Mapping the Evolving DOJ Enforcement Landscape

Hosted by the ACC Houston Veterans Networking Group
August 27, 2025

Panelists:
Michael Galdo, King & Spalding, LLP
Brandt Leibe, King & Spalding, LLP
Victor Wright, Baker Hughes

Agenda

1

DOJ's Evolving Enforcement Landscape

- New White-Collar Enforcement
- Resolution Pathways & Whistleblowers

2

Areas of Enforcement

- Trade Compliance
- DEI & Civil Rights Fraud
- Cybersecurity Enforcement
- Drug Cartel Designations & ATA

King & Spalding

ACC Association of Corporate Counsel HOUSTON

Areas of Enforcement Priority

White-Collar & Corporate Prosecution Prosecution

Focus on new categories of potential misconduct misconduct and incentivizing voluntary self-self-disclosure.

Trade & Tariffs

Increased scrutiny on import/export violations associated with tariffs and the Administration's Trade agenda.

DEI & Civil Rights Fraud

New initiatives targeting diversity, equity, and inclusion (DEI) programs.

Cybersecurity

Aggressive enforcement against cyber threats, data breaches, and non- and non-compliance with cyber regulations.

Transnational Organized Crime

Targeting drug cartels, including by designating cartels as foreign terrorist organizations.

DOJ's Pivot: New White-Collar Enforcement Landscape for Corporate Counsel in 2025

The Justice Department has dramatically shifted its enforcement priorities and corporate resolution approaches in 2025. This change This change creates new compliance considerations and opportunities, requiring corporate counsel to prepare for a landscape defined by landscape defined by aggressive white-collar crime prosecution, heightened whistleblower incentives, and evolving liability theories. liability theories.

1

Aggressive New Enforcement Focus

Proactive and aggressive prosecution of white-collar crime, setting a new tone for corporate accountability in different priority areas.

