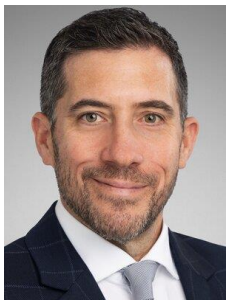
LAW360

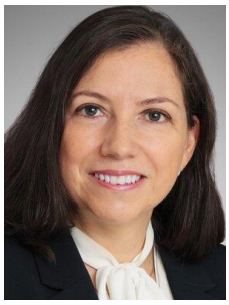
Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Mitigating The Risk Of Interacting With A Designated Cartel

By **Benjamin Haley, Adam Studner and Veronica Yepez** (March 20, 2025, 6:07 PM EDT)

Benjamin Haley


Adam Studner


Veronica Yepez

The Trump administration's recent designation of certain cartels and transnational criminal organizations as foreign terrorist organizations seeks to aggressively leverage U.S. criminal material support anti-terrorism laws to advance U.S. national security and foreign policy interests.

These designations create significant new risks for companies that may not be effectively addressed and mitigated by existing compliance policies and controls, as well as, potential civil claims under the Anti-Terrorism Act.[1]

Since taking office, the Trump administration has launched a whole-of-government effort to combat cartel and transnational criminal organization, activities. As part of this effort, on Jan. 20 the president signed Executive Order No. 14157, directing the secretary of state, attorney general, secretary of homeland security and director of national intelligence to evaluate international cartels and other transnational criminal organizations for designation as foreign terrorist organizations, or FTOs, and specially designated global terrorists.[2]

Following through on the order, on Feb. 20 the secretary of state designated eight criminal organizations as FTOs and specially designated global terrorists.[3] Six of the eight designated organizations are cartels that originated in Mexico, many of which now operate across Latin America and beyond.

Except for Carteles Unidos, each of the entities designated as an FTO was already on the specially designated nationals and blocked persons list maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control, and thus was already subject to sanctions prohibitions.

On March 18, OFAC issued an alert to raise awareness of the recent FTO designations.[4]

Existing U.S. primary sanctions generally prohibit U.S. persons, including non-U.S. nationals employed by a U.S. company, from engaging in transactions or dealings involving SDNs, or their property or interest in property, except as licensed by OFAC. They also prohibit non-U.S. persons from causing U.S. persons to violate primary sanctions. Non-U.S. persons may otherwise be exposed to potential secondary sanctions risk arising from certain transactions with SDNs.

While many companies will already be aware of sanctions risk with respect to the recently designated entities, OFAC now recommends that companies evaluate their existing compliance programs to account for these risks. As such, companies would be wise to revisit and consider enhancing existing screening programs and risk-mitigation measures.

Although FTO designations are not new, before the latest designations multinational companies often had significantly less exposure because the jurisdictions implicated by FTO activity were either conflict zones, e.g., Afghanistan, Iraq, Northern Mozambique and Yemen, or comprehensively sanctioned jurisdictions where sanctions and export control risks had already made it prohibitively difficult to operate, e.g., Iran and Syria.

Now, significant FTO risk exists in a country that is the U.S.' largest trading partner, as well as several other Latin American countries in which U.S. companies have significant operations.

The Criminal Material Support Provisions

U.S. criminal material support laws operate separate and apart from U.S. primary and secondary sanctions, and can apply to a broader array of conduct than sanctions prohibitions. The Antiterrorism and Effective Death Penalty Act, or AEDPA, makes it a federal crime to knowingly provide, or attempt or conspire to provide, "material support or resources" to a designated FTO.[5]

While the statute does not define "knowingly," we expect that the U.S. Department of Justice would take the position that willful blindness would satisfy the knowledge requirement in appropriate cases.

In addition to direct dealings with FTOs, liability may also arise from indirect dealings with FTOs through third-party entities or individuals. Material support prohibitions under the AEDPA have the potential to sweep in any type of support to an FTO, and there is no de minimis exception.

