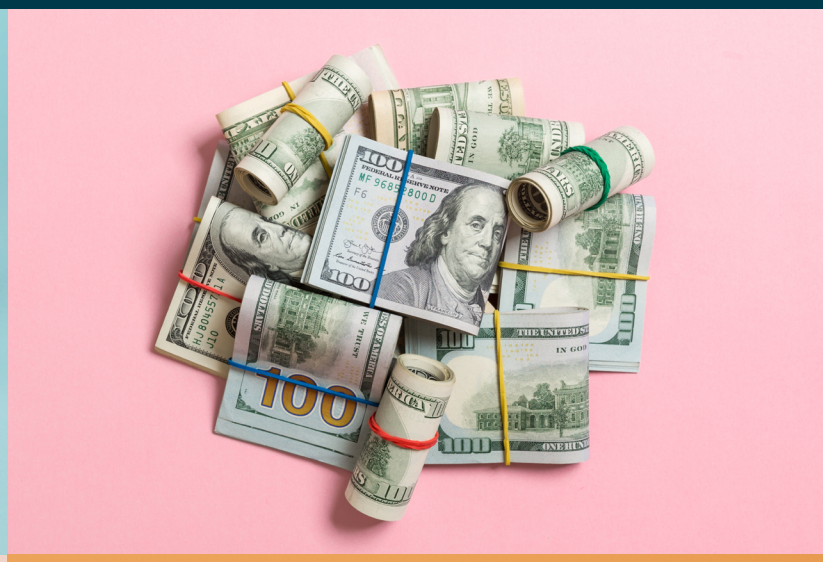
Areas of Heightened DOJ Scrutiny *in the Second Trump Administration*



BY CANDICE WONG,
LITIGATION PARTNER









In today's fluid and evolving enforcement landscape, legal and compliance teams face mounting pressure to stay ahead of regulatory developments - particularly as the DOJ under the second Trump administration recalibrates its priorities and resources. Recent developments in executive and DOJ policy have resulted in heightened scrutiny and enforcement across several critical areas, signaling new investigative trends and a reallocation of enforcement attention. Companies and institutions operating in sectors subject to DOJ oversight should be especially attuned to these developments, as they directly affect where, how, and when regulatory scrutiny may arise.

Fried Frank is proud to present "Areas of Heightened DOJ Scrutiny," which spotlights specific DOJ enforcement priorities drawing increased attention: healthcare (including False Claims and antitrust violations), financial enabling of cartels and Foreign Terrorist Organizations (FTOs), tariff and customs evasion, and cybersecurity and data security breaches. For each area, it outlines the regulatory context, recent DOJ actions, emerging risks, and practical guidance for navigating compliance challenges.

With the pace of DOJ announcements and initiatives, proactive monitoring and informed risk management are essential for organizations seeking to anticipate and respond effectively to enforcement trends under the current administration.

Healthcare – *False Claims and Antitrust* 3
Financial Enabling *of Cartels and FTOs* 5
Tariff and Customs *Evasion* 7
Cyber and Data *Security Breaches* 9

Healthcare – *False Claims and Antitrust Violations*



The DOJ is intensifying the spotlight on fraud and competition in the healthcare industry. Criminal fraud schemes, civil False Claims Act (FCA) actions, and some emerging risks – such as network adequacy and electronic records manipulation – are at the fore. Here's what you need to know:

1. Criminal Healthcare Fraud Schemes – Continued DOJ Priority

Criminal healthcare fraud was a priority of the first Trump administation and remains a central focus.

DOJ Priority: In May 2025, the DOJ Criminal Division's acting head ranked healthcare fraud as #1 on a list of updated list of white collar priorities. We expect continued robust charging of healthcare fraud schemes (18 U.S.C. §§1347, 1349), including those involving cross-border conspiracies, telemedicine and genetic testing fraud, and prescription opioid trafficking.

Record-Breaking Takedown: In June 2025, the DOJ announced the "largest coordinated healthcare fraud takedown in history" against 324 defendants for fraud schemes involving approximately $14.6 billion in false claims to Medicare, Medicaid and other programs. This follows similar record-setting takedowns in 2017 and 2018, during the first Trump administration.

