example: *A mid-size cryptocurrency exchange identifies a pattern of rapid conversions between stablecoins across multiple blockchain networks—classic chain-hopping—linked to wallets associated with a pig butchering scheme. Although the exchange filed SARs, it neither froze nor exited the relationships. Treasury's 2026 assessment documents this exact typology as a known laundering methodology. Prosecutors may argue the exchange was on notice and that its failure to act beyond SAR filing constitutes willful blindness. Counsel should advise digital asset clients to evaluate whether escalation protocols should extend beyond SAR filing when transactions match documented typologies.*

Sanctions enforcement risk is escalating. Treasury identifies Chinese actors as playing a "more widespread role" in sanctions evasion and characterizes Russia-DPRK military ties as a "major PF threat." For companies in the technology, manufacturing, and defense sectors, the proliferation financing assessment highlights exposure tied to front companies, DPRK IT worker schemes, and dual-use goods.

- Companies dealing in dual-use technologies should immediately audit their customer and vendor screening processes for connections to Chinese intermediaries, DPRK-affiliated IT contractors, and Russian procurement networks.
- Companies should assess whether their existing OFAC compliance programs adequately address newly emphasized non-state actors, including Hizballah, the Houthis, and designated cartels.
- Engage counsel to evaluate whether voluntary disclosures to OFAC or BIS are warranted for any previously identified compliance gaps before enforcement agencies come knocking.

Example: *A U.S. semiconductor distributor learns through media reporting that one of its overseas resellers has been shipping components to a Russian defense contractor via a China-based intermediary. The 2026 NPFRA specifically identifies this type of supply chain exploitation. Counsel should advise the client to immediately suspend shipments to the reseller, engage forensic trade compliance consultants to trace end-use, and evaluate whether a voluntary self-disclosure to BIS under the Export Administration Regulations is warranted—recognizing that BIS has publicly stated it views voluntary disclosures as a significant mitigating factor in enforcement decisions.*

Shell companies remain a central enforcement focus. Despite narrowing CTA beneficial ownership reporting, Treasury continues to identify shell company misuse as a core money laundering vulnerability. Expect prosecutors to continue aggressively pursuing cases involving opaque corporate structures. The delay of the investment adviser AML rule to 2028 may leave a gap that enforcement agencies address through targeted investigations.

- Clients under investigation should scrutinize whether the government's theory relies on shell company structures identified in these assessments and be prepared to challenge the sufficiency of beneficial ownership evidence where CTA reporting was not required.
- Companies using complex but legitimate entity structures should document the business rationale now before those structures are characterized as concealment.
- Investment advisers should not treat the 2028 deferral as a compliance holiday. Treasury's continued focus on

the sector signals that enforcement actions under existing authorities will continue.

Example: *A private equity fund uses a series of Delaware LLCs and offshore holding entities to structure investments across multiple jurisdictions. The structures serve legitimate tax and liability purposes, but the fund's documentation does not clearly memorialize the business rationale for each entity. If a portfolio company becomes the subject of a money laundering investigation, prosecutors may characterize the layered entity structure as evidence of concealment—particularly given Treasury's continued emphasis on shell company misuse. The best practice is to create a contemporaneous record explaining each entity's purpose, ensuring a defensible narrative if questions arise.*

These assessments are not merely policy documents, they provide a roadmap for where DOJ, FinCEN, and OFAC are likely to direct investigative resources. Clients should engage with experienced counsel to evaluate their exposure now, particularly regarding the newly designated TCOs, digital asset activity, and sanctions compliance, rather than waiting for a subpoena to force the conversation.

FOR MORE INFORMATION

For more information, please contact:

Brittain Shaw
212.908.3940
Brittain.Shaw@ThompsonHine.com