MAYER|BROWN

# FINANCIAL INSTITUTIONS AND CARTEL "TERRORISTS": CRIMINAL, REGULATORY AND CIVIL LITIGATION RISKS POSED BY EXPANDING FTO DESIGNATIONS

Legal Framework, Enforcement Trends, Corporate Risk Exposure, and Compliance



# AGENDA

1. Introduction (Policy Shift)
2. Enforcement Trends
3. Criminal Liability
4. Civil Liability
5. FCPA
6. Financial Enforcement
7. Compliance & Risk Mitigation



# 01

## INTRODUCTION

# CARTELS, TCOS, AND FTOS

## KEY TERMINOLOGY

### CARTELS

+ Organized criminal groups primarily engaged in drug trafficking and related crimes. Many function as quasi-governmental actors, exerting territorial control, imposing taxes, and using violence to enforce compliance—making them increasingly comparable to insurgent or terrorist organizations.

### TRANSNATIONAL CRIMINAL ORGANIZATIONS (TCOS)

+ Sophisticated networks operating across borders that engage in a wide range of illicit activities beyond drugs, including financial crimes, money laundering, human trafficking, or sanctions evasion.

### FOREIGN TERRORIST ORGANIZATIONS (FTOS)

+ Groups formally designated under US law. Any material support—financial, logistical, or otherwise—triggers severe criminal and civil consequences, including asset freezes.





CONFIDENTIAL

# US POLICY SHIFT: CARTELS & FTOS A NATIONAL SECURITY THREAT

## Evolution from Criminal Enterprises to National Security Threats

- Historically, cartels were treated primarily as profit-driven narcotics trafficking organizations, addressed through traditional criminal-law enforcement.
- In early 2025, executive orders directed agencies to designate cartels as Foreign Terrorist Organizations (FTOs) and dismantle them using counterterrorism mechanisms.
- As a result, enforcement has shifted from a purely criminal framework to a national-security paradigm, expanding enforcement tools and potential exposure for companies, individuals, and financial institutions.

CARTELS ARE NO LONGER JUST A LAWENFORCEMENT ISSUE — THEY ARE NOW A **CORE COMPLIANCE RISK.**



CONFIDENTIAL

# WHITE COLLAR ENFORCEMENT PRIORITIES

- **February 5, 2025**
  - US Attorney General memorandum: "**Total Elimination of Cartels and Transnational Criminal Organizations**"
  - Prioritizes cases involving **foreign bribery tied to Cartels and Transnational Criminal Organizations (TCOs)**
- **May 11, 2025**
  - DOJ's memorandum: "**Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime**"
  - Identifies **10 high-impact enforcement priorities**, including treatment of cartels and TCOs as national-security threats, not just as criminal-law issues
    - Target conduct threatening US national security, including:
      - Risks to the US financial system, such as financial institutions and their insiders that commit sanctions violations or enable transactions by drug cartels, TCOs, hostile nation-states, or FTOs
    - Material support by corporations to FTOs
- **June 10, 2025**
  - **FCPA enforcement pause lifted** and new DOJ guidelines issued
  - Prioritize misconduct causing identifiable harm to US interests and cases involving individual wrongdoing
  - Avoid burdensome investigations of companies absent evidence of systemic compliance failures
  - Limit undue burdens on US companies operating abroad
  - Focus on foreign companies that compete with US companies, and on cases involving TCOs or cartels