2. Civil False Claims Act (FCA) Enforcement – Accelerating Activity

Civil FCA enforcement is expanding through new initiatives, increased reliance on data, and new areas of focus.

Revived DOJ-HHS FCA Working Group: Announced in July 2025, this group signals escalating FCA enforcement. The FCA penalizes those who knowingly submit or cause to be submitted false "claims" to the government or knowingly make false records or statements to get a false claim paid. Actions can be brought both by the DOJ and by qui tam whistleblowers, who can initiate actions, prosecute (even if the DOJ declines to intervene) and receive up to 30% of recoveries. FCA liability carries hefty consequences, including per-claim penalties and treble damages. It can also result in suspension and debarment from federal contracting, as well as reputational harms.

Data Analytics and Intelligence Sharing: The Working Group has touted increased reliance on data analytics and cross-agency intelligence sharing in its fraud-detection efforts, which — together with recent FCA settlement announcements — signals a faster investigative turnaround.

Recent Enforcement Trends: FY2024 saw the second-highest number of DOJ actions (nearly tripling since 2019) and the highest-ever number of qui tam actions (a 60% rise since 2019). Qui tam actions drive the lion's share of FCA actions and recoveries; in 2023, $2.3 billion of the overall $2.68 billion in FCA recoveries came from qui tam actions. Despite a percolating legal question about whether the FCA's qui tam provision is constitutional under the Appointments Clause (*see United States ex rel. Zafirov v. Florida Medical Associates, LLC, et al.*), this administration has continued to give full-throated endorsement to qui tam FCA enforcement.

Key Takeaways

Healthcare and life sciences companies should consider whether updated internal controls or protocols are warranted by the recalibration of enforcement priorities.

Internal Complaints: Given the universal focus on whistleblowers, consider strengthening internal complaint pathways to facilitate in-house remediation of noncompliance.

Data Awareness: Given the infusion of data analytics into enforcement, understand internal data and potential red flags.

Due Diligence: Acquisitions or sales should account for emerging enforcement areas, such as EHR manipulation or patient access barriers.

3. Specific FCA Healthcare Priorities

The DOJ-HHS FCA Working Group has articulated as priorities several longstanding areas of enforcement as well as two areas that represent more uncharted territory.

Traditional Priorities:

- Medicare Advantage fraud: Insurers and providers exaggerating diagnoses to increase reimbursements (CMS announced expanded auditing efforts for MA plans in May)
- Drug, device and biologics pricing
- Kickbacks: Pharmaceutical companies, hospitals and pharmacies making illegal payments to boost prescriptions
- Materially defective medical devices

Emerging Priorities:

- Barriers to patient access to care and network adequacy
    - In May, the DOJ filed an FCA complaint against three of the nation's largest health insurance companies and three insurance broker organizations, alleging kickbacks and discrimination against disabled Medicare beneficiaries, who were perceived to be less profitable.
- Manipulation of Electronic Health Records, such as instances involving AI use in clinical decision-making.

4. Antitrust Scrutiny – New Whistleblower Incentives

The DOJ and FTC continue to scrutinize healthcare deals and consolidation, with greater emphasis on regulatory burdens and whistleblower tips.

Deal Oversight: The DOJ Antitrust Division and FTC seem poised to continue scrutinizing deals between direct competitors and the consolidation of physician practices, and pursuing lower healthcare and drug prices. In framing the underlying concerns with the healthcare industry, however, the current administration has shifted away from the prior administration's emphasis on the involvement of private equity acquirers and alleged "corporate greed," instead highlighting how regulatory burdens have acted as barriers to entry.

Whistleblower Rewards: In July, the DOJ and United States Postal Service announced the first-ever "Whistleblower Rewards Program," an effort to replicate the success of whistleblower-initiated investigations in the FCA context. The program promises financial incentives to those who provide tips on price-fixing, bid-rigging and market allocation schemes, as well as other criminal violations that undermine competition in industries, including, specifically, "healthcare." Healthcare and life sciences companies that send products through the mail, or have otherwise entered contracts with the USPS, may be among the most exposed to whistleblower-initiated antitrust investigations, as well as the ramifications of mistaken submissions being made directly to the government.

