Skadden

White Collar Defense and Investigations

March 25, 2025

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

Understanding and Mitigating Legal and Compliance Risks Relating to Cartels and Transnational Criminal Organizations

On his first day in office, President Trump signed Executive Order 14157 calling for the designation of certain cartels and transnational criminal organizations (TCOs) as foreign terrorist organizations (FTOs) or specially designated global terrorists (SDGTs). Then, Attorney General Pamela Bondi issued a memorandum calling for a "fundamental change in mindset and approach" to "pursue *total elimination*" of cartels and TCOs and announcing that Department of Justice (DOJ) resources would shift to these efforts.

The U.S. has now designated eight cartels[1] and TCOs as FTOs and SDGTs. On March 18, 2025, the U.S. Office of Foreign Assets Control (OFAC) issued an alert to raise awareness of these recent terrorist designations and the resulting sanctions and criminal liability risks for U.S. and foreign financial institutions and other entities with exposure to these cartels.

This increased focus and resource allocation by U.S. authorities exposes financial institutions and companies with potential touchpoints to these groups to heightened risk of criminal and civil liability, as well as sanctions violations.

Key Points

- Knowingly conducting or facilitating a transaction on behalf of a designated cartel (including through willful blindness or deliberate indifference) may give rise to criminal liability. This may also result in substantial reputational damage that may prompt financial institutions to engage in de-risking measures.
- Providing support or resources to FTOs, including through extortion or protection payments, may give rise to criminal liability even where there are limited touchpoints to the U.S. Also, terrorism support statutes in the U.S. have broad jurisdictional hooks and extraterritorial application.
- Civil liability may arise under the U.S. Anti-Terrorism Act (ATA) as a result of providing services and support to designated cartels. Lawsuits under the ATA frequently entail expensive and intrusive discovery processes in the U.S. Plaintiffs' attorneys have indicated they expect to dramatically increase ATA lawsuits over the next year following the Trump administration's focus on FTOs.
- OFAC may also use so-called "secondary sanctions" to deter and penalize non-U.S. financial institutions that engage in transactions with cartels.

[1] Tren de Aragua (a group with roots in Venezuela); Mara Salvatrucha, or MS-13 (a gang founded by Salvadoran immigrants in the U.S.); Sinaloa Cartel; Jalisco New Generation Cartel; Northeast Cartel, or Los Zetas; New Michoacán Family; United Cartels; Gulf Cartel.

- Whistleblower reports to U.S. authorities relating to cartels and TCOs may increase, leading to more investigatory and enforcement activity.
- U.S. and foreign companies that are required to file annual and quarterly reports with the U.S. Securities and Exchange Commission — Form 10-K, annual reports on Form 20-F and quarterly reports on Form 10-Q — may be required to report transactions or dealings they or their affiliates have with designated cartels and TCOs. Section 13(r) of the Securities Exchange Act of 1934 requires that reporting companies disclose dealings with parties sanctioned under specific U.S. sanctions authorities, including terrorism. Any contract, transaction or dealing conducted knowingly by the reporting company or an affiliate with a person designated as an SDGT must be reported regardless of transaction value or whether the activity had any U.S. jurisdictional nexus.

Criminal Material Support of Terrorism

U.S. laws criminalize providing (i) "material support or resources" with the knowledge or intent that the support will be used in the preparation for, or for the carrying out of, terrorism or related offenses, and (ii) providing or collecting funds with the intention or knowledge that they will be used to carry out acts of terrorism. U.S. laws also criminalize knowingly providing material support or resources to FTOs.[2]

The terms "material support" and "resources" are broadly defined and may include any kind of financial assistance or services, property (tangible or intangible), lodging (including providing accommodations, safehouses or other facilities), weapons, lethal substances, explosives, personnel (which can include the offender), false identification documents, communications equipment, transportation, and training or expert advice.[3]

The material support statutes have extraterritorial reach and apply to acts that take place outside the U.S. if those acts have even a minimal impact on U.S. interstate or foreign commerce.

A corporate defendant may be fined up to $500,000 per violation or twice the gross pecuniary gain or loss resulting from the offense under "material support" statutes. An individual may be imprisoned up to 20 years (or up to life if the commission of the offense results in death) and/or fined up to $250,000 per violation. Material support prosecutions are subject to an eight-year statute of limitations.

Importantly, extortion, protection or ransom payments may be considered "material support and resources" in certain circumstances. For example, in 2022, the DOJ announced its prosecution of Lafarge, a French cement company, and its Syrian subsidiary, for providing material support to FTOs. Lafarge pleaded guilty to conspiracy to provide material support to FTOs, specifically ISIS and the al-Nusrah Front, by paying regular protection payments in Syria. Jurisdiction was based on a single wire transfer through a U.S. correspondent bank account and the use of U.S. email accounts. Lafarge agreed to pay $778 million in fines and forfeiture.

