Mexican Cartels Designated as Foreign Terrorist Organizations (FTO): What Changes for Companies and How to Strengthen Their Compliance

Two attorneys specialized in international litigation and regulatory compliance explain the real scope of the FTO designation of Mexican cartels, the new legal, financial, and operational risks, and the concrete measures that business leaders, legal directors, and investors must adopt to anticipate them.

The designation of the main Mexican cartels as Foreign Terrorist Organizations (FTO) by the United States government has redefined the risk landscape for any company with operations in Mexico or commercial ties with Mexican companies. What was previously managed as a security issue or an anti-money laundering matter is now located in the much more severe field of anti-terrorism law.

To understand what this change means and how organizations should prepare, we spoke with Isabela Hernández-Peredo, an associate at Diaz Reus International Law Firm, with experience in complex litigation, commercial dispute resolution, and international matters; and with Hilel Silvera, a Mexican attorney with more than 20 years advising national and international companies in litigation, corporate matters, and highly complex legal strategies. Both agree on a central message: the cost of not anticipating today is much higher than the cost of acting.

What Does It Mean for an Organization to Be Designated as a Foreign Terrorist Organization (FTO)?

“An FTO designation is not symbolic. It has immediate and very concrete legal consequences,” explains Hernández-Peredo. The designation of an FTO consists of the formal recognition by the U.S. Government of a criminal organization as a terrorist organization. This figure is provided for in section 219 of the Immigration and Nationality Act (8 U.S.C. § 1189) and authorizes the U.S. Department of State to designate certain organizations as FTOs.

In February 2025, the Secretary of State designated eight organizations —including six Mexican cartels: the Sinaloa Cartel, the Jalisco New Generation Cartel (CJNG), the Northeast Cartel, the Gulf Cartel, La Nueva Familia Michoacana, and Cárteles Unidos— as FTOs and, simultaneously, as Specially Designated Global Terrorists (SDGT).

One of the most relevant legal consequences is that persons subject to U.S. jurisdiction may be exposed to committing the crime of material support to facilitate terrorist activity (“material support”). Under 18 U.S.C. § 2339B, knowingly providing “material support or resources” to an FTO is a federal crime.

“And here is the key that many companies do not fully grasp,” warns Hernández-Peredo: “‘material support’ is not limited to money or weapons. It is a broad concept, which may include services, transportation, logistics, expert advice, training, or helping, facilitating, or contributing in some way to activities linked to an organization designated as an FTO.”

Added to this is the narco-terrorism statute (21 U.S.C. § 960a) and the dual SDGT nature, which incorporates these organizations into the Specially Designated Nationals (SDN) list of the Office of Foreign Assets Control (OFAC).

Why Has This Issue Become So Relevant?

“What changed is not the existence of the cartels, but the legal framework that now applies to them,” says Silvera. “Before, a company facing extortion on a transportation route saw it as an operational or security problem. Today, that same payment may be interpreted as financing terrorism.”

The relevance has intensified due to the pace of enforcement. Throughout 2025 and 2026, OFAC has sanctioned financial networks linked to cartels —from fuel theft schemes (huachicol) and crude oil smuggling to timeshare fraud—. In February 2026, OFAC sanctioned a Mexican resort complex linked to CJNG and blocked 17 entities and five individuals.

“The trend is clear,” Silvera notes: “authorities are pursuing business models with a legitimate appearance that allegedly channel illicit resources. That brings the risk closer to companies that never considered themselves exposed.”

What Are the Main Compliance Risks for Companies with Operations in Mexico?

Hernández-Peredo identifies three liability regimes that should not be confused:

The first is the OFAC sanctions regime, which operates under a strict liability standard in civil matters.

“A company can be sanctioned for a transaction with a blocked entity even if it had no intent or knowledge. It is enough that the operation occurred.”

Banks, payment processors, and any person subject to U.S. jurisdiction must identify, freeze, and report funds linked to entities on the SDN list.

The second, under the Anti-Terrorism Act § 2333(d)(2), may also involve civil liability risks, particularly if it is alleged that the company helped, facilitated, or contributed in some way to activities linked to an organization designated as an FTO.

It does not necessarily require the company to have a direct relationship with the designated organization; the risk may arise if, with sufficient knowledge of certain facts, it participates in a transaction, provides services, channels payments, or facilitates activities that ultimately benefit that organization.

The third is the crime of “material support,” which requires the element of “knowledge.”

“But pay attention,” she emphasizes: “the doctrine of willful blindness allows that knowledge to be established. If a company deliberately ignores evident signs that its counterparty is linked to an FTO, it will not be able to shield itself by saying ‘I didn’t know’.”

Payments for “derecho de piso,” ransoms, “passage fees,” or agreements with third parties controlled by cartels may result in liability for aiding and assisting terrorism.

The Chiquita Scenario: Extortion Is Not a Defense

Both attorneys cite the Chiquita Brands precedent as a warning. The company made payments to a terrorist organization in Colombia between 1997 and 2004, pleaded guilty to one count, and paid a $25 million fine; years later, the families of victims obtained civil judgments for $38.3 million.

“The judicial message was forceful,” says Silvera: “claiming that you paid under extortion does not exempt you. And civil liability can far exceed the criminal fine.”

