ALM | LAW.COM

New York Law Journal

Extortion and the New Terrorist Designations

By Howard Master and Alberto Orozco

March 5, 2025

Several months ago, one of us wrote in this Journal about the proper scope of the extortion defense under the Foreign Corrupt Practices Act (FCPA). *See* Howard Master, "Economic Extortion and the Foreign Corrupt Practices Act," *NYLJ* (Oct. 14, 2024).

The Trump administration's shift in enforcement policy away from foreign corruption and towards the fight against Transnational Criminal Organizations (TCOs) such as drug cartels, a shift that adds a spate of new designations of cartels as terrorist groups, may reduce the immediate risk to global businesses of an FCPA prosecution based on alleged extortion payments.

However, the same shift raises new threats to those businesses under statutes, including the Anti-Terrorism Act (ATA), that prohibit engagement of any kind with terrorist organizations, do not recognize an extortion defense, and may give rise to civil as well as criminal liability.

Businesses operating in environments where they are subject to demands for "protection" payments or other extortionate threats must investigate carefully and maintain strong compliance programs to minimize prosecution and litigation risks.

freshidea - stock.adobe.com

Trump's Enforcement Priorities

President Donald Trump has indicated his intent to use the ATA and related statutes in addition to existing tools to combat cartels and other TCOs, even while he has deprioritized FCPA enforcement. In one of his first actions after inauguration, President Trump signed an executive order directing the State Department to designate cartels and other TCOs as Foreign Terrorist Organizations ("FTOs") and Specially

Designated Global Terrorists (SDGTs). EO 14157 (Jan. 20, 2025).

On Feb. 20, 2025, the State Department designated eight TCOs, including organizations with significant operations in Mexico, Central America, and Venezuela, as FTOs and SDGTs pursuant to the Executive Order. 90 Fed. Reg. 10030 (Feb. 20, 2025).

On Feb. 5, Attorney General Pam Bondi issued a memorandum, "Total Elimination of Cartels and Transnational Criminal Organizations," that directed the Department of Justice's FCPA enforcement efforts to "prioritize investigations related to foreign bribery that facilitates the criminal operations of Cartels and TCOs, and shift focus away from investigations and cases that do not involve such a connection."

Five days later, Trump issued an executive order directing that the Department of Justice (DOJ) "cease initiation of any new FCPA investigations or enforcement actions, unless the attorney general determines that an individual exception should be made." EO 14207 (Feb. 10, 2025). It appears likely that any exceptions granted by the attorney general will relate to cases with a connection to cartels or TCOs, particularly those that are subject to FTO/SDGT designation.

The Extortion Threat Presented by TCOs

Organized crime and threats of extortion or other harm have long been major concerns for companies operating in Latin America, where security-related expenses and losses due to crime impose considerable financial burdens. According to a 2024 survey by the American Chamber of Commerce Mexico, which polls its member companies:

- 12% of respondents reported that organized crime has taken partial control of their sales, distribution, and/or pricing.
- 49% stated that their trucks had been attacked.
- 45% reported receiving demands for protection payments.

These figures highlight the widespread and persistent nature of the problem.

TCOs also have corrupted many government officials in Latin America, as reflected by the recent federal indictments and prosecutions of many leaders arising out of unlawful relationships with TCOs, including the former President of Honduras; the leadership of Venezuela; and the governor of Mexico's Tamaulipas State.

Moreover, in some places with weak or corrupted governments, TCOs have assumed state-like functions, providing public protection and other public services.

Changing Legal Ramifications

While the threat of extortion is an enduring issue for international businesses, the shifts in enforcement priorities and FTO/SDGT designations dramatically change the landscape in regions where FTOs/SDGTs wield significant power.

An extortion payment made by a business to a non-designated cartel, for example, should not give rise to any US legal liability: the company is a victim of extortion under the law and may even have legal claims for restitution of the extorted funds if the cartel or its members are ever prosecuted for their conduct.

The same payment, if extorted by a public official, may give rise to FCPA liability,

although if made in a "true extortion" situation, one in which the payor faced a real threat of significant harm in the absence of a payment, the business would have a potential defense under the FCPA.If that public official was demanding payment on behalf of a non-designated cartel it is even more likely to constitute "true extortion" because of the fear of harm that the official's relationship to organized crime would engender.

Consider that same payment if (a) made to the same cartel, but one that the business has learned is newly designated as an FTO/SDGT, or (b) made to a corrupt public official who is acting on behalf of the same designated cartel.

Under the ATA, it is illegal for anyone within US jurisdiction or subject to US law abroad to knowingly provide "material support or resources" to a designated FTO. 18 U.S.C. §2339B. "Material support or resources" means any property or service that is provided to the FTO, including payments made to them. 18 U.S.C. §2339A(b)(1). Related statutes and regulations prohibit engaging in financial transactions of any kind with SDGTs. *See* 50 U.S.C. §1705, 31 C.F.R. §594.204 (the "SDGT prohibitions").

It does not matter under the ATA or the SDGT prohibitions whether payments were extorted or given wholly voluntarily because neither statutory scheme recognizes an extortion defense. While the FCPA requires proof of corrupt intent, which a victim of "true extortion" does not possess, the ATA requires only knowing provision of material support to an entity that the provider knows has been designated as an FTO or is engaging in terrorist activity.

The SDGT prohibitions similarly do not require evidence of corrupt or malicious intent. While the affirmative defenses of duress and necessity may be available in material support and SDGT-related prosecutions, a business is unlikely to be able to establish these defenses if the conduct involves more than a payment made upon threat of immediate physical harm.*See In re Chiquita Brands Int'l, Inc.*, 284 F. Supp. 3d 1284, 1305-06, 1333-35 (S.D. Fla. 2018) (duress defense not clearly viable in material support cases and in any event unavailable to company that made repeated protection payments to FTO over a multi-year period).

