MAYER|BROWN

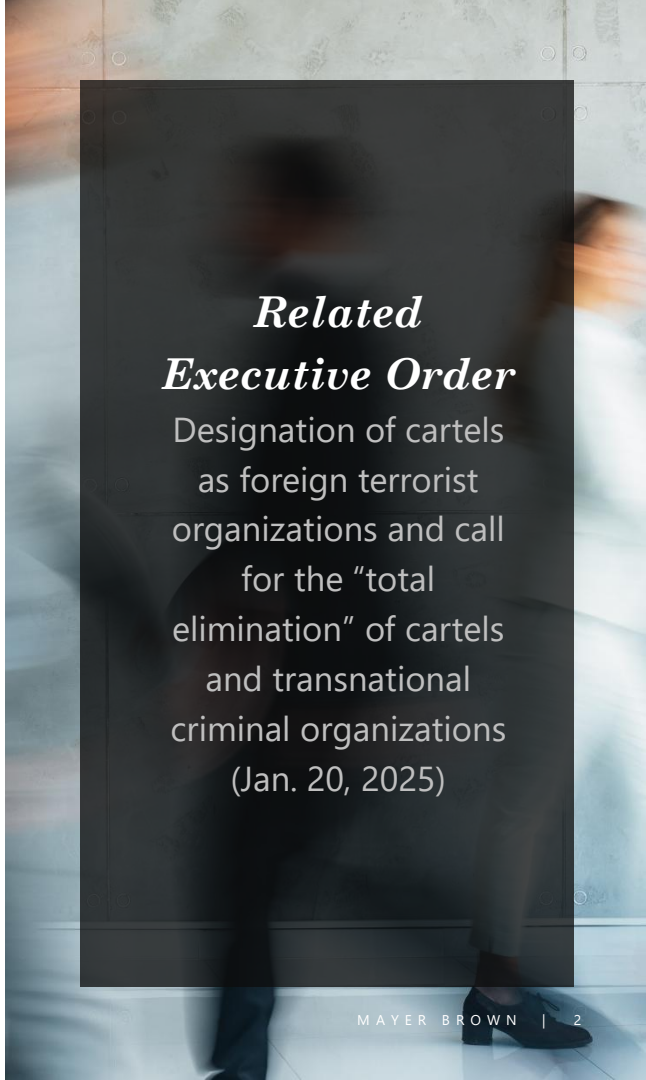
CROSS-BORDER ENFORCEMENT CHALLENGES

2025

CHANGE IN PRIORITIES…

US Enforcement Trends: Priorities Remixed….

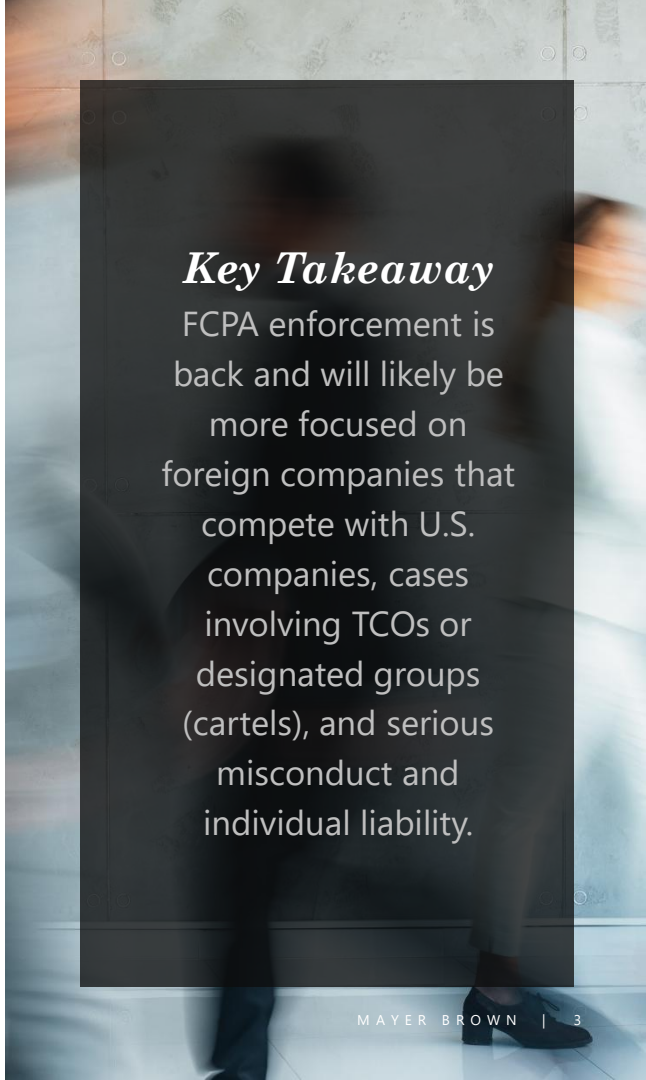
- **Feb. 5, 2025 – AG Memorandum:** FCPA Unit instructed to prioritize investigations related to foreign bribery that facilitates criminal operations of Cartels and Transnational Criminal Organizations (TCOs), and shift focus away from cases without such a connection (e.g., bribery to facilitate human smuggling or trafficking of narcotics and firearms).
- **Feb. 20, 2025 – Executive Order:** DOJ directed to pause new FCPA investigations without AG approval; AG must issue revised guidelines for all ongoing and future enforcement. Justified in part because FCPA enforcement has "prohibited [U.S. companies] from engaging in practices common among international competitors, creating an uneven playing field."
- **May 11, 2025 – Criminal Division Guidance: Prosec**utors directed to focus on "[b]ribery and associated money laundering that impact U.S. national interests, undermine U.S. national security, harm the competitiveness of U.S. businesses, and enrich foreign corrupt officials," as well as "[m]aterial support by corporations to foreign terrorist organizations, including recently designated Cartels and TCOs."