2

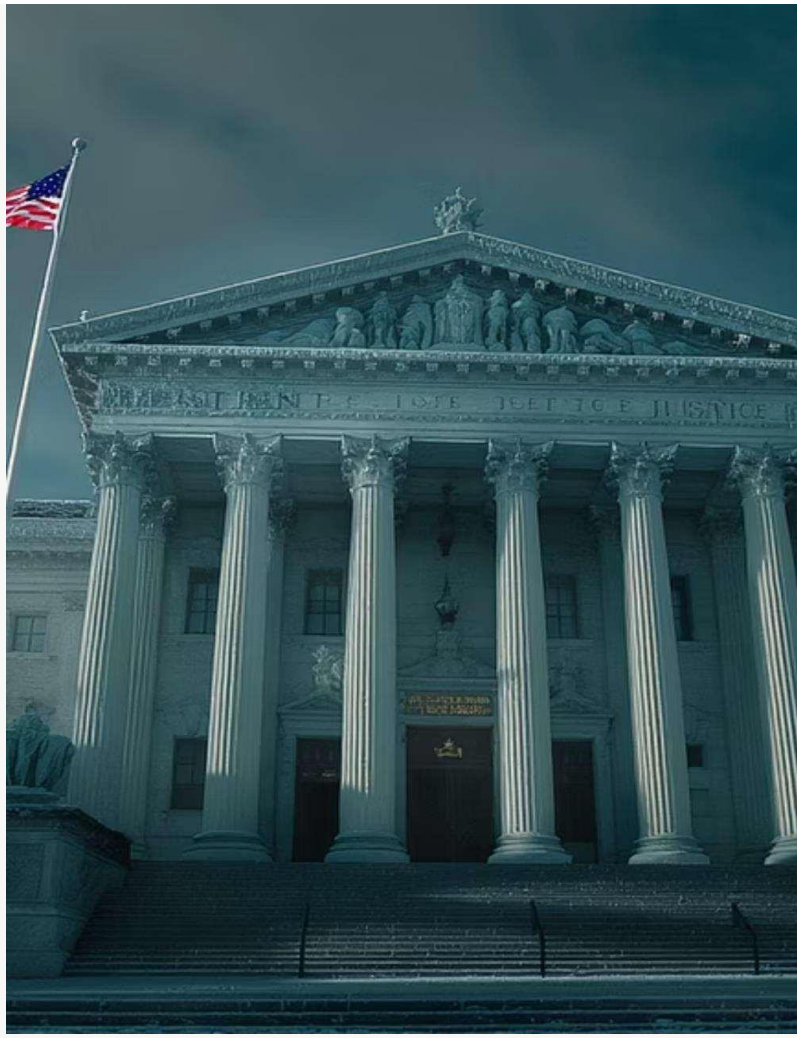
Enhanced Whistleblower Incentives

Increased pathways and protections for individuals to report misconduct, amplifying risk for non-compliant entities.

3

Evolving Liability Theories

Broader application of existing statutes to new scenarios, expanding the scope of potential corporate and individual liability. liability.



K&S King & Spalding

ACC Association of Corporate Counsel HOUSTON

DOJ Enforcement: Resolution Pathways, Whistleblowers & Strategic Focus Focus

Monitorship Reform: Rarer, Narrower, Cheaper

New May 2025 guidance: monitors imposed only when necessary, with capped hourly rates, required budgets, and biannual DOJ-company-monitor meetings monitor meetings. Existing monitorships (e.g., Glencore) have already seen early termination

Revised Corporate Enforcement Policy

Declination Path

Voluntary self-disclosure, full cooperation, remediation, and no aggravators can lead to full declination.

Near-Miss Benefits

Even with aggravators/near-misses, companies can get NPAs, <3-year <3-year terms, no monitors, and 75% fine reduction.

Whistleblower Incentives

New DOJ policies and expanded incentive programs are elevating whistleblower risk

Enhanced Incentives

The DOJ's whistleblower program offers financial awards for awards for tips leading to successful enforcement actions actions across various violation types, including sanctions and sanctions and cartel behavior.

Increased Reporting Channels

With multiple agencies now offering whistleblower incentives, employees have more avenues to report misconduct, increasing the likelihood of external disclosure. disclosure.

Heightened Internal Scrutiny

Companies must now swiftly address internal reports, as as prompt self-disclosure to the DOJ (within 120 days) can be days) can be a key factor in securing declinations or reduced reduced penalties, even if an employee also reports externally.

Key Insight: Assume issues are more likely than ever to be reported by insiders, making robust internal controls and rapid response critic al.

The False Claims Act: DOJ's Powerful Enforcement Tool

The False Claims Act (FCA) is the primary statute under which the U.S. government recovers losses from fraud. It allows the government to recover billions of dollars annually through civil litigation and civil litigation and settlements, often initiated by whistleblowers (known as "relators") under its *qui tam* provisions. This makes the FCA a critical mechanism for the DOJ to act on whistleblower tips and enforce whistleblower tips and enforce compliance across various sectors.

Key aspects of the FCA include:

- **Treble Damages & Penalties:** Companies found liable face significant financial penalties, including three times the amount of damages the government sustained, plus civil penalties per claim.
- penalties per claim.
  Whistleblower Rewards: Relators can receive between 15% and 30% of the government's recovery, strongly incentivizing individuals to report fraud.
- **Broad Scope:** The FCA applies to any false claim for payment submitted to the government, covering a wide range of industries from healthcare to defense contracting and now, increasingly, trade and increasingly, trade and tariffs.

Trade Compliance: DOJ’s Intensified Focus

The Department of Justice is intensifying its focus on trade compliance violations, establishing the establishing the Market, Government, and Consumer Fraud (MGCF) Unit within the Criminal Division. Criminal Division.

This unit specifically targets tariff evasion and trade fraud, prosecuting activities such as misclassification, undervaluation of imports, transshipment, and mislabeling to obscure origin or evade duties.

DOJ's enforcement initiative aligns directly with the administration's broader trade agenda, reinforcing key national priorities

Strategic Context: Why Now?

- **Economic Security:** Protecting domestic industries and intellectual property from unfair competition and illicit trade practices.
- **Geopolitical Landscape:** Responding to global trade tensions, supply chain chain vulnerabilities, and the use of economic coercion.
- **National Security:** Preventing the flow of goods that could compromise national security interests, including dual-use technologies and materials.
- **Data-Driven Enforcement:** Leveraging enhanced analytical capabilities to better to better identify evasion patterns and prioritize investigations.