**December 4, 2025 ACI's 42nd Annual Conference on FCPA and Global Anti-Corruption**

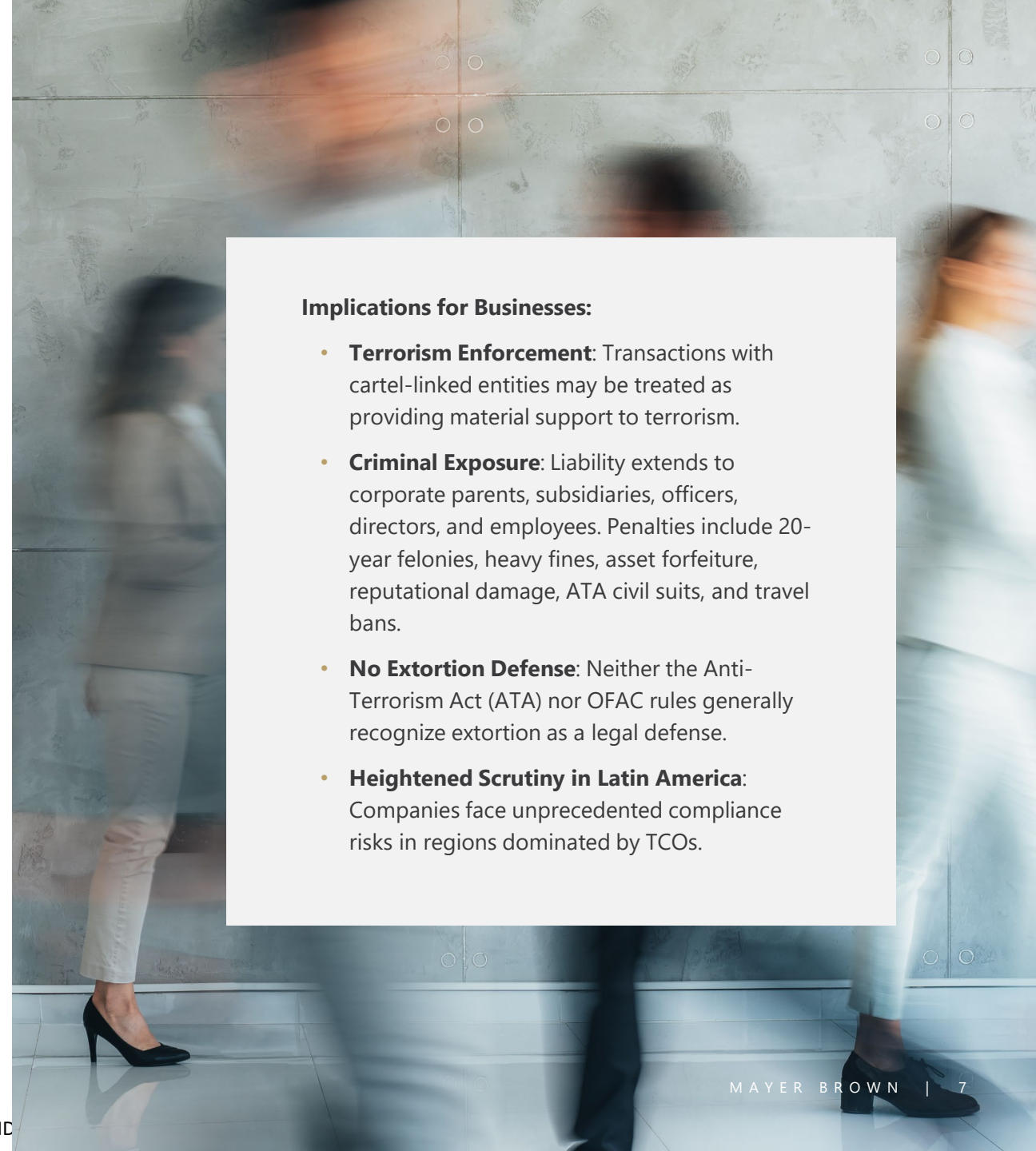
- Todd Blanche (Deputy Attorney General) insisted DOJ is pursuing such cases with "*precision and vigor*."
- Matt Galeotti (DOJ, Head of the Criminal Division) highlighted a return to a "*traditional cadence*" of enforcement, urging companies to invest in compliance and voluntary self-disclosure



CONFIDENTIAL

# EXPANSION OF FTO DESIGNATIONS TO LATIN AMERICAN CARTELS

- **February 20, 2025:** The Trump Administration designated **eight Latin American cartels and criminal organizations as FTOs** under Executive Order 14157. The initial designations include:
  - Six Mexican cartels—Cártel de Sinaloa, Cártel Jalisco Nueva Generación (CJNG), Cártel del Noreste (CDN, formerly Los Zetas), La Nueva Familia Michoacana (LNFM), Cártel del Golfo (CDG), and Cárteles Unidos (CU).
  - Two regional organizations—Venezuela's Tren de Aragua (TdA) and El Salvador's Mara Salvatrucha (MS-13)
- **Subsequent Designations (Post-February 2025):** Seven additional organizations have since been designated:
  - **Haiti**: Viv Ansanm; Gran Grif; **Ecuador**: Los Choneros; Los Lobos; **El Salvador**: Barrio 18; **Venezuela**: Cartel de los Soles; **Colombia**: Clan del Golfo
  - These actions bring the total number of Latin America–linked FTOs to **nineteen**
- **Pre-2025 Designations**
  - **Colombia**: National Liberation Army (ELN); Segunda Marquetalia; Revolutionary Armed Forces of Colombia – People's Army (FARC-EP); **Peru**: Shining Path (Sendero Luminoso, SL)
- **2026 Designation**
  - **Brazil**: Primeiro Comando da Capital (PCC) and Comando Vermelho (CV)
  - Designations significantly expand FTO-related compliance exposure for companies operating in or dealing with Brazil



**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 generally recognize extortion as a legal defense.
- **Heightened Scrutiny in Latin America**: Companies face unprecedented compliance risks in regions dominated by TCOs.



CONFID

# GEOGRAPHIC EXPOSURE TO FTO DESIGNATIONS AND US ENFORCEMENT

| Country | FTO Designations | US Cooperation | Status |
|---|---|---|---|
| **Argentina** | Argentina designated foreign groups: CJNG (Mexico); Los Choneros (Ecuador); Los Lobos (Ecuador) | High | Aligned with US |
| **Bolivia** | Supportive of designations | Moderate | Partial alignment |
| **Brazil** | Resists FTO label for PCC/CV | Limited; Sovereignty concerns | Dissenter |
| **Colombia** | Segunda Marquetalia; ELN; FARC-EP; Clan del Golfo | Moderate<br><br>(President under investigation) | High tension |
| **Ecuador** | Los Choneros; Los Lobos | Very High (joint operations) | Strongly aligned |
| **El Salvador** | MS-13; Barrio 18 | Selective cooperation driven by sovereignty concerns | Broadly aligned on goals |
| **Haiti** | Viv Ansanm; Gran Gri | High (MSS mission) | Ongoing crisis |
| **Mexico** | Cártel de Sinaloa; CJNG; CDN; LNFM; Gulf Cartel; Cárteles Unidos | Mixed (sovereignty disputes) | Central risk |
| **Paraguay** | Paraguay designated foreign groups: PCC and CV (both from Brazil) | Very High (SOFA signed) | Strongly aligned |
| **Peru** | Sendero Luminoso | High | Aligned |
| **Venezuela** | Tren de Aragua;  Cartel de los Soles | Adversarial | Sanctions exposure |