2025 Milestones
Key actions shaping enforcement

5.12.2025 – DOJ memorandum on "Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime"

5.19.2025 – DOJ memorandum on "Civil Rights Fraud Initiative"

5.21.2025 – DOJ announcement of the first political appointee to oversee DOJ Civil Division's Commercial Litigation Branch, which handles the False Claims Act

5.21.2025 – CMS announcement of expanded auditing of MA plans

6.30.2025 – DOJ announcement of the largest-ever healthcare fraud takedown

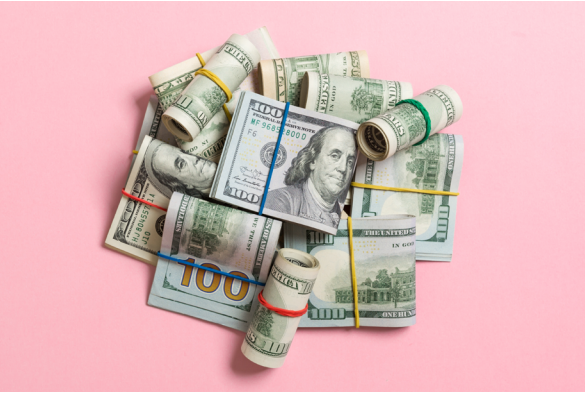
7.2.2025 – DOJ announcement of "DOJ-HHS False Claims Act Working Group"

7.8.2025 – DOJ announcement of Antitrust Division-Postal Service "Whistleblower Rewards Program"

Keep An Eye On:

The Administrative False Claims Act (AFCA) The refashioned AFCA (31 U.S.C. § 3801 et seq.), which became law at the end of 2024, could potentially lead to a rise in agency-initiated, non-DOJ claims.

Financial Enabling *of Cartels and Foreign Terrorist Organizations (FTOs)*



Federal enforcement against drug cartels and transnational gangs now designated as FTOs and Specially Designated Global Terrorists (SDGTs) is intensifying, exposing companies to heightened risks of criminal and civil liability for any direct or indirect interactions. Businesses operating in high-risk sectors or regions must strengthen due diligence and compliance.

1. Heightened Enforcement Risks: Cartels and Gangs as FTOs

Targeting drug cartels and gangs as FTOs poses heightened risks to US and foreign companies operating in Central and South America, given heavy scrutiny of any interaction with such organizations, even if unwitting or indirect.

Expanded Designations and Legal Risks: The State Department's designations in February of six Mexican cartels (including Sinaloa and CJNG) and two transnational gangs (Tren de Aragua and MS-13) as FTOs and Specially Designated Global Terrorists — all but one had previously been designated as blocked persons under other OFAC authorities — further expand the risk of criminal and civil liability, sanctions violations, blocking sanctions and listing on the Specially Designated Nationals and Blocked Persons List for those implicated in any transactions.

Complex Compliance Challenges: Compliance can be complex because cartels often infiltrate legitimate industries (e.g., agriculture) and because they are generally not formal entities with clear memberships.

Industries at Elevated Risk: Industries commonly targeted by cartels include
(1) logistics and transportation firms
(2) construction and infrastructure developers
(3) utility monopolies or service providers
(4) sectors with influential labor unions

2. Material Support of Terrorism Statute

Expect to see the material support of terrorism statute, 18 U.S.C. §2339B, deployed against any companies and individuals found to have transacted with FTOs.

Broad Definition of "Material Support": "Material support" is broadly interpreted as including the provision of any property or services, including currency, financial services, lodging, personnel, and transportation. This would encompass paying fees for protection, for safe passage of goods, or for the ability to operate in an area, or sales of goods or services to a cartel-owned business.

Executive and Corporate Liability: Liability extends to company executives who authorized such transactions and, under respondeat superior, the executive's employer.