Trade Compliance: DOJ's Partners

Paperwork is filed when importing or exporting, as well as extensive recordkeeping requirements for US businesses.

As a result, there is an extensive paper trail containing potentially false representations for government investigators with administrative authority to follow.

Administrative Tools

- **BIS OEE:** Regulatory authority to demand internal business records related to exports—may include internal emails
- **DHS:** DHS entities, including CBP and HSI, can use administrative subpoenas to request business records related to imports
- **Task Forces:** BIS and DHS are both in multiple task forces with DOJ, resulting in sharing information gathered for regulatory purposes for potential criminal or civil enforcement

Reverse False Claims Act Risk in the Trade Context

Context

DOJ's focus on trade compliance extends to "reverse" False Claims Act (FCA) cases, imposing liability on companies that knowingly conceal or avoid knowingly conceal or avoid obligations owed to the U.S. government, particularly in customs and import duties.

Key Concepts

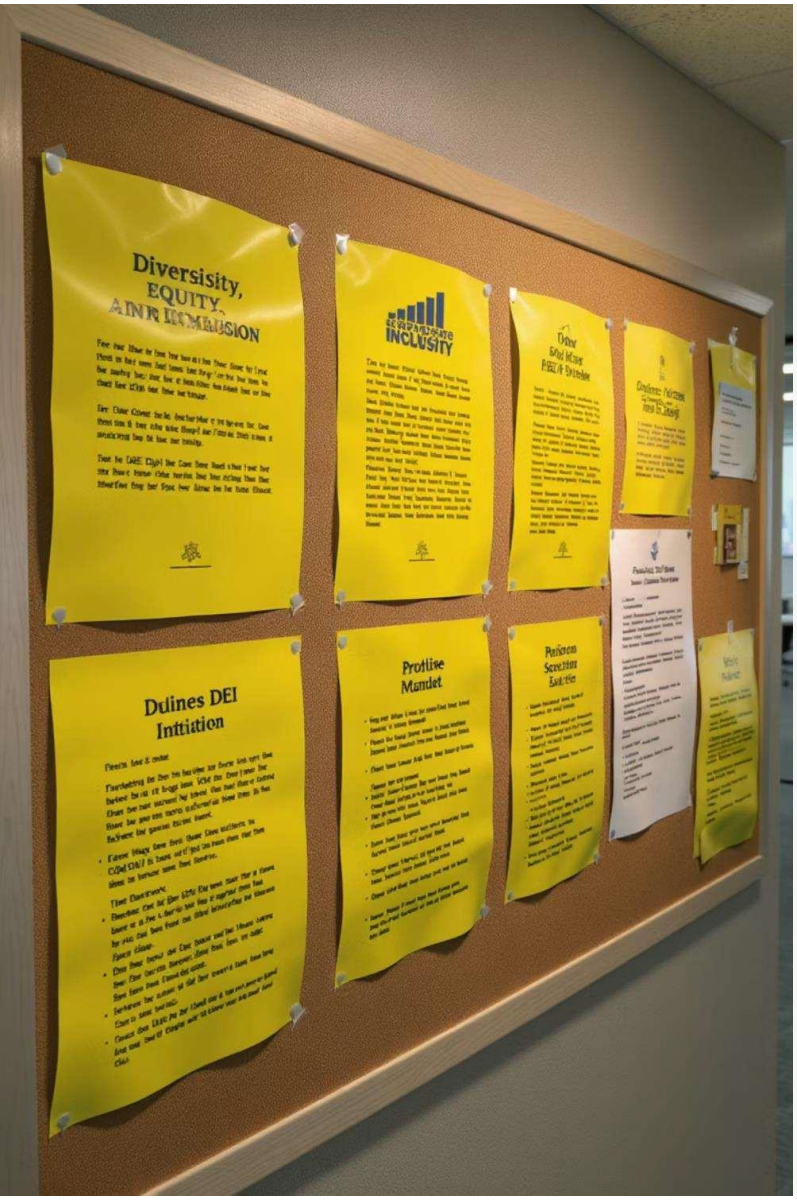
- The "reverse" FCA targets failure to pay tariffs, duties, anti-dumping/countervailing duties, or other customs fees.
- **Triggering Conduct:** Misclassification, undervaluation, false country-of-origin labeling, or circumvention of tariffs (e.g., Section 232/301).
- Liability can attach even without an affirmative false statement; knowing failure to pay is sufficient.