CONFIDENTIAL

# RISK IMPLICATIONS FOR COMPANIES

- **Compliance and legal exposure:** increased risk of inadvertent dealings with designated or soon-to-be-designated entities
- **Heightened scrutiny** under FTO, sanctions, AML, and material-support frameworks
- **Operational and personnel risk:** proximity to military or enforcement activity elevates risks to employee safety and physical assets
- **Commercial and contractual risk:** supply-chain disruption, contract nonperformance, and higher likelihood of **force majeure** claims
- **Strategic and reputational risk:** elevated expectations from regulators, counterparties, and shareholders regarding due diligence, monitoring, and risk mitigation

# EXPANDING SECURITY AND ENFORCEMENT ACTIONS IN LATIN AMERICA

- **Legal enforcement is unfolding alongside a broader regional security strategy**
  - The US and its partners are increasingly pairing criminal prosecutions with multinational military cooperation and intelligence-sharing to disrupt cartel and TCO operations
- **Escalating Multinational Military Cooperation**
  - Joint military and intelligence actions now directly target cartel infrastructure across multiple countries
  - March 2026 commitments by 18 nations at US Southern Command (SOUTHCOM) signal sustained regional coordination and escalation
  - US-supported military strikes have begun expanding beyond border areas, with plans covering nearly 20 Latin American and Caribbean countries
- **High-level corruption prosecutions involving elected officials**
  - US prosecutors are actively pursuing cases involving sitting governors, legislators, and senior officials alleged to have protected cartel leadership. These cases demonstrate that systemic government corruption is now a central enforcement focus, increasing counterparty and sovereign-risk concerns



CONFIDENTIAL



# 02

## ENFORCEMENT TRENDS

# ENFORCEMENT TRENDS AFFECTING FINANCIAL INSTITUTIONS

**NATIONAL-SECURITY-DRIVEN ENFORCEMENT**

- Regulators are increasingly reliant on **counterterrorism, sanctions, and national-security authorities**, rather than traditional criminal or anti-bribery frameworks. This enables:
  - Lower evidentiary thresholds
  - Broader theories of liability
  - Faster and more disruptive enforcement actions (asset freezes, blocked transactions)

**FOCUS ON "FACILITATION" RATHER THAN INTENT**

- Enforcement no longer centers on whether companies *intended* to support criminal or terrorist activity. Instead, authorities focus on whether:
  - Company payments, access, logistics, or services **enabled or benefited** cartel-controlled networks
  - Risk indicators were present but **not adequately escalated or mitigated**





CONFIDENTIAL

# WHERE AND HOW ENFORCEMENT IS TARGETING COMPANIES

**HEIGHTENED SCRUTINY OF THIRD-PARTY ECOSYSTEMS**

Investigations increasingly examine:

- Contractors, security vendors, transport providers, port operators, customs brokers
- Joint-venture partners and state-owned entities
- Government-facing intermediaries

Failure to detect indirect ties to designated or emerging FTOs is now a **primary enforcement vulnerability.**

**MULTI-AGENCY, PARALLEL ENFORCEMENT**

- Enforcement actions increasingly involve **multiple US agencies simultaneously,** combining:
  - Criminal prosecution
  - Sanctions enforcement
  - AML and financial-crime actions
  - Civil penalties and forfeiture

**GEOGRAPHIC EXPOSURE IS BECOMING A RISK FACTOR**

- Authorities are prioritizing cases involving operations in cartel-influenced regions
- Enforcement actions increasingly evaluate awareness of cartel-related exposure

*Failures are framed not just as compliance gaps, but as national security risk management failures.*



CONFIDENTIAL



# 03

## CRIMINAL LIABILITY

*Holder* confirms that once cartels are designated as FTOs, ordinary commercial activity—if coordinated with or benefiting those groups—can create criminal exposure under US terrorism-support laws, regardless of intent.

# BROAD INTERPRETATION OF "MATERIAL SUPPORT"

## STATUTORY FOUNDATION

- **18 C. § 2339B(a)(1)** makes it a federal crime to **knowingly provide material support or resources** to a designated **FTO**.
- Under **18 C. § 2339A(b)(1)**, "material support or resources" is defined **expansively** to include **any property or service**, tangible or intangible—including currency, financial services, facilities, transportation, and personnel (with narrow exceptions for medicine and religious materials)

## SUPREME COURT INTERPRETATION

- In **Holder v. Humanitarian Law Project**, 561 US 1 (2010), the Supreme Court held that:
  - Even **peaceful, benign, or humanitarian support** may qualify as prohibited material support
  - Liability attaches where support is **coordinated with**, provided **at the direction of**, or **in service of** an FTO
  - Congress intentionally crafted the statute to be **preventive**, addressing support that could legitimize or strengthen terrorist organizations

## KEY LEGAL PRINCIPLES FROM HOLDER

- **No requirement of violent intent** or endorsement of terrorism
- **Services and expertise**—not just money or weapons—can trigger liability
- **No de minimis exception**: small or routine assistance can still qualify
- The statute reaches **conduct that would otherwise be lawful commercial activity**