CHANGE IN PRIORITIES…

Exposure Remains (in the US)….

- **June 10, 2025: FCPA Pause Lifted and New Guidelines Issued:** DOJ announced that FCPA investigations and prosecutions will resume. The Guidelines refocus FCPA enforcement by directing prosecutors to investigate misconduct that causes identifiable harm to US interests, to prioritize cases involving individual wrongdoing, and to avoid burdensome investigations into companies without evidence of systemic issues to prevent disruption of lawful business.
- The Guidelines reflect the Administration's view that FCPA investigations and prosecutions should (1) limit "undue burdens on American companies that operate abroad," and (2) target "enforcement actions against conduct that directly undermines US national interests."



Key Takeaway

FCPA enforcement is back and will likely be more focused on foreign companies that compete with U.S. companies, cases involving TCOs or designated groups (cartels), and serious misconduct and individual liability.

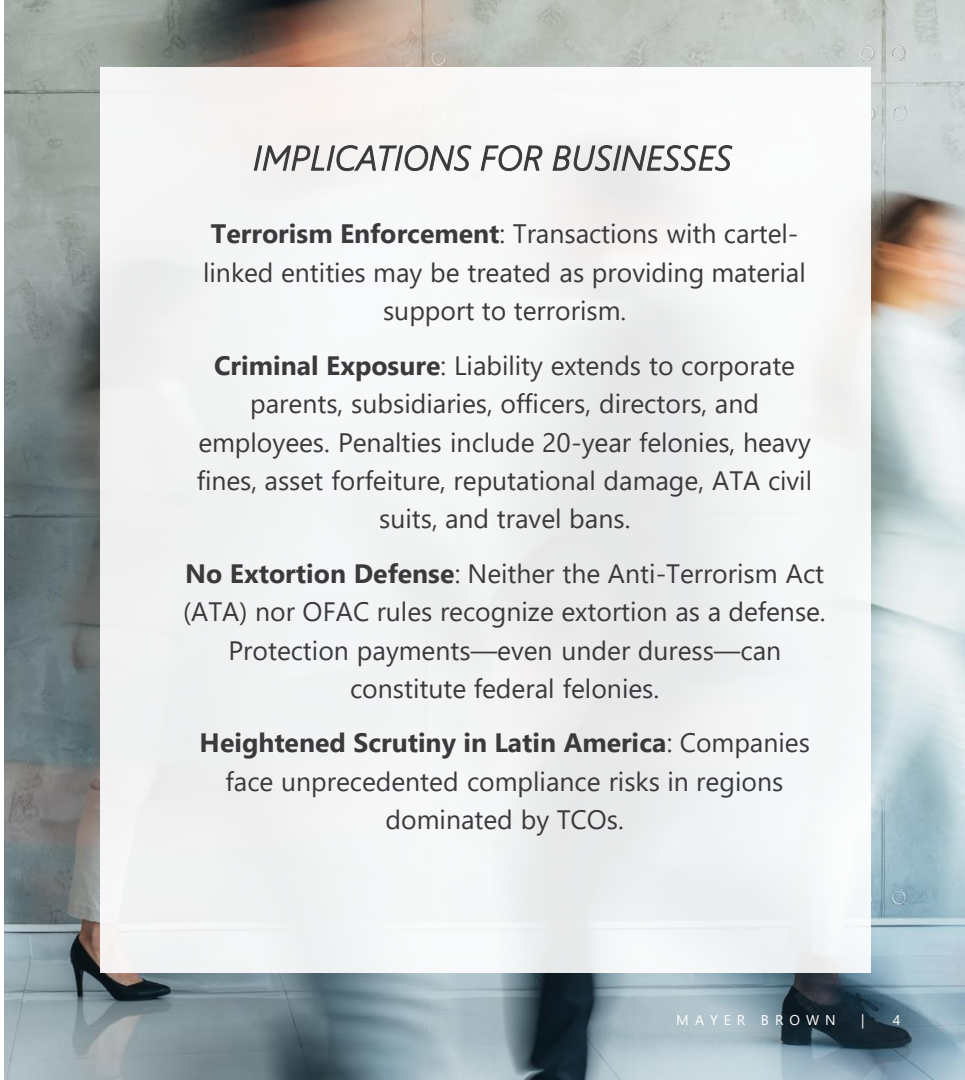
SHIFT TO TARGETING CARTELS AND ORGANIZED CRIME

On **February 20, 2025**, the U.S. State Department designated **eight transnational criminal organizations (TCOs)** as terrorists under the **January 20, 2025 Executive Order**.

Designated Groups:

1. Cártel de Sinaloa (Sinaloa Cartel)
2. Cártel Jalisco Nueva Generación (CJNG)
3. Cártel del Noreste (CDN, formerly Los Zetas)
4. La Nueva Familia Michoacana (LNFM)
5. Cártel del Golfo (Gulf Cartel)
6. Cárteles Unidos (CU)
7. Tren de Aragua (TdA)
8. Mara Salvatrucha (MS-13)

These organizations operate primarily in **Mexico, Central America, and South America**, exerting **quasi-governmental authority** over regions, imposing "taxes," and using violence to enforce compliance.



IMPLICATIONS FOR BUSINESSES

Terrorism Enforcement: Transactions with cartel-linked entities may be treated as providing material support to terrorism.

Criminal Exposure: Liability extends to corporate parents, subsidiaries, officers, directors, and employees. Penalties include 20-year felonies, heavy fines, asset forfeiture, reputational damage, ATA civil suits, and travel bans.