Risks & Penalties

1. **Civil Liability**
   Treble damages for unpaid duties and significant statutory penalties per violation.
2. **Criminal Exposure**
   Willful schemes can lead to charges like conspiracy, wire fraud, or smuggling for both corporations and individuals.
3. **Collateral Consequences**
   Loss of trade privileges, exclusion from government contracts, reputational harm, and parallel proceedings by other agencies. agencies.

K&S King & Spalding

ACC Association of Corporate Counsel HOUSTON



DEI and Civil Rights Fraud Enforcement Enforcement

DOJ's enforcement focus targets race/sex-based preferences in hiring, promotion, or subcontracting when federal funding is involved, viewing such practices as potential false claims.

Coordinated Enforcement Strategy

DOJ's Civil Fraud and Civil Rights Sections are actively collaborating to pursue False Claims Act (FCA) cases against federal contractors violating civil rights laws. These cases are premised on the notion that civil rights compliance is a **material condition of payment**, giving rise to FCA liability.

Whistleblower-Driven Enforcement

The DOJ encourages qui tam filings for civil rights compliance. This creates significant risk from internal from internal whistleblowers identifying problematic DEI practices.

This initiative expands FCA enforcement into areas previously addressed by administrative remedies or Title VII litigation, making civil rights compliance a critical focus for contractors.

K&S King & Spalding

ACC Association of Corporate Counsel HOUSTON

DOJ's Enforcement Framework and Liability Theories

This initiative leverages specific liability theories within the False Claims Act to target non-compliance. These theories expand the scope of liability for federal liability for federal contractors and recipients of federal funds.

False Certification

If a federal contractor allegedly is not in compliance with relevant civil rights statutes, even implicitly, and submits a claim for payment, it can be held liable under the FCA. This means that violations of non-discrimination laws, such as Title VI or Title VII, when tied to federal funding or contracts, can directly trigger FCA liability.

SAM.gov & FAR Certifications

Federal Acquisition Regulation (FAR) clauses and certifications made in systems like SAM.gov (System for Award Management) require ongoing declarations of compliance with various laws and regulations, including those pertaining to equal opportunity and non-discrimination. Any false certification made at the time of contract award, or a failure to correct a prior false certification as conditions change, can serve as a basis for FCA liability. This puts a continuous burden on contractors to ensure accuracy in their certifications throughout the lifecycle of federal contracts.

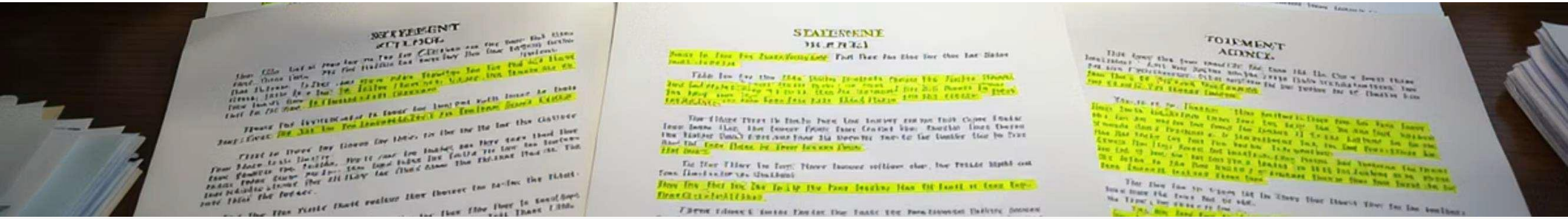
Cybersecurity Threats

Evolving Criminal Threats
- Crime-as-a-service proliferates
- AI enables more complex attacks
- Annual increases in cyber-enabled fraud