Civil Claims Under the Anti-Terrorism Act

The ATA provides a civil cause of action to U.S. nationals for death and injuries caused "by reason of an act of international terrorism." Private plaintiffs can bring ATA claims against companies and financial institutions that are alleged to have provided support to terrorist groups.

"Primary liability" applies where a defendant engaged in conduct that "proximately caused" acts of terrorism. "Secondary liability" may apply for aiding and abetting or conspiring with an FTO by knowingly and substantially assisting terrorist activity by the FTO. For example, secondary liability may apply to processing transactions, laundering money intended for terrorists, providing logistical support or expert advice to someone who is providing material support, and other indirect means of support.

The civil ATA provisions impose treble liability for damages, creating a risk of significant monetary damages, and are subject to a 10-year statute of limitations.

Many ATA lawsuits have targeted international banks, financial services firms and corporates for purportedly providing services to terrorist groups, including financial services, communication support, provision of equipment and protection payments. For example:

- U.S. service members and civilians sued Swedish telecommunications company Ericsson in 2022 in connection with deaths, injuries or kidnappings that occurred in terrorist attacks in Iraq, Syria, Turkey and Afghanistan between 2005 and 2021. The plaintiffs alleged that Ericsson violated the ATA through its protection payments to various terrorist organizations.[4]
- In 2021, U.S. service members and their families filed an ATA lawsuit against MTN Group, South Africa's largest telecom company, and Chinese telecoms companies ZTE Corporation and Huawei Technologies, relating to injuries they sustained

[2] It is not necessary that the "material support or resources" be linked directly to any criminal terrorist activity. Prosecutors must only show that the offender knows that the group they were supporting has been designated as an FTO or has engaged in terrorism.

[3] Provision of medicine or religious materials is excluded.

[4] The court has not yet ruled on Ericsson's motion to dismiss.

in a series of terrorist attacks that took place in Iraq and Afghanistan. The plaintiffs alleged that the defendants did business with Iranian entities that served as fronts for the Iranian Islamic Revolutionary Guard Corps.[5]

- Pakistan's largest commercial bank, Habib Bank, faces claims that it allegedly operated as the primary terrorist finance arm of Pakistan's intelligence service, which supported the Taliban, al-Qaeda and Lashkar-e-Taiba. Plaintiffs alleged that Habib Bank knowingly provided accounts and facilitated essential transactions that allowed money movement to terrorists committing attacks on Americans in post-9/11 Afghanistan.[6]
- In 2015 a jury awarded a judgement of $100 million against Arab Bank, stemming from claims that it facilitated Hamas-perpetrated terrorist attacks. The Second Circuit Court of Appeals vacated the judgment based on an error in jury instructions and the parties entered into a confidential settlement.

US Sanctions Considerations

U.S. sanctions impose restrictions and prohibitions on activities that have certain touchpoints with the U.S. (a "U.S. nexus"), such as the involvement of U.S. companies, citizens, permanent residents or the clearing of payments through the U.S. financial system. Among other things, sanctions generally prohibit transacting with persons on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), which includes SDGTs and sanctioned TCOs. The ban extends to providing funds, goods or services to such entities or for their ultimate benefit, as well as receiving any of the same from those entities. The sanctions also apply to any entity owned in the aggregate, directly or indirectly, 50% or more by one or more persons on the SDN List.

Therefore, if there is a U.S. nexus, non-U.S. companies and financial institutions generally risk civil and criminal liability if they deal, directly or indirectly, with such sanctioned parties. In the civil context, sanctions violations are strict liability, meaning that knowledge that an activity is prohibited is not required.

The U.S. government may also implement so-called "secondary sanctions" under certain programs to target non-U.S. persons even where there is not a U.S. nexus. For example, a foreign financial institution can be sanctioned if it knowingly conducts or facilitates a "significant transaction" for anyone blocked as an SDGT. These sanctions can include (i) prohibiting the opening of a correspondent account or payable-through account in the U.S., and (ii) imposing strict conditions on maintaining such accounts. OFAC has a broad interpretation of what constitutes a "significant transaction" and has wide discretion in making this determination.

Individuals or entities can also be added to the SDN List if they are determined "to have materially assisted, sponsored or provided financial, material or technological support for, or goods or services to or in support of," an SDGT or an act of terrorism. OFAC has not clearly defined what "materially assisted" means, giving the U.S. government significant discretion in making these determinations.

Considerations for Commercial Contracts

The U.S. government's designation of cartels as terrorist organizations may also affect commercial contracts with other companies and financial institutions. Commercial contracts and credit agreements will often contain covenants or representations or warranties that require the company to maintain compliance with applicable U.S. laws and regulations. By dealing directly or indirectly with FTOs or SDGTs in violation of U.S. law, particularly the ATA, companies may also find themselves liable to third parties, including to lenders, for breach of contract.