Extraterritorial Reach: Liability potentially extends to non-US entities based on conduct abroad, given the statute's extraterritorial reach. For instance, in the first-ever corporate prosecution for material support in 2022 against French manufacturer Lafarge — for making payments to ISIS and the al-Nusrah Front — jurisdiction appeared to be based on a single wire transfer through a US correspondent bank account and the use of US-based email accounts.

Asset Forfeiture Consequences: Material support violations trigger expansive asset forfeiture, and an FTO designation makes it easier for the DOJ to carry its burden of showing that assets are related to a criminal offense.

Key Takeaways

Familiarize Yourself with the Red Flags of Cartel Activity: e.g., 3/31 FinCEN alert on methodologies of Mexico-based cartels for smuggling and repatriating bulk cash.

Identify Exposure Points within the Business Operations: Look closely at any counterparties in narcotics trafficking corridors or regions with a high volume of organized crime.

Consider Enhancing Due Diligence: Review third parties and vendors, agents, consultants, distributors and sales representatives.

Consider conducting transaction-level audits on red flags like cash payments, frequent invoice overpayments, and ambiguous remittance details.

Companies may also wish to review contracts to include uniform, counsel-vetted anti-cartel or transnational criminal organization clauses.

3. Material Support Prosecutions: A Focus on Criminal Liability

The USAOs have already demonstrated a willingness to levy material support charges against both US and foreign nationals.

In April 2025, SDTX announced the "First Instance of [a] TdA Member [Being] Charged with Terrorism Related Crimes" *(U.S. v. Jose Enrique Martinez Flores)*.

In May 2025, WDTX became "the first in the nation to charge a Mexican national with providing material support to a designated foreign terrorist organization based on her involvement with the Cartel de Jalisco Nueva Generación (CJNG)" *(U.S. v. Maria Del Rosario Navarro-Sanchez)*.

Also in May 2025, SDTX brought material support charges against two Utah men for conspiring to aid CJNG "in the form of U.S. currency" through their operation of a Texas-based crude oil company *(U.S. v. Max Sterling Jensen, et al.)*.

This effort is analogous to the initiative in the first Trump administration to charge MS-13 leaders with material support of terrorism, not just RICO and VICAR crimes.

4. Civil Liability Risks Under the Anti-Terrorism Act

Companies also face heightened exposure under the civil liability provisions of the Anti-Terrorism Act, 18 U.S.C. §2333, and in particular, secondary theories of liability.

Private Right of Action and Treble Damages: The ATA provides a private right of action to any US national injured in an act of international terrorism. Such violations impose treble damages when the act was "committed, planned or authorized" by a FTO, in addition to intrusive discovery and reputational consequences. The case of *Linde v. Arab Bank, PLC* (EDNY 2014) — where a jury found Arab Bank liable for knowingly supporting Hamas-linked militant attacks in Israel based on providing financial services to charities that were alleged agents of Hamas — remains a cautionary tale. Arab Bank faced the prospect of a $100 million+ damages award, though the parties ultimately settled.

Secondary Liability Theories: Civil ATA plaintiffs have often availed themselves of "aiding and abetting" and "conspiracy" theories of liability against banks, telecom providers, social media companies and state-owned enterprises, accusing them of supporting FTOs. While the Supreme Court has imposed limits on such liability — requiring an aider-and-abettor to have "knowingly provid[ed] substantial assistance [to] another … in the commission of … an act of international terrorism" — companies should anticipate that victims of cartel activity will seek to hold liable businesses that allegedly provided services and support to designated cartels.

5. Blocking Sanctions and CAPTA Restrictions Are Likely, Irrespective of Any US Nexus

Regardless of any US nexus, the US government may impose blocking sanctions on non-US persons determined to have provided "material support" to the organizations, and the US government may impose correspondent account/payable through account (CAPTA) restrictions on non-US financial institutions determined to have knowingly conducted or facilitated a significant transaction on behalf of an SDGT.