Insider Threats
Employees with privileged access present unique risks through:
- Unintentional security lapses
- Malicious data exfiltration
- Potential whistleblower claims

Nation-state Actors
- Financial theft (N. Korea & Iran)
- Intellectual property theft
- Persistent network presence
- Intelligence gathering operations

King & Spalding
ACC Association of Corporate Counsel HOUSTON



DOJ Priorities & Enforcement Landscape

The Department of Justice's stance on cybersecurity enforcement is clear:

> "Companies that knowingly provide deficient cybersecurity products or services, knowingly knowingly misrepresent their cybersecurity practices or protocols, or knowingly violate violate obligations to monitor and report cybersecurity incidents and breaches face the full face the full weight of the department's enforcement capabilities."
>
> — Deputy Attorney General Lisa Monaco, March 2024

This aggressive stance expands upon the 2021 Civil Cyber-Fraud Initiative, signifying a sustained focus on cyber-related accountability and a broader pivot in white-collar enforcement.

The Evolving Enforcement Landscape: Key Shifts

Corporate counsel must be aware of an intensified enforcement environment, marked by several significant shifts:

- **Increased Individual Accountability:** A heightened focus on prosecuting corporate corporate executives and individuals for misconduct.
- **Proactive Compliance & Transparency:** Greater expectations for companies to implement implement robust compliance programs, self-report issues, and foster a culture of integrity. of integrity.
- **Expanded Use of Data Analytics:** Leveraging advanced tools and data analysis to identify and investigate potential misconduct more efficiently.
- **Cross-Border Cooperation:** Enhanced collaboration with international partners to address global enforcement challenges.
- **Deterrence Through Prosecution:** A more aggressive stance on pursuing criminal deter future crimes.

King & Spalding

ACC Association of Corporate Counsel HOUSTON

FCA Cyber Violations: Key Risks & Penalties

Materially False Statements About Cybersecurity

Federal contracts increasingly incorporate specific cybersecurity standards, and many federal programs require certification of compliance.

When a company falsely represents compliance with these standards, it faces potential liability under the False Claims Act. The DOJ has signaled that cybersecurity misrepresentations will be a top enforcement priority through at least 2027.

Severe Penalties for FCA Violations

- Triple the government's damages
- Statutory penalties per violation
- Attorney fees
- Potential debarment from future federal contracts

Enforcement Priorities

Targeting Government Contractors

Increased scrutiny on entities providing goods and services to federal agencies, particularly those handling sensitive data or critical infrastructure.

Emphasizing Self-Disclosure & Cooperation

DOJ encourages companies to proactively report cybersecurity incidents and compliance failures for more favorable resolutions.

Individual Accountability

Focus on holding individuals accountable for cybersecurity failures, including executives and compliance officers, in addition to corporate entities.

Supply Chain Vulnerabilities

Prioritizing cases involving cybersecurity weaknesses within federal supply chains, recognizing the recognizing the cascading risk to government systems.

King & Spalding

ACC Association of Corporate Counsel HOUSTON

FCA Cybersecurity Enforcement Possibilities

The FCA creates liability for anyone who knowingly submits false claims to the government or causes another to submit a false claim. Your organization may face significant FCA risk if you operate in FCA risk if you operate in areas with:

Direct Government Contracts

Prime contractors with federal agencies are directly subject to contractual cybersecurity cybersecurity requirements.

Subcontractor Relationships

Vendors for entities that contract with the government often must meet the same security security standards.

Grant Recipients

Federal grant conditions frequently include cybersecurity attestations and requirements. requirements.

Healthcare Providers

Recipients of Medicare/Medicaid payments must certify compliance with applicable security standards.

The DOJ is increasingly leveraging the False Claims Act to target cybersecurity-related fraud, holding companies liable for misrepresenting their cyber posture or failing to meet compliance obligations. meet compliance obligations. The FCA's qui tam provisions also empower whistleblowers to file suits, offering significant incentives for reporting deficiencies and adding another layer of risk. another layer of risk.