"Material support" is broadly defined to include "any property, tangible or intangible, or service" including currency or monetary instruments, financial services, lodging, training, expert advice or assistance, communications equipment, facilities, personnel, or transportation.[6]

Importantly, to be liable under the statute, a party need not have specific intent to support the FTO's terrorist activities. It only needs to have knowledge that an entity is designated as an FTO or has engaged in or engages in terrorist activity.[7]

To this point, in 2010, in Holder v. Humanitarian Law Project, the U.S. Supreme Court held that a violation of [the material support provisions of AEDPA require] only that a party have knowledge that the entity is a designated terrorist organization or that the organization engages in statutorily defined "terrorism."[8] The court held that there is no requirement of specific intent to "further the organization's terrorist activities."[9]

In line with Holder, in U.S. v. El-Mezain, the U.S. Court of Appeals for the Fifth Circuit's 2011 decision affirmed the material support conviction of a U.S.-based charity that provided money to zakat committees — Islamic charitable organizations — in the West Bank, knowing that the funding of these zakat committees ultimately supported Hamas' social wing.[10]

In addition, the material support provisions have broad jurisdictional reach, and the statute expressly states that there is extraterritorial jurisdiction, with no statutorily imposed limiting principle.[11]

The full reach of the material support provisions has not been tested in litigation against corporations. However, the DOJ's first and — to date — only corporate enforcement action under the criminal material support law is a good example of the broad jurisdictional reach of the provision.

In that case, the DOJ charged Lafarge S.A., the French multinational building materials company, and its Syrian subsidiary, Lafarge Cement Syria, for payments made in Syria to designated FTOs, where the U.S. nexus — as described in the public charging documents — was limited to alleged U.S. dollar-denominated transactions and correspondence using "email accounts serviced by U.S.-based email service providers to carry out the conspiracy."

Lafarge and LCS pled guilty to conspiring to provide material support to FTOs, and agreed to pay $778 million in fines and forfeitures, and to three years of probation.

Practical Steps Companies Can Take to Reduce Risks

Given the scope of the prohibitions, material support can attach not only to obvious scenarios, such as extortion payments, but also to ordinary-course interactions and transactions that may seem wholly legitimate on their face, but which may involve some nexus to an FTO. There are two principal fact patterns that could present this risk.

The first, which is easier to spot, is direct dealings with criminal activity, like extortion for security payments; so-called tolls, vaccines or safe-passage fees; and similar payments.

The second, which is more difficult to identify, is the cartels' and transnational criminal organizations' use of seemingly legitimate, often registered, tax-paying businesses to generate profit or launder money and goods across borders. This can create risk, for example, in dealings with local distributors, suppliers and vendors. In other words, risk may attach to seemingly legitimate transactions for value third parties that have links to an FTO.

In light of these enhanced risks, companies that operate in Mexico, and Central and South America, across a range of industries — including financial services, mining and energy, logistics, hospitality, consumer goods, manufacturing, and agriculture — should reassess their risk management frameworks to ensure that they are adequately identifying and mitigating these risks.[12]

While it is not yet clear how aggressively the administration will prioritize enforcement under the material support provisions or the existing sanctions regime, companies will be well served by taking a proactive, risk-based compliance approach in this area. Still, companies may face various — and potentially intractable — practical and security challenges to effectively addressing FTO-related risks.

In many ways, the steps companies can take involve adapting well-developed methods of dealing with other types of risks — for example, risks associated with interacting with government officials — and deploying those strategies to a different category of risk.

And of course, relevant mitigation and remediation measures will not take the form of a one-size-fits-all approach, and will need to be tailored to companies' specific risks and business considerations.

Below, we highlight certain steps that companies can take to identify and mitigate potential risks.

Assess Risk and Compliance Programs

While being mindful of security risks and personnel safety concerns, conduct an assessment of: (1) potential FTO-related exposure based on, among other things, the footprint of business operations, manufacturing sites, and procurement and logistics networks, to help better understand how evolving cartel influence may affect operations in specific jurisdictions; and (2) the effectiveness of existing screening processes, controls, and reporting mechanisms.

Such assessments will help inform which additional risk-mitigation measures should be considered.

Establish FTO-Focused Compliance and Security Protocols

Establish an internal compliance and security task force specifically focused on FTO-related risks to monitor developments related to the new designations and to develop strategies that support company-wide compliance and safety.

Conduct Enhanced Due Diligence and Tailor Contractual Obligations

Consider how to leverage due diligence efforts to support FTO-related risk identification, and conduct enhanced due diligence where appropriate.