CONFIDENTIAL

# CORPORATE LIABILITY UNDER ANTI-TERRORISM LAWS

**United States v. Lafarge S.A. (2022) & France v. Lafarge (2026)**

- **US Enforcement Action (Material Support to FTOs)**
  - In **2022**, the US Department of Justice charged **Lafarge S.A.**, a multinational cement company, and its Syrian subsidiary with **conspiracy to provide material support to Foreign Terrorist Organizations**, specifically **ISIS** and the **al-Nusrah Front (ANF)**, in violation of **18 C. § 2339B**
  - From 2013–2014, Lafarge admitted that it made payments to ISIS and ANF to:
    - Move employees, raw materials, and finished products through checkpoints, and
    - Continue operating and protecting its cement plant in **northern Syria**
  - The payments were framed internally as operational necessities but were also intended to **preserve Lafarge's market position and disadvantage competitors**
  - DOJ asserted US jurisdiction because at least one related wire transfer passed through the US financial system (a New York bank), causing part of the offense to occur in the United States
  - Lafarge pleaded guilty and agreed to pay approximately **$777.8 million** in fines and forfeiture
  - DOJ did not, at that time, charge individual executives in the US case
- **Compliance significance:**
  - This case confirms that **operational payments made to sustain business activity can constitute criminal material support**, even absent ideological intent



CONFIDENTIAL

# ENERGY SUPPLY CHAINS AS TERRORISM-FINANCING INFRASTRUCTURE

**USA v. Jensen et al. (S.D. Tex. 2025)**

- Operators of a Texas-based crude oil terminal charged with:
  - **Conspiracy to provide material support to CJNG**
  - Money laundering
  - Oil smuggling and customs fraud
- Alleged scheme involved ~2,881 fraudulent oil shipments and payments to
- cartel-linked businesses
- DOJ pursuing **$300 million forfeiture**
- Exposure: **Up to 20 years per count**

*DOJ now treats **oil trading, storage, transport, and terminal operations** as potential terrorism-support mechanisms when they intersect with cartel-controlled commerce.*

# PRECURSOR CHEMICALS & INDUSTRIAL INPUTS

**USA v. Shandong Believe Chemical Company Pte Ltd. et al. (S.D. Ohio 2026)**

- A federal grand jury in the Southern District of Ohio indicted:
  - Two Chinese pharmaceutical / chemical companies
    - *Shandong Believe Chemical Company Pte. Ltd.*
    - *Shandong Ranhang Biotechnology Co. Ltd.*
  - Six Chinese nationals, including senior executives and sales intermediaries
- Chemical manufacturers charged with:
  - Narcotics conspiracy
  - Money laundering
  - **Attempted material support to the Gulf Cartel**
- Conduct involved sale of chemical precursors used to increase fentanyl yield
- Exposure includes life imprisonment (narcotics counts)

*The sale of dual-use or industrial chemicals, even through ordinary commercial channels, can trigger terrorism and narcotics liability if linked to cartel use.*



CONFIDENTIAL

# "SECURITY" AND "ACCESS" PAYMENTS ARE NOT A DEFENSE

**United States v. Chiquita Brands International, Inc.** ***(D.D.C. 2007)***

- DOJ prosecuted **Chiquita Brands International** for **criminal sanctions violations** arising from payments made to the **United Self-Defense Forces of Colombia (AUC)**
- Between 1997 and 2004, Chiquita made dozens of payments totaling approximately $1.7 million, characterizing them as payments for "security" and protection
- The payments were intended to ensure that the AUC did not harm Chiquita's personnel, facilities, or operations
- DOJ **rejected Chiquita's duress and necessity defenses**, emphasizing the repeated and sustained nature of the payments
- Chiquita **pleaded guilty** to criminal charges
- The company agreed to pay a **$25 million criminal fine**
- Unlike Lafarge, DOJ **did not charge Chiquita under the material-support statute (18 C. § 2339B)**; the case proceeded solely under **sanctions authorities**

Payments made to protect personnel, facilities, pipelines, terminals, or logistics routes can constitute criminal sanctions violations when the recipient is a designated group.

Coercion, security necessity, and employee-safety justifications do not excuse liability when payments are sustained or knowingly made.

Disclosure to authorities does not immunize continued misconduct.

Chiquita, together with Lafarge, demonstrates that:

- *Ordinary operational payments in high-risk regions can create national-security criminal exposure*
- *Enforcement theories can shift from sanctions law to terrorism statutes as designation frameworks evolve*

CONFIDENTIAL



# 04

## CIVIL LIABILITY

# CIVIL LIABILITY UNDER US ANTI-TERRORISM LAWS

- **Anti-Terrorism Act (ATA)** — *18 U.S.C. § 2333(a)*
  - Allows US nationals injured by an act of international terrorism to bring civil lawsuits in federal court and recover treble damages
  - The statute defines "international terrorism" in 18 U.S.C. § 2331(1) as violent or dangerous acts that violate criminal-law, appear intended to intimidate or coerce civilians or to influence government conduct
- **Justice Against Sponsors of Terrorism Act (JASTA)** — *18 U.S.C. § 2333(d)*
  - The Justice Against Sponsors of Terrorism Act (JASTA) expanded the civil cause of action under the Anti-Terrorism Act (ATA)
  - JASTA imposes civil liability on any person or entity that: **Aids and abets**, by *knowingly providing substantial assistance*, or **Conspires with** a person who commits an act of international terrorism
  - JASTA secondary liability claims available only for attacks committed, planned or authorized by a designated Foreign Terrorist Organization

Direct commercial dealings, operational support, payments, logistics, or services tied to terrorist-designated groups may trigger civil liability.

Companies may face treble damages, extensive discovery, and reputational harm even without criminal prosecution.

JASTA creates significant civil exposure where a company knowingly and substantially assists terrorist-linked activity—particularly through direct commercial or operational involvement, not merely passive association.