K&S King & Spalding ACC Association of Corporate Counsel HOUSTON

DOJ's Focus on FCA Cybersecurity: Key Cases & Precedents

> "The Justice Department will continue to pursue federal contractors that place such data at risk by failing to meet material cybersecurity requirements in their contracts."
>
> — **Brett A. Shumate** Acting Assistant Attorney General Justice Department's Civil Division February 2025

This statement underscores the DOJ's consistent commitment to prioritizing cybersecurity enforcement, as evidenced by recent high-profile cases and settlements under the False Claims Act.

False Claims Act Case Examples

Aerospace Contractor Settlement

A major aerospace contractor settled for millions after allegations of failing to implement cybersecurity controls required by its government contracts, leading to data breaches.

Healthcare Provider Enforcement

A healthcare provider faced penalties for misrepresenting misrepresenting its compliance with HIPAA and other other cybersecurity standards, impacting patient data data integrity.

IT Service Provider Case

An IT service provider was investigated for allegedly failing to protect sensitive government data, despite certifying compliance with security protocols in its contracts.

These cases highlight the DOJ's aggressive stance and serve as a clear warning to companies that misrepresent their cybersecurity posture or fail to meet contractual obligations.

Key FCA Cybersecurity Cases

1

US v. Guidehouse

Settled for $7.6M for failing cybersecurity requirements, including unperformed security testing and unauthorized cloud storage of PII.

2

US v. Georgia Tech

Pending case alleging "no enforcement" of federal cybersecurity regulations in DOD research contracts (e.g., failed antivirus installation, false assessments).

3

US v. Aerojet Rocketdyne

Settled for $9M over misrepresentations regarding cybersecurity cybersecurity compliance in DOD and NASA contracts.

4

US v. Verizon Business Svcs

Settled for $4M after **self-disclosing** failure to provide required required cybersecurity controls for government IT services.

The IT Whistleblower

IT professionals are uniquely positioned to become whistleblowers due to their specialized knowledge and access to knowledge and access to detailed documentation regarding cybersecurity vulnerabilities. This makes them them particularly credible and well-documented sources, leading to significant False Claims Act (FCA) exposure for exposure for companies.

External Threat Actors

Sophisticated hackers constantly probe systems for vulnerabilities, creating ongoing compliance challenges.

Specialized Knowledge

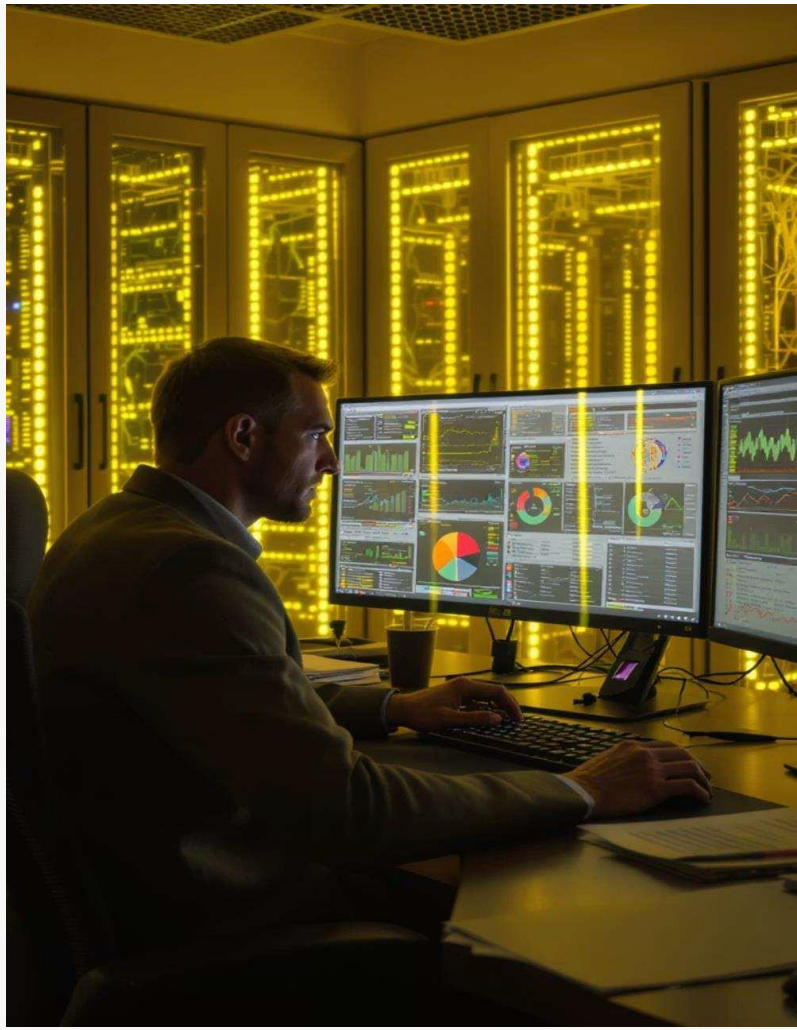
IT professionals have unique insight into security gaps and vulnerabilities within systems.