No Extortion Defense: Neither the Anti-Terrorism Act (ATA) nor OFAC rules recognize extortion as a defense. Protection payments—even under duress—can constitute federal felonies.

Heightened Scrutiny in Latin America: Companies face unprecedented compliance risks in regions dominated by TCOs.

SHIFT TO TARGETING CARTELS AND ORGANIZED CRIME

- **Chiquita Brands (2007):** Chiquita Brands admitted to making over 100 payments ($1.7 million) to Colombia's AUC disguised as "security expenses," paid a **US$25 million fine.**
- **Lafarge S.A. (2022):** Lafarge S.A. pleaded guilty to supporting ISIS and al-Nusrah Front through protection payments in Syria, resulting in a **US$778 million penalty**.
- **CJNG Crude Oil Case (2025):** DOJ charged crude oil operators with conspiring to provide material support to a recently designated cartel, CJNG, by smuggling crude oil shipments and directing payments to cartel-linked businesses; the case carries **potential 20-year prison terms, fines, and asset forfeiture.**

Key Takeaways

1

Drug trafficking cases are being transformed into terrorism cases with potential long-tail civil exposure.

2

Liability arises from **providing "any property, tangible or intangible, or service,"** not intent.

3

Even well-resourced multinationals are vulnerable when local managers treat extortion as routine.

What FCPA Enforcement Looks Like on the Ground

- In cartel-dominated areas, business operations intersect with coercive power.
- “Security” or “permit” payments often reflect extortion—but U.S. law sees no distinction.
- With cartels designated as FTOs, intent is irrelevant—even coerced payments may qualify as terrorism support.
- Routine activity in energy, logistics, and manufacturing can trigger FCPA or ATA violations.
- Move from check-the-box compliance to threat-based risk management.
- Integrate HUMINT, OSINT, and community mapping to identify red zones and at-risk intermediaries.