To the extent not already in place or covered by broad compliance-with-law provisions, establish a contractual right to immediately terminate relationships if a partner is suspected of being linked to an FTO, regardless of jurisdictional nexus.

Evaluate Payment Controls

Review financial controls to evaluate alignment with heightened regulatory expectations around know-your-customer and know-your-vendor requirements, to detect and prevent illicit financial flows.

Leverage Monitoring and Audit Programs

Consider how to leverage or enhance monitoring or auditing programs, including with continuous monitoring or screening, to support the identification of FTO-related risks. Develop escalation protocols for addressing potential red flags and, subject to evaluating security risks, conduct forensic audits of key supply chains to identify potential exposure to FTO-linked entities.

Establish Secure Channels For Reporting and Internal Investigations

In light of the security and personnel-safety risks associated with reporting potential links to FTO activities, confirm that the channels for employees and business partners to report conduct anonymously appropriately protect reporter identities.

Companies also need to focus on the security risks that will arise in the context of internal investigations, which are typically more acute in this context than in other compliance areas.

Implement Mandatory Employee Training

Implement mandatory training for employees, especially those in procurement, finance, logistics,

human resources and security roles, to educate employees on how to identify and mitigate risks associated with potential interactions with FTOs, and to communicate enhanced security around anonymous reporting channels.

Develop and Regularly Evaluate Crisis and Incident Response Plans

Develop and regularly evaluate crisis and incident response plans for applicable scenarios, including extortion attempts, threats to personnel and regulatory investigations. Consider periodically conducting tabletop exercises with senior leadership to simulate crisis scenarios and ensure rapid, coordinated responses. As a part of this exercise, implement employee assistance programs for personnel exposed to high-risk environments.

As companies consider the appropriate approach, it is important to document both the steps taken to address risks and the practical and security challenges that may limit companies' potential mitigation and remediation options to create a record that can be leveraged if the government comes calling.

Benjamin Haley, Adam Studner and Veronica Yepez are partners at Covington & Burling LLP.

Covington partner Jennifer Saperstein and associate Shayan Karbassi contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.cov.com/-/media/files/corporate/publications/2025/02/drug-cartels-terrorist-label-raises-litigation-risk-for-cos.pdf.

[2] https://www.whitehouse.gov/presidential-actions/2025/01/designating-cartels-and-other-organizations-as-foreign-terrorist-organizations-and-specially-designated-global-terrorists/.

[3] https://www.state.gov/designation-of-international-cartels/.

[4] https://ofac.treasury.gov/media/934096/download?inline.

[5] 18 U.S.C. § 2339B(a)(1).

[6] 18 U.S.C. § 2339A(b)(1).

[7] Holder v. Humanitarian Law Project, 561 U.S. 1 (2010).

[8] As defined in either section 212(a)(3)(B) of the Immigration and Nationality Act ("INA") or section 140(d)(2) of the Foreign Relations Authorization Act ("FRAA"), Fiscal Years 1988 and 1989. The INA defines terrorism as, "any activity which is unlawful under the laws of the place where it is committed (or which, if it had been committed in the United States, would be unlawful under the laws of the United States or any State)" and includes "[i] the seizing or detaining, and threatening to kill, injure, or continue to detain, another individual [ii] in order to compel a third person (including a governmental organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained." The FRAA defines terrorism as "premeditated, politically motivated

violence perpetrated against noncombatant targets by subnational groups or clandestine agents."

[9] Holder v. Humanitarian Law Project, 561 U.S. 1, 17 (2010). The Supreme Court in Holder stated that the text of the statute makes clear that "Congress chose knowledge about the organization's connection to terrorism, not specific intent to further its terrorist activities, as the necessary mental state for a violation."

[10] U.S. v. El-Mezain, 664 F.3d 467 (5th Cir. 2011).

[11] Section 2339B contains both a descriptive and a general statement of extraterritorial jurisdiction. The more general statement of extraterritorial jurisdiction was included in the original law, while the more descriptive statement appeared as part of the Intelligence Reform and Terrorism Prevention Act of 2004.

[12] In its March 18 alert, OFAC emphasized that foreign financial institutions that knowingly facilitate a significant transaction or provide significant financial services for any of the designated organizations may be subject to U.S. correspondent or payable-through account sanctions.