Detailed Documentation

They often create detailed records of identified issues, providing concrete evidence for claims.

Frustration & Access

Deprioritized security concerns can lead to frustration, and they have direct access to technical evidence to substantiate claims.



K&S King & Spalding

ACC Association of Corporate Counsel HOUSTON

What to do: Navigating Cybersecurity & Self-Disclosure

01

Assess Current Risk

Conduct a privileged review of cybersecurity compliance to identify and document document gaps between stated and actual practices.

02

Assess Vendor Risk

Review third-party security practices and contractual representations to mitigate vendor-related liability.

03

Monitor Regulatory Changes

Implement a process to track evolving government cybersecurity standards (e.g., standards (e.g., NIST 800-171, CMMC 2.0, FedRAMP).

04

Investigate for Disclosure Readiness

Conduct prompt, thorough investigations into compliance issues to make informed make informed decisions about potential self-disclosure.

05

Evaluate Disclosure Criteria

Assess if the issue meets the criteria for voluntary self-disclosure, considering considering factors like timeliness, cooperation, and remediation efforts.

06

Weigh Benefits vs. Risks of Disclosure

Analyze potential benefits (e.g., cooperation credit, mitigation of penalties) against penalties) against risks (e.g., additional scrutiny, potential enforcement actions). actions).

What to Do: Cybersecurity & M&A

01

Conduct Pre-Acquisition Due Diligence

Assess the target's cybersecurity posture, incident history, and compliance status prior to acquisition to identify material risks and potential liabilities.

02

Perform Post-Acquisition Assessment

Conduct a comprehensive, privileged review of the acquired entity's cybersecurity posture post-acquisition to identify vulnerabilities, assess critical infrastructure status, and confirm compliance with contractual obligations.

03

Implement Strategic Risk Mitigation

Proactively address identified issues to mitigate liability and prevent future whistleblower complaints. This includes integrating security controls, resolving known controls, resolving known deficiencies, and considering self-disclosure for significant findings.

Drug Cartel Designations: Expanded Liability & Enforcement Risks Enforcement Risks

Recent shifts in U.S. policy are increasingly categorizing major drug cartels as Foreign Terrorist Organizations (FTOs) or other similar entities. On February 20, 2025, six drug cartels and two transnational criminal organizations were officially organizations were officially designated as FTOs by the U.S. Government, creating unprecedented liability risks for businesses globally. These classifications significantly expand the scope of potential liability, particularly under "material particularly under "material support" statutes and civil enforcement actions like the Antiterrorism Act (ATA), requiring enhanced due diligence and compliance measures across various industries.

Mexican Drug Cartels Designated as FTOs:

- Sinaloa Cartel
- Jalisco New Generation Cartel (CJNG)
- Northeast Cartel (CDN) - former Los Zetas splinter group
- La Familia Michoacán
- United Cartels (Carteles Unidos)
- Gulf Cartel

Additional TCOs Designated:

MS-13

El Salvadoran/Los Angeles origin gang with transnational presence

Tren de Aragua

Venezuelan gang with expanding presence throughout South America and the United States

These designations fundamentally alter the compliance landscape for businesses, exposing them to expanded civil and criminal liability under U.S. law for providing any form of "material support" to these entities, whether directly or indirectly. This includes financial services, technology, logistics, and any sector operating in or connected to affected regions.