“On the ground, the distinction between corruption and coercion disappears fast. The new enforcement reality criminalizes what used to be called 'the cost of doing business.'”

CRIMINAL DIVISION'S CORPORATE ENFORCEMENT AND VOLUNTARY SELF-DISCLOSURE POLICY (CEP)

- The "CEP" is a set of guidelines issued by the U.S. DOJ to address corporate wrongdoing in federal criminal matters. It explains when and how the DOJ's Criminal Division will reward a company that (1) voluntarily tells prosecutors about its own misconduct, (2) fully cooperates with the government's investigation, and (3) promptly fixes the underlying problems. The policy seeks to make enforcement more transparent, predictable, and fair—thereby encouraging companies to come forward rather than conceal wrongdoing.
- Traditionally, many companies hesitated to alert authorities because doing so seemed to invite costly penalties and prolonged scrutiny. To reverse that instinct, the DOJ crafted the CEP as a concrete incentive structure: if a company meets the policy's standards, prosecutors may decline to bring criminal charges altogether, or—if charges are necessary—substantially reduce fines and oversight requirements.

CRIMINAL DIVISION'S CORPORATE ENFORCEMENT AND VOLUNTARY SELF-DISCLOSURE POLICY (CEP)

To qualify for the policy's primary benefits, a company must satisfy three core criteria:

- **Voluntary self-disclosure:** A company must report the misconduct before the DOJ learns of it, when there is no legal duty to disclose, and within a reasonably prompt time after discovery. The CEP also includes a whistleblower carve-out: if a whistleblower reports first, a company can still qualify if it self-reports within 120 days of the internal report.
- **Full cooperation:** The company must proactively and promptly share all non-privileged facts, identifying individual wrongdoers, preserving and producing relevant documents—including those overseas—and making knowledgeable employees available for interviews, including those located abroad.
- **Timely and appropriate remediation:** The company must conduct a root-cause analysis, strengthen compliance and ethics programs, discipline responsible personnel, implement strict record-retention controls (including on personal or ephemeral messaging platforms), and take steps such as aligning compensation structures (e.g., clawbacks) to discourage misconduct.

CRIMINAL DIVISION'S CORPORATE ENFORCEMENT AND VOLUNTARY SELF-DISCLOSURE POLICY (CEP)

At the heart of the CEP are three resolution "tracks."

- First, a company that satisfies four core factors (voluntary self-disclosure, full cooperation, timely and appropriate remediation, and absence of serious aggravating circumstances) is eligible for a complete declination of prosecution, though it must still pay disgorgement, forfeiture, and restitution to victims.
- Second, a "near-miss" category applies if the company self-reports in good faith but either misses a technical disclosure requirement or faces certain aggravating factors; in those cases, the DOJ will generally offer a non-prosecution agreement lasting fewer than three years, waive the need for an outside compliance monitor, and cut up to 75 percent off the bottom of the U.S. Sentencing Guidelines fine range.
- Third, where a company falls short on one or more key factors, prosecutors retain discretion to impose an appropriate criminal resolution but will ordinarily still consider cooperation and remediation when deciding penalties, typically capping fine reductions at 50 percent, usually applied from the low end of the Sentencing Guidelines range when cooperation and remediation are meaningful

CRIMINAL DIVISION'S CORPORATE ENFORCEMENT AND VOLUNTARY SELF-DISCLOSURE POLICY (CEP)

Key Recent Example: Liberty Mutual Insurance Company (August 2025)

- DOJ **formally declined to prosecute Liberty Mutual Insurance Company** for FCPA violations uncovered at its Indian subsidiary, Liberty General Insurance ("LGI").
- Between 2017 and 2022, LGI employees paid approximately $1.47 million in bribes to officials at six state-owned banks in India to secure referrals of the banks' customers to LGI's insurance products, generating roughly $9.2 million in revenue and $4.7 million in profit.
  - ***The scheme was concealed through false marketing expense classifications and the use of third-party intermediaries.***

DOJ declined prosecution after evaluating the factors set forth in the CEP, including:

- **Timely voluntary self-disclosure** in March 2024;
  - **Full and proactive cooperation,** including the provision of all relevant facts about individual wrongdoers); and
  - **Extensive remediation efforts,** such as removing culpable personnel, performing a root-cause analysis, restructuring compliance functions, and enhancing controls over third-party payments and the use of social media and ephemeral messaging.