CONFIDENTIAL

# CIVIL LIABILITY UNDER US ANTI-TERRORISM LAWS

- **Aiding and abetting liability standard:**
  - (1) the primary actor must perform a wrongful act that causes an injury, (2) the defendant must be **generally aware** of its role as part of an overall illegal or tortious activity at the time that it provides assistance, and (3) the defendant must **knowingly and substantially assist** the principal violation.
- In ***Twitter, Inc. v. Taamneh*** **(2023),** the Supreme Court confirmed that:
  - Claim requires plausible allegations that defendant "consciously, voluntarily, and culpably participated" in the terrorist attack at issue
  - Tandem showing of mental state and substantiality
  - Concrete nexus between defendant conduct and terrorist attack, or assistance that is so "pervasive and systemic" as to create liability for all attacks.



CONFIDENTIAL



# FEATURES OF ATA CONSPIRACY AND AIDING-AND-ABETTING CLAIMS

- **Legitimate businesses targeted**
  - US and non-US financial institutions, cryptocurrency platforms, telecommunications companies, pharmaceutical manufacturers / distributors, construction companies, cybersecurity firms, social media companies
- **Reputational risk substantial**
  - Consumers, shareholders, counterparties, regulators
- **Regulatory/enforcement actions provide backdrop for follow-on civil claims**
  - Sanctions violations equated to liability for acts of terrorism
- **Aggressive, creative plaintiffs' bar**
  - Consistently pursuing new theories, factual settings



CONFIDENTIAL



# TERROR-RELATED LITIGATION TRENDS

- **Direct customer or counterparty relationships targeted**
  - Post-*Twitter*, claims predicated on attenuated, intermediated relationships to terrorist actors have been found insufficient. *See, e.g.*, *Freeman v. HSBC*, *Ashley v. Deutsche Bank*
  - Plaintiffs thus seek to plead direct relationships with bad actors. *See, e.g.*, *Atchley v. AstraZeneca*, *Zobay v. MTN Group*
  - Allegations can support liability even absent designation or sanction violation
- **"Special Treatment" or "Unusual Services"**
  - Plaintiffs point to tailored services to allegedly terror-aligned customers to suggest scienter
- **Cartels and TCOs provide new landscape for ATA claims**
  - Any act of international terrorism committed, planned, or authorized by FTO-designated cartels or TCOs after February 20, 2025, that injures a U.S. national could give rise to JASTA claims
  - Allegations of services to individuals or entities associated with the cartels or TCOs could give rise to JASTA claims.
  - *Zapata* case illustrates risk
- **Non-ATA claims**
  - Common law claims / foreign law claims. *See, e.g., Kashef v. BNP Paribas*



CONFIDENTIAL



# 05

## FCPA

# FCPA AS A NATIONAL-SECURITY TOOL

- DOJ has explicitly stated that **foreign bribery tied to cartels and TCOs** is a **priority enforcement area**
- FCPA enforcement increasingly overlaps with:
  - Cartel activity
  - Sanctions violations
  - Money laundering
  - Material-support theories



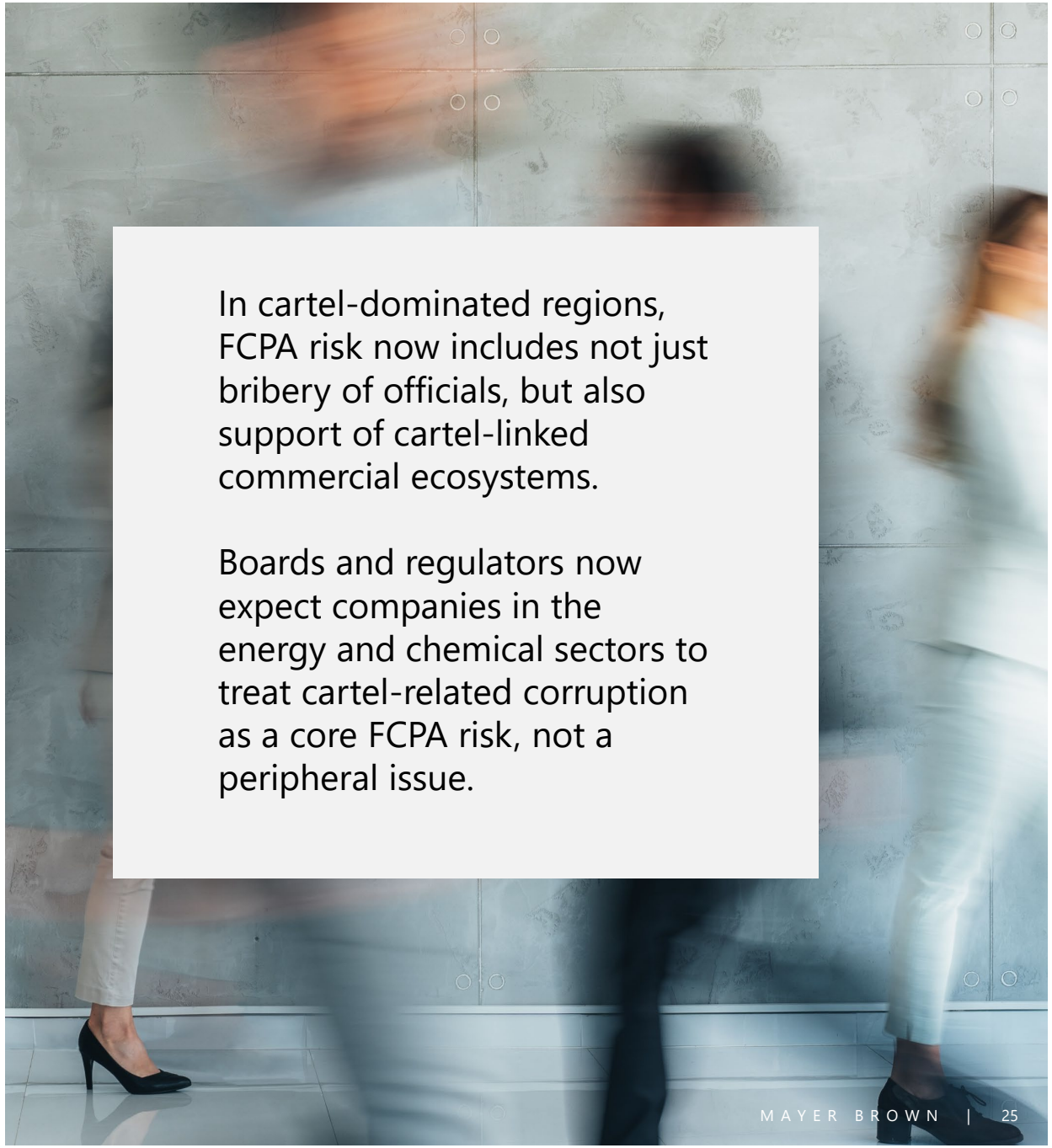
Cartel-related corruption is no longer "*ordinary bribery*" — it is treated as conduct that can undermine US -security, triggering heightened DOJ scrutiny.