2025 Milestones
Key actions shaping enforcement

1.20.2025 – EOs on "Designating Cartels and Other Organizations as Foreign Terrorist Organizations and Specially Designated Global Terrorists," "Protecting the United States from Foreign Terrorists and Other National Security and Public Safety Threats," and "Protecting the American People Against Invasion"

2.5.2025 – DOJ memoranda on "General Policy Regarding Charging, Plea Negotiations, and Sentencing" and "Total Elimination of Cartels and Transnational Criminal Organizations"

2.20.2025 – State Department makes 8 FTO/SDGT designations

3.18.2025 - OFAC alert to financial institutions warning of liability risks from cartel exposure

3.31.2025 – FinCEN alert on Mexico-based TCOs

5.12.2025 – DOJ revision of "Corporate Whistleblower Awards Pilot Program" to extend to cartel- or TCO-related violations

6.24.2025 and **7.17.25** – OFAC sanctions of Tren de Aragua leaders

Keep An Eye On:

Forthcoming OFAC sanctions against individuals tied to the newly designated FTOs, which typically follow organizational designations.

Tariff and Customs *Evasion*



The DOJ is homing in on customs and tariff evasion — a growing enforcement frontier at the intersection of trade, fraud and national competitiveness. Civil and criminal actions under the False Claims Act (FCA) and other fraud statutes are likely, fueled by whistleblowers and cross-agency data sharing. Companies with global supply chains face heightened scrutiny of country-of-origin declarations, product classifications and valuation practices.

1. New and Prioritized Enforcement

Combatting customs and tariff evasion has catapulted into a key administration priority and relatively new enforcement frontier.

Tougher Penalties Ahead: Historically, administrative remedies of Customs and Border Protection have been relied upon to enforce customs and tariff laws, with penalties ranging from multiples of the underpaid duties to full domestic value of the mechanism. The Trump administration, however, has promised to enforce tariffs aggressively, including through criminal and civil penalties.

Primary Areas of Trade Violations:

1. **Misrepresenting country of origin:** Falsifying stated origin of goods on customs entry documents, invoices or product labels to minimize tariffs, often occurring when products are routed through lower-tariff countries for minor processing before export to the US.
2. **Misclassification:** Categorizing or classifying goods incorrectly to pay lower duties.
3. **Undervaluation schemes:** Submitting false invoices that significantly underreport the value of imported goods to lessen tariff or tax obligations.

2. FCA Enforcement Expands to Customs Violations

Civil liability under the FCA will be pursued against those who evade tariffs and customs duties under the "reverse false claims" provision.

FCA Deployment: As early as February, the DOJ Civil Division announced that the FCA would be deployed to enforce payment of customs duties on imported goods and pursue illegal foreign trade practices.

Recent Settlements: Various 2025 settlements underscore the strong emphasis on customs enforcement:

- $54.4 million FCA settlement with US-based distributor of tungsten carbide products to resolve allegations that distributor knowingly misrepresented the country of origin and failed to pay duties owed on tungsten carbide products imported from the PRC.
- $6.8 million FCA settlement with two subsidiaries of a multinational manufacturer operating in the plastics and industrial packaging sector, which voluntarily disclosed their failure to accurately report the country of origin and value of resin imports from the PRC.
- $4.9 million FCA settlement with a US furniture company for evading antidumping and countervailing duties.

Key Takeaways

Risk Assessment: Conduct targeted risk assessment to understand exposure points on country-of-origin information, including through transshipment, misclassifying of goods and undervaluation.

Supply Chain Monitoring: Consider enhanced supply chain due diligence or monitoring efforts to detect irregularities in shipments or import channels.

3. Criminal Tools to Combat Tariff Evasion

Criminal liability appears likely to be pursued for egregious violators alleged to have harmed US businesses.

DOJ Prioritizes Trade Fraud: In May, the DOJ Criminal Division's acting head described prosecuting trade and customs fraud as a priority to help "ensure that American businesses are competing on a level playing field in global trade and commerce." (DOJ 5/12 Memo, at 3.)