EXPOSURE REMAINS (IN THE US)…

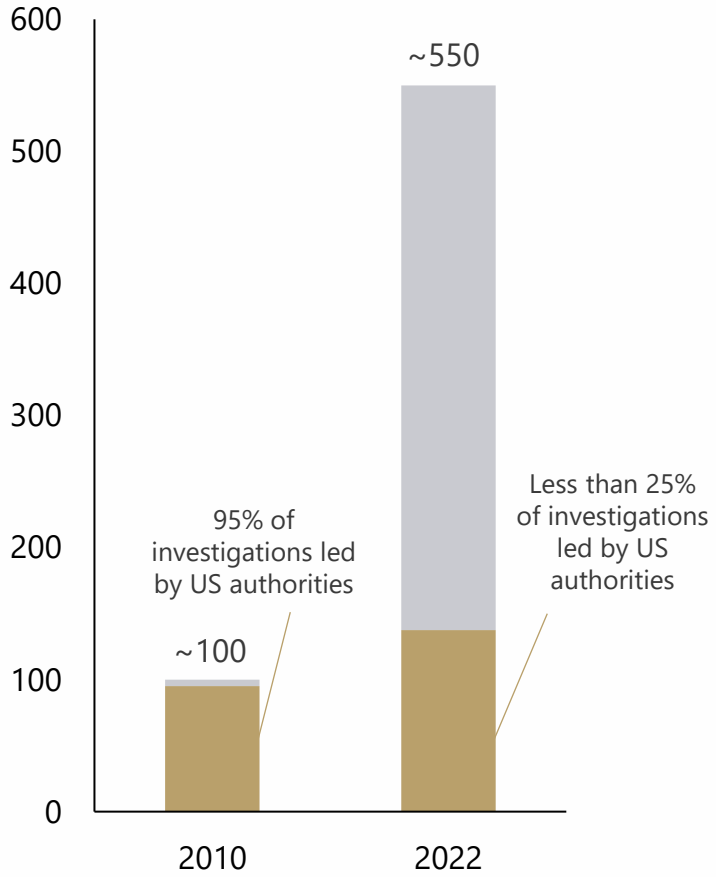
FCPA Risk and Broader Legal Exposure

- **Bribery of officials and commercial bribery** remains illegal under state laws (e.g., TX, CA, NY) and often involves other federal offenses like money laundering, FEPA, wire fraud, and securities fraud.
- **FCPA statute of limitations** is at least five years for bribery, six years for internal accounting violations, and up to eight years when DOJ seeks foreign evidence (which DOJ almost always does)—meaning current conduct may still be prosecuted by a future administration, even considering ramping up time for the DOJ investigation.
- **Enforcement expected to continue,** with a shift toward prioritizing FCPA cases that impact U.S. businesses, and/or harm U.S competitiveness, with an increased focus on foreign companies, as reflected in the new FCPA Guidelines.
- **Civil liability risk remains,** including securities fraud, shareholder derivative actions, and contract-related suits involving anticorruption and bribery representations.

…AND ABROAD…

U.S. enforcement has been less determinative of outcomes in recent years. Instead, **foreign authorities play a greater role in investigations**, and the number of investigations has multiplied for various reasons:

- Unprecedented global **transparency and scrutiny** (3.5BN smartphones in active daily use, global spread of social media)
- Changing economic, social and **political understanding** of the **costs and harms of tolerating bribery** & corruption
- From paper trails to digital footprints: new technologies and **increased cooperation of national authorities** driving new investigative techniques
- **Investigations are politically popular and self-funding** from fines



WHY ABC SHOULD STILL BE TOP OF MIND

WHY CARE ABOUT ANTIBRIBERY & CORRUPTION (ABC) GOVERNANCE?

Legal and Regulatory Compliance Risk

Corruption violations can result in severe penalties under the FCPA, UK Bribery Act and similar global anti-corruption statutes

Board members and senior officers can be held personally liable for oversight failures

Reputational Risk Management

The perception of corruption can damage a company's public image, erode trust among customers, investors, and partners, and lead to lost business opportunities

Institutional investors increasingly demand strong anticorruption measures as part of ethical governance and responsible corporate behavior

Sustainable Business Growth

Strong ABC practices create a culture of integrity that builds trust for enduring business relationships and market access

A strong compliance culture boosts employee morale and retention

MANAGING THIRD-PARTY RISK ANALYSIS

Keep in mind, the FCPA expressly prohibits corrupt payments made through third parties or intermediaries

You can't do indirectly (i.e., via a third party) what would be impermissible to do directly.