CONFID

# CARTEL INFLUENCE EXPANDS FCPA RISK BEYOND TRADITIONAL BRIBERY

- Cartel presence increases FCPA risk when:
  - Officials are **corrupted** by cartels
  - Payments are made to:
    - Secure permits or licenses
    - Expedite customs or border clearance
    - Maintain access to ports, terminals, pipelines, or refineries
  - Third-party intermediaries:
    - Pay bribes on behalf of companies
    - Funnel payments through cartel-controlled entities
  - Bribes are **financed with or tied to cartel proceeds**






CONFIDENTIAL

# FCPA ENFORCEMENT WHERE CARTEL PROCEEDS FUND BRIBERY SCHEMES

- **USA v. Comunicaciones Celulares S.A., d/b/a TIGO Guatemala, (S.D. Florida, 2025)**
  - DOJ found that some bribe payments were financed with laundered narcotrafficking proceeds, linking corruption to organized-crime money flows.
  - Resolution included: $60 million criminal penalty
  - $58.2 million administrative forfeiture
  - Total financial impact exceeding $118 million
- DOJ's focus on:
  - Corruption intertwined with organized crime
  - Failures at subsidiaries in high-risk jurisdictions
  - Governance breakdowns that delay or undermine internal investigations
- Reinforces that FCPA exposure can escalate quickly where corruption and criminal financing intersect

Cartel or narcotrafficking proceeds flowing through a business—even indirectly—can convert ordinary bribery into a higher-risk national-security enforcement issue.



# 06

## FINANCIAL ENFORCEMENT



# MONEY LAUNDERING RISK: CENTRAL TO CARTEL & FTO EXPOSURE

**How Cartels Use Financial Systems**

Cartels and TCOs rely on complex laundering schemes to:

- Move proceeds from **drug trafficking, fuel theft, and fraud**
- Fund operations through:
    - **Shell companies**
    - **False invoicing and trade-based money laundering**
    - Cash-intensive intermediaries and MSBs

**Enforcement Is Increasing**

- DOJ, FinCEN, and Treasury are prioritizing:
    - **Cartel-linked money laundering**
    - Financial flows enabling **drug production and trafficking**
- Enforcement includes:
    - Parallel **AML, sanctions, and FCPA investigations**
    - Increased review of **Suspicious Activity Reports (SARs)** involving companies



CONFIDENTIAL

- Treasury and FinCEN enforcement is now a primary mechanism for disrupting cartel-linked activity—and companies are often the first collateral impact.
- Financial enforcement has significantly intensified, with FinCEN and the US Treasury targeting:
  - Institutions
  - Transaction flows
  - Financial networks linked to cartel activity

# FINANCIAL ENFORCEMENT INTENSIFIED

- US policy increasingly relies on **financial-system controls**, not just prosecutions, to disrupt cartels and FTOs
- Tools include:
  - **OFAC sanctions (SDGT / FTO-linked)**
  - **FinCEN orders and Section 311 actions**
  - **Geographic Targeting Orders (GTOs)**
  - Asset freezes, transaction bans, and correspondent-bank restrictions



ENTIAL

# SECTOR IMPLICATIONS

FinCEN actions can strand assets and payments overnight—posing major operational and contractual risks.