King & Spalding

Association of Corporate Counsel HOUSTON

Expanded Liability: Material Support & Civil Enforcement

The designation of drug cartels as Foreign Terrorist Organizations (FTOs) significantly expands the scope of both criminal (material support) and civil liability under U.S. law for businesses law for businesses operating in regions with cartel presence. Building on the criminal liability discussed, this section details the critical civil enforcement aspect.

Criminal Enforcement: Material Support of Terrorism

Under U.S. law, specifically 18 U.S.C. § 2339A and § 2339B, it is a federal crime to provide "material support or resources" to designated Foreign Terrorist Organizations (FTOs). This statute broadly defines "material support" to include any property, service, training, expert advice or assistance, or personnel. This means that providing seemingly innocuous services or goods that indirectly benefit a designated cartel could expose individuals and corporations to severe criminal penalties, including lengthy prison sentences and substantial fines, even if there was no intent to further the cartel's illicit activities directly.

Civil Enforcement: The Antiterrorism Act (ATA)

The Antiterrorism Act (ATA)

The Antiterrorism Act (ATA) creates a civil cause of action for victims of international terrorism. Under the ATA, liability may be asserted against any person or business providing substantial assistance to a Foreign Terrorist Organization (FTO) if injury arises from an act of international terrorism committed or authorized by that FTO.

Specialized law firms actively pursue civil suits under this statute, previously targeting entities allegedly supporting groups like ISIS and al-Qaeda.

Enforcement & Industry Impacts

The FTO designation of drug cartels significantly expands the scope of potential defendants for FTO criminal investigations and ATA litigation, now including businesses no prior terrorism-related concerns.

Impacted Industries

Finance/Fintech

- Money laundering risks (crypto, stablecoins, instant transfers, BMPE)
- Remittances and asset forfeiture risks

Transportation/Logistics

- Shipping through cartel-controlled ports
- Paying "taxes" or "tolls" for cross-border operations
- Risk of employee smuggling contraband

Energy

- Operations in cartel-controlled territories
- Extortion; security costs as "material support"

Indirect Impacts

- Supply chain disruptions & third-party vendor exposure
- Increased compliance costs and due diligence complications

King & Spalding

ACC Association of Corporate Counsel HOUSTON

What To Do Now: Actions & Self-Disclosure

Review Procedures

Evaluate due diligence for high-risk regions and implement enhanced screening for newly designated FTOs.

Assess Direct Exposure

- Map business activities in cartel-controlled areas
- Identify subsidiaries, affiliates, and acquisitions with potential exposure
- Review security payment arrangements for "material support" risks

Evaluate Indirect Impacts

- Conduct supply chain risk assessment
- Identify potential forfeiture risks
- Review M&A strategy for targets with exposure

Implement Remediation

Develop privileged risk mitigation strategies and consider operational changes in high-risk regions.

Consider Self-Disclosure

Assess benefits of voluntary self-disclosure, including leniency. Consult legal counsel to navigate policies.

Self-Disclosure Considerations

The DOJ now offers enhanced incentives for self-disclosure but imposes greater penalties for non-reporting. Effective decision-making requires:

Privileged Assessment

Conduct privileged investigations to fully understand violations before before disclosure.

Policy Expertise

Analyze specific requirements of relevant self-disclosure programs programs (Antitrust, FCPA, FCA, Export Controls).

Timing Considerations

Many programs require disclosure prior to imminent threat of investigation for full credit.

Strategic Decision-Making

Balance potential benefits (reduced penalties, declination) against risks (increased scrutiny).

Consult experienced counsel familiar with current DOJ enforcement priorities for self-disclosure decisions.

Brandt Leibe
Partner
Special Matters and Government Investigations
bleibe@kslaw.com
713.751.3235

Mike Galdo
Counsel
Special Matters and Government Investigations
mgaldo@kslaw.com
512.457.2081

Victor Wright
Vice President
Global Labor and Employment Law
Baker Hughes
victor.wright@bakerhughes.com

King & Spalding

ACC Association of Corporate Counsel HOUSTON

Questions?

Mapping the Evolving DOJ Enforcement Landscape