Fraud Section Expansion: This culminated in July's announcement that the Criminal Division is retooling and enlarging the Fraud Section's Market Integrity and Major Frauds Unit — formerly focused on procurement fraud and market manipulation — into a Market, Government, Consumer Fraud Unit focused on long-running frauds involving senior executives and large losses from tariff evasion schemes.

Potential Criminal Charges: Prosecutions could include:

- IEEPA violations (50 U.S.C. §1701-05)
- Smuggling (18 U.S.C. §545)
- Entry of goods falsely classified (18 U.S.C. §541)
- Entry of goods by false statements (18 U.S.C. §542)
- False statements (18 U.S.C. §1001).

These carry potential penalties of imprisonment and seizures, and could exert powerful leverage over companies, given the heavy legal and reputational risks.

4. Trade Fraud Task Force Highlights Interagency Collaboration

The DOJ-DHS "Trade Fraud Task Force" signals increased data-sharing across agencies.

Launch: The cross-agency "Trade Fraud Task Force," announced in July, is designed to increase information sharing between CBP, HSI and the Civil and Criminal Divisions and to further promote enforcement actions.

Data Mining: HSI is likely to seek to mine the information CBP maintains regarding import items and associated transaction values and applicable duties in case-targeting efforts.

New Actions: In December, DOJ publicly credited several actions to the Task Force for the first time, including a resolution of a criminal trade fraud investigation with a plastic resin distributor and an FCA settlement with a tungsten carbide products distributor, both relating to the evasion of customs duties.

5. Whistleblowers Encouraged

The Trump administration has strongly encouraged whistleblower referrals to initiate cases.

Specific Whistleblower Rewards: The Trump administration has consistently encouraged whistleblowers to provide leads for DOJ investigations into tariff and customs evasion. In May, the DOJ Criminal Division added "trade, tariff and customs fraud by corporations" to the categories eligible for whistleblower rewards. Such whistleblowers are likely to be US-based competitors to importers of goods subject to tariffs.

6. Navigating a Fast-Moving Tariff Landscape

The array of country-specific and sector-specific tariffs being imposed presents challenges for companies that import goods into the US.

Tariff Risk: Importers with complex supply chains, or importers linked to tariff-sensitive products like textiles, aluminum, solar, steel and automobile parts, should engage carefully in steps to mitigate risk and stay on top of fast-moving changes and governing laws on classification, valuation and origin of items being imported to ensure that accurate data is being reported.

2025 Milestones
Key actions shaping enforcement

2.20.2025 – DOJ Civil Division official speech on FCA priorities, highlighting trade

5.12.2025 – DOJ Criminal Division memoranda on "Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime" and "Corporate Whistleblower Awards Pilot Program"

7.10.2025 – DOJ Criminal Division announcement of Market, Government, Consumer Fraud Unit

8.29.2025 – DOJ-DHS announcement of "Cross-Agency Trade Fraud Task Force"

12.18.2025 – DOJ announcements of the first actions attributed to the Trade Fraud Task Force

Keep An Eye On:

Additional country- and sector-specific developments in tariffs based on geopolitical developments.

Cyber and Data *Security Breaches*



The DOJ has ramped up and refined its focus on cybersecurity and data governance through its new Data Security Program (DSP) — spelling out sweeping restrictions on cross-border data transfers and compliance requirements for companies handling sensitive US data. At the same time, False Claims Act (FCA) enforcement in the cybersecurity space continues to grow, with recent multimillion-dollar settlements highlighting the risks of misrepresenting compliance in government contracts.

1. DOJ's Data Security Program: What Companies Must Know

Government contractors and global companies handling US personal or government data should acquaint themselves with the new requirements of the DOJ's Data Security Program (DSP).

Executive Order 14117: One of the Biden-era Executive Orders that the second Trump administration has prioritized has been EO 14117, which seeks to prevent access to Americans' bulk sensitive personal data and government-related data by "countries of concern" (China — including Hong Kong and Macau — Russia, Iran, North Korea, Cuba and Venezuela).