- Even lawful payments can become unprocessable
- Trade finance, commodity payments, and joint-venture cash flows may be disrupted
- Companies may be forced to exit markets abruptly

# FINCEN ENFORCEMENT TOOLS

**FinCEN Authorities**

- **Section 311 of the USA PATRIOT Act** allows Treasury to designate:
  - A financial institution, class of transactions, or jurisdiction
  - As a **"primary money laundering concern"**
- Consequences include:
  - Restrictions on correspondent accounts
  - De-risking by global banks
  - Loss of access to USD clearing

**Recent Cartel-Linked Applications**

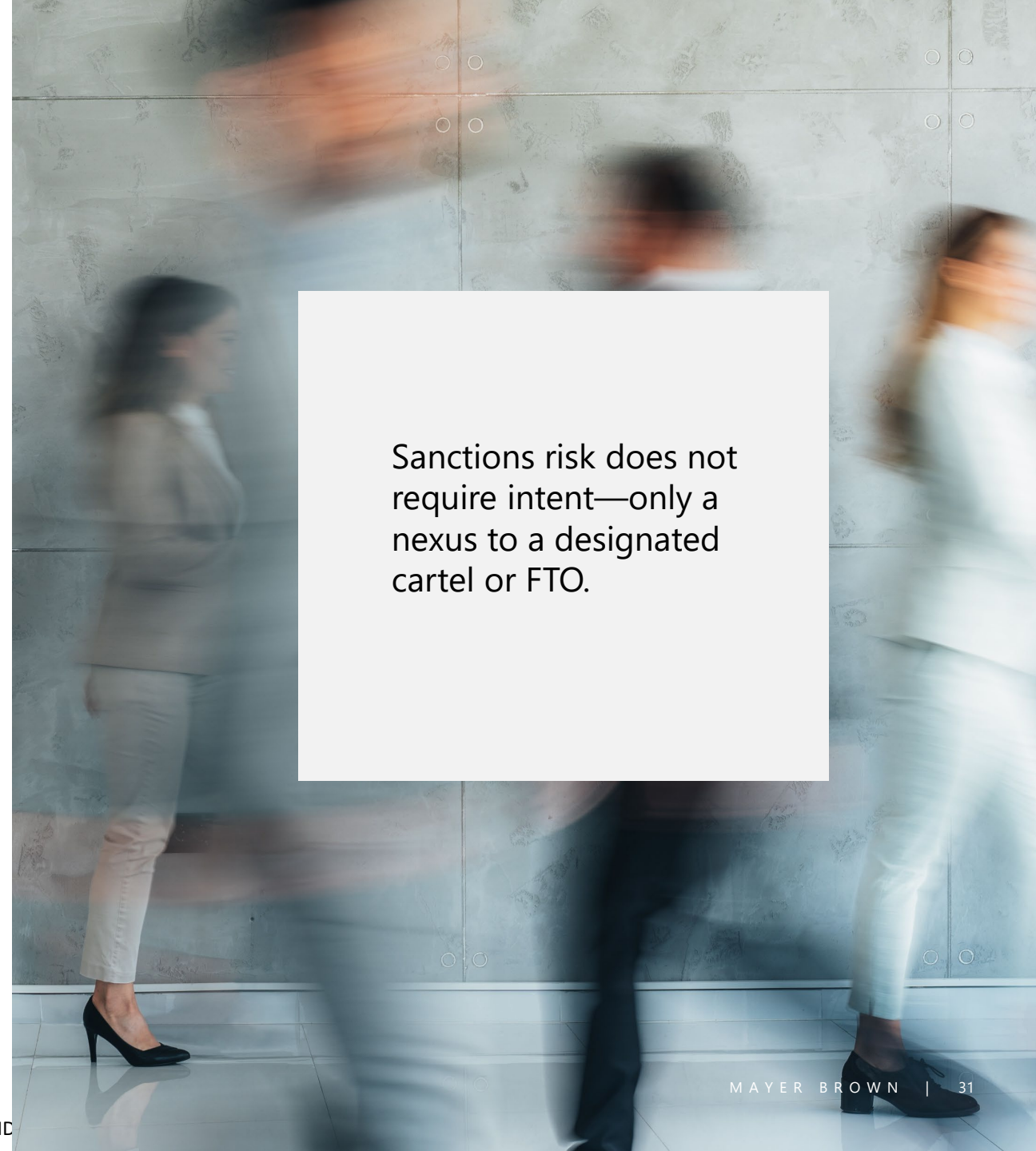
- FinCEN orders and actions tied to:
  - Mexican financial institutions
  - Border-region Money Services Businesses (MSBs)
  - Transactions involving cartel-linked fuel theft, oil smuggling, and precursor chemicals



CONFIDENTIAL

# OFAC SANCTIONS: STRICT LIABILITY MEETS CARTEL DESIGNATIONS

- Cartels designated as:
  - Foreign Terrorist Organizations (FTOs), and/or
  - Specially Designated Global Terrorists (SDGTs)
- OFAC sanctions impose:
  - Strict liability
  - Asset blocking
  - Prohibition on any dealings by US persons



Sanctions risk does not require intent—only a nexus to a designated cartel or FTO.



CONFID

# KEY DEVELOPMENTS

## MEXICAN FINANCIAL INSTITUTION DESIGNATIONS

- June 25, 2025: FinCEN issued its first orders under the FEND Off Fentanyl Act against:
  - CIBanco
  - Intercam Banco
  - Vector Casa de Bolsa
- Designated as **primary money laundering concerns**
- Orders (effective October 20, 2025) prohibit US financial institutions from processing transactions involving these entities
- Energy and chemical companies operating in Mexico or paying Mexican counterparties can be collateral damage, even with no wrongdoing, or forced to unwind contracts or halt operations

## BORDER-REGION MSBS (MONEY SERVICES BUSINESSES)

- FinCEN has focused on **MSBs operating near the US–Mexico border**, including:
  - Currency exchangers
  - Wire transmitters
  - Cash-intensive payment processors
- Tools used:
  - **Geographic Targeting Orders (GTOs)**
    - March 2025: FinCEN issued GTO covering the US southwest border
    - September 2025: Expanded to lower reporting threshold to $1,000
    - January 2026: New GTO for Minnesota (Hennepin & Ramsey counties): Requires reporting of transactions ≥ $3,000
  - Enhanced CTR/SAR reporting thresholds
  - Large-scale data sweeps and referrals to DOJ/IRS
- Even if your company does not use MSBs, your vendors might—creating indirect exposure