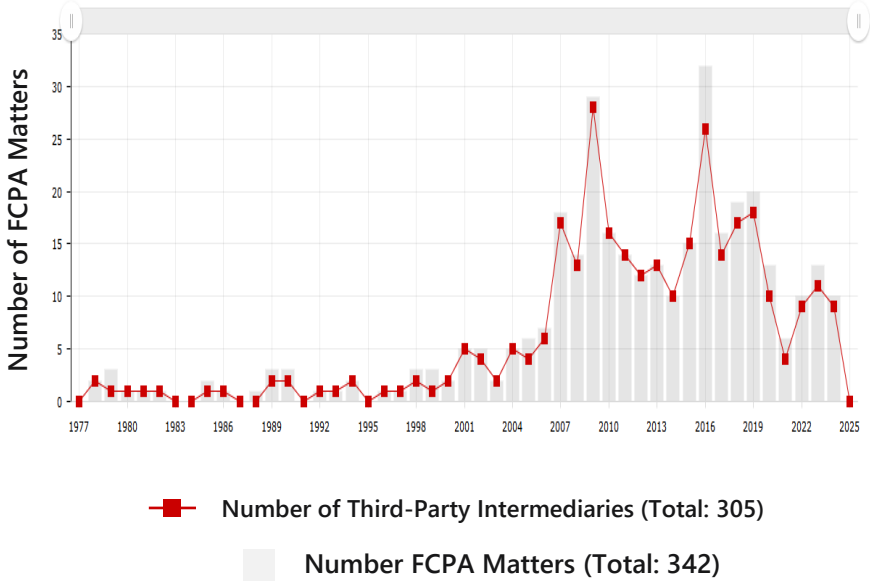
Use of third-party intermediaries poses some of the greatest corruption risks for U.S. companies doing business abroad

The vast majority of FCPA enforcement cases involve the use and activities of third parties.

Historical ties between the police and military and the cartels also raises sanctions risks.

Nearly 90% of all enforcement actions involved third-party intermediaries.

Third-Party Intermediaries Disclosed in FCPA-Related Enforcement Actions



Intelligence-Driven Compliance

- DOJ's 2025 directives merge financial crime with national security — compliance must be predictive.
- Private intelligence can bridge the gap between field risk and legal exposure.
- Conduct link analysis between suppliers, intermediaries, and designated entities.
- Map local power structures—who controls territory, ports, and logistics corridors.
- Monitor social and media signals for cartel encroachment or corruption.
- Framework: Know the Ground, Know Your Intermediaries, Know Your Signals.

"Lawyers look at exposure in hindsight. Intelligence exists to prevent the headline."

MANAGING THIRD-PARTY RISK: COMMON ISSUES

Types of third parties that pose higher ABC, sanctions and export controls risk to Huntsman

Local Agents, Intermediaries and Distributors

- Risk of bribery to secure licenses, permits, or favorable treatment. Red flags include lack of transparency, excessive commissions, or political connections.
- Sanctions and export control-risks result from lack of visibility into end users and other counterparties of the intermediaries since liability applies for both, direct and indirect dealings on a strict liability basis

Logistics, Customs Brokers, Freight Forwarders

- Risk of bribes to expedite the movement of equipment, raw materials or exports across borders. Red flags include frequent cash payments, undocumented fees or extensive operations in high-risk countries.
- Reliance on these parties does not constitute a defense from sanctions and export controls perspective, and their activities in connection with your exports may create exposure (e.g., reporting violations, shipping product in sanctioned vessels)

Security Providers

- Risk of bribes or improper payments to police, military or private security firms. Red flags include lack of licensing, aggressive tactics, or ties to political or criminal organizations. As noted previously, this also raises sanctions risks.