Implications for Banks, Financial Institutions, and Foreign Payment Providers

“Banks and other financial intermediaries play a central role in risk management,” states Hernández-Peredo.

Foreign financial institutions also face the risk of secondary sanctions: they may be sanctioned for processing transactions for the benefit of designated persons, even without a direct nexus to the U.S.

“A Mexican or Latin American bank that carries out or facilitates transactions of an entity linked to an FTO may face consequences ranging from restrictions in its correspondent banking relationships and access to the U.S. financial system, to potential risks of economic sanctions or, in certain cases, civil or criminal liability.”

This requires banks to apply greater scrutiny, strengthen transactional monitoring, know your customer (KYC), and the detection of beneficial owners through an anti-terrorism lens, not only an anti-money laundering lens.

Risks for U.S. Companies with Partners or Supply Chains in Mexico

“The risk is no longer only the direct supplier, but the entire chain,” explains Silvera.

Sectors with high territorial exposure —agribusiness, avocado, lime, transportation and logistics, mining, energy and fuels, construction, real estate, and tourism— face greater scrutiny.

An illustrative case: in November 2025, a company in the oil sector disclosed that certain payments prior to the acquisition of a Mexican business “were likely made to persons associated with an organization designated as an FTO or SDGT.”

“That is what keeps legal directors awake at night,” Silvera adds: “inherited risk in mergers and acquisitions. You buy a company and inherit its payment history.”

What About Non-U.S. Companies?

Yes, they may face consequences. Hernández-Peredo is clear:

“The extraterritorial reach of certain U.S. laws can be considerable. A European, Asian, or Latin American company that uses U.S. dollars, operates through the U.S. financial system, maintains subsidiaries, employees, or directors subject to U.S. jurisdiction, or participates in transactions with some link to that country, could be exposed to relevant regulatory and compliance risks.”

The company’s nationality is not a shield against the risks associated with FTO designations.

Most Common Mistakes When Assessing Risk

The interviewees agree on several:

First, assuming that an anti-corruption or anti-money laundering compliance program is sufficient to mitigate the risks associated with FTOs.

“Although AML and anti-corruption programs constitute an important foundation, they are not necessarily designed to identify risks related to organizations designated as FTOs,” says Hernández-Peredo. “These are different risks that require specific controls and processes,” explains Hernández-Peredo.

Second, underestimating third parties and the indirect chain. Many organizations examine the first-tier supplier, but not carriers, intermediaries, land lessors, or subcontractors.

Third, assuming that being a victim of extortion constitutes, by itself, a sufficient defense against potential legal consequences. The Chiquita precedent demonstrates otherwise.

Fourth, lacking a protocol for payments under coercion.

“When an employee is kidnapped, the decision is made in minutes. Without a prior protocol, the company improvises, and improvisation creates liability,” warns Silvera.

Compliance Recommendations and Best Practices

For companies, investors, banks, and organizations with exposure to Mexico, the experts recommend:

Updating the compliance program with an anti-terrorism component, integrating a sanctions section, implementing, among other things, review of OFAC's SDN list and FTO lists, not only anti-corruption checks.

Strengthening third-party due diligence throughout the entire supply chain: suppliers, carriers, logistics, lessors, partners, and financial institutions, with emphasis on areas and industries under cartel influence.

Conducting a regional and geographic risk assessment to evaluate risk by route, municipality, and sector, mapping where third parties operate, who their counterparties and/or third parties are, what logistical routes they use, in which areas they have assets, and what payments they make.

Auditing historical payments and M&A operations to identify potential inherited risks before the closing of a merger or acquisition.

Establishing clear protocols for payments under coercion (extortion, ransoms, "derecho de piso"), with escalation to legal and compliance areas and specialized advice before acting.

Strengthening transactional monitoring and KYC in financial institutions, with detection of beneficial owners and attention to secondary sanctions.

Documenting due diligence: in the face of an investigation, demonstrating that one acted in good faith and with reasonable controls is the best defense against the willful blindness standard.

Training local teams, the legal and compliance teams and compliance should not be the only ones who understand the risk. Procurement, logistics, finance, operations, security, business development, and treasury must know how to identify red flags.

Conclusion: Anticipation Is a Key Tool in Risk Management

The FTO designation of Mexican cartels structurally raised the level of legal, financial, and reputational risk for any company with a presence or ties in Mexico.

The consequences—criminal liability for material support, OFAC sanctions under strict liability, secondary sanctions for the financial sector, and substantial civil lawsuits for civil liability—are no longer hypothetical.

"The main recommendation for business leaders is to act preventively: evaluate your exposure today, not when the risk has already materialized," concludes Hernández-Peredo.

"Having a compliance program aligned with recent developments in the U.S. regulatory framework can constitute an essential tool to mitigate risks that may give rise to the imposition of economic sanctions or the creation of civil or criminal liabilities for companies."

Silvera summarizes it this way:

“The law changed category. Whoever continues managing these risks with the tools of five years ago is exposed without knowing it. Anticipating, with specialized advice and documented controls, is the only defensible strategy.”

This article is for informational purposes only and does not constitute legal advice. Each situation requires a particular analysis. To evaluate your specific exposure, consult with legal advisors specialized in international sanctions and cross-border regulatory compliance.