DSP Overview: In April, the DOJ National Security Division announced the DSP, which implements the EO. The DSP imposes strict prohibitions on certain data transfers outside the US, as well as rigorous privacy, cybersecurity and data governance restrictions on a broader set of transactions outside the US. The rule also has significant impact on US companies that conduct international data transactions.

Covered Data: Health and biometric data, human genomic data, financial data, personal health data, government identification numbers, demographic and contact information, and network, device and advertising identifiers.

Who Is Impacted: Among the types of companies implicated are those relying on large-scale data training for AI development; businesses leveraging data brokers to acquire bulk user data for targeted advertising initiatives; and business-to-consumer companies (e.g., automotive, e-commerce, healthcare, AI and robotics entities) whose services require the collection of sensitive US personal data that is transferred overseas for processing.

2. DOJ DSP: Compliance Deadlines and Penalties

The DSP's due diligence, audit and reporting requirements went into effect on October 6.

Penalties for Noncompliance: Noncompliance with the DSP is punishable by civil and criminal penalties under IEEPA. Civil penalties can reach up to $368,136 or twice the transaction's value. Willful violations can be punished criminally, with fines up to $1 million and imprisonment up to 20 years.

Key Takeaways

Audit and Reporting:
Understand and comply with the new audit, reporting and certification requirements.

Data Mapping:
Map and identify categories of data (collected, processed or shared) and data flows within the business operations.

Risk-Based Procedures: Evaluate tailored, risk-based procedures for cybersecurity and data security.

Good-Faith Compliance:
Implement the 10 "examples … of good-faith efforts" at compliance detailed in the DOJ "Implementation and Enforcement" guide. (4/11 DOJ Memo, at 2-3.)

Senior Engagement:
Ensure careful engagement at senior levels with any cybersecurity compliance affirmations in contracts.

Enforcement Signaling: The DOJ has signaled a strong appetite for enforcement of the DSP by providing a 90-day grace period (which expired in July) for companies to undertake good-faith efforts to come into compliance. It is now assumed that companies have had the opportunity to update their policies and practices and will act in conformance with the DSP.

Effective Date: The following key provisions of the DSP went into effect on October 6:
- **Subpart J:** Due diligence and audit requirements for restricted transactions
- **§202.1103:** Reporting requirements for certain restricted transactions
- **§202.1104:** Reports on rejected prohibited transactions

3. FCA Risks for Government Contractors: Cybersecurity Misrepresentations

Parties to government contracts may be exposed to False Claims Act liability for cybersecurity-related misrepresentations.

Enforcement Priority: The DOJ Civil Division has signaled that noncompliance with federal cybersecurity standards or false certifications of security readiness to win contracts continue to be a top priority in FCA enforcement.

Recent Settlements: In July, the DOJ's twin announcements of settlements for $9.8M and $1.75M, respectively, for false certification of cybersecurity compliance underscore the DOJ's continued focus on FCA cybersecurity enforcement, and the need for government contractors certifying compliance with regulatory and contractual requirements to remain vigilant.

CMMC Compliance Risks: FCA liability risks may escalate for defense contractors now that the Pentagon's final Cybersecurity Maturity Model Certification (CMMC) rule has gone into effect; solicitations and contracts may now begin incorporating CMMC certification requirements, whereby self- or third-party assessments to certify compliance with applicable cybersecurity requirements may be needed to obtain DOD contracts.

4. FCA Cybersecurity Enforcement: Universities in the Spotlight

Universities have been, and are likely to remain, under heightened scrutiny for any cybersecurity-related false claims.

Recent Cybersecurity Actions: Actions have been brought against universities for misrepresentation of cybersecurity capabilities.

- **Georgia Tech:** Last year, the government intervened in an FCA action by whistleblowers (members of Georgia Tech's Cybersecurity Team) against Georgia Tech for allegedly failing to meet cybersecurity requirements in connection with DOD contracts.
- **Penn State:** The DOJ also announced a $1.25 million settlement by Penn State to resolve FCA claims that the university failed to comply with cybersecurity requirements in 15 DOD or NASA contracts.