Community liaison officers or local NGOs

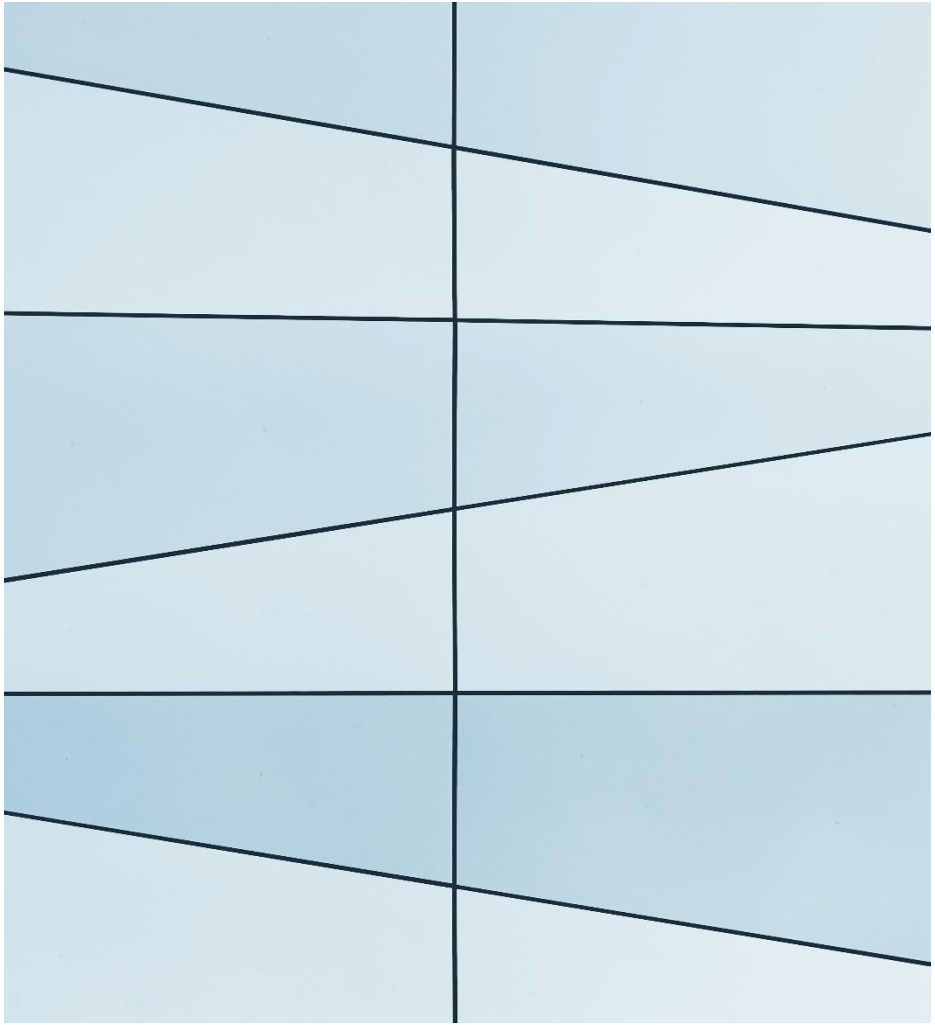
- Risk of payments intended for community development can be misused or redirected as bribes. Red flags include weak governance structures or lack of financial transparency.

Consultants and lobbyists

- Risk that they may improperly influence officials or gain preferential treatment under the guise of advisory services. Red flags include no clear deliverables, vague scopes of work, or success-based fees.

ANTI-TERRORISM ACT (ATA) – CIVIL LIABILITY PROVISIONS

- 18 U.S.C. § 2331, et seq.
  - U.S. national injured "by reason of an act of international terrorism" may bring civil claim against the perpetrator of that act
- Justice Against Sponsors of Terrorism Act (JASTA)
  - In 2016, Congress amended the ATA through JASTA to provide for secondary liability claims for: (i) conspiracy and (ii) aiding-and-abetting



FTO DESIGNATIONS AND JASTA CLAIMS

- JASTA claims available only for injuries arising from acts of international terrorism committed, planned, or authorized by a designated FTO, **as of the date** on which the act was committed, planned, or authorized
- Act of International Terrorism must:

1. involve violent acts or acts dangerous to human life; and
2. appear to be intended to intimidate a civilian population, influence government policy, or affect the conduct of government by certain specified means. 18 U.S.C. § 2331(1)


Q&A

DISCLAIMER

These materials are provided by Mayer Brown and reflect information as of the date of presentation.

The contents are intended to provide a general guide to the subject matter only and should not be treated as a substitute for specific advice concerning individual situations.

MAYER | BROWN