Risk Mitigation

While completely eliminating the risks associated with TCOs and cartels may not be feasible in some markets, it is important to build a pro-compliance record that demonstrates the board and management team took risk-based mitigation measures.

Below are 12 steps companies can take now to help identify and address TCO- and cartel-related risks:

1. **Engage the board and senior management:** Ensure the board and senior management have oversight of the organization's compliance with rules governing anti-money laundering (AML), counterterrorist financing and sanctions. The board should receive periodic updates regarding the risks related to cartels and TCOs, as well as the steps being taken to mitigate potential vulnerabilities. Document board and senior management engagement, and ensure "tone-from-the-top" is communicated across the organization.
2. **Review periodic risk assessment design:** Confirm whether the risk assessment process appropriately accounts for potential exposure to sanctioned persons or entities, including TCOs and SDGTs, in the company's customer base and supply chain, and with respect to intermediaries and other counterparties. The risk assessment should cover the company's varied product and service offerings, and the geographies where the company operates.

[5] The court has allowed the case to proceed on aiding and abetting theories of liability. The court refused attempts by ZTE Corporation and Huawei Technologies to resist service of the complaint, and on March 18, 2025, the parties agreed to a briefing schedule and import of prior orders on motions of the defendants' U.S. subsidiaries.

[6] The court granted Habib Bank's motion to dismiss on primary liability claims, but denied the motion to dismiss as to secondary liability claims.

Understanding and Mitigating Legal and Compliance Risks Relating to Cartels and Transnational Criminal Organizations

3. **Address known compliance gaps:** Confirm whether compliance gaps or risks identified in recent risk assessments or internal audit reports have been appropriately remediated. Ensure policies and procedures relating to AML, sanctions and financial crime risks related to TCOs and cartels are fit for purpose.
4. **Review KYC and due diligence approaches:** Review customer and counterparty onboarding and maintenance processes, including know-your-customer policies and procedures, to ensure they position the company to obtain information sufficient to identify connections between customers or counterparties and TCOs, cartels and other sanctioned persons. Consider supply-chain risks and whether due diligence and third-party policies and procedures are adequately designed to identify and address potential issues.
5. **Identify patterns of suspicious activity:** For banks and others that conduct transaction monitoring, determine whether relevant policies, procedures and monitoring tools are able to adequately detect patterns that may indicate potential drug cartel-related or other drug trafficking activity. Consider enhancements and remediation where there are gaps.
6. **Document, document, document:** Establish robust and transparent documentation, recordkeeping, approval and reporting processes for expenses and transactions with third parties.
7. **Test compliance controls:** Ensure recent and periodic independent testing and auditing of the company's compliance controls, including with respect to high-risk business activities, counterparties or geographies. Ensure proper documentation of audits and reviews.
8. **Conduct periodic employee training:** Training should include AML, sanctions and financial crime risks related to TCOs and cartels using real-world case studies and identification of red flags.
9. **Review recent acquisition targets:** Assess whether acquired entities have been incorporated into the company's risk assessment and compliance framework. Determine whether they may present areas of heightened risk that should be addressed.
10. **Prepare response plans and communication strategies:** These should be designed to address potential reputational risks from inadvertent exposure to cartels and TCOs.
11. **Review whistleblower and internal investigation procedures:** Ensure the organization has clear procedures for responding to whistleblower reports, conducting internal investigations and self-reporting as necessary to relevant authorities or other parties.
12. **Maintain legal privilege:** Be mindful about the applicability, preservation and potential waiver of legal privilege when engaging third-party auditors, consultants or similar service providers in connection with internal reviews or audits.

Contacts

Brooks E. Allen
Partner / Washington, D.C.
202.371.7598
brooks.allen@skadden.com

Alessio Evangelista
Partner / Washington, D.C.
202.371.7170
alessio.evangelista@skadden.com

Eytan J. Fisch
Partner / Washington, D.C.
202.371.7314
eytan.fisch@skadden.com

Raquel Fox
Partner / Washington, D.C.
202.371.7050
raquel.fox@skadden.com

Alejandro Gonzalez Lazzeri
Partner / New York
212.735.3318
alejandro.gonzalez.lazzeri@skadden.com

Ryan D. Junck
Partner / London
44.20.7519.7006
ryan.junck@skadden.com

Timothy G. Nelson
Partner / New York
212.735.2193
timothy.g.nelson@skadden.com

Bora P. Rawcliffe
Counsel / Abu Dhabi
971.50.897.5149
bora.rawcliffe@skadden.com

Ondrej Chvosta
Associate / Washington, D.C.
202.371.7579
ondrej.chvosta@skadden.com

Zaneta Wykowska
Associate / London
44.20.7519.7129
zaneta.wykowska@skadden.com