Ongoing Risk: This trend is likely to continue given this administration's multipronged investigative efforts against universities.

2025 Milestones
Key actions shaping enforcement

2.20.2025 – DOJ Civil Division speech highlighting cybersecurity as a FCA priority

4.11.2025 – DOJ National Security Division announcement of the Data Security Program and related issuance of a Compliance Guide, Implementation and Enforcement Policy, and Frequently Asked Questions document

7.8.2025 – Expiration of the 90-day grace period for DSP enforcement

7.31.2025 – DOJ Civil Division announcements of two FCA cybersecurity settlements

10.6.2025 – Effective date of DSP due diligence, audit and reporting requirements

11.10.2025 – Effective date of DOD's final CMMC cybersecurity rule

Keep An Eye On:

How the Pentagon's contracting officers exercise their wide discretion to include CMMC requirements, potentially including third-party assessment requirements, in contracts and solicitations now that the CMMC rule is in effect, and the impact on False Claims Act risk.

About Our White Collar Practice

Fried Frank represents multinational publicly traded corporations and financial institutions, their boards of directors and special committees, and high-profile executives in a wide range of white collar matters, parallel regulatory and civil litigation, and internal investigations.

Our deeply experienced team includes multiple former senior federal prosecutors and government officials, including former US Attorneys, high-ranking officials from the US Department of Justice, the former Deputy US Attorney for the Southern District of New York, the former head of the SEC's national Asset Management Unit and Associate Regional Director, along with numerous lawyers with extensive white collar defense, regulatory enforcement, and investigations experience. We are routinely recognized for our work in the white collar space and ranked among the best in the country by Chambers USA and Legal 500.

We have an international reputation for successfully defending corporations and individuals under investigation for alleged securities, commodities, and other financial frauds, insider trading, market manipulation, anti-corruption violations, criminal antitrust, money laundering, and procurement and healthcare fraud. Our litigators have tried dozens of federal criminal cases to verdict and argued numerous criminal appeals before federal and state appellate courts.

We regularly conduct internal investigations in high-profile matters where our work is kept confidential, as well as in matters where the results of the investigation are expected to be widely disseminated and receive public scrutiny. Our skill, integrity, and reputation for forceful and principled advocacy have been central to maintaining or restoring public and regulator confidence in our clients. Often, we and our clients define success by representations that never became public.

Market Recognition

"Notable strength in criminal and civil investigations and enforcement proceedings, drawing on its strong bench of former prosecutors and experienced litigators."

"The Fried Frank team has been constantly excellent. They're well respected by regulators, colleagues and the marketplace."

"A very deep and accomplished bench for litigation matters, which is second to none in terms of the quality of its work."

— CHAMBERS AND PARTNERS ON OUR WHITE COLLAR PRACTICE

Candice Wong is a partner in Fried Frank's Litigation Department, representing companies and individuals in high-stakes disputes, white collar criminal defense, and government and internal investigations. Candice draws on nearly 10 years at the US Department of Justice (DOJ)—both at the country's largest US Attorney's Office, where she tried 28 cases to verdict, and at the DOJ's Criminal Division, where she served in the third-highest ranking leadership position during the first Trump Administration. In her roles as the Criminal Division's Acting Deputy Assistant Attorney General and Chief of Staff, Candice supervised three litigating sections and the Criminal Division's Office of Policy and Legislation. She was also a lead drafter of the DOJ's inaugural *Evaluation of Corporate Compliance Programs* guidance.

A seasoned trial and appellate litigator, Candice has litigated a broad range of constitutional, statutory and regulatory issues and is a former law clerk to US Supreme Court Justices Sandra Day O'Connor, Sonia Sotomayor, and Brett Kavanaugh (then a Judge on the DC Circuit). Candice also serves as a Senate-confirmed Commissioner on the US Sentencing Commission.

For more information on the latest trends and developments, please contact:



CANDICE C. WONG
LITIGATION PARTNER
+1.202.639.7489
CANDICE.WONG@FRIEDFRANK.COM

Attorney advertising. Prior results do not guarantee a similar outcome.