DOJ enforcement actions and civil litigation demonstrate the gravity of the risk faced by companies operating in the new environment. In 2007, Chiquita Brands International pleaded guilty to violating the SDGT prohibitions for making protection payments to the Autodefensas Unidas de Colombia ("AUC"), an SDGT and FTO. Chiquita had made these payments over six years to shield its employees and assets in Colombia from harm by the AUC, recording the payments as "security expenses."

In 2007, DOJ fined Chiquita $25 million for this conduct. In 2024, the company was ordered in civil litigation to pay an additional $38.3 million to some of the AUC's victims under a provision of the ATA that was added in 2016 and that permits victims of FTOs to seek damages not only from the FTOs themselves, but also from anyone else "who aids and abets, by knowingly providing substantial assistance, or who conspires with" the FTO. 18 U.S.C. § 2333(d)(2).

In 2023, global building materials manufacturer LaFarge S.A. pleaded guilty to conspiring to provide material support to the Islamic State of Iraq and al-Sham, better known as ISIS, and the al-Nusrah Front, both FTOs, in part for making protection payments so that their trucks could traverse checkpoints controlled by the armed groups.LaFarge was required to pay $778 million in penalties as a result of its conduct.

Complexity of the Extortion Threat

The increased legal risk to businesses of making extortion payments to TCOs is accompanied by an increased risk that such demands will be harder to avoid. In recent years, extortion has become increasingly prevalent in areas where the newly designated cartels operate, with some cartels demanding "protection" fees and charging businesses for *derecho de piso*, "floor rights," effectively granting them permission to operate in cartel-dominated territories.

The nature of organized crime also is shifting as cartels diversify their operations away from a single focus on drug trafficking. They are expanding into other business sectors, taking control of infrastructure, and compelling businesses to purchase illicit goods, such as stolen fuel, or overpriced services, like overpriced internet connections. This evolution makes it harder for businesses to identify and manage potential extortion threats and legal risk. Payments to criminal entities often pass through intermediaries, which obscures their true nature and requires comprehensive monitoring systems to detect.

The lack of transparency into government officials' and even "legitimate" businesses' potential ties with criminal groups, coupled with the increasing sophistication of cartel operations, heighten the vulnerability of companies. Businesses may make illicit payments, risking criminal and civil liability under US law, without knowing which organization ultimately demanded or benefited from the payments.

Mitigating Extortion Risks

Considering the substantial legal, financial, operational, and reputational consequences of extortion, companies must implement strategies to identify, mitigate, and manage extortion risk. A solid compliance program and strong internal controls are critical to preventing and detecting potential violations.

However, these measures must be tailored to address the risk of making illicit payments to entities connected with organized crime. Anti-corruption and anti-money laundering measures, while crucial, may not fully cover the threat of TCO-related extortion. To strengthen their defenses, businesses should consider additional safeguards, including:

Developing Clear Policies and Procedures: Establish policies that provide guidance on how to handle requests for "protection payments" and other extortionate demands. These should include defined escalation protocols, steps for documenting and reporting incidents, and guidance on how to protect the safety of employees while ensuring compliance with legal obligations.

Conducting Comprehensive Risk Assessments: Regularly assess the risk posed

by third parties, including suppliers, contractors, and other partners. The risk assessment should include components aimed at identifying individuals and third parties who may be linked to criminal organizations. These assessments should focus on assessing vendor hiring and monitoring procedures to identify third parties engaged through non-standard procedures.

Enhancing Business Intelligence and Due Diligence: Strengthen due diligence practices for third parties by conducting thorough background checks, particularly in regions in which extortion is prevalent. Businesses should monitor for and follow up on red flags such as unusual payment requests or vendors that offer multiple unrelated services, as well as any changes in ownership, financial stability, or legal standing.

Training Employees on Extortion Risks: Train employees to recognize potential signs of extortion and understand the protocols to follow when faced with such threats. Employees should know how to escalate the matter, protect themselves and the company's interests, and ensure compliance with the law.

Strengthening Supply Chain Controls: Review and assess supply chain vulnerabilities, particularly in transportation and logistics, and implement, as needed, additional measures that reduce the risk of extortion. Ensure that new supply chain partners are thoroughly vetted and monitored for potential ties to criminal organizations.

Conclusion

Extortion's impact on businesses can be profound. It can lead to operational disruptions, legal ramifications, and reputational damage. As the Trump Administration's policy priorities continue to evolve, companies must be vigilant and active in managing the growing threat of organized crime.

By implementing rigorous compliance programs, conducting thorough due diligence exercises, and fostering a culture of transparency, businesses can better protect themselves from extortion threats and navigate the complexities of operating in high-risk environments.

Howard S. Master *is a partner and counsel to the CEO of the investigative firm, Nardello & Co. He is also an adjunct professor at the University of Pennsylvania Carey Law School, where he teaches an advanced seminar on corruption law.* **Alberto Orozco** *is a managing director with Nardello and Co.'s financial investigations & forensic accounting practice. He has led global investigations into financial fraud, bribery, asset misappropriation and vendor fraud, with particular focus on Latin America.*

Reprinted with permission from the March 5, 2025 edition of the NEW YORK LAW JOURNAL © 2025 ALM Global Properties, LLC. All rights reserved. Further duplication without permission is prohibited, contact 877-256-2472 or asset-and-logo-licensing@alm.com. #NYLJ-3062025-61533