CONFID

# KEY DEVELOPMENTS

## SECTION 311 PROPOSED RULEMAKING

November 2025: FinCEN issued NPRM identifying transactions involving:

- **10 Mexico-based gambling establishments** linked to **cartel networks (including Sinaloa Cartel)**
- If finalized: US institutions would be **prohibited from maintaining correspondent accounts** tied to these entities

## OFAC SANCTIONS EXPANSION

- June 2025 – April 2026: OFAC sanctioned:
  - Cartel networks
  - Affiliated businesses and intermediaries
- Targeted activities include:
  - Timeshare fraud schemes
  - Casino operations
  - Fuel theft and oil smuggling networks
  - Precursor chemical supply chains (India–Guatemala–Mexico)



CONFID

# COMPOUNDING RISK

- **Parallel Investigations and Regulatory Coordination**
- Financial enforcement is increasingly coordinated across AML, sanctions, and FCPA regimes—creating overlapping scrutiny and rapid business disruption, even where exposure arises indirectly through transaction networks.
- Where potential **FCPA or sanctions issues** are identified:
    - FinCEN may initiate **parallel AML inquiries**
    - Financial institutions may be asked to review **Suspicious Activity Reports (SARs)** involving companies or counterparties
- DOJ guidance (June 2025) confirms a focus on:
    - Cases involving **cartels, TCOs, or related money laundering**
    - Integration of **anti-corruption enforcement into the broader financial-crime framework**

# A SINGLE SET OF FACTS CAN TRIGGER:

- OFAC sanctions violations
- FinCEN scrutiny / Section 311 exposure
- Money laundering liability
- Material-support theories
- FCPA exposure (where officials or SOEs are involved)

EXAMPLES

- Jensen (oil smuggling) → money laundering + material support
- Shandong (chemicals) → narcotics + financial facilitation
- TIGO Guatemala → FCPA + narcotrafficking proceeds
- Chiquita → sanctions + later civil exposure





CONFIDENTIAL



# 07

## COMPLIANCE & RISK MITIGATION

# MANAGING CARTEL, FTO, AND FINANCIAL-CRIME EXPOSURE

### 1. Strengthen Risk Assessment & Governance

- Integrate cartel/FTO risk into enterprise risk management (ERM)
- **Identify exposure** across:
  - Geographies (cartel-influenced regions)
  - Assets (pipelines, terminals, facilities)
  - Transactions (payments, logistics, chemical sales)
- Elevate oversight to senior management and board level

### 2. Enhance Third-Party Due Diligence

- **Expand screening** beyond customers to include:
  - Contractors, transporters, security providers, brokers
  - Distributors and chemical buyers
- **Assess**:
  - Ownership structures (shell companies)
  - Geographic risk and cartel presence
- **Implement continuous monitoring**, not one-time onboarding

### 3. Strengthen Financial Controls & Transaction Monitoring

- **Increase scrutiny** of:
  - Unusual payment structures (cash, layered transfers, crypto)
  - False invoicing and trade-based money laundering risks
- Align controls across:
  - AML, sanctions, and FCPA frameworks
- Establish escalation protocols for high-risk transactions

### 4. Prepare for Disruption from Financial Enforcement

- **Develop contingency plans** for:
  - Banking disruptions (FinCEN / Section 311 actions)
  - Sanctions designations or counterparty de-risking
- **Review contracts** for:
  - Termination rights
  - Force majeure provisions

### 5. Strengthen Internal Reporting & Response

- **Ensure effective whistleblower channels** and escalation processes
- **Train** frontline employees (operations, procurement, logistics) to identify:
  - Cartel influence
  - Coercive payment demands
- **Enable rapid investigation and decision-making**
- **Enforcement and discipline**

### 6. Implement Compliance Hallmarks

- Tone at the top
- Update Code of Conduct, Policies and Procedures
- Deploy compliance resources and systems
- Implement tools to evaluate the program effectiveness and detect violations
- Implement compliance reviews and audits (internally and by third parties)



CONFIDENTIAL

# OUR TEAM



PARTNER

## ROBERT W. HAMBURG

NEW YORK+1 212 506 2297
RHAMBURG@MAYERBROWN.COM



PARTNER

## GINA M. PARLOVECCHIO

NEW YORK+1 212 506 2522
GPARLOVECCHIO@MAYERBROWN.COM



AMERICAS HEAD OF SANCTIONS
SOCIETE GENERALE CORPORATE

## ALICE ROJAS

NEW YORK



CONFIDENTIAL

# 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.

You may not copy or modify the materials or use them for any purpose without our express prior written permission.




This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global legal services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England & Wales), Mayer Brown Hong Kong LLP (a Hong Kong limited liability partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively, the "Mayer Brown Practices"). The Mayer Brown Practices are established in various jurisdictions and may be a legal person or a partnership. PK Wong & Nair LLC ("PKWN") is the constituent Singapore law practice of our licensed joint law venture in Singapore, Mayer Brown PK Wong & Nair Pte. Ltd. More information about the individual Mayer Brown Practices and PKWN can be found in the Legal Notices section of our website.
"Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown. © 2025 Mayer Brown. All rights reserved.